Network Resilience Architecture and Analysis for Smart Homes

By

Alex Amir Modarresi

Submitted to the graduate degree program in Electrical Engineering & Computer Science and the Graduate Faculty of the University of Kansas in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Chairperson: Prof. Victor S. Frost

Prof. Fengjun Li

Prof. Bo Luo

Prof. Morteza Hashemi

Prof. John Symons

Date Defended: 23-March-2020

The Dissertation Committee for Alex Amir Modarresi
certifies that this is the approved version of the following dissertation:

Network Resilience Architecture and Analysis for Smart Homes

Chairperson: Prof. Victor S. Frost

Date approved: 14-April-2020

Abstract

The Internet of Things (IoT) is evolving rapidly to every aspect of human life including, healthcare, homes, cities, and driverless vehicles that makes humans more dependent on the Internet and related infrastructure. While many researchers have studied the structure of the Internet that is resilient as a whole, new studies are required to investigate the resilience of the edge networks in which people and “things” connect to the Internet. Since the range of service requirements varies at the edge of the network, a wide variety of technologies with different topologies are involved. Though the heterogeneity of the technologies at the edge networks can improve the robustness through the diversity of mechanisms, other issues such as connectivity among the utilized technologies and cascade of failures would not have the same effect as a simple network. Therefore, regardless of the size of networks at the edge, the structure of these networks is complicated and requires appropriate study.

In this dissertation, we propose an abstract model for smart homes, as part of one of the fast-growing networks at the edge, to illustrate the heterogeneity and complexity of the network structure. As the next step, we make two instances of the abstract smart home model and perform a graph-theoretic analysis to recognize the fundamental behavior of the network to improve its robustness. During the process, we introduce a formal multilayer graph model to highlight the structures, topologies, and connectivity of various technologies at the edge networks and their connections to the Internet core. Furthermore, we propose another graph model, technology interdependence graph, to represent the connectivity of technologies. This representation shows the degree of connectivity among technologies and illustrates which technologies are more vulnerable to link and node failures.

Moreover, the dominant topologies at the edge change the node and link vulnerability, which can be used to apply worst-case scenario attacks. Restructuring of the network by adding new links associated with various protocols to maximize the robustness of a given network can have distinctive outcomes for different robustness metrics. However, typical centrality metrics usually fail to identify important nodes in multi-technology networks such as smart homes. We propose four new centrality metrics to improve the process of identifying important nodes in multi-technology networks and recognize vulnerable nodes.Finally, we study over 1000 different smart home topologies to examine the resilience of the networks with typical and the proposed centrality metrics.

Acknowledgments

I would like to sincerely appreciate my advisor, Prof. Victor S. Frost for his full support and accepting me after sudden and sadness passing of my late advisor, Prof. James P.G. Sterbenz. I have been inspired by his critical thinking, precious advises, and knowledge within technical field.

I would like to remember my late advisor, Prof. Sterbenz, that I spent most of this journey with him and learned a lot from him.

I would like to appreciate Prof. John Symons for his unconditional supports and inspiration.

I would like to thank the committee members: Prof. Bo Luo, Prof. Fengjun Li, and Prof. Morteza Hashemi for being in my committee.

I would like to thank Siddharth Gangadhar for his guidance from my early stage in the group until now. I also would like to thank Mohammad Alenazi and Truc Anh N. Nguyen for their suggestion and discussions about research ideas.

I would like to thank the Information and Telecommunication Technology Center (ITTC) network system administrators and the ITTC administrative staff for their support during my study. Michael Hulet, and Wesley Mason have always been helpful in assisting whatever the computing problems I faced.

Finally, I am very grateful to my dear family, especially my mother, for their never-ending support.

Page left intentionally blank.

Contents

Page left intentionally blank.

List of Figures

Page left intentionally blank.

List of Tables

Chapter 1

Introduction and Motivation

The Internet of Things (IoT) [21, 22] refers to the rapidly growing ecosystem of internet-enabled devices beyond conventional computing and internet access platforms such as smart phones. However, the basis for the Internet of Things (IoT) goes back many years when the Auto-ID Center at MIT introduced low-cost radio frequency identification (RFID) to store serial numbers on a microchip embedded in merchandise tags. The idea was to decrease the price by using simple microchips at high frequencies instead of using complex chips with memory. This concept was developed to connect objects to the Internet through the tags with their information kept in databases [23]. Since then this idea has been enhanced with various terms applied, including the *Internet of Things* or *Internet of Everything*. Although this is currently a hot area of research, to the best of our knowledge there is still no standard universally-accepted model for the IoT and environments utilizing it such as smart home. Despite a number of proposed models for the IoT, they are generally conceptual with a high-level of architectural abstraction. IEEE describes the IoT as a network of elements embedded with sensors connecting to the Internet [24]. The International Telecommunication Union (ITU) defines the IoT as a global infrastructure that enables advanced services by interconnecting things with current communication technologies [25]. ITU has also updated the definition of the telecommunication system for the IoT by adding “anything” to it. *Anything* in this definition means any type of communication among humans, computers, and “things” (smart devices). The Internet Engineering Task Force (IETF) focuses on potential factors for enabling the IoT communication by considering RFID tags, sensors, and mobile phones as enablers of this technology. The National Institute of Standards and Technology (NIST) defines the IoT as a cyber-physical systems (CPS) technology to connect smart devices in various sectors such as transportation, healthcare, and energy [21]. Finally, Cisco in the commercial sector defines the IoT under the umbrella of “Internet of Everything” as a technology to connect people, processes, data, and things to change the information to valuable experiences, capabilities, and economic opportunity [26].

The IoT has dramatically increased the number of devices attached to the Internet [16]. Edge networks, such as home, city, and the industrial networks, are the most affected areas to the growth of attached devices. New terms and buzz words including, smart homes, smart cities, and Industrial Internet of Things (IIoT) have been introduced to reflect such changes and technology variants involved. Since many such devices have limited computational power and rely on cloud-based services, their usefulness depends on stable connectivity to the Internet. This connectivity is particularly important when IoT devices provide services related to security or safety.

Systemic resilience has not been a priority for the manufacturers or consumers of IoT devices to date. The low computational power of edge devices along with the easy installation of IoT devices by non-technical consumers encourage manufacturers to ignore many useful features such as failover strategies or other important security features that improve robustness and system resilience. Even though the IoT is being developed without sufficient attention to the security and resilience, a number of protocol specifications do consider such features. Furthermore, many IoT edge network technologies do not use the normal IP stack and provide some isolation from conventional IP devices in a smart environment, assuming that the consumer gateway devices are secure. This is critical and serious vulnerabilities, since consumer IoT devices have already been exploited by considering such a false assumption.

Designs that leverages technological diversity which will be part of system using IoT, can produce solutions that support system level resilience. However, it can do so only as in-depth understanding that reflects both the physical features of systems and their network topologies. For example, one very practical lesson of this work is that mesh access points that are currently sold to the home-consumer market as range extenders, can be installed in ways that improve network resilience during link disruptions or interference. There are a variety of strategies for leveraging the diversity of technologies in design for system-level resilience in IoT. We include evidence from studying 1500 smart home topologies to understanding general principles for the promotion of system-level resilience in IoT design.

1.1 Problem Statement

IoT has changed the structure and topology of the edge networks from simple and monolithic to multilayer and multi-technology networks. Therefore, it is essential to understand how diverse technologies can contribute to the resilience of edge networks. Heterogeneity of technologies can promote network resilience through diversity of mechanisms. However, heterogeneity increases complexity and cost as well as security vulnerability. The goal of this research is to study generalized structure of a smart home containing typical technologies as one of the modifying edge networks by IoT and significantly evaluate the robustness of such smart home networks. This modeling and analysis will promote the development of robust smart home. Therefore, our *thesis statement* is as follows:

Modeling smart home networks can be useful to understand and promote the resilience of the network via technological diversity and network connectivity improvement and applying a various set of typical and new centrality metrics to different smart home topologies to study robustness and vulnerability of such networks.

1.2 Proposed Solution

We propose a graph-theoretical approach to model and analyze the robustness of smart home networks. First, we propose a reference model for a typical smart home and use it to obtain the associated graph model in Chapter 3. During this process, we also propose an abstract model for smart homes.

As the second step in Chapter 4, we evaluate the smart home graph by graph-theoretical metrics. We identify metrics that can explain the characteristics of the smart home network such as importance of particular nodes. Regardless of the size of smart home networks, they can be considered as complex networks since various technologies with different features are involved. Therefore, it is expected that common metrics and approaches cannot explain the behavior of such network.

As the third step, we evaluate the resilience of the smart home networks by defining and applying a framework for targeted attacks. We propose a multilayer network to highlight critical links and nodes connecting technologies and proper metrics to measure the robustness of the network in Chapter 5. Furthermore, we generate 1500 smart home topologies to study the resilience of such networks with typical and proposed centrality metrics in Chapter 6.

1.3 Contributions

The main contributions of this dissertation are as follows:

1. Development of a smart home abstract model and a smart home reference model to study and analyze system-level resilience in Section 3.1. This step starts by proposing a generalized scenario for a typical smart home. This scenario helps us to extend the idea to an abstract smart home model applicable for any building size. We recognize a high-speed backbone in which other technology variants are connected constructing an star of technologies around the backbone. The type of services used in a particular home identify technology variants. This process reveals that a simple monolithic graph representation is not suitable for a multi-technology network.

2. Development a new technology interdependence graph to represent the connectivity of the technologies at the edge networks when various technologies are involved in Section 3.2. This new representation provides the abstract relationship among utilized technologies for easier graph analysis.

3. Graph theoretic analysis on various instances of the abstract smart home model is presented in Chapter 4. Though some of the selected centrality metrics identify important nodes in the models, many of them fails to provide accurate results in a multi-technology environments. This is the result of nodes logical functionality in different technologies in which a simplex graph cannot represent them correctly.

4. Development of a graph-theoretical framework that can extend the multilevel and multiprovider graphs [27] to multilayer graphs with arbitrary dimensions to represent and highlight heterogeneity and diversity of the technology variants at the edge networks. This multilayer framework represents multi-technology networks with

considering many aspects including technology variants in Chapter 5. This model help us to propose three degree centrality metrics based on utilized technologies in a particular edge network, since the model emphasizes on interconnected edges among layers.

5. Analysis of the modified smart home graph during targeted challenges through analysis of the technology interdependence graph in Section 5.3. This analysis identifies features and weakness of a particular smart home model among the utilized technologies. From this analysis, we find that *bi*-connectivity among technologies improve the overall system resilience. This improvement is gained when devices supporting multiple technologies are utilized in a model which leads to increasing cost and energy consumption.

6. Heterogeneity in technology may increase path diversity to improve system resilience. We combine different technologies and generate 1500 smart home topologies to study the effect of adding cellphones as a device supporting multiple technoloies in Section 6.1. Though heterogeneity of the technologies can provide divers paths, many selected typical centrality metrics fail to identify devices with supporting multiple technologies as important nodes in such networks. We provide the results of the study and compare the corresponding results with our proposed centrality metrics designed to identify nodes with supporting multiple technologies in Sections 6.2.1 and 6.2.2.

1.4 Relevant Publications

The research presented in this dissertation has resulted in a number of publications, including the following.

Peer-Reviewed Conference Proceedings

- **A. Modarresi**, and John Symons, "Technological Heterogeneity and Path Diversity in Smart Home Resilience: A Simulation Approach" in *Proceedings of The 11th International Conference on Ambient Systems, Networks and Technologies*, Warsaw, Poland 2020

- **A. Modarresi**, and John Symons, "Modeling and Graph Analysis for Enhancing Resilience in Smart Homes" in *Proceedings of the 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019)*, Coimbra, Portugal 2019

- **A. Modarresi**, and John Symons, "Modeling Technological Interdependency in IoT - A Multidimensional and Multilayer Network Model for Smart Environments" in *Proceedings of the 11th International Workshop on Resilient Networks Design and Modeling (RNDM 2019)*, Nicosia, Cyprus 2019

- **A. Modarresi**, and James P.G. Sterbenz, "Towards a Model and Graph Representation for Smart Homes in the IoT" in *Proceedings of the 4th IEEE International Smart Cities Conference (ISC2 2018)*, Kansas City, USA 2018.

- **A. Modarresi**, and James P.G. Sterbenz, "Multilevel IoT Model for Smart Cities Resilience," in *Proceedings of the 12th International Conference on Future Internet Technologies CFI'17*, Fukuoka, Japan 2017, pp. 7: 1-7: 7.

- **A. Modarresi**, and James P.G. Sterbenz, "Toward resilient networks with fog computing," in *Proceedings of the 9th International Workshop on Resilient Networks Design and Modeling (RNDM 2017)*, Alghero, Italy 2017.

- **A. Modarresi**, S. Gangadhar, and James P.G. Sterbenz, "A framework for improving network resilience using SDN and fog nodes," in *Proceedings of the 9th In-*

ternational Workshop on Resilient Networks Design and Modeling (RNDM 2017), Alghero, Italy 2017.

1.5 Summary

In this chapter, we introduce our thesis statement and contributions of this research. We start our research with proposing an abstract model for smart homes as one of the edge networks that is changing rapidly due to the emergence of the IoT. The analysis of the model shows that many typical graph metrics may not be appropriate to explain the characteristics of the multi-technology networks. Then, we propose a multilayer model to represent each technology with a separate layer and highlight the interconnection among layers. This representation leads us to introduce a new graph metric based on the number of utilized technologies in the network to recognize the important nodes. Such nodes should be protected appropriately against targeted attacks. We analyze the effectiveness of our newly graph metric with our technology interdependence graph. We also compare the results of the selected typical centrality metrics with our proposed metrics over 1500 smart home topologies.

Chapter 2

Background and Related Work

This chapter is divided into five various topics related to the rest of this dissertation. We review topology, features, and physical characteristics of network technologies utilized at the edge of networks and more specifically smart homes in Section 2.1. In Section 2.2 and 2.3, we review common IoT models and edge computing models respectively. These two parts of the study are our inspirations for designing the smart home model in Chapter 3. Resilience and survivability principles are reviewed in Section 2.4 as our road map to investigate resilience of various instances of smart home models throughout this dissertation. Finally in Section 2.5, most centrality metrics utilized in Chapter 4 to analyze the instances of the smart home models are reviewed.

2.1 Network technologies at the Edge

Various services at the edge networks require different bandwidth and other characteristics. Many technologies with distinct features and topologies are available to fulfill the requirement of each service from high to very low bit-rate. In addition, diversity of technologies, discussed in Section 2.4, is a resilient principle to improve the overall network resilience. Furthermore, understanding the features of each technology and related protocols are necessary to implement topologies and analyze smart home models with network simulators.

In this section, we investigate the features and characteristics of common technologies used at the edge networks focusing on those utilized in smart homes. We divide this section based on the coverage of such technologies into proximity, short-to-medium range from WPAN to WLAN, and long range technologies. The features summary of these technologies is provided at the end of this section in Table 2.2.

2.1.1 Proximity Technologies

Very short communications start with Radio Frequency Identification (RFID) tags. RFID is a general term to describe a system that is able to transmit the identity of an object by radio wave signals. Such systems consist of a microchip attached to an antenna mounted on a substrate [28] and they are called *tags*. Considering power source, tags are divided into three broad categories, namely passive, semi-passive and active. Passive tags harvest the energy from the reader radio wave signal and act as a passive transponder. They have lower capability and communication range compared with other types. On the other hand, the active tags have their own local power source like a battery and can be identified hundreds of meter away from the reader. Furthermore, the key feature of this group is that they can initiate a connection to the reader or other tags. Similarly, semi-passive tags have a power source on board; however, they can not initiate a communication. These tags are activated when they are close to a reader. Moreover, since they have a power source, they have longer communication range than passive tags.

Tags work in wide range of frequencies from low frequency (LF) to ultra-high frequency (UHF). There are also various tags work in 2.4 and 5.8 GHz. Global Standard One (GS1) [29], an organization to develop standards for business communication, defines protocols for RFID tags. The capability of tags identifies which protocol should be used. A complete communication link between the interrogator and tag from physical layer coding and command structure is called *Air Interface* in GS1 terminology. Many of these protocols have been ratified by ISO in the standard family of 18000. These technologies are usually used for identification. The usage of RFID technology is common in stores and industrial facilities. These technologies can be utilized in smart homes in services such as tracking and sorting objects, object discovery, and smart washing machines and dryers [30–32].

Near Field Communication

Near Field Communication (NFC) [33] is a set of protocols standardized by ISO under two major groups ISO/IEC 14443 and ISO/IEC 18092 [34]. ISO/IEC 14443 is a four-part standard for contactless smart card consisting of ISO 14443-1 through ISO/IEC 14443-4 [35–38] for physical characteristics, radio frequency power and signal interface, initialization and anti-collision and transmission control requirements, respectively. ISO/IEC 18092 defines communication modes for NFC and its interfaces and protocols for interconnection of computer peripherals. The standard data rate for ISO/IEC 14443 is 102 kb/s in half-duplex communication that makes total communication rate of 212 kb/s; while the standard data rate for ISO/IEC 18092 can reach to 424 kb/s. In both standards, the operational frequency is 13.56 MHz, the same frequency used by HF RFID tags, with the proximity of 10 cm from the reader. NFC tags in ISO/IEC 14443 are usually passive, while ISO/IEC 18092 defines both active and passive modes. These standards explain three modes of operations for NFC devices as below:

- *Reader/writer*: In this mode defined in ISO 14443, an NFC reader can read information stored in NFC tags and write data if the NFC tag has writing capability.

NFC smart posters are a sample of this group.

- *Peer-to-peer*: Defined in ISO 18092, two devices can exchange data in this group. Exchanging virtual business cards and digital photos are some of the examples.

- *Card emulation*: In this mode, an NFC capable device emulates the behavior of a traditional contactless smart card. Using an NFC capable smart phone as a smart card for electronic payment is one of the examples of this group. This mode allows smart devices with high capability, work as smart cards without changing the whole infrastructure.

The short range communication of NFC technologies enforces the physical proximity of the NFC tags when security is satisfied by the physical presence of the owner of a NFC tag. In smart home, NFC technologies are usually combined with other longer range communication technologies such as Bluetooth to initialize and setup the connections before starting data communication.

2.1.2 Short-to-medium Range Protocols

In this section, we present the current and common technologies used for short-to-medium range transmissions covering wireless personal area networks (WPAN) to wireless local area networks (WLAN) with range of a few meters to hundreds of meters such as IEEE 802.11 family and IEEE 802.15.4.

IEEE 802.15.4

IEEE 802.15.4 [1] has been introduced for wireless personal area network (WPAN) in the frequency range of 900 MHz and 2.4 GHz to convey information over a short range from 10 to 100 meters with little or no structure. IEEE 802.15.4 is the base physical and MAC protocols for other upper layer protocols such as Zigbee [39, 40]. This standard defines physical layer and medium access control (MAC) sublayer for low data-rate connectivity from 250 kb/s to 20kb/s and slower. The data rate provided to user applications is lower, due to the protocol overhead. The physical layer provides data and management services. The data service consists of transmission and reception of physical protocol data units (PPDUs) over the radio channels; while management service includes activation and deactivation of the radio transceiver, channel selection, clear channel assessment (CCA) and sending and receiving packets over the physical medium.

The MAC sublayer also provides data and management services. The MAC data service is responsible for sending and receiving MAC protocol data units (MPDUs). The management services include beacon management, channel access, frame validation, acknowledged frame delivery, association, and disassociation. Figure 2.1 (from [1]) shows the location of IEEE 802.15.4 regarding other layers in the network stack.

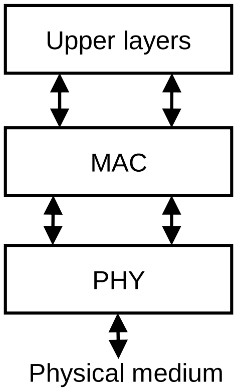


Figure 2.1: Layers in IEEE 802.15.4 [1]

IEEE 802.15.4 has capability to support networks with the star (Figure 2.2) and peer-to-peer topologies. It uses 64-bit extended addresses for unique addressing and 16-bit short addresses for allocated addressing. Carrier sense multiple access with collision avoidance (CSMA/CA) or ALOHA can be used for channel access.

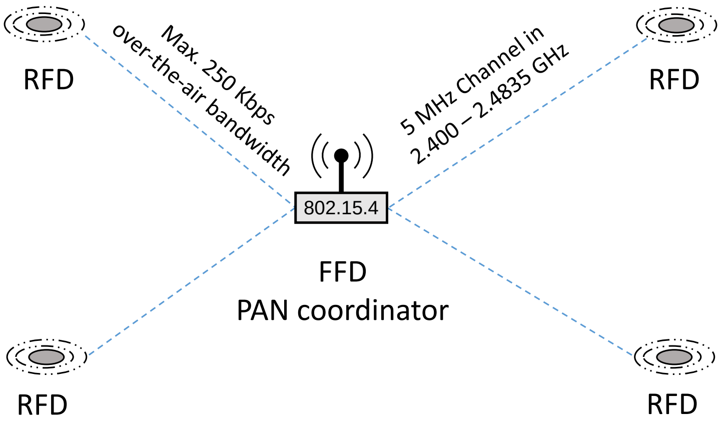


Figure 2.2: IEEE 802.15.4 star topology

Two different type of devices can join an IEEE 802.15.4 network, namely full-function devices (FFD) and reduced-function devices (RFD). While an FFD is capable to serve as a coordinator in the network, RFDs do not have such capability and they intend to be used for simple applications with low data rate and can be implemented with minimal memory and resources. In each WPAN network conforming to this standard, there should be at least one coordinator and many RFDs; however, RFDs can associate to just one FFD as their coordinator. In the star topology, RFDs always communicate with the PAN coordinator, where RFDs are always initiator or terminator of the communications. The PAN coordinator is responsible for route communication in addition to termination and initiation of a communication. The peer-to-peer topology also has a PAN coordinator which is usually selected by nomination, but in this topology, any devices can communicate with any other devices in the network while they are in the signal range of each other. This topology allows the formation of the more complex topology like mesh network; however, this formation is performed by the higher layer. Furthermore, the higher layer can also impose some restrictions on the forming topology. Figure 2.3 shows a cluster tree as an example of a complex topology. In this network, the first PAN coordinator, shown with the black dot, can select other coordinators for each cluster when they meet specific requirements. Other devices can join as a child to each cluster and adds the coordinator of the cluster, gray dots, as their parents in their neighbor list. Such structures can cover a larger area; however, the message latency is increased as well.

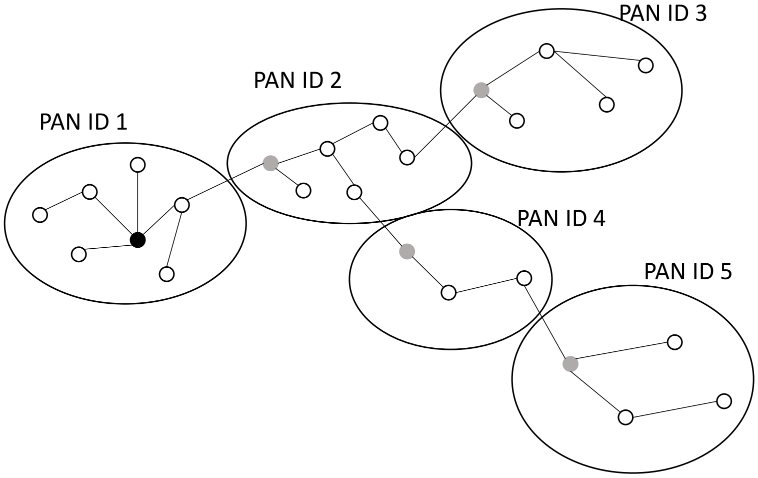


Figure 2.3: An example of a cluster tree network [1]

One of the responsibilities of the coordinator in each topology is sending beacons. The coordinator can support both a beacon-enabled and non-beacon enabled network. If synchronization or low latency are required, beaconing will be activated. In such cases, the coordinator defines a superframe structure containing 16 slots between two consecutive beacons. If guaranteed time slots (GTSs) are necessary, the superframes can be divided into contention access period and contention free periods. The devices that have data to send, compete for time slots in contention access period using slotted CSMA/CA or ALOHA mechanism. In a beacon enabled PAN with superframes, devices should track and synchronize themselves with the beacons, then they can send their data in a proper slot. In contrast, in a non-beacon enabled PAN, devices simply transfer their data with unslotted CSMA/CA. If the acknowledgment is required, the coordinator sends the acknowledgment with the same rule. Beaconing is always necessary for neighbor discovery in this mode.

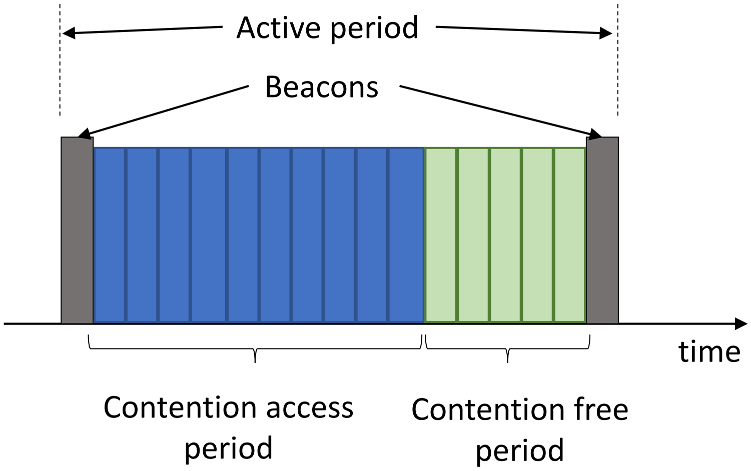


Figure 2.4: A superframe with GTSs [1]

Three types of data transfer transaction are defined in IEEE 802.15.4. These are including data transfer to coordinator from devices, from coordinator to devices, and between two peer devices. The last transaction happens only in a peer-to-peer topology. The mechanism for each transfer type changes whether the network is beacon-enabled or not. If the network is beacon-enabled, devices should synchronize themselves with the beacon in the first transfer type. In the second type, the coordinator indicates in the beacon that the data message is pending. The devices listen to beacons periodically and if the data message is pending they transmit a MAC command to request the data. The acknowledgments are exchanged for reliable communications. In a peer-to-peer topology, devices communicate directly when they are in their communication range. In order to do that, devices should either synchronize with each other or receive data constantly.

IEEE 802.15.4 can be used for fixed or mobile devices; however, coverage area can change drastically when nodes move. Therefore, a well-defined coverage area is not defined for IEEE 802.15.4.

Zigbee

ZigBee [39,40] is a very low-cost, low-power, two-way communication standard based on IEEE 802.15.4. It defines a network layer and a framework for application layer over physical and medium access control layers provided by IEEE 802.15.4-2003. ZigBee over IEEE 802.15.4 results in lower bandwidth and higher latency compared to IEEE 802.15.4. ZigBee uses the same physical characteristics of IEEE 802.15.4 including signaling and channel bandwidth; however, it provides additional network layer supports for star, tree and mesh topologies. In a mesh network, full peer-to-peer and hop by hop communication is possible to expand the network range. Figure 2.5 shows communication between node *A* and *D* through nodes *B* and *C*. However, ZigBee is not fully compatible with IEEE 802.15.4 beaconing in the mesh topology.

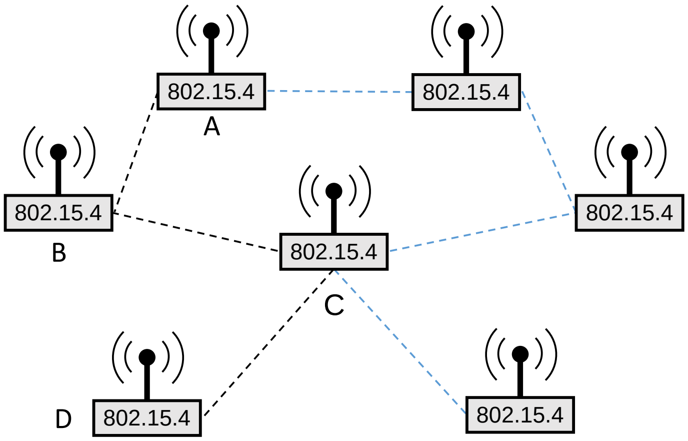


Figure 2.5: ZigBee mesh topology

Figure 2.6 illustrates ZigBee architecture and its relation to IEEE 802.15.4. In the figure, application support sub-layer (APS) works as an interface between the application (APL) and the network layer providing a set of services that are shared between Zigbee Device Object (ZDO) and manufacturer-defined application objects. The network layer controls the correct functionality of MAC sublayer in one end and providing a proper service interface to the application layer on the other end. The functionality of the two lower layers was explained in the previous section.

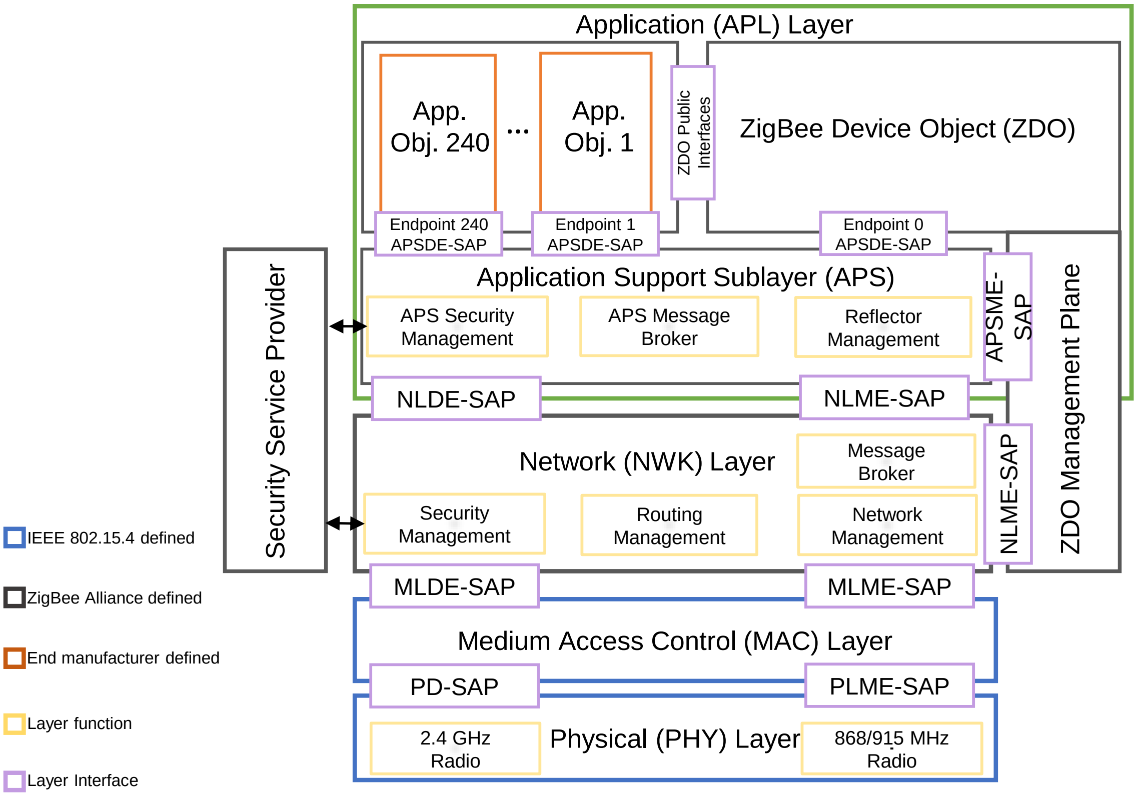


Figure 2.6: ZigBee Stack Architecture [2]

Zigbee also defines a standard as Zigbee IP protocol stack over IEEE 802.15.4-based wireless mesh network [2]. This specification utilizes IETF and IEEE standard protocols including IPv6, 6LoWPAN, and RPL over IEEE 802.15.4 illustrated in Figure 2.7.

In this model, the link layer is responsible for the discovery of IEEE 802.15.4 PAN, frame transmission with a maximum payload size of 118 bytes, frame buffering and polling for sleeping devices, and frame security. A Zigbee IP (ZIP) host at link layer must implement RFD functionality while ZIP router and coordinator support FFD functionality. 6LoWPAN adaptation layer fragments and reassemble of IPv6 packets larger than maximum payload size in MAC layer, and compresses and decompresses IPv6 and UDP header.

Though at this layer, RFC 4944 for carrying IPv6 over 802.15.4 with mesh addressing is supported, ZIP node does not use the link-layer mesh under routing configuration. The network layer performs IPv6 addressing including IPv6 stateless address auto configuration and Duplicate Address Detection (DAD), router and neighbor discovery, and route computation using Routing Protocol for Low power and Lossy Network (RPL) protocol. The transport layer provides reliable and unreliable services along with multiplexing of packets. The management entity calls and manages various protocols to provide desired behavior including power management, node boot strapping, authentication and key distribution using PANA (Protocol for Carrying Authentication for Network Access) protocol and transferring the network communication parameters using MLE (Mesh Link Establishment) protocol.

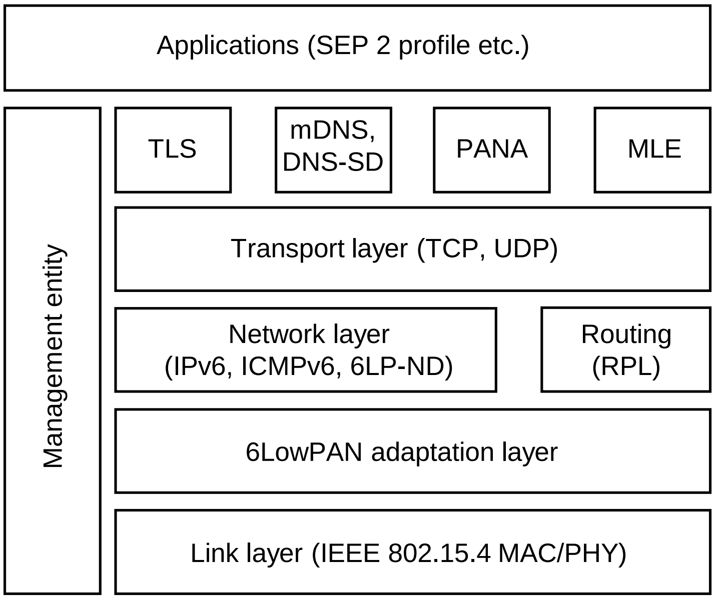

Applications (SEP 2 profile etc.)
Management entity
TLS
mDNS, DNS-SD
PANA
MLE
Transport layer (TCP, UDP)
Network layer (IPv6, ICMPv6, 6LP-ND)
Routing (RPL)
6LowPAN adaptation layer
Link layer (IEEE 802.15.4 MAC/PHY)

Figure 2.7: ZigBee IP stack protocols [2]

IEEE 802.15.1 and Bluetooth

IEEE 802.15.1 [3] is another member of 802.15 group for transmitting information over a short distance in wireless personal area network (WPAN), offering robustness, low power consumption, and low cost communication. This standard defines physical and Medium Access Control (MAC) specification for wireless connectivity among fixed or mobile devices. The standard limits the communication up to 10 m which is called personal operating space (POS) with the bit rate of 1 Mb/s.

The devices in this network share a physical radio channel and synchronize themselves with a common clock provided by one of the devices in the network called master. The other devices are known as slaves and the whole group called a *piconet*. The devices in the piconet use a specific frequency hopping pattern over 79 frequencies with the capability of excluding the areas suffer from interference by other devices. Time slots are used to divide the physical channel in order to convey packets in the slots. Above the physical channel, other layers and control protocols are defined. Within a physical channel, a physical link is formed between the master and a slave. No physical link can be established directly between two slaves. A physical link can consist of more logical links that support unicast or broadcast traffic. Logical links are multiplexed onto the physical link to occupy slots defined in physical links.

IEEE 802.15.1 defines the lowest four layers of this architecture which makes the basic layers of this standard. Extra layers may be necessary to provide other services to applications which are not part of this standard and they are defined in *Bluetooth* specification. IEEE does not maintain standardization for 802.15.1 anymore. Currently, Bluetooth Special Interest Group (GIC) maintains the standard for this protocol and known as Bluetooth protocol. The last version that IEEE worked on this standard was version 1.2 in 2005. This version had data rate of 1 Mb/s.

Figure 2.8 shows the basic layers in its simple form without illustrating the functional blocks in each layer. In the figure, the lowest three layers sometimes form a group together and called a *controller*. If they are implemented all together, they are called a host controller interface or HCL. The remaining of the system including the L2CAP (Logical Link Control and Adaptation Protocol) and higher layers are known as *host*. The baseband (BB) layer works at the bit and packet levels and is responsible for operations such as forwarding error correction (FEC), encryption, CRC calculation and Automatic Repeat Request (ARQ) protocol. The link manager (LM) layer controls the connection establishment and release, authentication, traffic scheduling and power management. The L2CAP layer provides an interface between standard data transport protocols and lower layers by performing the segmentation and reassembly (SAR) for large packets. It also provides resource management, level of QoS and further optional error detection and retransmission.

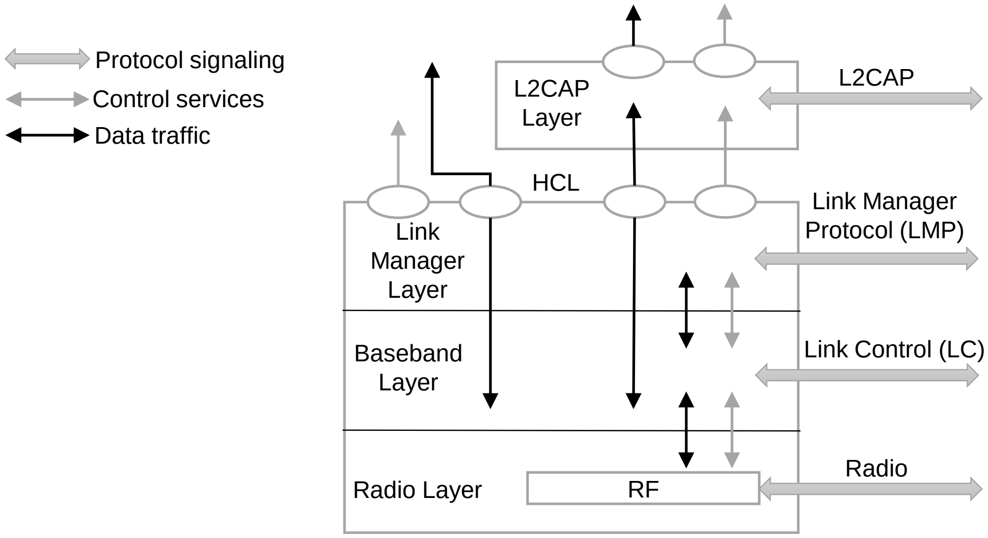


Figure 2.8: Core system architecture [3]

Bluetooth defines two wireless technology systems including Basic Rate (BR) (721.2 kb/s) and Low Energy (LE) described in Section 2.1.2. Both system support device discovery, connection establishment, and connection mechanisms. The BR system may include

Enhance Data Rate (EDR) with bit rate of 2.1 Mb/s and high speed operation up to 54 Mb/s with Alternative MAC/Physcial layer extension to carry Bluetooth over 802.11. Version 5 supports two types of controllers in the core specification known as primary and secondary controllers. The primary controller can be one of the options including BR/EDR, LE, or combined BR/EDR and LE controllers. The secondary controller is an AMP controller (or multiple of AMP) including an 802.11 Protocol Adaptation Layer (PAL), 802.11 MAC and PHY layers [41].

Bluetooth Low Energy

The current popular Bluetooth version is version 4 and it is known as Bluetooth Smart. Its specification includes Bluetooth Classic, Bluetooth high speed and Bluetooth Low Energy (BLE). Bluetooth version 5 deployed in 2016 and emerged in communication products in 2017 with focus on the IoT systems. BLE is designed for the use cases with lower data rate and duty cycle.

BLE has a new protocol stack with the capability of setting up simple links rapidly [19] and it is totally different than BR/EDR introduced in version 2.1 using usually for higher data rate and streaming. The purpose of BLE is providing lower power consumption, lower complexity, and lower cost compared with BR/EDR by introducing a simpler transceiver with binary frequency modulation and supporting a bit rate of 1 Mb/s with optionally support error correction down to 125 kb/s [41]. This protocol enables manufacturers to design smaller sensors running on tiny coin-cell batteries for months or even years. In some cases, solar or kinetic energy is enough to power sensors [42]. However, BLE is not backward compatible with high-bit-rate version. In order to solve this problem, BLE specification defines dual mode hosts that have two stacks installed.

BLE employs both Frequency Division Multiple Access (FDMA) with forty channels, separated by 2 MHz, and Time Division Multiple Access (TDMA) when devices transmit packets at a predetermined time. Three out of 40 channels are utilized as the primary advertising channels and they locate in the non-overlapping Wireless LAN channels. These channels promote rapid link establishment and device discovery [20].

Figure 2.9 from [4] shows the relation and compatibility among different version. Table 2.1 [19, 20] compares the specifications of the both Bluetooth and Bluetooth Smart. Similar in all stacks, above the physical channel there are concepts of links, channels and associated control protocols.

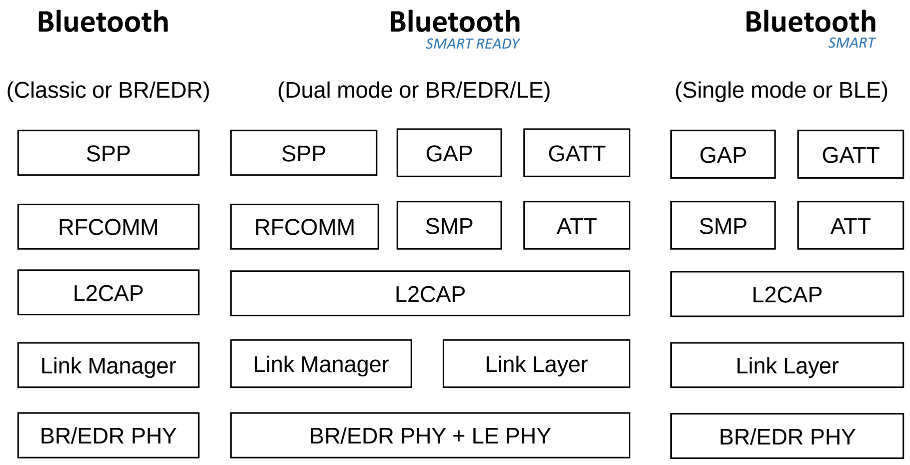


Figure 2.9: Bluetooth versions and their stacks from [4]

In an LE physical channel, multiple slave devices can operate simultaneously with some restrictions on establishing physical links. Slaves establish physical links with a master with permitting to establish multiple links with more than one master. However, there is no direct physical link between two slaves in one piconet. Furthermore, the devices can be master and slave at the same time; however, device role changing is not supported at this time [41].

Technical Specification	Bluetooth Technology	Bluetooth Smart Technology
Frequency	2400 to 2483.5 MHz	2400 to 2483.5 MHz
Nominal data rate	1 – 3 Mbps	1 Mbps
Application data rate	0.7 – 2.1 Mbps	0.27 Mbps
Distance	100 m	$>$ 100 m
Active slaves	7	No limited
Security	56 to 128 bit	128 bit-AES
Latency	100 ms	6 ms
Power consumption	1 W	0.01 to 0.5 W
Peak current consumption	$<$ 30 mA	$<$ 15 mA
Voice capable	Yes	No

Table 2.1: Bluetooth and Bluetooth Smart specification from [19, 20]

ANT

ANT [5, 43] is an ultra low power, 2.4GHz frequency band wireless protocol, designed for low data rate sensor network topologies. ANT is used as a PAN protocol as well as LANs in houses. It was designed for sports, fitness and some health applications. ANT protocol stack is compact and it can be run on microcontrollers with minimal resources. It can support various topologies including peer-to-peer, star, connected star and mesh with deterministic and ad-hoc mode data transmission scheduling. The simplicity of the protocol allows it to be run on a low-cost 4 to 8 bits microcontrollers (MCU), or a System on Chip (SoC). An ANT module or chip is usually connected through the ANT messaging or API to an application host in a typical ANT host. Three layers are implemented on an ANT MCU or ANT SoC. If the layers are implemented on an ANT MCU, they include *Physical Layer/Radio control*, *Link Layer and ANT protocol*, and *ANT messaging* which connects the ANT MCU to the Host MCU with a serial interface. The Host MCU has a similar ANT messaging layer to establish the connection. On top of this layer, *applications and ANT+ profile* layer is located. If ANT is implemented on a SoC, it has three layers including *Physical Layer/Radio control*, *Link Layer and ANT protocol*, and *ANT SoC Interface (API)* in SoC ANT stack and one layer, *SoC* *applications and ANT+ profile*, on top of the SoC ANT stack.

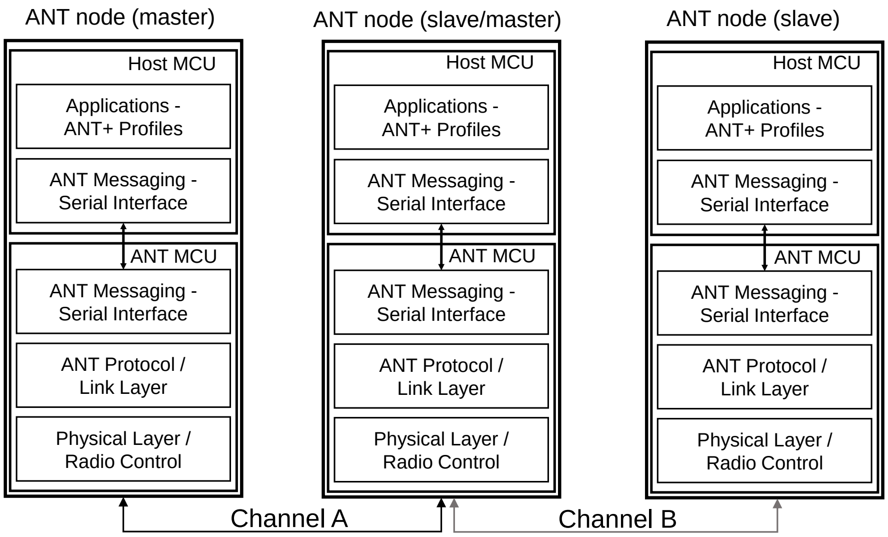

ANT node (master)
ANT node (slave/master)
ANT node (slave)
Host MCU
Applications - ANT+ Profiles
ANT Messaging - Serial Interface
ANT MCU
ANT Messaging - Serial Interface
ANT Protocol / Link Layer
Physical Layer / Radio Control
Channel A
Channel B

Figure 2.10: ANT layers in a simple network from [5]

Each ANT node can connect to another node over a 1 MHz dedicated channel with master/slave model; although, a slave can be a master in another channel to extend the network. Yet, channels can use the same frequency band but on a different slot in TDMA transmission. Most ANT channels are synchronous, independent, and bi-directional. Each specific channel is identified by a few channel parameters including type, RF frequency, ID and channel period. On each channel, there is one master and one slave. The master is the primary transmitter on an individual channel. Before using a designated channel, the master node performs a search to find a free channel period in channel time slots. After that, the master node always transmits at the same channel period of all time slots. If the channel is used bi-directional, the master node keeps its receiver on for a short time after each transmission. There are other options for channel type including *shared bi-directional slave channel* to be used by different slaves, *master transmit only*, and *slave transmit only* channels. The channel parameters are fixed before a communication and usually stays unchanged during the communication.

As mentioned, ANT supports a various range of topologies from a simple 2-node unidirectional connection between a transmitter and a receiver to a multi-transceiver system with point-to-multipoint communication model. All the complexity of the establishing and maintaining ANT connections encapsulates in the ANT engine that is the first part of a two-component model of an ANT node. The second part, called Host and connected with a serial interface to the ANT engine, handles the requirements of an application. ANT has profiles with specific parameters for data formats, channel parameters and the network key for various applications including heart rate monitoring, speed and distance monitoring, temperature sensor and fitness equipment data sensors.

Z-Wave

Z-Wave [44–47] is an ITU open standard communication protocol for consumer grade devices including remote controlled light dimmers, lamps, electronic door locks, and temperature sensors with the purpose of reliable data transfer, interoperability, and ease of installation. The Z-Wave protocol stack covers all network layers including PHY, MAC, network, transport, and application layers. The physical and MAC layer of Z-Wave defined in ITU-T G.9959 [6] and works in 908/860 MHz bands. Figure 2.11 illustrates a generic LAN architecture while Z-wave-capable devices build Home Area Network (HAN) in the architecture. Z-Wave is a low bandwidth, reliable, and half duplex protocol to transmit very short messages of few bytes long, for the real time but non-critical services. The MAC layer supports up to 232 nodes in one HAN with low overhead for a robust mesh routing. Collision avoidance algorithm with automatic retransmission is supported at MAC layer for a reliable data transfer. Long battery life consumption is enabled with a dedicated wake up pattern while power operated devices can stay awake for all times to reduce delay in the communication. Probably, the most important contribution of Z-Wave is introducing a common language of descriptors and commands at the application layer to provide interoperability across various product types, brands, and applications. Z-Wave has the ability to express the capabilities of smart devices through classes, commands, and reports.

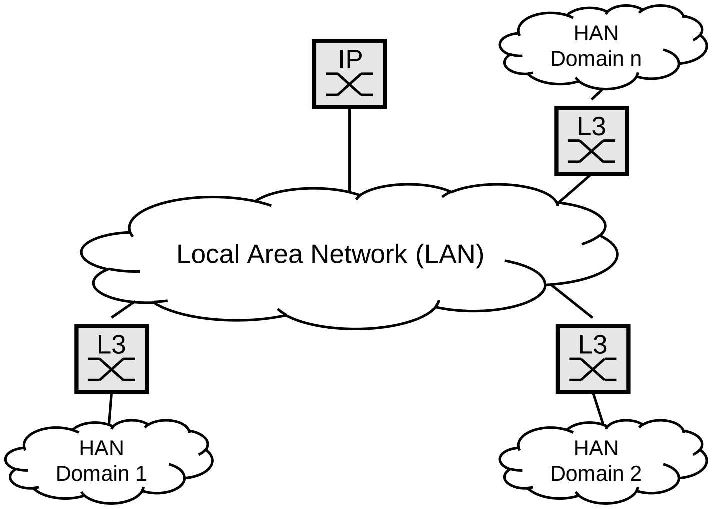


Figure 2.11: Generic architecture [6]

Z-Wave as a communication protocol can add and remove nodes in a network. Each node in a network has a unique *NodeID*, and *HomeID*, sharing among all nodes in the same network. These ids are assigned to the nodes by a primary controller at the time of joining the network. While other controllers may exist in the network, they do not participate in the addressing process. Only controllers have predefined HomeID to share with other nodes.

All frames in the network carry a checksum to ensure the integrity of frames. The checksum field is one byte to control up to 64 bytes of data with a simple checksum algorithm which is the weakness of the Z-Wave at this layer. After receiving each frame an Ack message is transmitted to notify the sender about the correct arrival of the frame; though it does not mean that the receiver has understood or executed the command in the frame. If no Ack message comes back after three unsuccessful transmissions, the sender considers the link to be down and starts the process of finding a new path. Therefore, Z-Wave provides a reliable communication path at this level. The routing functionality can be direct or hop-by-hop with static source routing mechanism in all over the network with maximum of 4 hops between a specific source and destination. During each node bootstrapping, the primary controller asks the node to discover all of its neighbors. The primary controller builds the network topology from this information and discovers different possible paths to each node. Hence, the primary controller can use other paths, if available, when the primary path is down. If all known paths are not available a new route discovery is initiated. The added information in the frame when it passes over each node is used as the return path to the controller. Other non-controller nodes, called slaves, may participate in the routing process depending on their capabilities. All of such nodes know their neighbors; however, simple slave nodes do not forward any frame to their neighbors. They only reply to a received frame by sending an ACK frame. Other slaves can send unsolicited messages to a few predefined nodes. These nodes only have partial information about the routing table in the controller. When a node joins the network, it sends a special frame called *Node Information Frame* (NIF) to describe its network and application capabilities.

The Z/IP defines the architecture to allow Z-Wave nodes to be represented as IP hosts. The application commands can be exchanged through the standard Z-Wave UDP port assigned by IANA. In this case, a Z/IP client can send IP packets to a Z/IP Gateway directly. The Z/IP Gateway may work as an IPv6 router and represents the Z-Wave network as an IPv6 subnet.

IEEE 802.11 and WiFi HaLow

IEEE 802.11 is a standard family for wireless local area network (WLAN). They have designed to work in ISM radio frequency. The members of the family have various bandwidth and coverage. IEEE 802.11 a/b/g/n are the older members of this family.

IEEE 802.11ac is the newer member with higher bit rate compared to others. The older members plus 802.11ac are usually used in devices equipped with a power supply or long lasting battery such as laptops and cell phones.

One of the emerging members of the IEEE 802.11 standard is 802.11ah [48], also known as WiFi HaLow by Wi-Fi Alliance [49], which provides long-range and low-power operations. It is also a proper candidate for wireless sensor networks (WSNs) and other multiple node networks such as smart meters and smart grids. It supports more nodes compared with other 802.11 standards. 802.11ah works in sub 1 GHz spectrum and has more penetration into obstacles compared to other variants of 802.11 protocols; however, its bit rate is lower than the others. The minimum throughput of 100 kbps and a maximum of 40 Mbps is the expected specification for this standard. It is also expected that this standard enables a variety of IoT devices in various areas including smart home, smart vehicle, digital healthcare and smart city. Figure 2.12 modified from RF Essential [7] illustrates the coverage area of some members of 802.11.

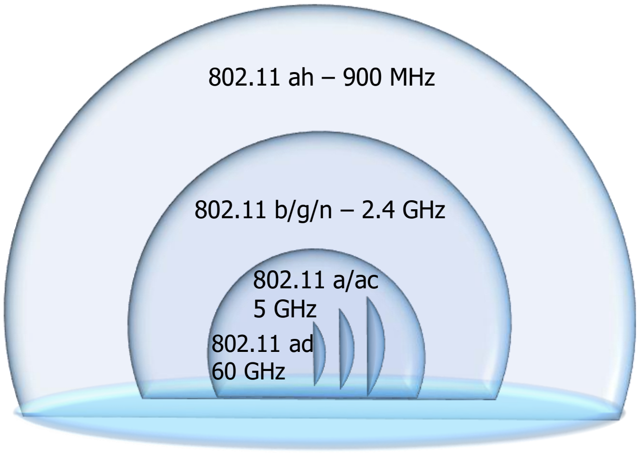


Figure 2.12: The coverage of some of 802.11 members [7]

IEEE 802.11ah is suitable for short bursty data packets with longer sleep time between transmission to save more power, especially with battery-powered sensors. The physical layer of 802.11ah is a ten times down-clocked model of the 802.11ac [50]. Instead of supporting 20, 40, 80 and 160 MHz bandwidth, it supports 2, 4, 8 and 16 MHz. One MHz bandwidth operates differently and both access point and station should support it. In addition, 802.11ah supports two-hop relay that can extends network coverage especially for the low-powered sensor nodes and nodes which are out of access point coverage. It also improves power consumption for battery-powered nodes due to shorter TX-RX cycle [51].

IEEE 802.11ah has various enhancements in the MAC layer compared with other 802.11 standards. First, 802.11ah can support more stations than other standards. This is due to the modified hierarchical version of *Association IDentifer (AID)* that allows registration of 8191 stations instead of 2007 in 802.11 legacy standard. AID is a unique identifier that an access point assigns to each station during the association process. The limitation of AID is caused by *Traffic Indication Map (TIM) Information Element (IE)* where each bit of it corresponds to a unique AID and support power management in stations. Second, IEEE 802.11ah has an enhanced power management mode. There is two power management mode in legacy 802.11. In *active* mode, the radio component of the node is always *awake* and it can sense all the incoming signals instantaneously. However, in *power saving* mode, the station alternates its status between *awake* and *sleep* state. In *sleep* state, nodes turn off their radio component; hence, they can not sense any incoming signal during this period. In this case, the access point buffers the station's packets until the node wakes up and request the buffered packets by a control frame, called *Power Saving poll frame*. After receiving the buffered packets, the station goes back to sleep mode. This is a downside to this model when the number of stations increases in the network. In this case, the length of the beacon frame is long, due to carrying a longer partial virtual bitmap in TIM IE. In addition, heavy buffered traffic may keep the power saver stations awake if the node cannot receive all of the buffered data during beacon interval period. This problem is solved in 802.11ah by introducing *TIM and page segmentation* mechanism. In this mechanism, the access point divides the partial virtual bitmap of one page to many pages and each beacon is responsible to carry the buffering status of a certain page. Considering the timing, each particular station wakes up at correct beacon time. As a result, the length of the beacon frame decreases and the power saving station just wakes up at the time of beacon that carries the buffered information for that particular segment [50]. Third, the compact packet format with reduced header size has been proposed to cover the low data rate of 802.11ah.

IEEE 802.11s

IEEE 802.11s [8, 52–54] expands the wireless coverage by providing a mesh topology for 802.11. IEEE 802.11 relies on several entities (known as Distribution System Medium (DSM)) such as wired networks to connect access points in order to expand the coverage area constructed by star topologies. This extended area is called Extended Service Area (ESA). Wireless stations can roam within the ESA. However, due to the regulatory limitation, a transceiver power cannot exceed a predefined standard value. This limitation makes the mesh topology as a suitable solution for the area expansion. Mobile ad-hoc networks (MANET) [55–57] also provide a solution for networks with no fixed infrastructure and mobile nodes. The routing algorithms utilized in the MANET network layers are usually IP-based. This is due to the fact that, the MAC layer does not provide a clear interface to report physical metrics to the network layer. Therefore, metrics such as link quality cannot be considered as a trusted value at the network layer and be involved in the routing decision making. IEEE 802.11s covers this limitation and provides routing at MAC layer.

The basic entity in 802.11s is called a Mesh Point (MP) with relay capability that can exchange frames over multiple hops. Similar to IEEE 802.11, a Mesh Basic Service Set (BSS) contains a group of MPs that may be able to communicate with each other when a mesh path exists. In addition, as part of IEEE 802.11, a Mesh BSS must support any kind of unicast, multicast, and broadcast communication.

A mesh MAC frame contains a mesh header field with four to six octets. The first octet includes the Mesh flag field with Address Extension (AE) value in its first bit. This value indicates that whether an AE exists in the frame. The rest of the octets includes Mesh Time to Live (TTL) and sequence control field to hold Mesh End-to-End sequence numbers. If AE flag is set, the Mesh Address Extension field may contain up to six addresses to identify other MPs on the Mesh path. Figure 2.13 borrowed from [8] illustrates 802.11s frame format.

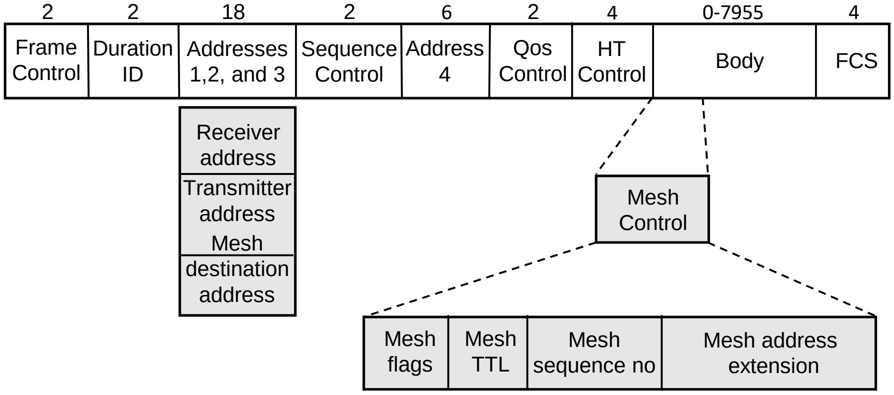


Figure 2.13: IEEE 802.11s frame format [8]

IEEE 802.11s performs path selection to select an optimal route in layer two. Although it is possible to use various path selection protocols, only one protocol can be active is a Mesh BSS at any time. Hybrid Wireless Mesh Protocol (HWMP) must be implemented on each Mesh Point. HWMP uses three various data unit including Path Request

(PREQ), Path Error (PERR), and Path Reply (PREP) in three different modes. The first mode is the on-demand driven path selection scheme which works similar to Ad-hoc On-Demand Distance Vector (AODV). The second mode is a tree-based scheme with an MP as the root of the tree. In this scheme, all MPs keep a path to the root by transmitting PREQ. On the other hand, Root Announcement (RANN) messages assist MPs to build a path to the root on-demand. The third mode is null path selection that indicates an MP does not forward frames. In all cases, each MP keeps a path table and updates it when new information is available.

2.1.3 Long-range Technologies

In this subsection, we present common long-range technologies employed in the edge networks including LoRaWAN, Sigfox, and 3GPP that can be utilized in smart homes. These technologies usually have very low bit-rate and energy consumption suitable for sensors transmission up to a few kilometers.

LoRaWAN

LoRaWAN [10, 58] is an open standard, long range, low power, low speed, bi-directional protocol designed for mobile or fixed battery-powered end devices with star-of-stars topology. A typical network includes a gateway which relays messages between end devices. The gateways are connected to a network server at the backbone with standard IP connections while end devices connect to one or more gateways through single-hop LoRa (a proprietary spread spectrum modulation) or FSK communication. The LoRa modulation technique is a derivation of Chirp Spread Spectrum (CSS) that improves resilience and robustness against interference and multipath fading [59]. LoRaWAN data rate varies from 0.3 kbps to 50 kbps depending on communication range and message duration. It uses adaptive data rate (ADR) scheme to control the data rate and RF power output for each individual end device. This scheme helps to maximize the battery life of end devices and network performance. Figure 2.14 illustrates LoRaWAN architecture [9].

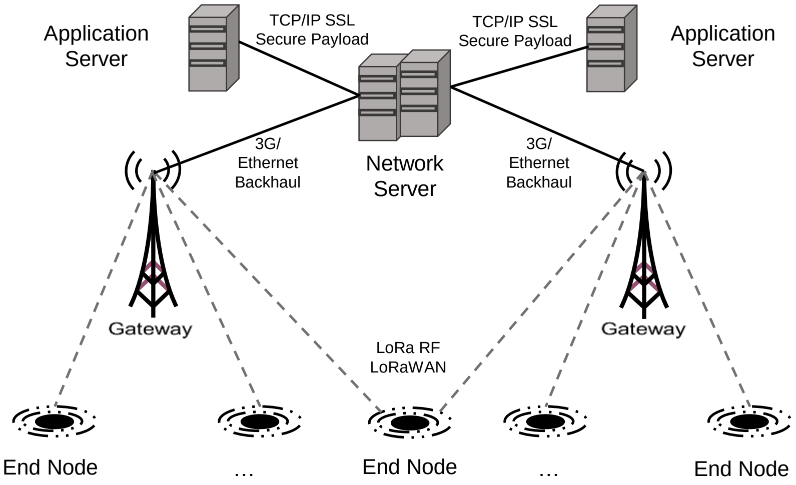


Figure 2.14: LoRaWAN architecture [9]

LoRaWAN specification defines three classes of MAC functionality, namely *Class A*, *Class B*, and *Class C*. While implementation of Class B and C are optional on MAC layer of LoRaWAN devices, Class A should be implemented. The other two classes must be compatible with Class A at all time. All three classes can coexist all together; however, there is no message in LoRaWAN to inform the gateway about the class of a device. The application specifies which class should be used. Figure 2.15 from [10] illustrates MAC options in LoRaWAN stack. Class A provides the best energy consumption among all the classes. It has been designed for devices that require more uplink transmission than downlink. Class A uses ALOHA-type MAC protocol where transmission slots scheduled by end devices based on the communication needs. Class B provides extra receive slots at scheduled times synchronized by beacons from the gateway. It helps the server to know when the end device is listening. Class C provides continues open receive windows proper for end devices that need more receiving than sending data. Class C consumes the most energy among all; however, it provides the lowest latency between the server and the end devices.

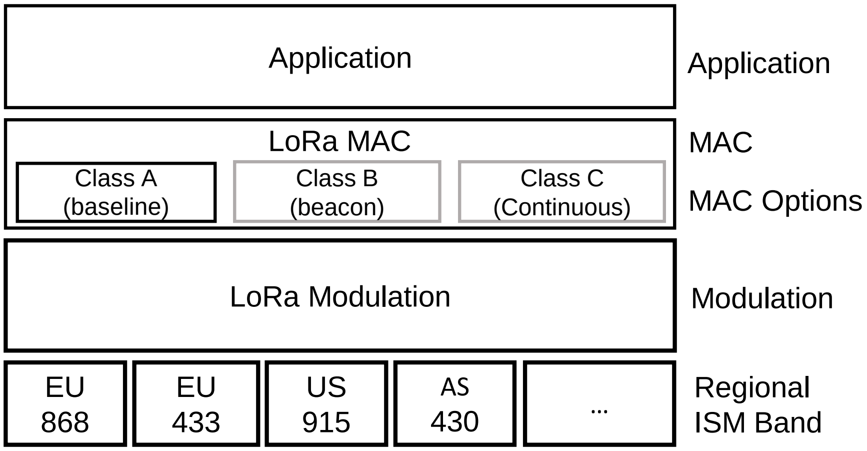


Figure 2.15: LoRaWAN classes [10]

LoRaWAN is a proper choice for environmental control, material leak detection, metering, smart agriculture, parking, street lighting, waste collection, and overall for all applications with relaxed delay constrains. On the other hand, LoRaWAN is not suitable for any real time applications required low latency with bounded jitter such as industrial monitoring and actuators with real time operation; or any control loops require a response time less than 1 ms. LoRaWAN is not suitable for services with low latency requirement such as Intelligent Transportation System (ITS) and video surveillance [59].

Sigfox

Sigfox [11, 60, 61] is a Ultra Narrow Band (UNB) communication technology for full duplex, long range, low power, and low throughput with high signal penetration data transmission suitable for underground equipment data transmission such as water pipe monitoring. UNB allows the coexistence of a large number of devices in a cell without significant interference. The uplink bandwidth is 600 Hz with 600 baud in the USA and DBPSK modulation. The uplink frame can carry a payload of 96 bits with 16 to 40 bit field for the authentication. FCC assigns 900 MHz frequency spectrum for downlink in the USA. The downlink frame has a payload field up to 64 bits, authentication field with 16 bits and 8 bits frame check sequence field. Due to the regulatory constrains in ISM bands, the number of messages in uplink and downlink transmission per device are unbalanced.

A Sigfox topology complies with ETSI ERM TG28 [62, 63] Low Throughput Networks (LTN) standard and has the following components.

- Base Stations (BS) are radio hubs in the system.
- End Points (EP) are leaf nodes of the system that exchange application data between applications running on an EP and the network application.
- Network Application (NA) is an application in the network at the opposite end of the EPs.
- Registration Authority (RA) is a central entity to keep all allocated and authorized EP ids
- Service Center that is responsible for EPs and BSs management, EP authentications, data packets forwarding, and cooperative reception support.

The architecture of a LTN network is illustrated in Figure 2.16. As it is shown in the figure, the architecture is a single core network containing the SC and the RA. Several BSs can connect to the CS. While BSs perform L1 and L2 protocols, SC performs L3 functions. EPs can be mobile or static. A given EP can communicate with the SC through one or many BSs.

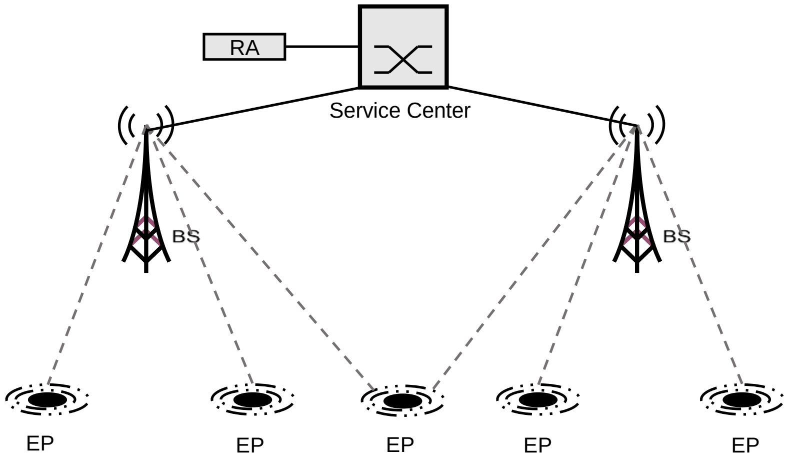


Figure 2.16: Low throughput network architecture [11]

3GPP Standards

3$^{\text{rd}}$ Generation Partnership Project (3GPP) [64] standardized NB-IoT (Narrowband-IoT) in Release 13 along with eMTC (enhanced Machine-Type Communication) and EC-GSM-IoT (Extended Coverage-Global System for Mobiles-IoT) to fulfill the various requirements of IoT market. The aim of introducing EC-GSM-IoT and eMTC is utilizing GSM (Global System for Mobile Communications) and LTE (Long Term Evolution) networks for better serving IoT, while NB-IoT has been designed for more complexity in the deployment to exploit a small portion of the available spectrum for ultra-low-end IoT applications with less backward compatibility with existing 3GPP devices. NB-IoT is the last standard in this group and extensively use LTE design [65].

NB-IoT [64, 66, 67] is a half duplex, narrowband radio technology for cellular communication designed for LPWAN with low impact on legacy GSM/WCDMA/LTE systems. Though other technologies in the release designed for Mobile IoT (MIoT) as well, NB-IoT focuses on indoor coverage, low cost, long battery life with supporting a large number of connected devices suited for smart metering, parking, building, cities and environmental

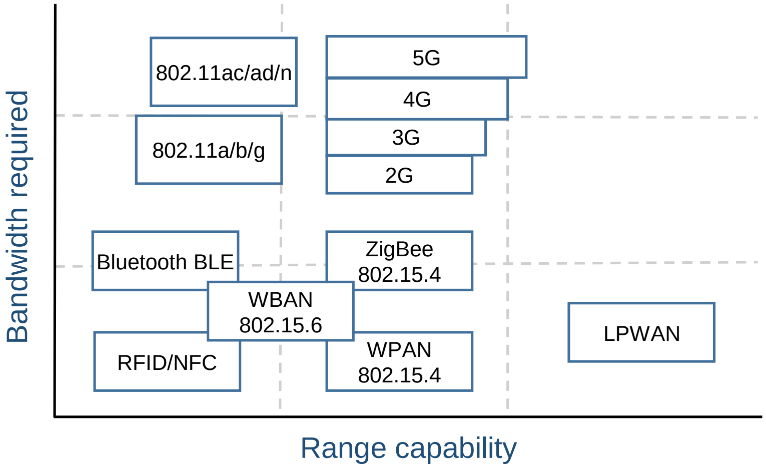


Figure 2.17: Range vs. bandwidth for various protocols [12]

sensor data collection. The uplink bandwidth varies between 20 kbit/s (single-tone) and 250 kbit/s (multi-tone), and the downlink bandwidth is 250 kbit/s with a long latency of 1.6 s to 10 s; however, the battery life expectation is 10 years. NB-IoT bandwidth is the lowest among the three standards and it is 180 KHz with three various deployments including in-band and guard-band LTE, and standalone, transparent to a user equipment.

eMTC has also designed for low device cost (higher than NB-IoT), long battery life and extended coverage. Similar to NB-IoT, it coexists with other LTE services and can be deployed in any LTE spectrum. Though it is a narrowband radio technology, it has a wider bandwidth than NB-IoT with the amount of 1.08 MHz. eMTC supports variable bit rates from 10 kbps to 1 Mbps depending on the required coverage. It has the shortest latency among all the three standards between 10 to 15 ms and can support both half and full duplex communications.

EC-GSM-IoT is also categorized in the narrowband radio technology with 200 KHz bandwidth, half duplex communication with 700 ms to 2 s latency. It has a data rate of 474 kbit/s in EDGE and 2 Mbit/s in EGPRS2B. Table 2.2 summarizes the features of the reviewed network technologies.

Protocols	Frequency	Data rate	Coverage	Topology	Standard
Sigfox	Regional sub-GHz	100 bps up 600 bps down	146-162 dB	Star	SIGFOX
LoRaWAN	Regional sub-GHz	0.3 - 50 kbps	150-157 dB	Star	LoRa Alliance
eMTC	LTE frequency	1 Mbps	156 db	Star	3GPP
NB-IoT	Inband LTE carrier	DL 250 kbps UL 20 to 250 kbps	164 dB	Star	3GPP
ZigBee	Regional sub-GHz and 2.4 GHz	250 kbps	100 m	Star, mesh	Zigbee Alliance
Z-Wave	Regional sub-GHz	9.6, 40 and 100 kbps	30 m	Mesh	ITU G.9959
WiFi	2.4 and 5.8 GHz	11 MHz to 6.9 Gbps	200 m	Star, mesh	WiFi Alliance
WiFi HaLow	Regional sub-GHz	100 kbps to 40 Mbps	1 km	Star	WiFi Alliance
ANT++	2.4 GHz	1 Mbps	50 m	Star	ANT++ Alliance
Bluetooth	2.4 GHz	1 Mbps	50 m	Star	Bluetooth SIG
Bluetooth LE	2.4 GHz	1 Mbps	50 m	Star	Bluetooth SIG

Table 2.2: Features of the reviewed technologies

2.2 IoT Models

Though IoT is still an active research topic, to the best of our knowledge there is no comprehensive and standardized model to explain the framework. Each current model has a tendency to explain some aspects of the IoT, depending on which group or organization has introduced it. In this section, we review the current and common IoT models. We start with IEEE model which is the simplest among all. ITU, IoT-A, and Cisco models are explained thereafter.

2.2.1 IEEE Model

One of the simplest models for the IoT has been introduced by IEEE P2413 [68]. It is a three-tiered model including sensing objects, the communication network, and application layers. In this model, sensing objects ("things") are in the first level of the model. The entire communication network is located as the middle level of this model while applications are the top level. While this model explains the major parts of the IoT, it does not provide any detail for each level, needed for resilience analysis. Furthermore, it focuses on just the physical aspect of IoT. IEEE P2413 is currently an active group that works standardising the IoT framework, identifying IoT domains, and commonalities among domains.

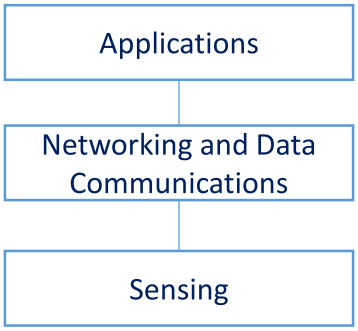


Figure 2.18: Three-tier architecture for IoT [13]

2.2.2 ITU Model

The ITU Y.2060 model illustrated in Figure 2.19 [14] focuses on integrating things to the communication networks, divided into two groups: objects in the physical world (*physical things*), and objects in the information world (*virtual things*) [25]. A device is the entity that maps every physical object into the information world, and must have communication capability. Devices can communicate with each other directly or through a gateway based on their communication capabilities and supported protocols. Other capabilities such as processing, sensing, or actuation are optional for such devices [14]. Although this model identifies a clear distinction between physical and logical worlds, it also does not provide any details about the communication network structure.

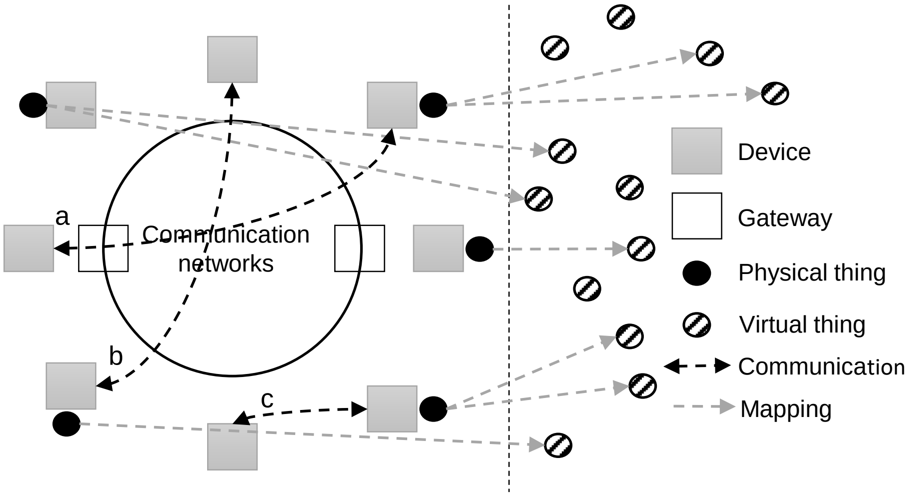


Figure 2.19: ITU overview of the IoT [14]

2.2.3 IoT-A Model

IoT-A [13, 15] is an European project to develop a reference model and architecture for IoT. It focuses on the interoperability of solutions at the communication and service level. The reference model has been designed in order to promote a common understanding and provides the highest abstraction level of the architectural reference model while the reference architecture describes the essential building blocks regarding functionality, performance, deployment, and security. The reference model includes IoT Domain Model, IoT Information Model to describe how IoT knowledge is modeled, and IoT Communication Model focuses on communication between various heterogeneous IoT devices and the Internet. The interaction of various models are illustrated in Figure 2.20. In Figure 2.20, the Domain Model is the main component of the reference model and introduces the main concepts of the IoT in the abstraction level independent of specific technologies. The Information Model defines the structure of all data and information that is processed in an IoT system on a conceptual level. This model is based on the domain and the related information to the concepts in the domain. The Functional Model represents all the functionalities that are key concepts of the Domain Model. Some of these Functional Groups (FG) build on top the other to represent the same relationship in the Domain Model. These Functional Groups provide the functionalities to interact with the instances of these concepts. Two examples of these Functional Groups illustrated in the figure, namely communication and security Functional Groups. In this case, the Communication Model represents concepts for handling the complexity of communication in heterogeneous IoT environment, and the Security Model introduces the security and privacy concepts.

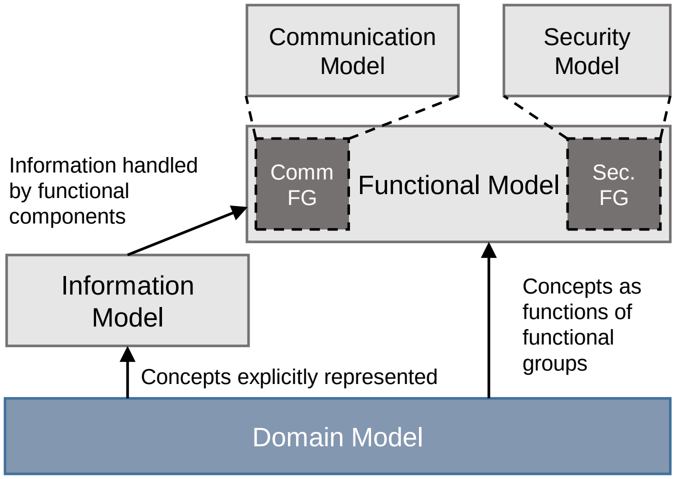

Communication Model
Security Model
Comm FG
Functional Model
Sec. FG
Information handled by functional components
Information Model
Concepts as functions of functional groups
Concepts explicitly represented
Domain Model

Figure 2.20: IoT-A sub models [15]

Though there are details for each component of the model and its reference architecture, the focus of this model is on entities and their instances in the IoT environment and presenting the abstraction of such systems.

2.2.4 Cisco Model

Cisco has introduced a seven-level IoT reference model, illustrated in Figure 2.21, considering physical devices, edge computing, people, and business processes [16]. In this model all physical end-devices including sensors and edge nodes are placed in the lowest *edge* level. Network devices and communication systems are defined in the second *connectivity* level. The third *edge computing* level is responsible for local packet-based processing [69] on behalf of simple devices with less processing power, data filtering, and transformation capabilities. The results may be stored for a short period of time in the *fog*, and are passed to the fourth *data accumulation* level for longer storage. After performing data integration and aggregation in the fifth *data abstraction* level, business analysis and reporting are conducted in the sixth *application* level. The top seventh *collaboration & processes* level is the place to impose policies to the whole system. While this is an interesting abstraction of the functional relationships of the IoT processing, it does *not* correspond to the physical and logical network layers.

2.3 IoT and Edge Computing Related Model

Emerging the Internet of Things (IoT) [14,68,70,71] has increased the growth of nodes at the edge networks. Introducing new types of network protocols suitable for different data rates, range, and energy consumption has boosted this growth substantially. Technology advancement leading to low price end point devices with high processing power is another factor for this growth. Finally, having the cloud as a powerful centralized processing entity with high capacity storage in the backbone structure satisfies all essential elements to push complex applications to the edge nodes and these nodes generate a huge amount of traffic back to the cloud. Increasing dependability to the cloud as a centralized structure makes the edge nodes more vulnerable to the occurrence of any challenges in the core

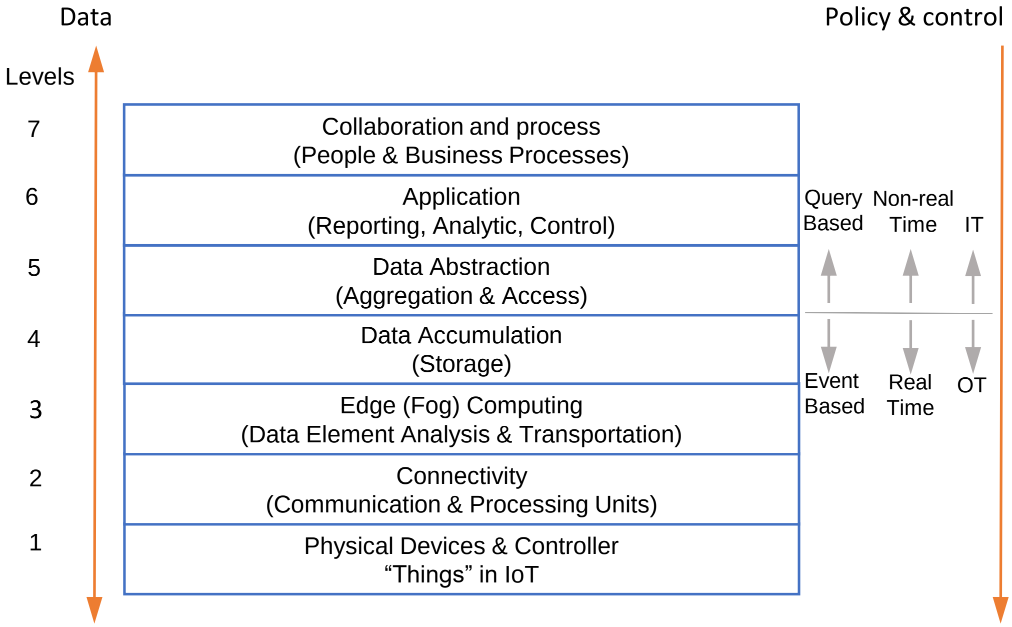


Figure 2.21: Cisco IoT reference model [16]

networks and the cloud. Furthermore, the long physical distance, usually hundreds of kilometers, between the cloud and edge nodes does not satisfy some application requirements such as low latency, low response time, and privacy protection. On the other hand, resource-poor devices at the edge networks require computation power to be provided by the cloud. Yet, the long physical distance from cloud to the edge nodes makes it hard to control the delay in WAN network for interactive applications. Unexpected irregular traffic over the capacity of the network is one reason that threatens the performability and usability of the applications at the edge networks leading to deficiencies in network resilience. Introducing Fog computing [69,72] and other related edge models are solutions to provide some answers to these problems.

2.3.1 OpenFog Model

The OpenFog consortium [17, 73], a group of companies and universities including Intel, Cisco, ARM, Dell, and Princeton University, expands the fog's definition after claiming that the current mandatory cloud connectivity is not adequate for IoT. OpenFog considers fog computing as a horizontal architecture to provide a continuum of distributed computing, storage, and network services from the cloud to the edge network. Moving computation near to the edge supplies enough resources for sensors, actuators, and cyber-physical systems; however, this definition does not avoid the cloud usage. On the contrary, the cloud and fog remain mutually beneficial architectures, in which some services work better on either. The application requirements and the current status of the network dictate which applications go to the cloud and which remains in the fog. Figure 2.22 illustrates the OpenFog architecture. Scalability, autonomy, RAS (reliability, availability, and serviceability), and hierarchy are considered as some of the primary attributes of this architecture.

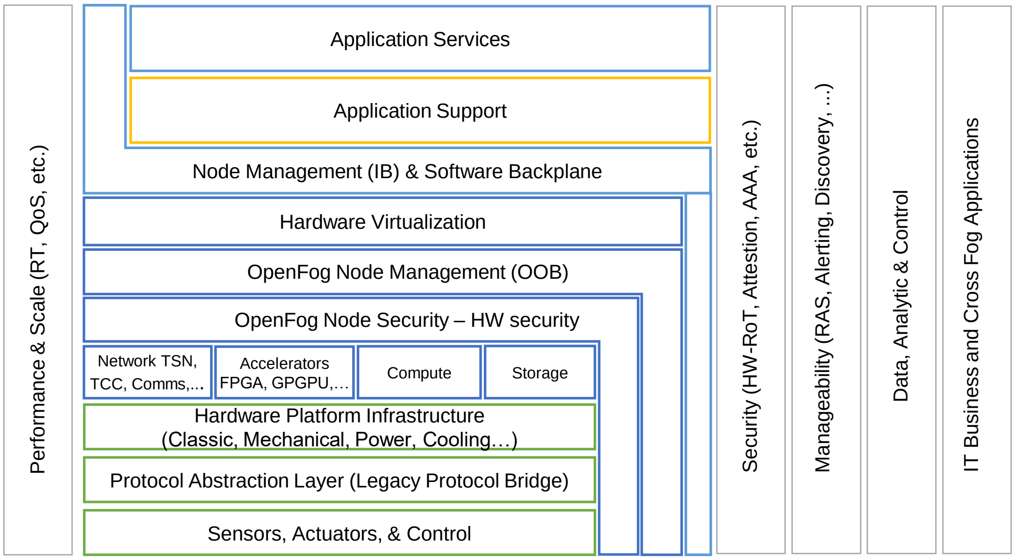

Performance & Scale (RT, QoS, etc.)
Application Services
Application Support
Node Management (IB) & Software Backplane
Hardware Virtualization
OpenFog Node Management (OOB)
OpenFog Node Security – HW security
Network TSN, TCC, Comms,...
Accelerators FPGA, GPGPU,...
Compute
Storage
Hardware Platform Infrastructure (Classic, Mechanical, Power, Cooling…)
Protocol Abstraction Layer (Legacy Protocol Bridge)
Sensors, Actuators, & Control
Security (HW-RoT, Attestion, AAA, etc.)
Manageability (RAS, Alerting, Discovery, ...)
Data, Analytic & Control
IT Business and Cross Fog Applications

Figure 2.22: OpenFog architecture [17]

2.3.2 Clouds at the Edge

Clouds at the edge is another solution by introducing private clouds and mini-clouds close to the edge [74]. It is suggested that this solution can be easily deployed in Long Term Evolution (LTE)'s Enhanced Packet Core (EPC). This solution is another way to confine the network traffic at the edge. It is also suggested that cloud enabled user devices can contribute to expand the edge cloud layer by leasing their resources.

2.3.3 Mobile Cloud Computing

There are other similar architectures including mobile cloud computing (MCC), cloudlet, and mobile edge computing (MEC); however, they have been utilized for other purposes especially for the mobile environment. For instance, MCC [75,76] has been specialized for the mobile environment by integration of cloud computing with the mobile environment to increase performance, tackle environmental obstacles such as scalability, availability, and security enhancement for mobile devices. In this architecture, cloud resources such as computing and storage are used to support and run applications on mobile devices. In other words, mobile networks offer some primary services to access the network, while the cloud resources are responsible for running the mobile applications and keep user data. Therefore, the same deficiency applies to the edge networks while they connect through the cellular network to the Internet. In another similar approach, resources from other mobile devices in the proximity are used to implement MCC [77]. Figure 2.23 illustrates MCC topology.

2.3.4 Cloudlet

Cloudlet [78] is a solution to overcome high delay and lack of resources in mobile phones by using trusted, resource-rich, well-connected computers to the Internet as a layer between

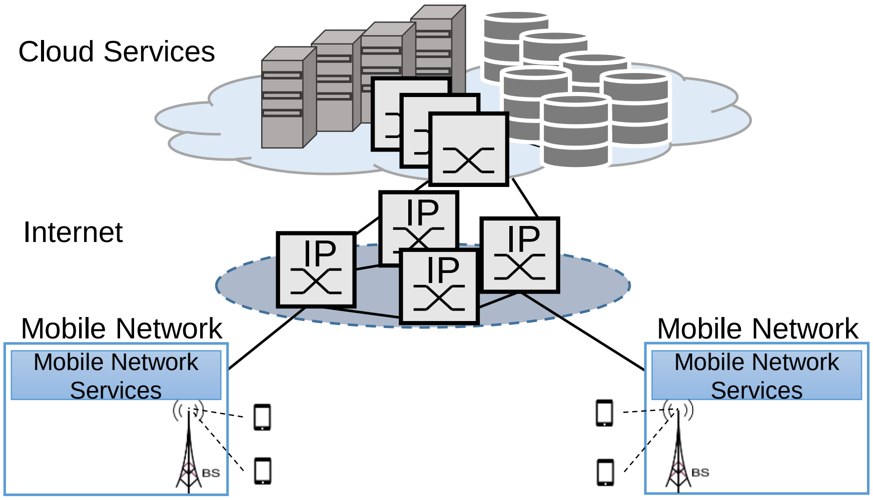


Figure 2.23: Mobile cloud computing topology

edge network and the cloud. In this solution, users run their requests on the local machines, installed in public areas to process user requests, instead of sending the requests to the cloud. A virtual machine is instantiated in the cloudlet according to the user request and destroyed when the service is completed. This solution redirects data traffic to wireless local area network to get the benefit of higher bandwidth and overcome the delay in the mobile environment to access the cloud resources. In traditional cellular networks, the base stations work as an access point to forward traffic to the core network without performing any processing. In order to reduce delay and traffic in the core network, MEC servers are attached to the base stations and supply computing power. If an MEC server can handle the process, the result returns to the user without entering the core network; otherwise, the request sends to the cloud for further processing [79]. Nokia [80] has deployed MEC commercially to support smart vehicle and industrial IoT among other use cases and it is considered as an edge cloud deployed in cellular networks. Figure 2.24 depicts the proposed topology for MEC, in which the MEC servers are capable of processing both user and control traffic, instead of sending data to the core network.

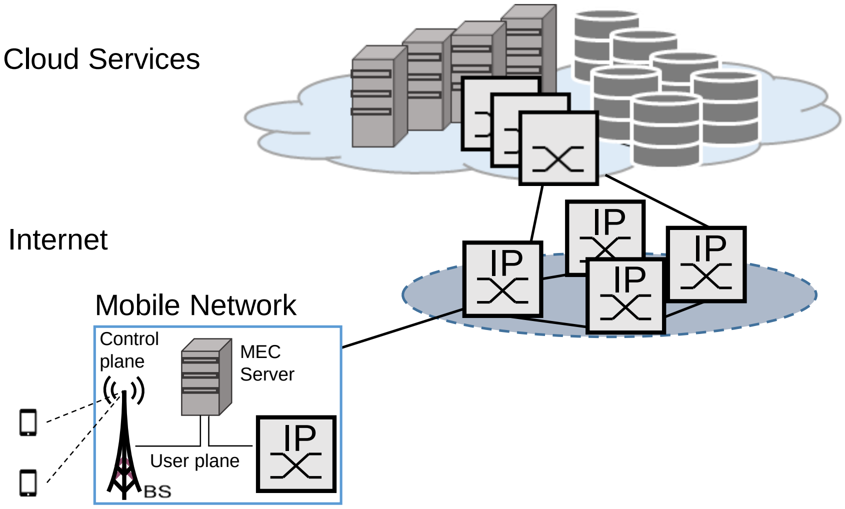


Figure 2.24: Mobile edge computing topology

2.4 Resilience and Survivability Principles

We now briefly review our ResiliNets strategy and principles [81] that we have previously used to analyse a number of Internet and domain-specific networks (such as MANETs – mobile ad hoc networks). We define resilience as *the ability of the system to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation* [82, 83]. In this definition, a *challenge* is any event that disrupts the normal operation of a network [18]. Any potential challenge that might exploits a *vulnerability* of a system is called a *threat*. A *fault* is a hypothesized cause of an error which is triggered by a challenge. In addition, an *error* is a system state deviated from its normal operation. If a correct service cannot be delivered or is deviated from its normal state a *service failure* happens [84].

Faults are classified to eight basic viewpoints including phase of creation or occurrence, system boundaries, phenomenological cause, dimension, objective, intent, capability, and persistence. The combination of these faults whenever they are valid are categorized to three major groups including development faults, physical faults, and interaction faults.

Development faults occurs during a development process such as software or hardware faults. Physical faults such as physical interference affect hardware. Finally, interaction faults include all external faults such as intrusion attempts [84]. In this study, we do not consider any development faults. We examine faults when a system is operational which includes mostly external faults and consequently interaction faults.

Since a challenge triggers a fault, there is a direct relationship between them; hence, a similar taxonomy can be considered for challenges. Challenges are categorized to phenomenological cause, target, objective, intent, capability, dimension, domain, scope, significance, persistence, and repetition [85]. We will investigate targeted challenges on an operational smart home to analyze resilience of its network.

Targeted challenges include all challenges that they target directly a communication infrastructure or target another infrastructure such as power grid that causes a collateral damage to the communication infrastructure. Furthermore, scope of a challenge includes all entities such as nodes, links, or a geographic area that it affects.

We also define survivability as *the ability of the system to tolerate correlated failures resulting from large-scale disaster and attacks* [**?**,82]. Survivability is a required attribute for network resilience.

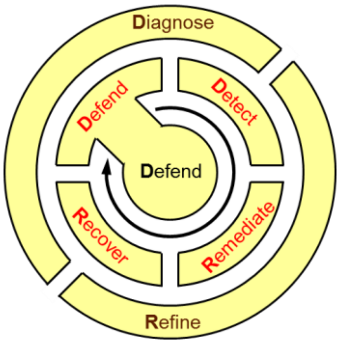


Figure 2.25: ResiliNets strategy from [18]

The ResiliNets strategy $D^2R^2 + DR$ is shown in Figure 2.25, and consists of two control loops: An inner loop to *defend* against challenges (consisting of structural defences in the middle, and active defences as part of the control loop), *detection* of challenges (including attacks and large-scale disasters) that penetrate the defences, *remediation* to provide the best possible service during and immediately after a challenge, and *recovery* to normal operations. The outer *diagnosis* of faults and vulnerabilities and *refinement* of future design and operation are beyond the scope of this dissertation.

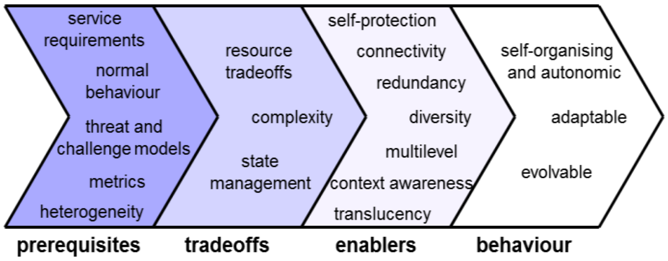


Figure 2.26: ResiliNets principles from [18]

In order to design resilient networks, ResiliNets [**?**] has defined a set of principles; the ones most relevant to this study are *redundancy* for fault-tolerance, *heterogeneity* and *diversity* for survivability, and *self-organising* and *adaptable* to remediate challenges.

2.5 Graph Centrality Metrics

The centrality indexes are metrics to identify the order of nodes and edges importance in a graph by assigning a real value to them. The value of centrality indexes depends on the structure of the graph [86]. Therefore, we can expect that many of such metrics cannot provide a correct centrality value when a node is logically important. For example, a smoke detector sensor at the edge of a network technology does not get a high centrality value with the most of the centrality metrics, but its operation is critical and should be considered as an important node. As a result, in a multi-technology network a modified version of the current metrics with proper weighting or new metrics considering logical importance of a node should be used.

In this section, we explore typical centrality metrics that can be used to analysis multi-technology networks such as smart homes.

Graph centrality metrics can be classified into three groups: *distance*, *connection*, and *spectra* classes [87]. The main criteria for distance metric measurements is the shortest path and the number of hop count over the shortest path. The node-degree value is the main consideration for the connectivity-based centrality metrics. Finally, eigenvalues and eigenvectors are the base concepts for the spectra metric measurements. Table 2.3 illustrates the summary of this classification. In the following subsections, we explain the centrality metrics utilized in our analysis.

Class	Metric	Symbol
Distance	Hop count	$d(v_i, v_j)$
	Efficiency	$E(G)$
	Diameter	Δ_G
	Radius	R
	Eccentricity	$\mathcal{C}_E(v_i)$
	Closeness	$\mathcal{C}_C(v_i)$
	Radiality	$\mathcal{C}_R(v_i)$
	Stress	$\mathcal{C}_S(v_i)$
	Betweenness	$\mathcal{C}_B(v)$
Connection	Degree	$d(v_i)$
	Neighborhood connectivity	$\mathcal{C}_N(v_i)$
	k-edge (node) connected	$\kappa(G)(\lambda(G))$
	k-core	$\mathcal{K}_i$
	Clique	$clique$
	Clustering coefficient	C, C_{v_i}
Spectra	Algebraic connectivity	λ_2
	Spectral radius	ρ
	Eigenvector centrality	x_i
	Katz	x_i

Table 2.3: Classification of the centrality metrics

2.5.1 Distance-based Centrality Metrics

Hop count is a distance-based metric illustrated by $d(v_i, v_j)$, and expresses the number of links on the shortest path between two nodes $v_i, v_j \in V$ of graph $G = (V, E)$. The hop count metric can be interpreted differently regarding values assigned to each link. For example, if a transmission delay is assigned to each link, the hop count between each node pair represents the overall transmission delay between two nodes.

The *average global efficiency* of graph G is the average efficiency of all node pairs in G where the efficiency of each node pair v_i and v_j is the multiplicative inverse of the shortest path distance between v_i and v_j [88, 89]. This metric measures the effectiveness of a graph to propagate information throughout graph G as follows:

$$E_{glob}(G) = \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{d(v_i, v_j)} \tag{2.1}$$

where $n = |V|$ represents the number of vertices in graph G. This metric returns a value in the range of $[0, 1]$ where 1 shows the maximum efficiency belong to a complete graph while 0 represents a fully disconnected graph.

The network *diameter* Δ_G represents the longest shortest path in graph G. This is a simple metric that shows the minimum number of hops to connect the farthest pair node in a particular network.

Eccentricity centrality is utilized to provide a solution for minimax problems. The minimax solutions indicate the location of a node in which it has the minimum distance to other nodes. Eccentricity measures the longest of all shortest path from each vertex v_i to all other vertices $v_j \in V$ as $e(v_i)$. The inverse of $e(v_i)$ is usually used to represent the centrality value as below:

$$\mathcal{C}_E(v_i) = \frac{1}{e(v_i)} = \frac{1}{max\{d(v_i, v_j) : v_j \in V\}} \tag{2.2}$$

where $d(v_i, v_j)$ shows the shortest path length from v_i to v_j.

This metric is employed to minimize the maximum distance of node v_i from any other nodes $v_j \in V$. Given a result, the higher value shows the proximity of node v_i to other nodes. Therefore, the small value shows that there is at least one node that is far from v_i. The high and low values are preferred to compare with the *average eccentricity* of graph G [90]. In addition, the set of vertices with minimal eccentricity denotes the center of G [86]. The eccentricity of graph G measures the average eccentricity over all the nodes in G.

The *radius* R of graph G is measured as the minimum node eccentricity over all the nodes in G:

$$R = min_{v_i \in V}(D) \tag{2.3}$$

Closeness centrality uses to solve minisum, known as median, problems in which a total distance of a node v_i to other nodes should be minimized [86]. Closeness centrality calculates the average shortest path for any node v_i to other nodes in a network. A network with a larger mean quantity of closeness centrality has the smaller average of the shortest path among all nodes and it shows that the nodes are more concentrated toward the center of the network. Closeness centrality for a node v_i is calculate as:

$$\mathcal{C}_C(v_i) = \frac{1}{\sum_{v_i \in V} d(v_i, v_j)} \tag{2.4}$$

where $d(v_i, v_j)$ is the shortest path distance between nodes v_i and v_j.

Radiality is a closeness related index and considers the shortest path to all reachable vertices regarding the graph diameter. The radiality of each vertex v_i is measured as the total subtraction of the graph diameter Δ_G from the shortest path between v_i and each $v_j \in V$.

$$\mathcal{C}_{\mathrm{rad}}(v_i) = \frac{\sum_{v_j \in V}(\Delta_G + 1 - d(v_i, v_j))}{n-1} \tag{2.5}$$

where $n = |V|$ is the number of nodes in graph G. A larger value for radiality of node v_i indicats, the node is closer to other nodes with respect to the network diameter. In other words, radiality shows that how well a node is integrated in the network. However, the value of radiality should be considered with eccentricity and closeness. A node with a high value of all of these three metrics indicates that it is in a central position in the graph [91].

Stress centrality measures the amount of communication that passes through an individual vertex v_i. It is measured based on the number of the shortest paths through a node v_i. Therefore, it is interpreted as the amount of 'work' that a node v_i performs in a communication network. Stress is calculated as:

$$\mathcal{C}_S(v_i) = \sum_{s \neq v \in V} \sum_{t \neq v \in V} \rho_{st}(v_i) \tag{2.6}$$

where $\rho_{st}(v_i)$ is the number of shortest paths through node v_i between the node pair s and t [86, 92]. Stress does not account any shortest path staring from or ending to v_i. This condition distinguishes stress centrality from betweeness explained in the following.

Betweenness centrality measures the fraction of the number of shortest paths between every two nodes s and t that contains a particular node v. If $\sigma_{st}(v)$ shows the number of shortest path containing v and σ_{st} identifies the overall shortest path between s and t then $\delta_{st} = \frac{\sigma_{st}(v_k)}{\sigma_{st}}$ represents the ratio of communication between s and t in which v is involved. Therefore, betweenness centrality is measured as [86, 93]:

$$\mathcal{C}_B(v) = \sum_{s \neq v \in V} \sum_{t \neq v \in V} \delta_{st}(v) \tag{2.7}$$

This value identifies the importance of a particular node in communication. In other words, this metric represents the role of a node to control the communication among others. In contrast to closeness centrality that is unable to work with disconnected graphs, betweenness centrality does not have such weakness.

The betweenness concept is applicable for edges defined as *edge betweenness centrality.*

2.5.2 Degree-based Centrality Metrics

Degree centrality in the communication networks is a measure of the importance of a node with respect to how well-connected it is. Degree centrality is a local measure and it is determined by the number of neighbors. A higher degree of vertex v_i suggests that more nodes rely on it for their communication. A node with high degree centrality in a communication network is a potential vulnerability in targeted attacks. The node degree of $v_i \in V$ is represented as $d(v_i)$.

Neighborhood connectivity measures the average number of neighbors of all v_i's neighbors [94, 95].

$$\mathcal{C}_N(v_i) = \frac{\sum_{v_k \in N(v_i)} |N(v_k)|}{|N(v_i)|} \tag{2.8}$$

where $N(v_i)$ is the set of v_i neighbors. Therefore, neighborhood connectivity has a direct relationship with degree centrality. The neighborhood connectivity of node v_i is small if v_i has neighbors with low degree centrality. On the other hand, nodes with low degree centrality connected to the neighbors with high degree centrality have high value. In other words, it shows the capability of any particular node to communicate with other non-neighbor nodes. Therefore, all nodes at the center of a star topology have a low neighborhood connectivity value. Although this metric can not consider a node criticality value and does not provide a direct connectivity measurement, it can identify a proper indication for the connectivity of the edge nodes. Since the edge nodes in a low-bit rate and low-energy consumption technologies usually connect to other nodes with a single link, neighborhood connectivity can indicate the well-connectivity of a particular edge node if the first hop is intact.

k-edge connected, or k-connected $\lambda(G)$, graph G is a connected graph with the maximum number of edges $\mid X \mid$ where $X \subseteq E$ and $\mid X \mid < k$ such that subgraph $G' = (V, E \setminus X)$ is still connected. In other word, k-edge connected implys that k separate paths exist between each node pair in G such that removing k edges partitions G. In k-edge connected graph G, it is required that $k \leq \delta(G)$ where $\delta(G)$ is the minimum degree of $v_i \in V$ [96,97]. k-vertex connected graph is defined similarly. The relationship between these two metrics are indicated as [87]:

$$\kappa(G) \leq \lambda(G) \leq \delta(G) \tag{2.9}$$

These two metrics are members of a group of metrics known as *reliability*. These group of metrics measures the number of removed elements resulting in disconnecting a graph.

A *k-core* is a maximal subset of vertices obtained from the recursive removal of all nodes of degree less than k. The result is a subgraph of graph G such that each vertex is connected to at least k other vertices [98]. Therefore, k-core can be interpreted as the stable part of the graph after $k - 1$ link failure.

A *clique* is a maximal subset of graph G vertices such that every vertex in the subset connects to other members of the subset forming a full mesh. In contrast to k-core, the cliques in a graph, if they are available, can be overlapped.

Clustering coefficient, C, is a concept obtained from the *transitive* relationship in the graph theory. Given three nodes u, v, and w in graph G and transitive relationship, if u is connected to v and v is connected to w, it does not always imply that u is connected to w unless these three nodes make a clique. Clustering coefficient measures the ratio of the number of triangle constructing by a closed path on each triad to the number of path of length two among each three nodes. Therefore, clustering coefficient of graph G

is calculated as below with a value in the range of $[0, 1]$ [98]:

$$C = \frac{number of closed path of length two}{number of path of length two} \tag{2.10}$$

Clustering coefficient can also be calculated locally for each node v_i. This metric shows how well the neighbors of v_i are connected together. Smaller values indicates that v_i is responsible to pass information among its neighbors. In other words, disruption of v_i also disrupts the information flow locally among its neighbors. The local clustering coefficient of node v_i is meastured as [98]:

$$C_{v_i} = \frac{Number of pairs of neighbors of i that are connected}{number of pairs of neighbors i} \tag{2.11}$$

2.5.3 Spectra Centrality Metrics

Spectra centrality metrics are based on eigenvalues and eigenvectors of the adjacency matrix of graph G. Let A represents the adjacency matrix of graph G, $\overrightarrow{v}$ shows eigenvector, and λ is the eigenvalue. The goal is calculating λ in the following equation:

$$A\overrightarrow{v} = \lambda\overrightarrow{v} \tag{2.12}$$

This equation can be represented as:

$$A\overrightarrow{v} = \lambda I\overrightarrow{v} \tag{2.13}$$

where I is the identity matrix. Therefore, λ is obtained from the following equation:

$$det(A - \lambda I) = 0 \tag{2.14}$$

Algebraic connectivity is the second smallest eigenvalue of the Laplacian matrix of G. Algebraic connectivity shows the connectivity of the network if its value is non-zero [98]. The graph Laplacian is a symmetric matrix with non-negative eigenvalue where the elements of the matrix are defined as:

$$L_{ij} = \begin{cases} d_i & \text{if } i = j \\ -1 & \text{if } i \neq j \text{ and there is an edge (i, j)} \\ 0 & \text{otherwise} \end{cases}$$

d_i is the degree of vertex i.

Spectral radius ρ is the largest positive nonzero eigenvalue of adjacency matrix A of graph G [87, 99]. Let λ is the set of eigenvalues of matrix A with n members and $\lambda_i \in \lambda$, the spectral radius of A is measured as:

$$\rho = max_{0 \leq i \leq n-1} \lambda_i \tag{2.15}$$

Spectral radius increases when the number of connections in graph G increases. Therefore, spectral radius can be considered as the overall reachability in graph G and it represents a measure of both percolation and network structure. Higher reachability can be interpreted as more influences that nodes have on each other leading to more vulnerability to casecade failures [99]. Thus, spectral radius is utilized to model cascade failures in a critical infrastructure network.

Eigenvector centrality is an extension of degree centrality that considers the importance of a node as the number of connections to the other important nodes [98]. The importance of a node in degree centrality is based on the number of connections to other nodes making them as a neighbor. If the idea is expanded and the importance of a node is considered based on the neighbors and neighbors of neighbors, eigenvector centrality is obtained. The eigenvector centrality of node v_i, represented by x_i, is measured as [98]:

$$x_i = \frac{1}{\lambda_{max}} \sum_j a_{ij} x_j \tag{2.16}$$

where λ_{max} is the largest eigenvalue of A and a_{ij} is the adjacency value between two elements i and j in matrix A. This equation gives a high centrality value to any node v_i if it has a high number of neighbors, a neighbor with many neighbors or both.

Katz centrality is an extension of eigenvector centrality. Similar to eignvector centrality, the importance of a node v_i depends on the number of direct neighbors, and neighbors of neighbors. However, the effect of neighbors of neighbors over the Katz centrality of v_i decreases when the distance from v_i increases. Katz centrality considers length of a walk between two vertices v_i and a neighbor v_j, and the effect of v_j over v_i [96,98]. Katz can consider nodes with various weights as a representation of the nodes importance in the centrality measurement. The centrality value of each node v_i, represented by x_i, is calculated as [98]:

$$x_i = \alpha \sum_j a_{ij} x_j + \beta_i \tag{2.17}$$

where α is a positive value that is usually chosen close to the value of the largest eigenvalues to increase the effect of the eigenvalue on the first sentence of the expression. β_i is also another positive value unrelated to the structure of the network and it can indicate the importance of node v_i in a network. Therefore, the overall Katz centrality value can be calculated as:

$$x = (I - \alpha A)^{-1} \beta \tag{2.18}$$

where β is a vector containing β_i values, I is the identity matrix and A is the adjacency matrix of graph G.

2.6 Summary

In this chapter, we study common communication network technologies applicable in smart homes. We divide these technologies into low, medium, and long range, and explain their characteristics briefly, related to this study. A typical smart home has a network integrated with various of these network technologies. Understanding characteristics and topology of these network technologies helps to analyze resilience of the smart home network.

In Sections 2.2 and 2.3, we review the current IoT models and edge models with their outstanding features and flaws. These models are our primary motivation to propose our smart home model in the next chapter. Though, there are many IoT models, to the best of our knowledge there is no standardized model, and a model to illustrate complexity and diversity of the network technologies for the smart homes suitable for this study.

In Section 2.4 we explain the existing ResiliNets' model and principles as the road map to analyze network resilience throughout this dissertation.

In Section 2.5, we reviewed graph centrality metrics divided into distance-based, degree-based, and spectra-based centrality metrics. These metrics are utilized in Chapter 4 for graph-theoretic analysis of various instances of smart home models.

Chapter 3

Smart Home Graph Models

In this chapter, we propose several smart home models to explore a proper representation for network resilience analysis. We use graph-theoretic models to evaluate and enhance smart home network resilience. First, we introduce our smart home reference model that captures a typical smart home services. We obtain the graph representation of our reference model as the next step. Our *end-system technology graph* illustrates the relationship of the end-systems in a smart home with the relevant technologies. Then, we introduce our new *technology interdependence graph* that represents the relationship among utilized technologies in a smart home [100]. This model can be used in any type of multi-technology networks to reveal dependency and connectivity of technologies. Then, we introduce our abstract model for smart homes. Additionally, we propose a colored-graph model to represent technology variants.

3.1 Smart Home Reference Model

In order to understand the structure of a typical smart home, we propose a reference model to represent the common services employed in such an environment. In addition to typical services in traditional homes supported by LAN and WLAN, a smart home is equipped with sensors and actuators in various devices to improve the quality of life of the home residents.

In this section, we present our model for a smart home that can be used to study network resilience. First, we define resilience in our context as *the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to the normal operation* [**?**, 82]. Challenges are categorized into various groups including target and scope [85] such that they cover all challenges with the impact on nodes and links of network infrastructure.

A typical smart home system is a combination of various sensors, actuators, controllers, control networks, and gateways [47]. The sensors generate data and send them to the controllers through control networks such as ZigBee or Z-Wave networks. The controllers manage the devices in the system containing actuators and sensors through the control networks while they are connected to the gateways to provide interconnection with other communication networks such as IP. Though this is the typical structure of a smart home system, what makes each of those systems different is the type of utilized network technologies dictating the topology of the networks, the number of such network technologies expanding the overall network size, and the variation of the technologies leading to the complexity of the overall network. Furthermore, each technology has unique physical and logical characteristics including the frequency bands, the network initiation process, the network components, the number of supported nodes, availability, and security. This heterogeneity of the technologies improves resilience through diversity. Since each non-IP network technology is self-contained, any disruption to the operation of the network technologies causes only that individual network inaccessible. On the other hand, many devices support various technologies; therefore, they can operate in many network technologies at the same time increasing the availability of the overall services and consequently network resilience.

Figure 3.1 illustrates our proposed smart home reference model of a typical smart home. In this model, various protocols are employed to fulfill the requirement of different services from interactive applications with high-bit-rate and low delay such as video streaming, to low-bit-rate sensors such as ambient light and thermal sensors. The typical wireless protocols running in a smart home are IEEE 802.11, IEEE 802.15.4/ZigBee, Bluetooth, as well as new protocols such as Z-Wave and LoRaWAN [10]. The topology of these protocols varies from a star to mesh. Though mesh topologies extend the network coverage and path diversity, they impose additional complexity of the routing protocol and computational power in mobile networks, and consequently may drain more energy in battery operated nodes.

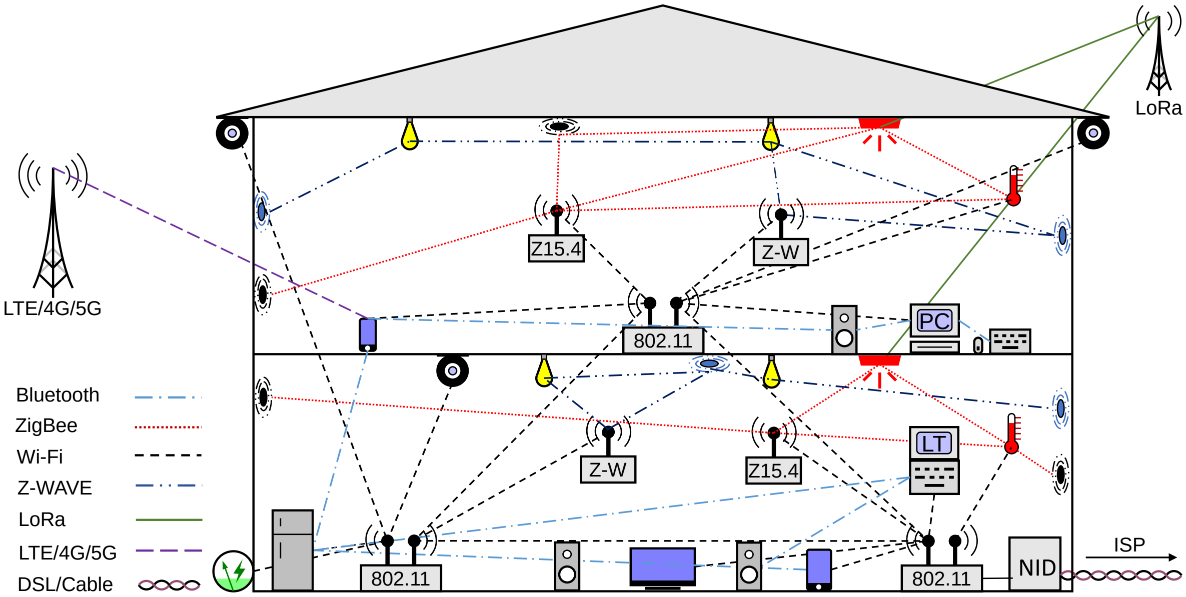


Figure 3.1: Smart home reference model

IEEE 802.11 in infrastructure mode constructs a star topology while IEEE 802.11s [52,53] utilizes a routing protocol at the link layer to provide a mesh topology. IEEE 802.15.5 provides mesh capabilities for IEEE 802.15.4. Alternatively, ZigBee builds a mesh over 802.15.4 running its own routing protocol. Bluetooth uses a piconet with a master/slave architecture in a star topology. In addition, Bluetooth Low Energy (BLE) is able to construct a mesh topology. The nodes in the network are capable of changing their roles from master to slave and vice versa to extend the range. Z-wave also builds a mesh topology managed by a controller with source routing.

As mentioned above, many of the protocols used at the edge network utilize their own native protocol stack including Bluetooth, ZigBee, and Z-wave. Therefore a gateway is required to interconnect with IP network to be accessible through the Internet. Consequently, any failure of the gateway results in loss of accessibility of such networks to IP network. Nevertheless, the isolated network should still be operational. In our model, we show a gateway with the name of its native protocol on its icon such as “Z 15.4” for 802.15.4/ZigBee. While in the real world of smart homes, any manufacturer may build a separate gateway to manage nodes of that particular native protocol and convert the native protocol to IP, gateways that support multiple protocols are available.

Figure 3.1 shows various services from high-bandwidth and low-delay such as streaming on a computer to low-bandwidth such as smart bulb and smoke detector. The technologies supporting each service are identified in the figure. This figure shows that various services are involved in a smart home and many technologies are used and connected together constructing a short size but a complex network. It is evident that the type of services and deployed technologies are different from one home to another, but the complexity and heterogeneity of the technologies are a common characteristics among all smart homes. These characteristics remain unchanged in the larger environments such as smart mulit-story houses or buildings. The only difference is that the size of the networks increase and other characteristics such as local metrics should be considered during the network design.

Heterogeneity of the technologies, observed in the smart home, is an essential factor to diversity of mechanisms leading to robustness of the system and consequently improving the smart home resilience.

We use a graph-theoretical model to represent our reference model formally. Given our reference model illustrated in Figure 3.1, we define a graph $\mathbb{G} = (V, E)$ as the connectivity graph of the model, such that v_i is a device in the model with a transceiver of a particular protocol and e_n is a communication link between two adjacent nodes v_i and v_j. Figure 3.2 illustrates the connectivity graph $\mathbb{G}$ associated with our reference model. Given our connectivity graph, we can measure and evaluate the robustness of the model with graph metrics. We perform this analysis in Chapter 4. In Figure 3.2, we use different colors for each type of link to represent the diversity of technologies. In addition, the thickness of edges represents the value of betweenness centrality, which measures the importance of an edge quantified as the number of traversing shortest paths. Each node in Figure 3.2 is annotated with $device\#_i\#_j$ as shown in the legend. It is corresponding to $device\ \#_j$ in floor $\#_i$ in Figure 3.1.

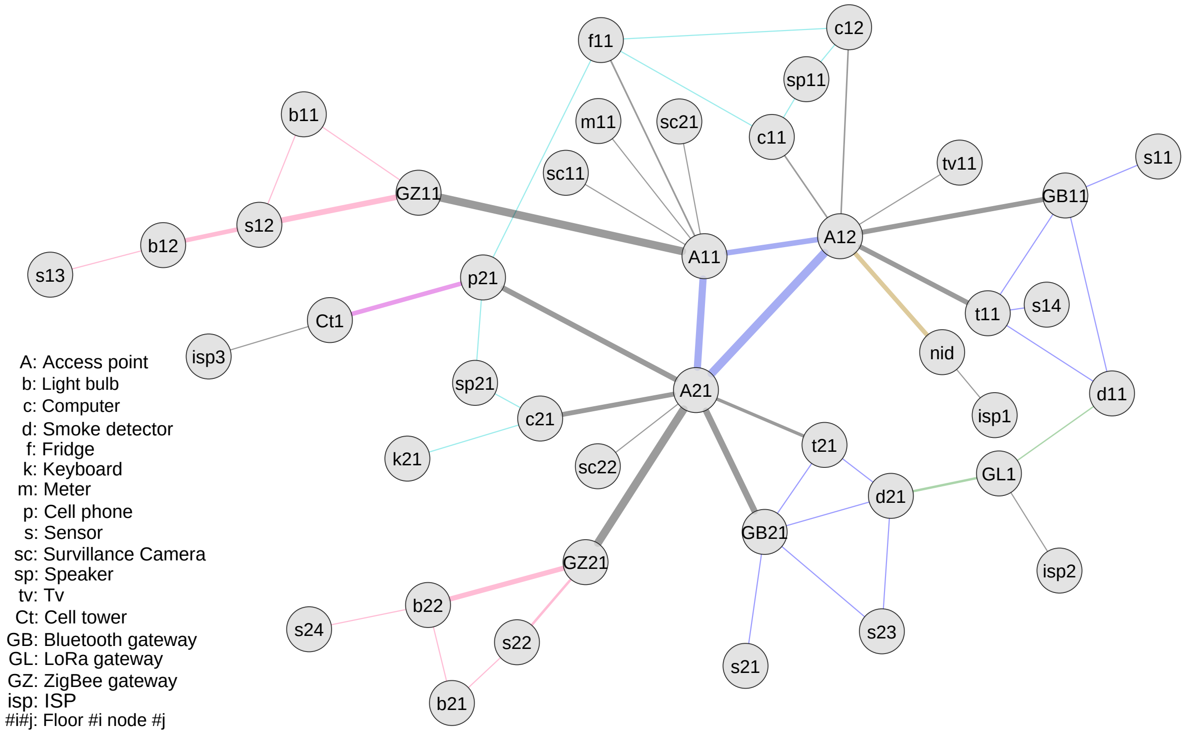


Figure 3.2: Smart home graph model

In addition to heterogeneity in technologies, path redundancy and diversity are another features that improve network resilience [101, 102]. As observed in our model and its corresponding graph, the heterogeneity of protocols consists of various WAN paths providing redundancy of the Internet access and diversity of networks. In our model, the smart home can access the Internet through one of the conventional end-user connection methods such as DSL or cable. In addition, cellular links can provide a second path to the Internet through LTE/4G/5G protocols. The low-power wide-area network (LPWAN) protocols such as LoRaWAN [10] and Sigfox [11] provide another path. If each of these WAN protocols establishes a connection to a different local ISP, then the diversity of the providers increases the network resilience. Consequently, any local targeted challenges such as a cable-cut or denial of service (DoS) attacks against the local ISP does not disrupt the other paths. This property is expanded if the local ISPs do not share the same upstream provider. However, one concern about the LTE/4G/5G tethered connections through cell phones is that the links are available only when the mobile user is at home. Therefore, we should consider these paths temporary unless a fixed LTE/4G/5G modem is installed. For the same reason, any mission-critical sensors such as smoke detectors and alarm systems should not rely on such temporary links. On the other hand, the LPWAN protocols do not have the LTE limitation as mentioned above, since they do not depend on a user being physically present. Hence, such protocols may be a better candidate for low-bit-rate, mission-critical sensors.

As illustrated in Figure 3.1, the model uses several Internet access technologies. Other protocols may be used to extend the smart home accessibility based on the availability of the services. For example, IEEE 802.11ah supports a lower bit rate but with wider coverage than other members of the 802.11 family, and it is suitable for battery-operated sensors and meters. Another option is conventional variants of IEEE 802.11 (e.g. 11n, 11ac) if the house is located in a smart city with city-wide wireless Internet coverage. We show physical and logical connectivity of the smart home to the Internet in Chapter 5.

3.2 Technology Interdependence Graph

In this section, first we introduce a new graph model to explain the relationship between the end systems and the corresponding technologies; and then, we propose our graph model to represent technologies relationships and their connectivity. These models will enable our future work on graph theoretic resilience analysis as in [103, 104].

As illustrated in Figures 3.1 and 3.2, various network technologies are identified in the model. Therefore, we construct another graph to show the relationship between nodes and the supporting technologies. We show this relationship with a bipartite graph. In this graph, one group of nodes represents technologies used in the model such as 802.11 and LTE, and the other group indicates the end systems that support a particular technology. Obviously, an end system with an interface of a particular technology has a direct connection to the corresponding technology vertex. If an end system has more than one type of interface such as cell phones equipped with LTE, 802.11, and Bluetooth, they have more than one edge to the corresponding vertices. Therefore, given our smart home graph model, we define each element of the incidence matrix B of the bipartite graph with size $n \times t$ where n is the number of end systems in the model and t is the number of technologies as follows:

$$b_{ij} = \begin{cases} 1 & \text{when node } i \text{ has interface type } j \\ 0 & \text{otherwise} \end{cases}$$

Figure 3.3 illustrates the *end-system technology graph* constructed from matrix B. In the figure, the grey nodes represnet the end systems and the cyan nodes show the technologies supported in a particular model. The edges between each group of nodes represent the technologies that each device supports. The thickness of the edges, drawn and calculated by Cytoscape [105], represents the value of edge betweenness centrality which shows the number of shortest path lies on each particular edge. As expected, the gateways, the access point connected to the Internet, and the cell phone provides tethering are on the most critical paths. In other words, any nodes that support more than one technology are on one critical path. Therefore, any failure of these nodes has more effect on the network connectivity.

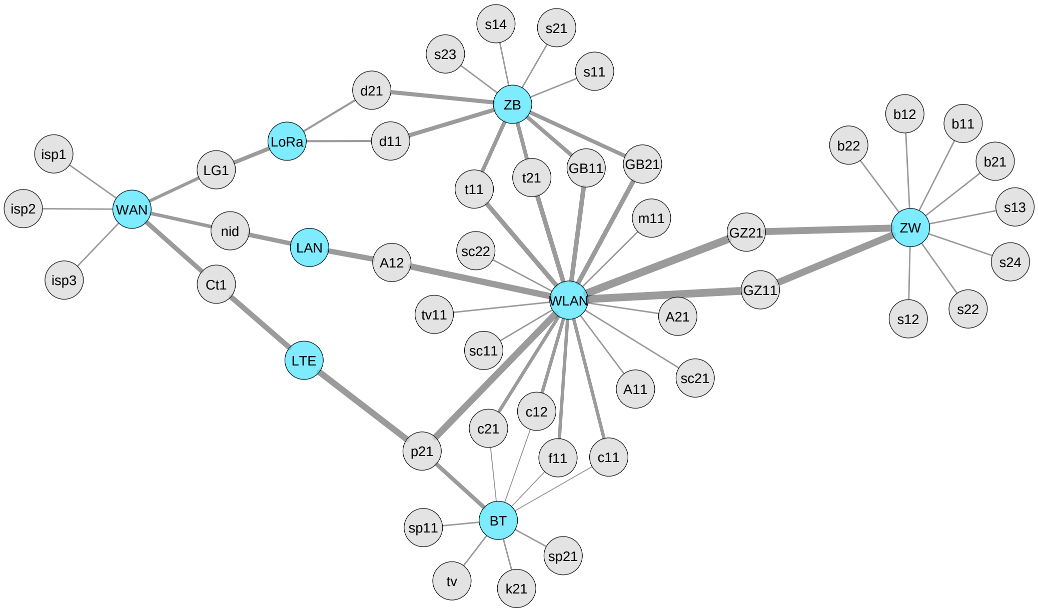


Figure 3.3: Smart home end-system technology graph

We also calculate the *one-mode projection* [98] of matrix B, using the Python NetworkX library [106], to obtain the direct adjacency between vertices of each technology, represented as our proposed *technology interdependence graph* shown in Figure 3.4. In the figure, WLAN has the highest degree-centrality value, connected to the most technologies in the model. Therefore, WLAN serves as the backbone of this model. Assuming only one access point is used in the network to provide wireless connectivity, the failure of this access point partitions the network. However, if IEEE 802.11s is used as illustrated in Figures 3.1 and 3.2, multiple access points can integrate to the mesh topology. While access points with the star topology provide wireless services to the end-points, 802.11s with the mesh topology improve the robustness of the wireless network through the path redundancy. Constructing a *bi*-connected mesh network protect the mesh wireless service from one-link failure.

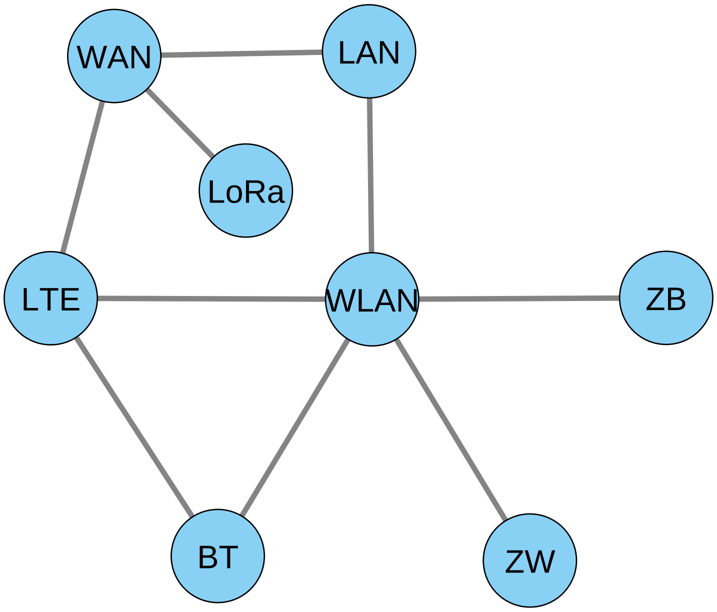


Figure 3.4: Smart home technology interdependence model

As observed, our technology interdependence graph hides the detail of the topological structure of each technology; however, it highlights the relationship among technologies. In other words, the technology interdependence graph provides a system-level overview of a particular configuration. Considering the above example and in order to improve the system-level resilience, *bi*-connectivity among technologies would be an essential factor to protect the system from link failure among technologies. As a result, a specific technology in a system that have k-connectivity for $k \geq 2$ is more reliable at the system-level than any other technologies with $k = 1$. We should emphasize that the overall system resilience of a model depends on both k-connectivity inside the network of a particular technology and between the employed technologies. However, k-connectivity inside and even between technologies is affected by supported topology. For instance, a particular

Bluetooth network with star topology cannot be more resilient than a ZigBee with mesh topology, even if both are *bi*-connected at the system level.

3.3 Smart Home Abstract Model

A typical smart home network contains a variety of network technologies, dividing between various network, and interconnected to each other. The types and number of network technologies depend on the types of services being fulfilled. A particular smart home service determines various network characteristics such as the amount of required bandwidth, the level of security, availability, and reliability. For instance, surveillance cameras and smart locks require a higher level of security compared to a smart light bulb; while a security camera needs higher bandwidth than a smart lock. Most IoT services require low bandwidth and incorporate battery-operated devices; thus, using such services in a smart home requires a network of networks with various technologies. As we have previously shown [100], WLAN and 802.3 usually establish the home backbone network to support high-bit-rate connectivity. Other technologies such as ZigBee, Z-Wave, and Bluetooth connect to the home backbone through a gateway. The topology of each technology varies from star to mesh.

In the context of networking, nodes in the center point of a star or the root node of a tree topologies usually have special capability; however, in a mesh topology, each node can usually connect to any other nodes; therefore, a mesh topology can be flexible enough to construct other topologies such as linear or star in special cases. While there is one path between each node pair in a star, tree, and linear topologies, a mesh network offers path redundancy making it more resilient compared to other topologies. However, diversity of mechanisms resulting from heterogeneity of technologies involves other factors including encoding, network setup process, forwarding algorithms, security, and energy consumption approaches. Each of these features provide opportunity for the improvement of network resilience. At this section, we only consider the topological feature of each technology.

Given these considerations, we introduce our abstract model in Figure 3.5 illustrating the essential elements of a standard smart home network [107]. This model shows the architecture and high-level structure as *home backbone* with other attached *home edge network* technologies. The home backbone is typically a mix of wired Ethernet and wireless 802.11 technology, but appears at the network layer to be a single IP-addressable network. In addition to end systems such as laptops (not shown in this figure), the home backbone provides connectivity to various other home edge network technologies, with disparate topology, protocols, and addressing. Because of this difference, they generally only interconnect through gateways to the home backbone, resulting in a star topology of networks, of which two are shown in the figure.

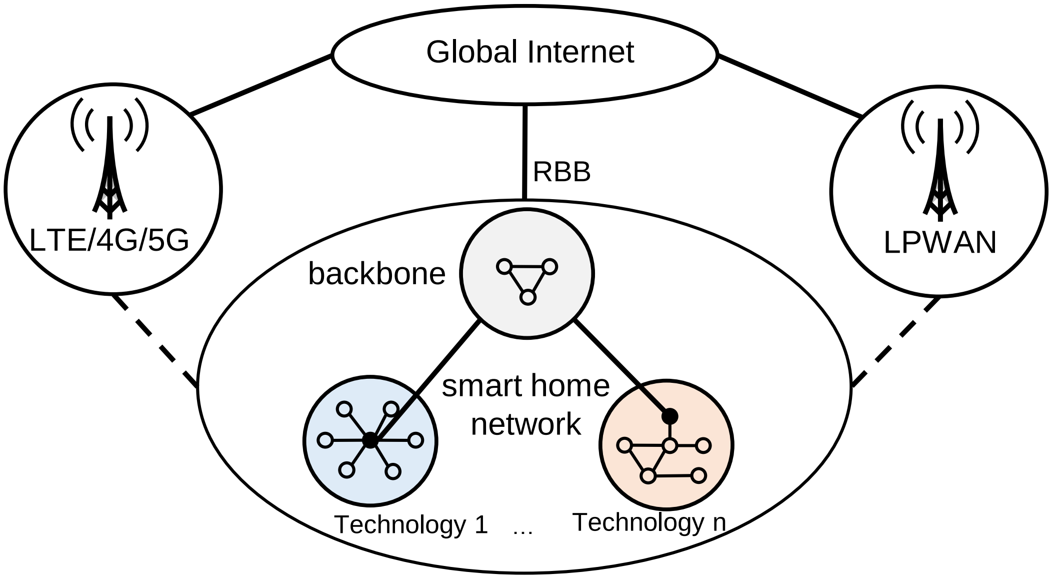


Figure 3.5: Smart home abstract model

Homes are typically connected to the Global Internet, traditionally for user access such as Web browsing, email, and media streaming. Additionally many *smart* home services use connectivity for remote access, for instance, controlling lights when away from home. Furthermore, many IoT devices use clouds-based services, increasing the attack surface, while providing poor resilience if they cannot operate when disconnected from the Internet.

While conventionally connecting through the Internet via an RBB (residential broadband) link such as DSL or HFC (hybrid fiber coaxial), increasingly LTE mobile networks (evolving to 4G LTE-advanced and 5G) are providing Internet access from homes. This enables the redundancy of a biconnected graph, while also providing diversity in communication medium such that wireless can be used if a cable is cut, and wired if the wireless channel is disrupted by heavy precipitation or jamming.

Given our new general abstract model, we generate an instance of the smart home graph model illustrated in Figure 3.6. In the figure, nodes with prefixes BT and ZB represent Bluetooth and Zigbee devices respectively. Nodes annotating with a number show WLAN workstations. A number assigned to a node, either as a postfix or stand alone, represents a sample device of a particular technology. As observed in the figure, high-bit-rate LAN technologies including Ethernet, 802.11, and 802.11s are used as the home backbone. While wireless LANs are dominant to construct the home backbone, they may suffer interference in a dense urban environment and may be jammed to disrupt home services and operation. Furthermore, each LAN technology usually supports a particular topology. As mentioned previously, IEEE 802.11 in the infrastructure mode builds star topology while 802.11s uses mesh topology. The range extension capability of 802.11s due to the mesh topology makes it preferable to basic 802.11 for the home backbone LAN. Furthermore, switched Ethernet can construct physical mesh with a logical spanning tree overlay on top to avoid loop in the network. Considering network resilience, a mesh network with k-connectivity of $k \geq 2$ should be constructed for the home backbone LAN. We consider k-connectivity of $k = 2$ for brevity of the model in the backbone structure while $k = 2$ offers minimum network resilience at the backbone.

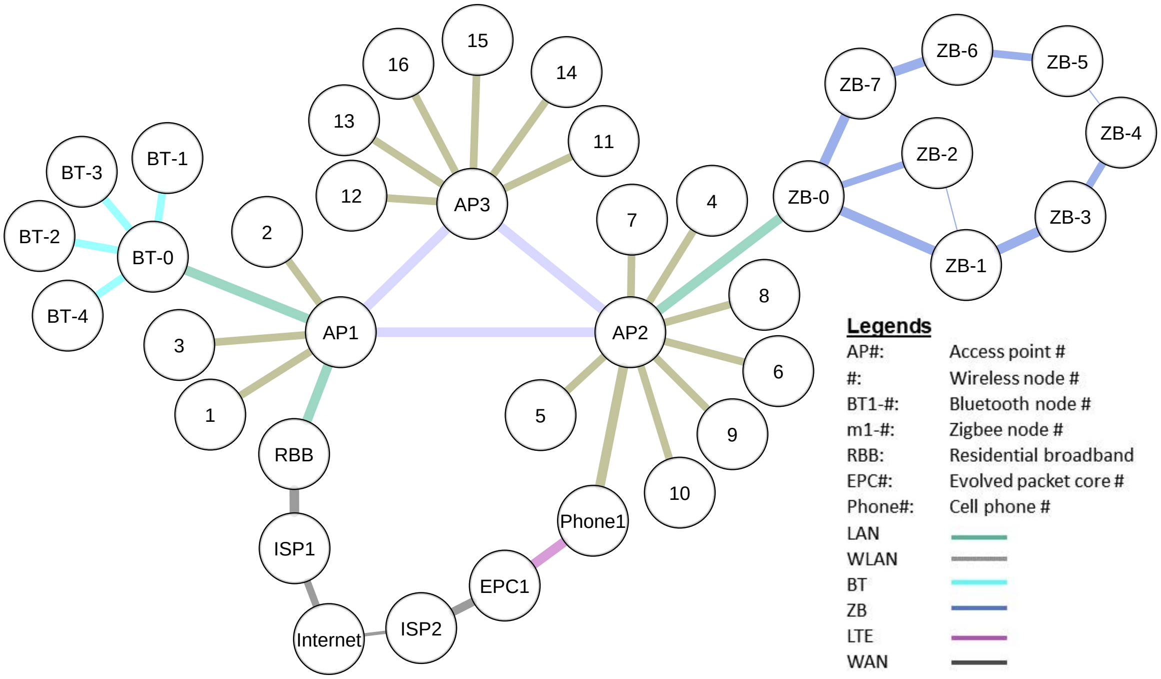


Figure 3.6: Colored smart home topology graph

The mesh nodes construct a mesh basic service set (MBSS). MBSS can be connected to an infrastructure BSS through a distribution system by a mesh gateway. Therefore, the infrastructure BSS supports other typical and high-speed IP services constructing a star topology around each mesh station equipped with an access point. Although the access points in 802.11 are the point of failure of this structure, mobile nodes can connect to other access points during failure of their native access point. On the other hand, implementing some of the mesh edges with Ethernet improves resilience more through the heterogeneity of the technologies and diversity of the protocol mechanisms.

Other network technologies are connected to the backbone through their gateways. Current typical technologies utilized in the network technologies of a smart home, including ZigBee and Z-Wave, can construct mesh topology. Other technologies including Bluetooth build star topology. Furthermore, Bluetooth can construct mesh topology by changing the role of a slave to a master node and vice verse.

While most of the low-bit-rate technologies such as ZigBee support a mesh topology, the ultimate topology of such networks depends on the density of the nodes in the network, the average distance among nodes, and the specialized nodes utilized in a particular technology such as coordinators and routers. The topology may be a star which is when all nodes are in the range of the coordinator or master node but far from each other, linear when the network coverage is extended, mesh when some nodes are in the range of the other nodes, and a combination of these options. In most low-bit-rate technologies including ZigBee and Z-Wave the battery-operated nodes do not participate in the routing or forwarding processes; therefore they are usually the endpoints of the network graph. We construct this part of the network graph by the *caveman* graph [108] algorithm with Python networkX library [109], which has the capability of generating a particular number of cliques with a specific size. This structure can emulate a controlled mesh network. We process the produced graph from caveman algorithm for the number of connected components and eliminate those nodes that are not part of the largest component in the graph to generate a graph with one connected component. Since both ZigBee and Z-Wave generate a mesh topology in an optimal condition, we consider one mesh network for brevity as a sample of these technologies in our model; although, many such networks with more complexity and number of nodes can exist simultaneously in a larger network. For instance, a simple network can have one particular network technology, while a multi-story building may have various types of the networks with more nodes. Since these network technologies are low-bit-rates and self-contained, any structural changes or failure have no or minor effects on the home backbone LAN. Therefore, these networks can be studied separately.

Other high-bit-rate technologies, including 4G/LTE/5G, can be integrated to the network to increase the path diversity to the Internet. When the network is in the normal operation, a cell phone can join the network through its 802.11 interface and act as a wireless station. However, during a WAN failure, a tethered cell phone can operate as an access point to connect the internal network to the Internet through a different path.

LPWAN technologies including NB-IoT and LoRaWAN can also be utilized in a smart home network. However, we do not use them in our home network graph instance; since, such technologies are part of larger networks mainly outside of the smart home network. Many technologies of this group, including NB-IoT, LoRaWAN, and Sigfox, have a star or star of star topologies similar to the topology in 4G/LTE/5G technologies. In all of these technologies, the center point of the star topology is usually out of the home network; therefore, they create a separate network. Such networks are connected to the home network at the ISP level or even an AS level. Hence, any failure in the lower levels of the network hierarchy does not affect both networks simultaneously; unless the failure happens at the same or higher levels of the network hierarchy in which the two networks are connected. We represent the point of connection between the two networks with the *Internet* node in our home network graph instance illustrated in Figure 3.6 assuming that the two ISPs are reachable with one hop to simplify the structural complexity of the Internet.

We expand the formal representation of our home model by an edge-coloured graph $\mathbb{G}_{\text{conn}} = (V_c, E_c, C, \chi)$ as the connectivity graph illustrated in Figure 3.6, such that $v_i \in V_c$ is a node with a transceiver t_{ik} of a particular technology and $e_n \in E_c$ is a communication link between two adjacent nodes v_i and v_j. Furthermore, C is a set of colors equivalent to the number of employed technologies in the graph and $\chi : E_c \rightarrow C$ is a function to assign a color to each edge. Precisely, we can define E_c as:

$$E_c = \{((u, c_i), (v, c_i)) \in V_c \times V_c | \chi(u, v) = c_i\}. \tag{3.1}$$

We can also assign various attributes representing the features of each technology to each color c_i such as bandwidth or average length of links.

Furthermore, this representation illustrates path diversity resulting from technological heterogeneity. It can also differentiate nodes that have different type of interfaces supporting various technologies in the model such as a technology gateway or a cell phone. These types of nodes work as a bridge to interconnect different technologies. Therefore, greater attention should be paid to these nodes and they should be given reinforced levels of robustness in order to promote system-level resilience.

As explained before, the thickness of the edges shows the value of edge betweenness centrality (the number of traversing shortest paths over a particular edge), which is one measure of edge importance. This shows that while high betweenness corresponds to some important edges (such as the home backbone triangle and Internet access links), it does not correlate well for others, such as one of the Bluetooth stubs. Thus we need to assign a separate set of weights critical nodes and edges, and to adjust depending on whether they support mission-critical and lifeline services. For example, a smoke detector link and the gateway to which it is attached are weighted as more significant than a non-critical light.

3.4 Summary

In this section, we propose several models for a smart home network resilience analysis. First, we introduce our smart home reference model. This graphical model helps us to understand and identify various services and technologies required in a smart home and shows the complexity and heterogeneity of a smart home network. Then, we define our smart-home graph model corresponding to the reference model. We use this graph-theoretic model for graph centrality analysis in the next chapter.

We propose a new technology interdependence graph obtained from any smart home graph instances as the next step. This model provides an abstract view from utilized technologies in a particular smart home model. It also illustrates connectivity among technologies which can be used for system-level resilience analysis.

Our smart home abstract model represents the general structure of a smart home proper for any building size. This model identifies a backbone at the center of the topology connected to other required technologies. It also shows the path diversity to the Internet.

In a formal definition, we use colored-graph model suitable to formalize various technologies and their features. This model represents the diversity of the technologies, and it will be utilized to quantify resilience when applying technology characteristics to the edges of a graph model is required.

Page left intentionally blank.

Chapter 4

Smart Home Graph Analysis

In this chapter, two baseline and four specific instances of home network topologies will be introduced and analyzed. The weakness of one layer analysis will be highlighted motivating us the development of the multilayer framework in the next chapter.

As part of four specific instances, we construct two smart home models from the abstract model introduced in Section 3.3, one for a small home and another for a larger building. We call them *home network* and *expanded home network* throughout this chapter. We also analyze models resulted from the main Internet connection failure of the *home network* and *expanded home network* as the rest of the instances. We call them *backup home network* and *backup expanded home network*, respectively. We compare these four models with the baseline home network architectures with star and mesh topology to study the characteristics of the smart home models regarding resilience. We use centrality metrics, reviewed in Section 2.5, for this analysis [107].

4.1 Baseline and Smart Home Instances

In this section, we explain and introduce all the instances used in this analysis. We divide this section into two subsections. Subsection 4.1.1 explains the baseline models utilized in the current home networks. In Subsection 4.1.2, we introduce two instances of smart home models that we expected to see them in the future smart home networks, *home network* and *expanded home network*, and their associated backup models, *backup home network* and *backup expanded home network*, during the Internet connection failure.

4.1.1 Baseline Home Models

We consider two baseline topologies for comparison with the smart home networks, *star* and *mesh* backbone, and construct their connectivity graphs. We consider a star wireless LAN implemented with IEEE 802.11 connected to the Internet by an Ethernet link through a DSL or HFC (hybrid fiber-coaxial) cable link (shown as RBB (residential broadband) node), typical of many traditional home networks, as *star network* and illustrated in Figure 4.1.

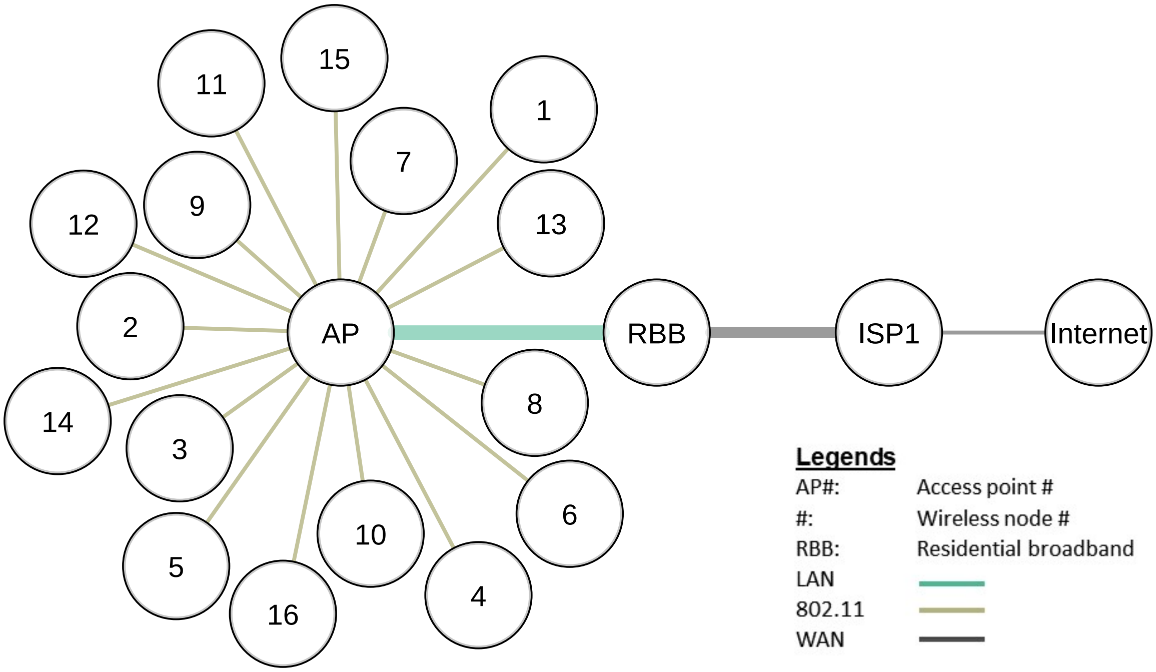


Figure 4.1: Connectivity graph of *star* topology

We then enhance the star network to incorporate a full-mesh backbone as would occur by replacing a single 802.11 access point with three meshed 802.11s nodes (AP1, AP2, AP3) in Figure 4.2. Each mesh node (defined as a mesh station in a mesh basic service set (BSS) [110]) also works as an access point and constructs a star topology with its 802.11 interface. Therefore, the final topology is a mesh of stars topology but we call it *mesh* for the simplicity throughout the rest of this chapter. The same though is applied for the *star* model since the topology is not star after integrating the *RBB*, *ISP1*, and *Internet* nodes. We consider the Internet with one node for the simplicity in order to show the connectivity of the networks to the Internet. This assumption helps to focus on the structure of the home networks without involving the details of the Internet structure.

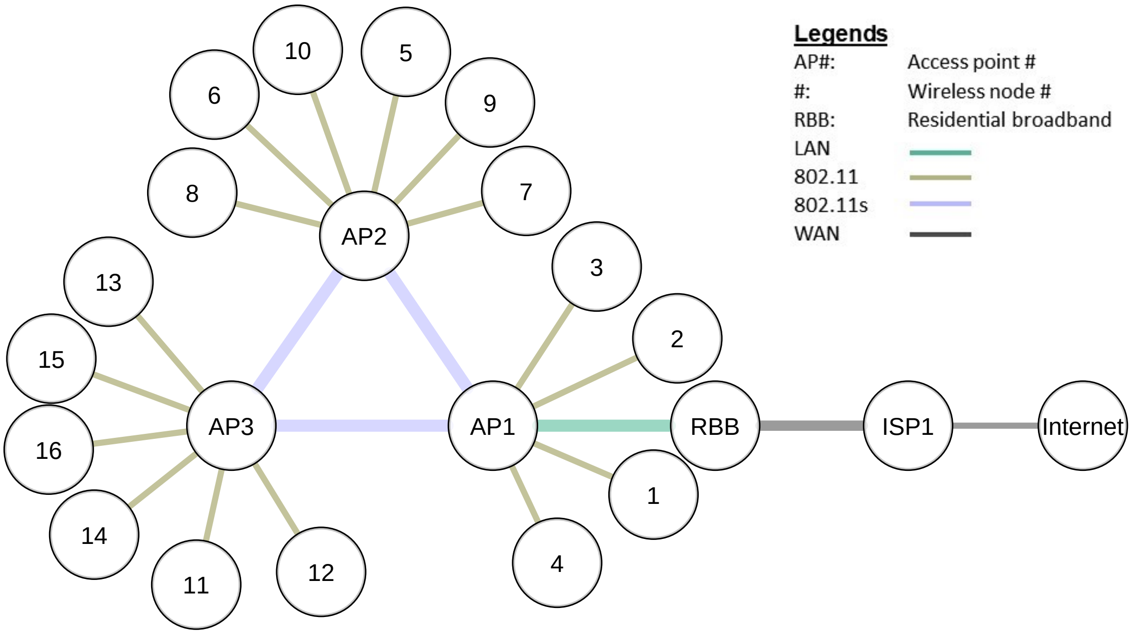


Figure 4.2: Connectivity graph of *mesh* topology

4.1.2 Smart Home Models and Formal Definition

First, we formally introduce the connectivity graph of our smart home models with multiple technologies utilized in our analysis.

Given the smart home abstract model proposed in Section 3.3, we define a graph $\mathbb{G}_{\text{conn}} = (V_c, E_c, C, \chi)$ as the connectivity graph, such that $v_i \in V_c$ is a node with a transceiver t_{ik} of a particular technology and $e_n \in E_c$ is a communication link between two adjacent nodes v_i and v_j. Furthermore, C is a set of colors equivalent to the number of employed technologies in the graph and $\chi : E_c \to C$ is a function to assign a color to each edge as defined in Section 3.3.

Since this formal definition represents networks with various technologies and topologies with any number of nodes, we use the term *instance* for an specific derivation of this definition. From analysis of these instances, we aim at results and conclusions applicable for all multi-technology smart home models.

Figure 4.3 illustrates an instance of the *home network* connectivity graph. In this graph a full-mesh network with 802.11s builds the backbone of the network containing nodes AP1, AP2, and AP3. Each mesh node equips with an access point to provide wireless connectivity through 802.11 infrastructure mode complying with the abstract model. Other technology networks can connect to the backbone through a supporting gateway. A *gateway* is a device that supports more than one protocol to establish interoperability among different type of network technologies [111]. The gateways connect to the backbone either with wireless or wired connections. Considering both wired and wireless connections enhances path redundancy through diversity of technologies leading to improve network resilience. In this case, the network can fail over to the second path if the first path fails. This mechanism is used in the current dual-interface laptops and PCs equipped with both 802.11 and 802.3 interfaces.

Figure 4.4 shows an instance of the connectivity graph for expanded home network. This graph obeys the same concept as the smart home abstract model in Section 3.3. In this instance, there is a backbone network connected with other technology networks

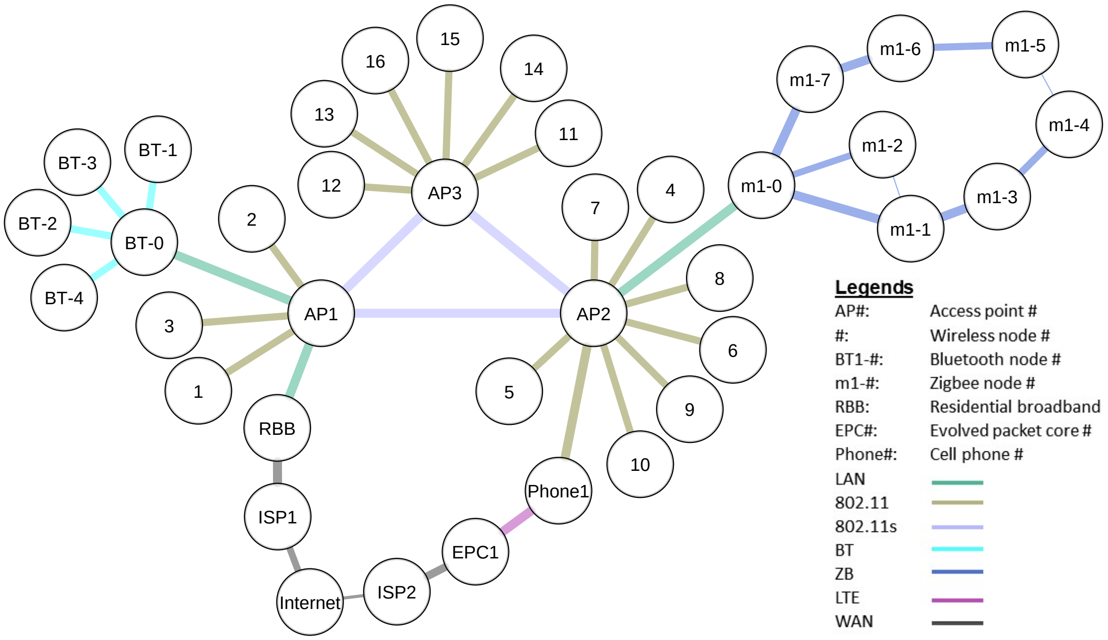


Figure 4.3: Connectivity graph of *home network* model

similar to home network. However, there are some differences compared with the model in Figure 4.3 that we explain in the following.

The backbone network is expanded to cover more area. Therefore, more nodes are used in the backbone network. The most important characteristic that stays the same in all similar instances is at the least bi-connectivity among nodes in the backbone networks. Though, heterogeneity of the utilized technologies improves the network resilience, the nodes in the backbone should be at least bi-connected to resist the network failure and partitioning against one failure. It is evident that more connectivity improves network resilience, but it also increases cost and complexity. With that condition in mind, there are many possibilities to construct the backbone network with various technologies and different number of nodes. For this specific instance, we consider a larger house or a similar building in a way that a triangle of three access points cover one area of the building; however, these two areas are far enough or blocked with obstacles from each other (such as two floors of a building) that the access points in each area are not in the range of each other. In this case, either more mesh nodes and access points should be used to cover the area, or we use wired networks between two areas. We choose the wired network in the presented instance. Utilizing mesh nodes or access points are more practical in other circumstances such as reducing the hassle and cost of wiring.

Another difference between two presented instance models is increasing the number of paths to the Internet. Assuming that a larger house has more residents, the probability of the presence cellphones increases. With this assumption, path redundancy increases leading to improving network resilience. More interesting option is that when the residents use different cellphone carriers in the same building. This condition increases both path redundancy and diversity with the outcome of improving network resilience. We consider the usage of one cell phone carrier in the expanded home network. Further research is required to explore the relationship between cellphone path diversity to the number of residents in a house and a larger building.

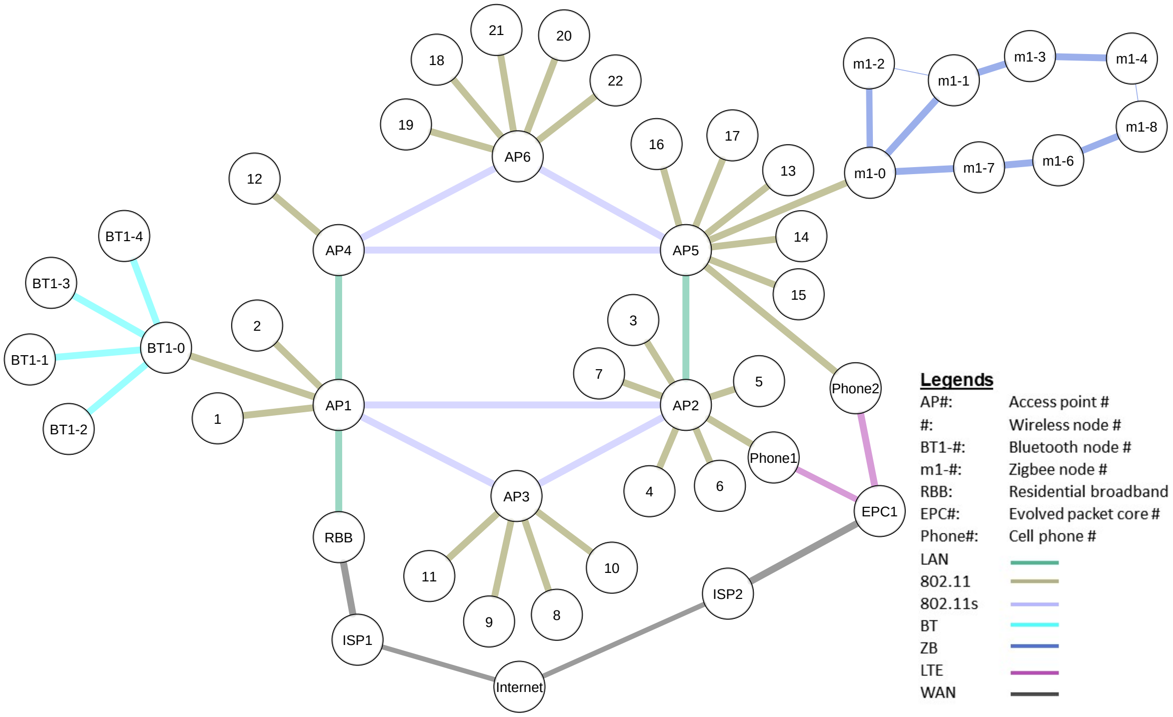


Figure 4.4: Connectivity graph of *expanded home network* model

Similar to the *home network*, we attach two various topologies to the network: star topology such as Bluetooth, and mesh topology such as ZigBee and Z-Wave, in order to explore the effect of diversity of topology on the network resilience. We refer to a particular network technology to show the possibility of the network implementation. In addition, a given network technology has a set of characteristics and constrains such as link bandwidth or the maximum number of hops in the network which differs one technology from the other. We consider such characteristics and limitations in the analysis when they impose a major difference.

Adding more technologies is possible depending on the type of required services as illustrated in Section 3.1. However, employing variety of technologies also increases complexity and cost of the network. It also increases the attack surface which makes the network more vulnerable to security attack. On the other hand, technology variance improves the network resilience. Therefore, a trade-off between resilience, cost, and complexity should be considered. As a result, Figures 4.3 and 4.4 illustrate a smart home connectivity graph taking into account both topology and technology variants. Colors in the graph assigned by function χ from set C represent technology variants while structure of each network technology shows the network topology.

Integrating technologies with different topologies changes the structure of the smart home networks. As discussed in Chapter 3 and shown in Figure 3.5, many of these network technologies are connected to the network backbone. In case of network technology with the star topology, a star network has a maximum length of 2. Therefore, adding a technology with a star topology may add the overall network diameter by 2. However, if a star technology gateway such as Bluetooth connects to an access point as shown in the home and extend home networks, the network diameter may only increase by 1. This is the result of integration of two network technologies such as 802.11 and Bluetooth to one node instead of connecting two separate networks. Figures 4.5, 4.6, and 4.7 illustrate

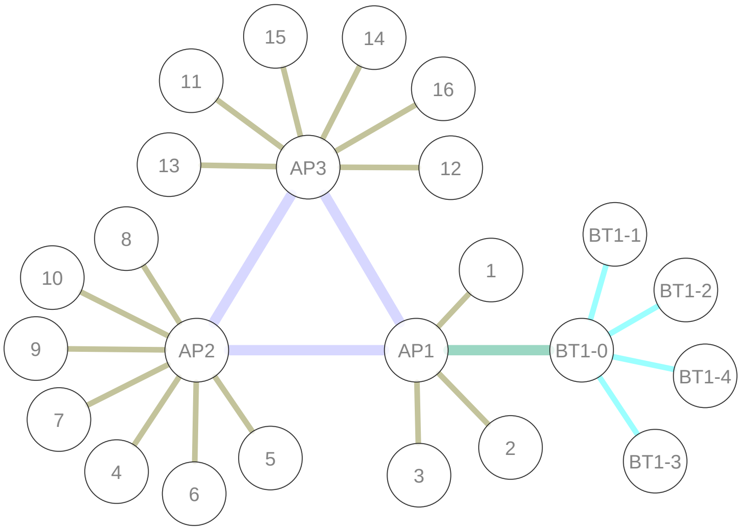


Figure 4.5: An star topology connected to a mesh, $\Delta = 4$, $R = 2$

several options of the integration of a star topology to the backbone. In the caption of figures, Δ represents the network diameter and R shows the network radius. Therefore, it is expected that in general, a star topology increases the diameter between 0 to at most 2 depending on how and where such networks are integrated to the backbone.

The analysis of the mesh topology related to associated technologies is not as simple as the star topology since such technologies can construct various type of networks from linear to a full mesh networks. However, the constraints of each technology may impose some limitation on the associated topology and makes the analysis simpler than a topology without any constraints.

802.11s is a flexible mesh technology to construct various range of topologies. The nodes in a network can build a topology from a linear to a full mesh graph, since this technology does not require any node with a special capability such as routing. All nodes are capable of performing any roles defined in the technology. The possible limitations are delay, packet size, network complexity and cost of nodes. A linear topology with a specific number of nodes has longer delay compared to the same number of nodes in a complete

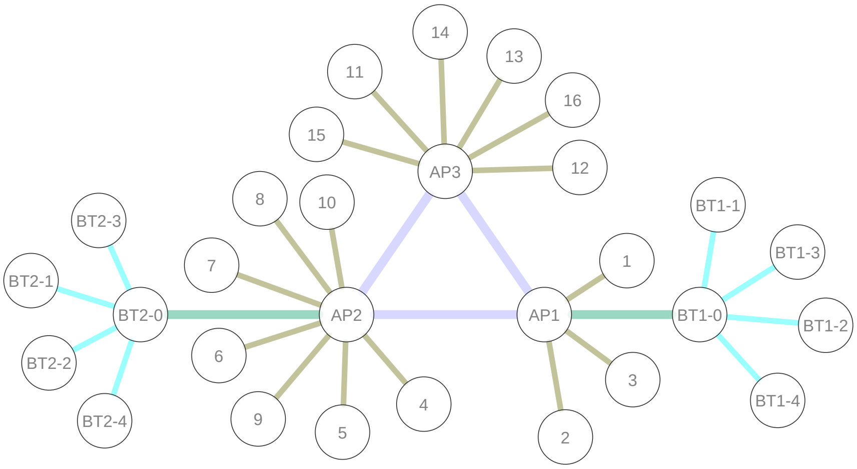


Figure 4.6: Two star topologies connected to a mesh, $\Delta = 5$, $R = 3$

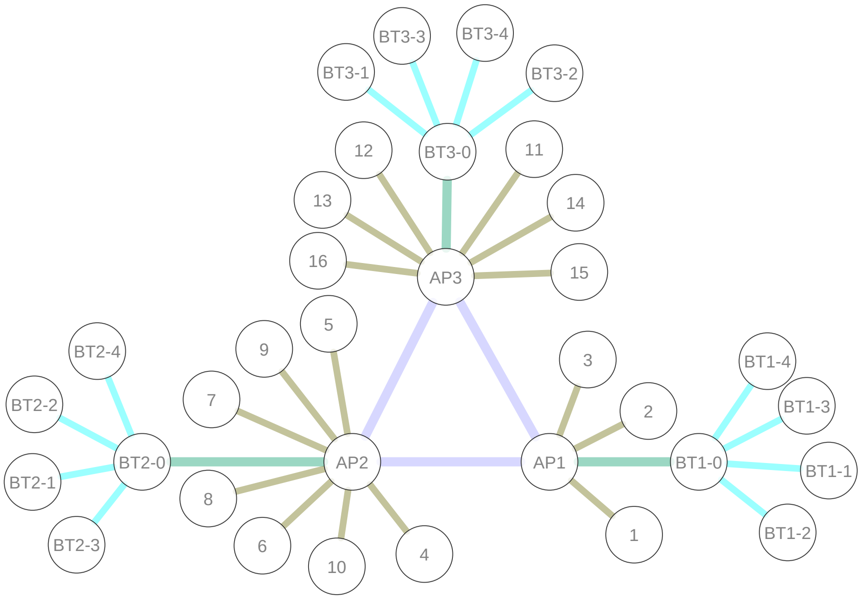


Figure 4.7: Three star topologies connected to a mesh, $\Delta = 5$, $R = 3$

graph built by a full mesh. While a linear topology can expand the range of a network, a complete graph increases network resilience in the face of link failure the outcome of expanded connectivity. Therefore, we consider at least bi-connectivity among the mesh nodes in the backbone, in order to improve resilience against one-link failure. If the network is small as illustrated in the *home network* in Figure 4.3, three nodes is the least number of nodes to provide bi-connectivity. In addition, these three nodes build a complete graph causing the shortest possible path and consequently delay.

If the backbone expands due to covering larger area, three nodes may not be enough to cover the area as *expanded home network* illustrated in Figure 4.4. If the 802.11s wireless nodes are out of the range of each other, constructing a complete graph without adding extra nodes is not possible leading to increase the length of the shortest path and consequently the diameter of the network. However, k-connectivity is less costly and complex and more achievable while it increases resilience. In such networks, the shortest path length among the backbone nodes is greater than 1 and it suffers a slightly more delay compared to a complete graph. Such delay in a small network such as a smart home is negligible.

The mesh topology of low-bit-rate technologies such as ZigBee and Z-Wave usually suffers from more limitations. For example, the longest path in the Z-Wave technology is 4 hops [47]. Therefore, even in a Z-Wave linear topology, the diameter of the network technology cannot exceed 4 hops. In addition, both Z-Wave and ZigBee require nodes with special capabilities such as routers with direct connection to a power supply to expand the network range. Therefore, we assume the maximum diameter of 4 for the mesh topologies to cover both ZigBee and Z-Wave. It is also worth mentioning that due to low bit-rate of such technologies each hop add significant delay to the data transfer.

As the next step, we consider our *home network* (Figure 4.3) and *expanded home network*

(Figure 4.4) graphs and compare with the two mentioned baseline topologies, star and mesh. Finally, we calculate the graph metrics for *backup home network* (Figure 4.8) and *backup expanded home network* (Figure 4.9) graphs resulting a failure on the Internet access link ($RBB \leftrightarrow ISP$) failing over to the backup access path through *Phone*. The number of 802.11 wireless workstations are the same in both baseline models and various instances of the home network models. However, the home network instances have extra nodes representing the network technologies connected to the home backbone.

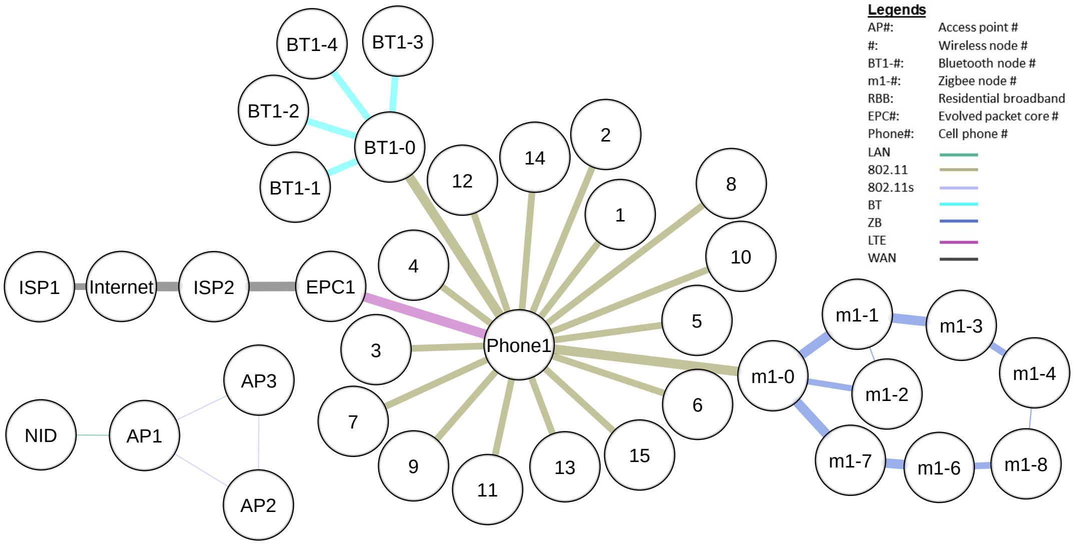


Figure 4.8: Connectivity graph of the backup home network topology

4.2 Graph Centrality Analysis

In this section, we analyze our home network, expanded home network, their backup models, and compare them with baseline models according to the results of centrality metrics explained in Section 2.5. We have two main goals in this section. One aim is to find the proper centrality metrics to explain multi-technology models adequately. Another goal is to find which model is more resilient compared to other models under the study.

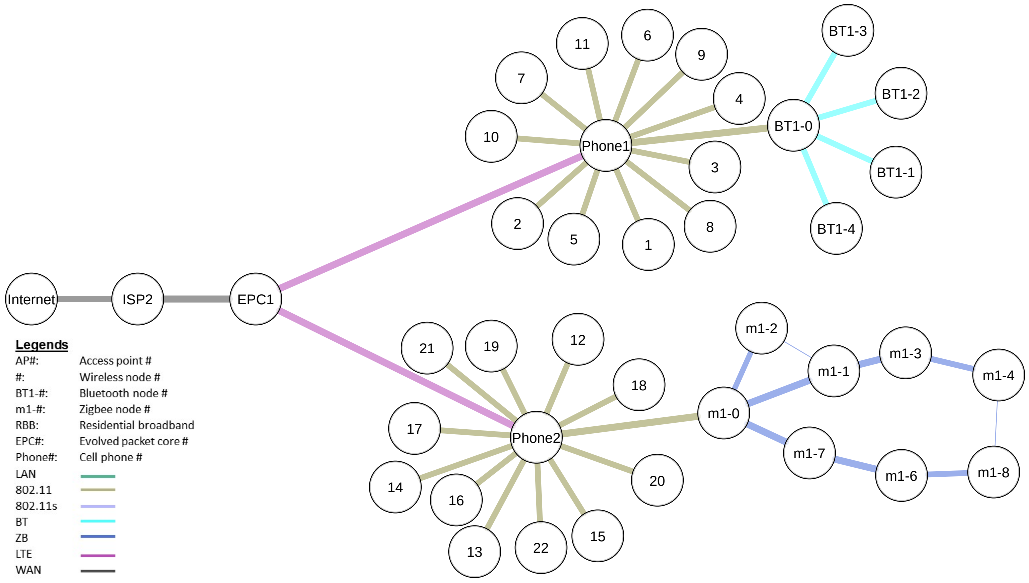


Figure 4.9: Connectivity graph of the backup expanded home network topology

In all of the presented figures in this section the thickness of edges represent the value of edge-betweenness centrality (number of traversing shortest paths) computed by Cytoscape [105] and each color represents a particular network technology.

Before starting the analysis, we distinguish metrics from measures. A measure is an indication to quantify an entity such as distance or dimension. While a metric is a measurement based on some standardized procedures and calculation methods. A graph measure is a calculation to identify a particular characteristic of a graph such as diameter or distance. However, a centrality metric follows a procedure to identify the importance of the network elements, edges and nodes. The level of a node's importance changes when calculation procedures change. Yet, the quantity of a particular metric value is not such an important factor in the graph-theoretic analysis as long as the order of values represents the significant of the elements. However, a good metric is the one that distinguishes each element adequately. Therefore, all metrics that provide measures with identifiable separation from each other are preferable. On the other hand, metric measurements are tied to the associated values, and the quantity of values show the differences such as measuring the diameter of a graph.

4.2.1 Distance-based Centrality Metrics

We start our analysis with the distance-based centrality metrics. First, we calculate distance-based measurements on the corresponding graphs of each model. These measurements can provide an overview of the network size. The results are provided in Table 4.1.

		Model					
Metrics		star	mesh	home	backup home	expanded home	backup expanded
Shortest path	mean	2.16	2.66	3.48	3.09	3.72	3.62
Diameter	value	4	5	8	8	8	8
Radius	value	2	3	4	4	4	4
Efficiency	mean	0.52	0.44	0.35	0.40	0.32	0.35

Table 4.1: Models distance-based measurements

The shortest path value in Table 4.1 shows the mean value in each model. As expected, the expanded home model has the largest value since it has extended backbone to cover larger area. However, one should note that though the shortest path length and all measurements based on the shortest path provide a structural view of the network. In multi-technology networks in which one hop in one technology does not have the same characteristic in another technology, the structural view of a network may not be matched with its corresponding functional view. This is also true when distance or bit rates are assigned to an edge even within a network with one particular technology. For example, if we look for the shortest delay in the network, the shortest path may not represent the shortest delay since the delay values on each hop may significantly different from another hop, especially in multi-technology networks. Therefore, in multi-technology networks considering weighted edges may provide a better result. However, any particular weighted attribute assigned to edges is interpreted as distance in distance-based centrality metrics.

The network *diameter* represents the longest shortest path in the network showing the minimum number of hops to connect the farthest node pair in a particular network. Regarding the graphs under study, one of the farthest node in all models is the *Internet* considering the number of hops and also distance. Therefore, diameter shows the shortest path from the farthest node to the *Internet* node. In home instances, the farthest node to the *Internet* is among one of the nodes in the technology networks placed at the edge of the graph. In the star model, all nodes around the access point have the same length. While in the mesh model, those nodes whose access points are not connected to the RBB directly are on the farthest path.

As mentioned above, since the network diameter is measured based on the shortest path length, it only provides an structural overview of the network and the value may not be applicable for any metric measurement such as delay unless edges are tagged with proper weights.

During the failure of the Internet access link and consequently in the corresponding backup models, the backbone component is partitioned and practically useless; therefore, the shortest path value of the connected component usually decreases, causing changes in the value of metrics depending on the shortest path measurement. However, the shortened diameter in this case, can not offer a shorter delay significantly; because, one high-speed component of the network has failed, and all network technologies with low-speed connectivity are intact. Therefore, diameter alone is not an adequate measurement in a multi-technology network. Moreover, a more accurate insight is gained when edges are weighted.

The *efficiency* value of each graph represents the similarity of the graph to a full-mesh graph interpreting as easy communication regarding the number of hops. However, the result may not be very accurate in a multi-technology graph in which nodes and links have different capabilities. For instance, two nodes in two different HAN in Z-Wave technology cannot communicate to each other; however, the structural view of the graph shows such connections and they are considered in the measurements such as efficiency. In other words, when functional roles are involved in a graph representation in which nodes and edges are different, many structural metrics fail to provide an adequate indication of network resilience. A mechanism such as a multilayer graph can highlight different types of edges and nodes in each technology. Then a proper or modified metric can be defined. The proposed multilayer framework in Chapter 5 will provide such representation.

Eccentricity represented in Table 4.2 increases from star to our home network graph due to adding network technologies and consequently the increment of the average shortest paths. Most centrality metrics assign higher value to more important nodes/edges. Eccentricity is one of the exceptions. In order to harmonize eccentricity values with other metrics, $1/eccentrcity$ may be used. If $1/eccentrcity$ values are considered the trend of eccentricity in the models decreases. Edge nodes in the network technologies have the highest eccentricity values in the network as well as the *Internet*, *ISP1*, and *ISP2* nodes which are the farthest nodes to the edge nodes of the network technologies. Since eccentricity measures the longest shortest path for *each node*, it provides better understanding about the network expansion, number of hops and consequently the average delay in the network; generally, the number of hops and consequently the associated delay in a small-size network with high speed network technologies is not significantly important. However, when low speed protocols are involved, each hop adds a considerable value to delay. The eccentricity values for all nodes in each instance and other metrics under this study are provided in Appendix A.

Closeness centrality calculates the average shortest path for any node v_i to other nodes in a network. Therefore a center node of a particular graph has the maximum closeness, or that node is the closest node compared to other nodes.

	Model					
Eccentricity	star	mesh	home	backup home	expanded home	backup expanded
Min.	2	3	3.48	3.09	4	4
Mean	3.80	4.5	8	8	6.30	6.30
Max.	4	5	4	4	8	8

Table 4.2: Eccentricity values of the models

The center node of the star topology has the maximum closeness centrality value. When a network is expanded, the node closeness centrality values decrease due to longer paths as observed in the home network and expanded home network graphs. In the backup home topology *Phone1* and in the backup expanded home topology *Phone2* have the highest closeness values. In addition, the overall closeness values for all nodes increase. This is due to the fact that the network gets shorter because of losing the backbone nodes. The same trend is observed in the expanded and backup expanded networks. A node with high closeness value and high degree centrality has an exceptional position in the network to disseminate information. However, such nodes in communication networks are vulnerable in targeted attacks. Therefore, distributing closeness among all nodes is a desired property in communication networks, which makes the home and expanded home network graphs more resilient than other topologies. In addition, closeness measurement is calculated when the edges have weighted value. In such circumstances, a multi-hop high speed path may have higher closeness centrality than a one-hop low-speed path.

	Model					
Closeness	star	mesh	home	backup home	expanded home	backup expanded
Min.	0.27	0.23	0.19	0.19	0.18	0.18
Mean	0.48	0.39	0.30	0.34	0.28	0.28
Max.	0.86	0.58	0.48	0.58	0.42	0.42

Table 4.3: Closeness values of the models

Radiality is another node centrality metrics. It represents the average tendency of a node to other nodes proximity or isolation. A low radiality value shows that the node is peripheral [105]. The radiality should be considered with closeness and eccentricity. A node with the highest value of radiality, closeness, and eccentricity indicates that it is in a central position in the graph [91]. Considering the highest value for radiality, closeness, and eccentricity, the center point of the star topology has the highest value of all three metrics. However, this is not straightforward in the mesh topology; because neither of the mesh nodes have the highest value of the three metrics all together. In the home network graph in Figure 4.3, the node *AP2* has the maximum value of all triple metrics radiality, closeness, and eccentricity placing it at the center of graph. The same condition applies for the node *Phone1* in the backup home graph in Figure 4.8. In the expanded home graph in Figure 4.4 *AP4* locates at the center of the network while this is true for *Phone2* in the backup expanded home model in Figure 4.9. Radiality, eccentricity, and closeness centrality values together identify the center point of a network in which most traffic passes through and it requires extra attention regarding the node resources, security, and possible redundancy to reduce the probability of the node failure and improves the network resilience regarding targeted attack. However, similar to other distance-based centrality metrics, the correct values are captured when an adequate weight assigned to edges.

Stress represents the number of shortest path through a node v_i. It can be interpreted as the amount of *work* that node v_i performs in communication. This metric can show the amount of resources that should be assigned to a node. Table 4.4 shows the summarized results.

	Model					
Stress	star	mesh	home	backup home	expanded home	backup expanded
Min.	0.00	0.00	0.00	0.00	0.00	0.00
Mean	22.00	34.91	98.26	67.03	163.79	102.40
Max.	236.00	238.00	946.00	904.00	1534.00	1046.00

Table 4.4: Stress values of the models

Edge betweenness centrality is an edge centrality metric measuring the fraction of the number of the shortest path between every pair of nodes v_i and v_j that passes over a particular edge e_k.

In all of the home network graphs, edges that connect a gateway to an access point have a high edge betweenness centrality values. Generally speaking, all edges connecting part of a network with a different technology to another have a high edge betweenness centrality value constructing a bridge between two parts of the network. Disruption of such edges partitions a network technology from the rest of the network. Therefore, such links should be considered as critical links; although, they do not have the maximum edge betweenness centrality in the network. The same condition is observed between *Phone1* and *EPC1* in the backup topology in which the home network is connected to the LTE network during the failure. The thickness of the edges in all figures in this chapter illustrates edge betweenness. Adding diverse paths in the proper place, either through the same or different technology, decreases edge betweenness centrality on bridges improving the network resilience through increasing technology heterogeneity. For instance, given a particular gateway, two wired and wireless interfaces to the same network technology decrease the edge betweenness value of the connected edges to the gateway. The limitation is observed during failure since the only high speed and long range available technology is LTE. Locating in a smart city with wireless access connectivity, it may provide another path to the Internet with a restriction; because all nodes should connect to the citywide wireless network as a station.

Although edge betweenness centrality can identify edges that connects parts of a network, it cannot recognize critical edges connecting important edge-nodes. All edges connecting edge-nodes to other nodes receive a low value with this metric while such nodes including sensors may gather critical data. One possible solution to alleviate the criticality of a node is installing redundant nodes at the same area by increasing system cost. Another solution is using a node with two different technologies to participate in two network technologies.

	Model					
Edge Betweenness	star	mesh	home	backup home	expanded home	backup expanded
Min.	38.00	42.00	8.00	8.00	8.00	8.00
Mean	43.16	55.91	126.73	126.73	195.37	138.0
Max.	102.00	114.00	496.00	496.00	828.00	800.0

Table 4.5: Edge betweenness values of the models

Node betweenness centrality, as a node centrality metric, measures the fraction of the number of shortest paths between every two nodes v_i and v_j that lies on a particular node v_k. This value identifies the importance of a particular node in communication among other nodes. This metric assumes that all the edges in the network have the same bandwidth and all traffic goes through the shortest paths. Therefore, it does not provide an accurate result in a multi-technology network when each group of links has different bandwidths. For instance, *AP1* connected to *RBB* handles both the Internet traffic and part of the local traffic while it has a lower value than *AP2* with more edges. Although assigned weights on edges can increase the accuracy of the measurement, weight normalization should also be considered in a multi-technology network. A saturated link in a low-bit rate technology has the same degree of importance for that particular technology as the corresponding link in a high-bit rate technology.

	Model					
Node Betweenness	star	mesh	home	backup home	expanded home	backup expanded
Min.	0.00	0.00	0.00	0.00	0.00	0.00
Mean	0.07	0.08	0.07	0.07	0.06	0.07
Max.	0.98	0.55	0.68	0.91	0.56	0.71

Table 4.6: Node betweenness values of the models

4.2.2 Degree-based Centrality Metrics

We analyze *degree centrality*, *neighborhood connectivity*, *k-edge connected*, and *k-core* metrics from this group. In this centrality category the number of neighbors is the main criteria to order important nodes.

Degree centrality is the simplest metric in this group that counts the number of neighbors of each node. Degree centrality in the communication networks is the measure of the node importance with respect to how well-connected a node is. A higher degree for a particular node suggests that more nodes rely on it for their communication. A node with high degree centrality in a communication network is a potential vulnerability in targeted attacks.

The center point of a star topology has the maximum possible value for the degree centrality ($n-1$ where n is the number of vertics), which makes it the most vulnerable node to any attack or failure. In a mesh topology, the WLAN backbone is divided among mesh nodes, decreasing degree centrality values and, consequently, distributing the effect of any failure or attack. We observe the same effect in the home and expanded home backbone network graphs, since these instances have a similar architecture. Although a node failure with high degree centrality in the home backbone LAN can disrupt communication, failure of a gateway, even with lower degree centrality, in a star or mesh network technology can disconnect the whole associated network technology, that may support critical edge nodes. Therefore, focusing on the degree centrality value alone can not identify the crucial components of a multi-technology network. This is the result of various connectivity in a multi-technology networks such as a smart home. Degree-based centrality metrics assume that similar edges connect nodes, while this assumption is not valid in a multi-technology network. Though a node with high degree value in a network with similar connectivity represents the importance of that particular node, this assumption is not valid in a multi-technology network. A node with two different type of connectivity may be more important compared to a node with multiple similar connectivity. The proposed multilayer framework introduced in Section 5.2 highlights such connectivities. Therefore, metrics considering various connectivity should be proposed to measure accurate centrality value. We propose four degree-based centrality metrics in Section 5.3.1.

	Model					
Degree	star	mesh	home	backup home	expanded home	backup expanded
Min.	1.00	1.00	1.00	1.00	1.00	1.00
Mean	1.90	2.00	2.16	2.06	2.25	2.05
Max.	17.00	8.00	11.00	18.00	10.00	13.00

Table 4.7: Degree values of the models

Neighborhood connectivity is another degree-based centrality that measures the average number of neighbors of all v_i's neighbors [94, 95]. Although this metric can not consider a node criticality value and does not provide a direct connectivity measurement, it can be utilized as a proper indication for the connectivity of the edge nodes. Since the edge nodes in a low-bit rate and low-energy consumption technologies usually connect to other nodes with a single link, neighborhood connectivity can identify well-connectivity of a particular edge node if the first hop is intact.

	Model					
Neighborhood	star	mesh	home	backup home	expanded home	backup expanded
Min.	1.06	1.50	2.00	1.44	2.00	1.38
Mean	14.30	6.38	5.76	10.16	5.51	8.71
Max.	17.00	8.00	11.00	18.00	10.00	13.00

Table 4.8: Neighborhood connectivity values of the models

A *k-core* of a given graph G is a maximal subgraph of G in which all nodes have degree greater or equal to k. The *core number* of node v_i is the largest k value of a k-core containing that node [112]. The k-number of all nodes for each model are provided in Appendix A.

Neither star nor backup models has 2-core subgraph. In other words, a node failure or attack partitions their network. The 2-core subgraph of the mesh network is shown in Figure 4.10. It is observed that the backbone of the network is *bi*-connected.

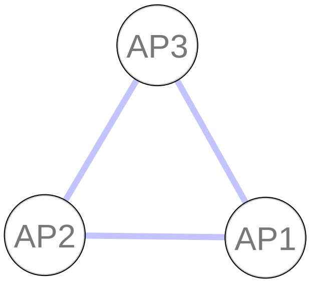


Figure 4.10: Mesh 2-core subgraph

The 2-core subgraph of the home model is illustrated in Figure 4.11. In addition to the backbone of the network, the mesh network is also bi-connected. In other words, according to the *k-node connected* definition in Section 2.5.2, the mesh network should be operational after one node failure or attack. However, if the failed node is the network technology gateway or router, the network would be disabled. As it is evident, k-core or k-connected subgraphs cannot capture such incidents. This is due to the fact that many graph-theoretic methods cannot recognize the functionality of nodes. However, those metrics that can accept weights alleviate this deficiency.

The same problem is observed in Figure 4.12 presenting 2-core subgraph of the expanded home model. Therefore, neither of presented models are fully *bi*-connected graphs. The home and expanded home models have 2-*component* (the subgraph counterpart of k-connected definition) subgraphs in their network backbone and network technologies that can establish mesh networks.

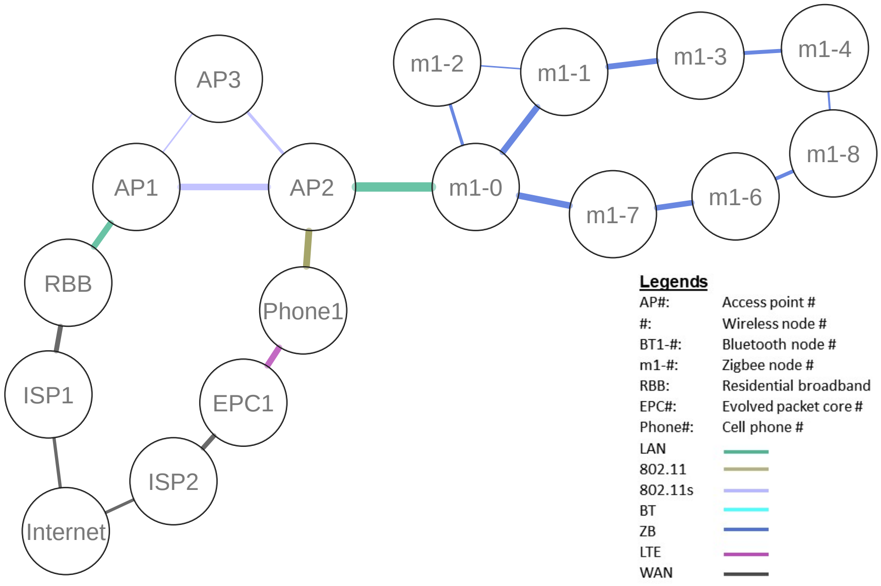


Figure 4.11: Smart home 2-core subgraph

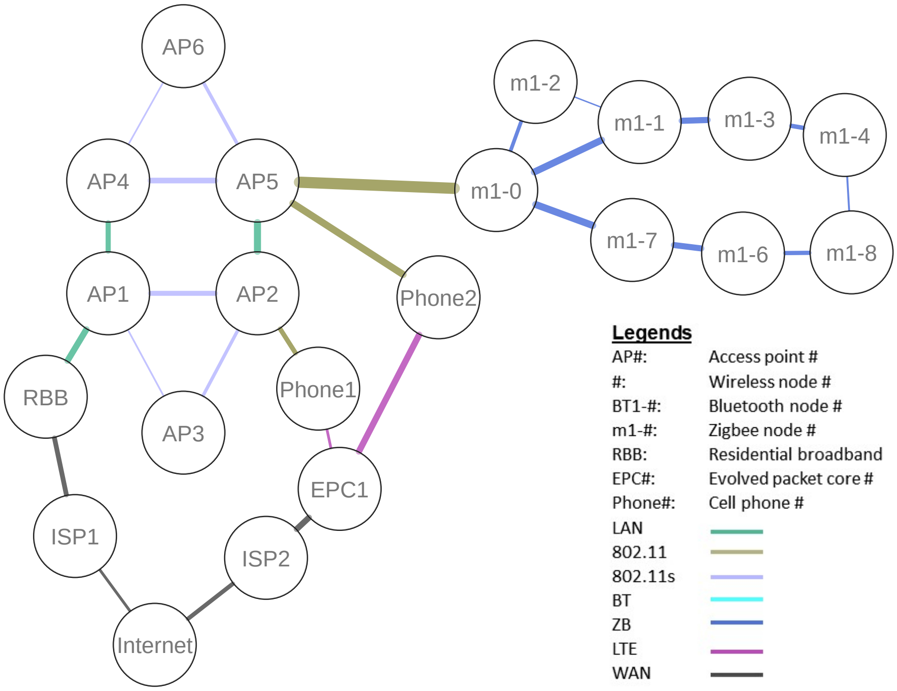


Figure 4.12: Expanded home 2-core subgraph

4.2.3 Spectra Centrality Metrics

We examine *algebraic connectivity*, *Eigenvector centrality*, and *Katz centrality* from this group. The *algebraic connectivity* of a graph G represents how well-connected a graph G is. Algebraic connectivity is the second-smallest eigenvalue (λ_2) of the Laplacian matrix of G. If G is a connected graph, algebraic connectivity value would be greater than 0. In general, a higher value represents a graph with shorter diameter and higher connectivity. In addition, algebraic connectivity values usually increases by adding more edges to the graph [113].

Table 4.9 shows the algebraic connectivity values for the models. It is observed that λ_2 has a decreasing trend from the star to backup expanded smart home model. While the number of nodes in expanded smart home model is more than other models, most nodes join to a star topology resulting to reduce in algebraic connectivity values. Moreover, when a network technology is added to the home backbone, at best condition when the topology is mesh, the new nodes can communicate directly to each other causing a graph with a shorter diameter; however, all nodes in any network technology should communicate with the rest of the network through their gateway limiting the degree of the overall connectivity in the network. This is one reason that makes the home network susceptible to one node/link failure.

	Model					
Algebraic Connectivity	star	mesh	home	backup home	expanded home	backup expanded
Value, λ_2	0.22	0.18	0.08	0.10	0.08	0.04

Table 4.9: Algebraic connectivity values of the models

Eigenvector centrality is an extension of degree centrality that considers the importance of a node as its number of connections to the other important nodes [98]. In other words, a node with high eigenvector value is connected to other highly connected nodes.

In the star topology the central node has the maximum eigenvector centrality value following by *RBB*. In the mesh topology, *AP2* has the highest value which has the highest degree in the network; however, *AP2* is not as critical as *RBB* that connects *AP1* to the Internet. This condition is the same in our home network graph. Similarly, *phone1* has the maximum centrality value in the backup topology. Although, this metric can identify an important node based on its number of connections in a homogeneous network, it cannot recognize such nodes in a mutil-technology network especially with battery-operated nodes that they have limited capability to establish multiple connections. Table 4.10 shows the eignvector centrality results for the models.

	Model					
Eigenvector	star	mesh	home	backup home	expanded home	backup expanded
Min.	0.01	0.01	0.01	0.00	0.00	0.01
Mean	0.18	0.17	0.12	0.13	0.10	0.12
Max.	0.71	0.49	0.56	0.69	0.46	0.49

Table 4.10: Eigenvector centrality values of the models

Katz centrality is an extension of eigenvector centrality. However, the effect of neighbors of neighbors over the Katz centrality of v_i decreases when the distance from v_i increases. Katz centrality considers length of a walk between two vertices v_i and a neighbor v_j, and the effect of v_j over v_i [96, 98]. Moreover, Katz centrality can consider nodes with various importance in the measurement. Assigning a weight to each node can provide a result considering the importance of nodes. Therefore, we assign a high weight value (weight= 3) to all access points and gateways in the models under study. A medium weight value, 2, is assigned to the important nodes and sensors such as smoke detectors and routers in a particular network technology. We assign the lowest value ,1, to other nodes. In contrast to other metrics, Katz centrality assigns proper centrality values to the edge nodes, if they are important. Table 4.11 shows the Katz centrality values for the models. The detail centrality results for each model and their corresponding nodes are provided in Appendix A.

	Model					
Katz	star	mesh	home	backup home	expanded home	backup expanded
Min.	0.11	0.10	0.09	0.08	0.13	0.13
Mean	0.20	0.18	0.14	0.15	0.16	0.15
Max.	0.59	0.44	0.26	0.50	0.31	0.31

Table 4.11: Katz centrality values of the models

4.3 Discussion

We conclude the result of our analysis in the previous section as a separate discussion here. The measurement of the various type of centrality metrics shows that the conventional centrality metrics cannot provide adequate results in many cases. *Distance-based centrality metrics* fail to identify important nodes and edges at the edge of the network such as sensors with critical functionality.

Degree-based centrality metrics simply consider the number of neighbors connected to a node. They cannot identify the type of connections. One important case is that when a node with degree 2 such as *RBB* or *Phone1* in the home network provides the only connectivity between two various network technologies. This node is more important compared with a similar node with the same degree connectivity providing connections between nodes in a one particular network.

Spectra-based centrality metrics are an extension of degree-based centrality with a wider view considering nodes multiple hops away in the calculation. Therefore, these metrics provide more accurate results than degree-based metrics in some cases. In addition, assigning weights in Katz helps the accuracy of the measurement.

Regarding the resilience of the models, since the home network is an extension of the mesh network in the backbone, we observe similar characteristics of the mesh network in the home network backbone. However, a new point of failure comes to the picture by integrating other network technologies. Such network technologies generally connect to the backbone by a single connection generating a bridge in the network and a new node, the gateway, as another point of failure. Though network technologies supporting mesh topology have improved resilience in their networks, this feature does not help the connectivity to the backbone and consequently the Internet. This is the result of many factors in design of such technologies. Since most of these technologies have been designed for low-energy-consumption nodes, they have simple addressing and routing protocols to reduce the size of each packet and consequently transmission energy. These routing protocols cannot support multiple access to another network. In addition, extra processing needs more resources imposing nodes with additional capabilities to the structure of such networks. Therefore, there is a trade-off between simple design to reduce energy consumption and functionality. As a suggested solution, an external node to the network with more processing power may contribute to the coordination of routing among multiple simple routers in such technologies. We consider this solution as part of the future work. If this problem is resolved, then the effect of bridging is alleviated resulting an improved connectivity between the network technologies and the backbone and consequently the network resilience.

Surprisingly, both the smart home and expanded smart home networks are internally (where network technologies are connected to the backbone) 1-connected networks, in spite of implementing a *bi*-connected backbone in these networks. Consequently, a single failure or attack to the network can partition it. The failure may not degrade the operation of the network technologies, but it affects the connectivity resulting disconnection from the backbone.

The *backup home* and *backup expanded home* networks are the results of one particular failure, the main Internet connection. These models show that heterogeneity of the technologies is helpful to improve network resilience regarding some specific failures; but currently these technology variations are not totally helpful for the internal network failure as mentioned above. In addition, the result of centrality analysis in this chapter shows that these two models are more vulnerable to any link/node failure in their current conditions. The topologies of these networks are very similar to star with the same vulnerability.

The above discussion shows that other methods, such as fog nodes, should also be consider to provide improved network resilience.

4.4 Summary

In this chapter, we analyze six specific network instances with various centrality metrics. We consider two instances from the abstract smart home model introduced in Chapter 3 and the same instances during the Internet connection failure. These four instances are compared with two conventional home models, star and mesh. We consider centrality metrics into three groups, distance-based, degree-based and spectra centrality. One difference between smart home instances and conventional models is that smart home instances usually utilize several technologies. This variance has an influence on the attributes of edges and functionality of the nodes since such network technologies are usually integrated as the edge networks. Connections using various network technologies have diverse characteristics such as distance or bandwidth. Such variations cannot be detected by conventional distance-based centrality metrics unless appropriate weights are assigned to edges manually. In other cases, even assigning weights may not be enough to obtain a correct centrality value, especially in case of edge nodes with critical functionality.

Conventional degree-based centrality metrics cannot detect the importance of a particular edge or neighbor using different technologies, since all nodes and edges are considered similar. However, in a multi-technology network this assumption is not valid.

The same problem is observed in spectra centrality metrics an extension of degree-based centrality metrics. However, these metrics consider the importance of each neighbors and neighbors of neighbors. Therefore, the centrality results identify important nodes more accurate compared with degree-based centrality metrics. In the Katz centrality metric assigning weights to nodes corresponding to their importance can cover some of these flaws in degree-based centrality.

The analysis of the instances of home models shows that although many network technologies with different topologies are utilized in such networks, these instances are k-connected networks where $k = 1$. A targeted attack or failure can partition the networks most of the time. However, heterogeneity of network technologies improves the network resilience for some particular attacks such as failure in the main Internet connection, if a proper technology, i.e., LTE, is available at the time of failure.

The analysis in this chapter also shows the weakness of the single-layer networks to represent networks utilizing multiple technologies. Though, using edge-colored graph as introduced in Section 3.3 can differentiate links with various technologies, the importance of edges connecting different network technologies are not highlighted adequately. In Section 4.2, we show that traditional centrality metrics such as closeness fail to distinguish such edges even in edge-colored graph. In the next chapter, a multilayer framework will be introduced to deal with the presence of multi-technology networks.

Page left intentionally blank.

Chapter 5

Multilayer Framework and Analysis

Graph-theoretic representations are utilized as a tool to reveal important information about characterstics of a system and its underlying network structure. Such representations show the relationship between the network functions and its structure [114]. However, simple graph representations fall short to express important attributes of complex systems in which many technologies interplay with each other. In contrast, multilayer networks offer a vivid illustration, among other benefits, to highlight *dependency edges*, edges connect two or more single-layer graphs. A multilayer network does not imply that it should be utilized only for large networks and interactions among entities. A multilayer network can represent a small system with complicated interconnections such as in smart homes. In addition, a multilayer network is suitable to represent interactions among various levels of a complex system.

As explained in previous chapters, a smart home network is a set of various independent smaller networks with different network technologies connected to each other to provide the overall smart home functionality. We also explained in Chapter 4 that a simple graph representation and related graph centrality metrics cannot provide an adequate explanation of the resilience properties of the underlying smart home graph. Therefore, a multilayer framework is proposed here to show interdependency among the networks and technologies in a smart home system. In addition, such representations have ability to show the connectivity among various components of the communication network in a larger scale. Moreover, multilayer networks can also represent temporal networks such as connectivity of the battery and power-operated devices before and after power failure.

We divide this chapter to the following sections. In Section 5.1 we represent a case of a smart home model integrated to the Internet with a multilayer model. In Section 5.2, we propose a multilayer framework to formalize the representation of the smart home models and other multi-technology networks such as smart cities. In Section 5.3 we analyze the inderdependency of the smart home model represented by our multilayer framework [115].

5.1 Smart Home Multilayer Multidimensional Model

Before we formally introduce our multilayer framework in Section 5.2, we explain how our smart home multilayer model can be described with our formal framework. We consider the following terminology to provide a clear distinction between various type of networks.

- *Monoplex network*: A single-layer network.
- *Multidimensional network*: A network with multidimension in which a *dimension* refers to various interactions between two entities. Dimensions may refer to different type of interactions or the same interaction with different values. A multidimensional network can be represented by the triple *multigraph* $G = (V, E, L)$ where L is a set of labels to indicate various interactions [116].
- *Complex network*: A network with non-trivial and irregular topology in which the newtork is neither purely random nor regular [114, 117, 118].

- *Multilayer network*: A set of networks that interact with each other represented by the triple $\mathcal{M} = (Y, \overrightarrow{G}, \mathcal{G})$ where Y is the set of layers, $\overrightarrow{G}$ is the set of networks in layers, and $\mathcal{G}$ indicates a set of graphs between layers [114].

- *Multiplex network*: A multilayer network with *inter-layer* edges only between representations of the same node in different layer (diagonal coupling) [119]. A multiplex network is represented by triple $G = (V, \mathbb{E}, C)$ where V is a set of nodes in the network, $\mathbb{E}$ is set of various types of edges in α layers, and C is a set of edges indicated by (v, v, l, k) between two representations of node v in layers l, k [120].

- *Interconnected network*: A multilayer network with *inter-layer* edges between any two nodes [121].

- *Interdependent networks*: Two or more networks connected via edges called *dependency edges* [119, 122]. In a bidirectional dependency, two nodes v_i and v_j are connected by an dependency edge and they are dependent to each other. Failure of one of such nodes causes failure of the other.

- *Multilevel network*: A multilayer network with a particular order of layers [123]

- *Multilayer multidimensional network*: A complex multilayer network with multiple dimensions as different kind of relationship among layers [124].

In order to understand the complexity of smart home models and their relationship with communication networks and the Internet, the smart home multilayer model is illustrated in Figure 5.1. In this model, the horizontal axis (x-axis) represents the network depth including core, access, and edge networks. The vertical axis (y-axis) shows the network levels while z-axis illustrates the technology variants. The legend in Figure 5.1 illustrates representation of each axis.

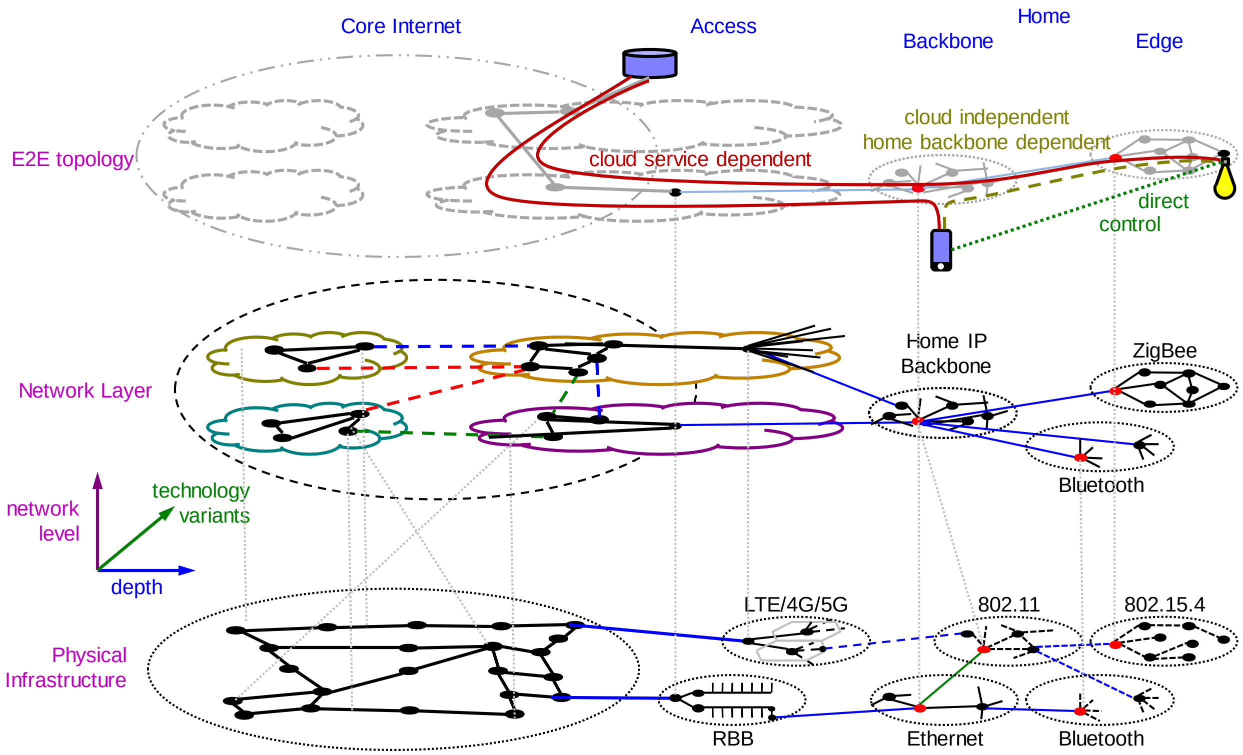


Figure 5.1: Smart home multilayer model

Consider the network representation offered in Figure 5.1. Here, the Internet is treated as a complex network with various functional *network levels* supervening on the lower levels [125]. The figure shows the *physical infrastructure* containing physical network connectivity, a logical *network layer* to provide logical path from a source to a destination, autonomous systems (AS) level organizing routing elements under control of autonomous entities, and *end-to-end (E2E) topology* level that represents an end-to-end connection between a source and a destination. Notice that, in this representation, the number of nodes and edges decreases from lower layers to higher layers. More precisely, in this representation the nodes in a particular layer are a subset of those in its lower layer.

Furthermore, in this representation the Internet is divided into *core*, *access*, and *edge networks*. The Internet core contains all tier 1 ISPs in different functional levels to establish internet connectivity. Tier 3 ISPs usually provide internet connectivity to end users through access networks such as hybrid fiber/cable (HFC) and DSL. The *depth* of the network should be understood as the distance from the Internet core to the edge of the network. The physical infrastructure of the access networks along with the routing levels is connected to the corresponding levels of the Internet core.

Currently, one rapidly growing part of the Internet is the edge networks composed of the end-user networks such as home, city, enterprise and industrial networks connected to the access networks. Regarding the addressing and forwarding methods, the routing level of the edge networks is likely not connect to the Internet core directly. Network address translation (NAT) and non-IP routing protocol such as ZigBee are two examples requiring a gateway to connected the network layer of an edge network to the corresponding access layer indirectly.

We observe especially high levels of diversity of the network technologies at the edge networks due to the highly diverse requirements of different services. While the main type of service in the Internet core is relatively error-free, high-bandwidth connectivity with low delay, required service types at the edge networks vary from very-low to high-bit-rate connectivity with different level of energy consumption. Variability with respect to range of service also affects the routing level to provide the routing services with a lower energy consumption and a shorter packet size.

We can identify three main planes in our model: *network level-depth*, *network level-technology variants*, and *depth-technology variants* planes. Since these planes illustrate a perpendicular cross cut of the network and they do not represent any numerical values, we call them *slices*. Each slice identifies with two features such as network level and depth in our model. We call each of these features an *aspect* of the model. Note that, each slice shows a cross cut of the network for a particular aspect value. Therefore, we may define parallel slices to each plane defined by two axis (aspects) for different values. The network level-depth slice represents all network levels for each part of the network containing the Internet core, access, and edge networks. The network level-technology variants slice illustrates what technology variants and protocols can be utilized in each network level. Finally, the depth-technology variants slice shows the technology variants used in each part of the network.

5.2 A Multilayer Formal Framework for Multi-technolgy Networks

We propose a flexible abstract framework that can explain various aspects of a network topology as large as the Internet core along with the edge networks such as smart home illustrated in Figure 5.1. In order to capture different network aspects, we define a multilayer framework $\mathfrak{G} = (\mathcal{G}, V_N, E_N, V, S, N, A)$. Each aspect represent one particular feature of the network such as functionality, geographic distribution, and technology variants with a set of values for each aspect illustrated in Figure 5.1. In other words, each aspect is equivalent to one feature which can be represented as one dimension of a multilayer network. Increasing the number of aspects is possible but we use three relevant aspects in our discussion for simple graphical presentation.

Figure 5.2 shows the abstract form of the graph $\mathfrak{G}$ with three aspects X, Y, and Z. Each plane in Figure 5.2 represents one *slice*. In other words, one slice is a plane containing all values for two particular aspects. The intersection of d slices, where d is the number of aspects, represents a *net*. Each net shows part of the overall graph with some specific value for each aspect. For example, in Figure 5.1, a net can represent the physical infrastructure of a home backbone implemented with 802.3 technology while a slice can show the whole physical infrastructure of the network with all technologies in the network depth. As another example, a net can be the physical infrastructure of the LTE technology employed in the access layer while the corresponding vertical slice containing the LTE physical infrastructure represents the network level aspect of various technologies in the access layer.

We can modify the level of network abstraction by changing the number of values of a particular aspect. For example, we can combine the home backbone and home edge in Figure 5.1 to one aspect value as *home* to consider all employed technologies in a smart home together. Note that, we use axes in Figure 5.2 for better presentation; however, the axes do not have any numeric value since the aspects have nominal values. Moreover, we can show network aspects more intuitive on these axes.

We summarize our model terminology as follow:

- network *aspects* are a set of features represented by a multilayer network.
- *values of an aspect* are a set of values represented by each aspect.
- *rules of an aspect* are a set of rules on values of each aspect such as order of values.
- one *slice* is a part of d dimensional network represented by a graph with a set of nodes and corresponding edges with $d-1$ aspects in common.
- a *net* is the intersection of d slices in a d dimensional network. A net represents a graph with a set of nodes and corresponding edges with specific values for all of the aspects in the network

We define our multilayer framework as $\mathfrak{G} = (\mathcal{G}, V_N, E_N, V, S, N, A)$ with the following conditions:

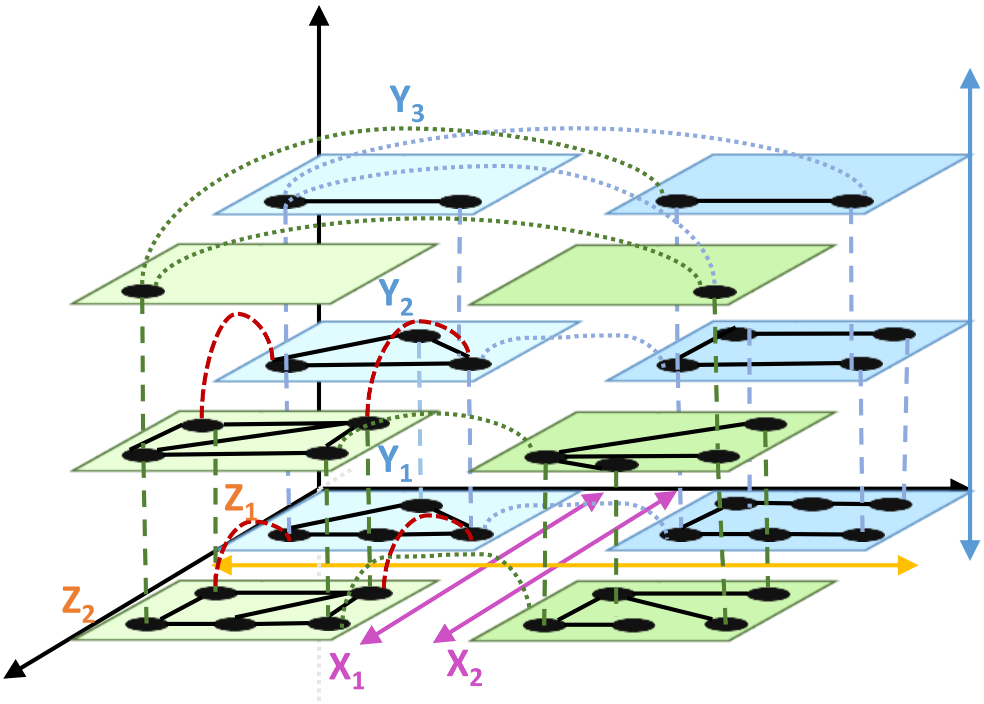


Figure 5.2: General representation

1. A is a set of aspects where $A = \{a_0, a_2, ..., a_{d-1}\}$ and d is the number of aspects in the network.

2. For each aspect $a_i \in A$, a_i has a set of values where $a_i = \{a_{i_0}, a_{i_2}, ..., a_{i_{q-1}}\}$ and q is the number of values in aspect a_i and $q \geq 0$. If $q = 0$ then the corresponding aspect is eliminated. Furthermore, $\mid a_i \mid$ represents the number of values for aspect a_i. Though, the definition allows infinite values for each aspect, in our cases, a set of values for each aspect is finite. The rule r_i for each a_i denotes a set of constraints on a_i such as the order of values.

3. A net n_l represent a simplex graph G_{n_l} for each value of the Cartesian product $l \in \{a_{0j} \times ... \times a_{d-1_k}\}$ where $0 \leq j \leq\mid a_0 \mid, ..., 0 \leq k \leq\mid a_{d-1} \mid$ with total number of members $\mid l \mid=\mid a_0 \mid \times ... \times \mid a_{d-1} \mid$.

4. N is a set of nets where $N = \{n_0, ..., n_{l-1}\}$.

5. A slice s_s represents an area identified with $d-1$ aspects where $s \in \{(a'_0 ... a'_{d-2}) \mid a'_i \in A\}$

6. S identifies a set of slices where $S = \{s_0, ..., s_{m-1}\}$ and $m = |s|$.

7. A graph $G_{n_l} = (V_{n_l}, E_{n_l})$ represents a simplex graph in net n_l with set of vertices V_{n_l} and edges $E_{n_l} \subseteq V_{n_l} \times V_{n_l}$

8. $E_N \subseteq V_{n_{l_1}} \times V_{n_{l_2}}$ for each n_{l_1} and $n_{l_2} \in N$ defines all intra- and inter-net edges.

9. V_N represents vertices in the set of nets N where $V_N = \{V_{n_0} \cup ... \cup V_{n_{l-1}}\}$

10. $\mathcal{G}$ shows a set of graphs of all nets G_{n_l} where $\mathcal{G} = \{G_{n_0}, ..., G_{n_{l-1}}\}$

11. V indicates the set of all nodes in $\mathfrak{G}$.

We present our multilayer model illustrated in Figure 5.1 as an example of our approach. Here, our multilayer model $\mathfrak{G} = (\mathcal{G}, V_N, E_N, V, S, N, A)$ contains three aspects $A = \{\text{network level, depth, technology variants}\}$. Each aspects a_i has the following values $a_{\text{network level}}$= {physcial infrastructure, network layer, E2E topology}, a_{depth}= {core Internet, access, home backbone, home edge}, and $a_{\text{technology variants}}$= {RBB, LTE/4G/5G, ethernet, 802.15.4,...}. The set of nets $N = \{n_0, ..., n_{l-1}\}$ are Cartesian product of values of each aspect, such as the physical infrastructure layer of the Internet core with a particular technology or the physical infrastructure of the home edge with Bluetooth. A slice defines all nets with different aspect values except one. We can identify three main slices for S in Figure 5.1 containing planes: *network level-depth*, *network level-technology variants*, and *depth-technology variants* slices. Each slice s_s identifies with two aspects such as *network level* and *depth* in our model. Note that, each slice shows a cross cut of the network for a particular aspect value. Therefore, we can define parallel slices in each axis direction for different values. The *network level-depth* slice represents all network levels for each part of the network containing the Internet core, access, and edge networks. The *network level-technology variants* slice illustrates what technology variants can be utilized in each *network level.* Finally, the *depth-technology variants* slice shows the technology variants used in each part of the network.

Given our multilayer graph of the home network model illustrated in Figure 5.1, consider the following example as a way of understanding the flexibility of our framework. Suppose that an edge network here is an end-user network connecting IoT devices to the Internet. A home network is one variant of the edge networks. If we limit our representation to the physical structure of the home network and consider technology variants, we can identify various technologies such as WLAN, Bluetooth, and ZigBee. Each technology network has its own characteristics which can be represented as a separate graph interconnected to other technology networks. Such graphs with corresponding nodes and edges can be represented by separate nets in our framework. This information is also mapped to the *depth-technology variants* slice. Since the order of the nets representing each technology is not important in this slice, we can place non-IP after IP-based technologies to show their deeper order in the edge network by defining *home-edge* value for the *depth* aspect, the way that we showed in Figure 5.1. We can easily add another aspect such as power grid as an example to study the components of the communication network and the power grid together.

Since the focus of this research is on the smart home modeling and resilience, we design our multilayer model with the framework for the home network model. We consider the home network shown in Figure 5.3. Figure 5.4 illustrates our multilayer home network model corresponding to the home network in Figure 5.3. In order to simplify the presentation, we abstract our model by eliminating network technologies in the access and the core Internet slices and also network layer and E2E topology. The network is still multidimensional since edges represents different values (network technologies) for physical

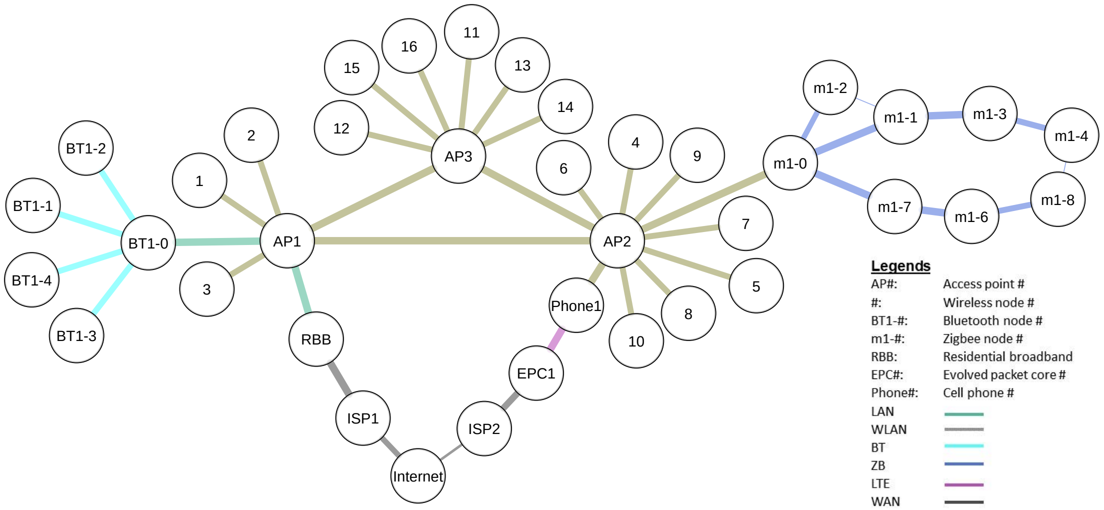


Figure 5.3: Connectivity graph of the home network model

connectivity. The network $\mathfrak{G} = (\mathcal{G}, V_N, E_N, V, S, N, A)$ has the following components:

- $\mathcal{G} = \{G_{\text{WLAN}},\ G_{\text{LAN}},\ G_{\text{Zigbee}},\ G_{\text{Bluetooth}},\ G_{\text{LTE}}\}$
- $V_N = \{V_{\text{WLAN}},\ V_{\text{LAN}},\ V_{\text{Zigbee}},\ V_{\text{Bluetooth}},\ V_{\text{LTE}}\}$
- V_{WLAN}= {AP1, AP2, AP3, Phone1, m1-0, 1,...,16}, V_{LAN}= {AP1, BT1-0, RBB}, V_{Zigbee}= {m1-0, m1-1,...,m1-7}, $V_{\text{Bluetooth}}$= {BT1-0,...,BT1-4}
- E_{WLAN}= {(AP1, AP2), (AP1, AP3), (AP2, AP3),...,(AP3, 16)}, E_{LAN}= {(AP1, BT1-0), (AP1, RBB)}, E_{Zigbee}= {(m1-0, m1-1),..., (m1-0, m1-7)}, $E_{\text{Bluetooth}}$= {(BT1-0, BT1-1), (BT1-0, BT1-4)}, E_{LTE}= {(Phone1, EPC1)}.
- $S = \{s_{\text{technology variants-depth}}\}$
- $N = \{n_{\text{WLAN}},\ n_{\text{LAN}},\ n_{\text{Zigbee}},\ n_{\text{Bluetooth}},\ n_{\text{LTE}}\}$
- A = {technolgy variants, depth}
- $a_{\text{technology variant}}$= {WLAN, LAN, Bluetooth, ZigBee, LTE/4G/5G}, a_{depth}= {home}

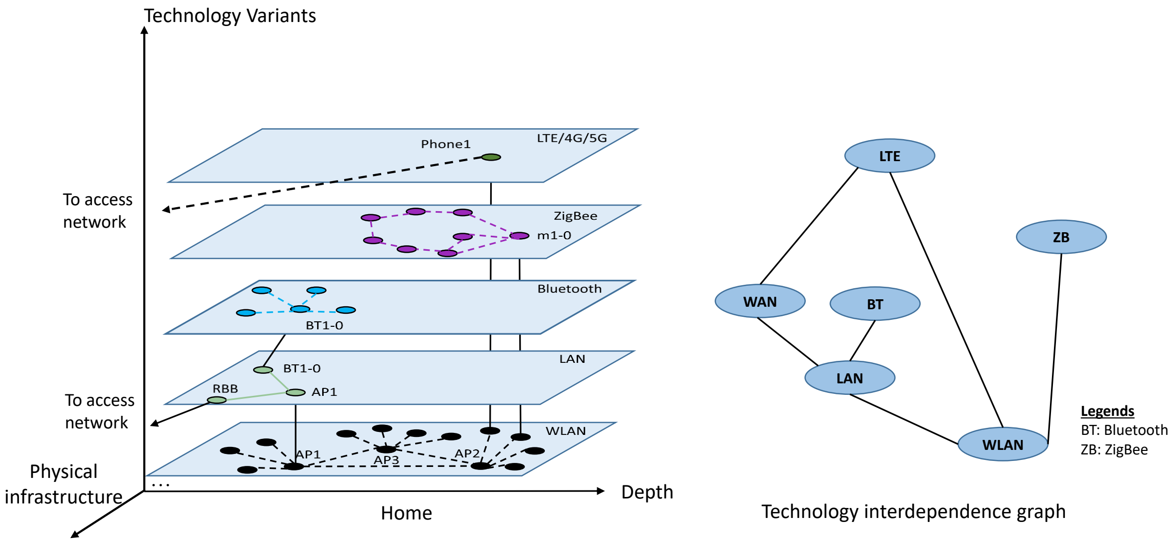


Figure 5.4: The multilayer home network model

5.3 Interdependence Analysis

In a multi-technology system, various networks with different characteristics are involved. The diversity of the technologies improves the robustness and resilience of the overall network. In such networks a node or link failure may have different effect on the overall user perceived services. For example a catastrophic Bluetooth network failure disrupt the services only in the Bluetooth network. Such failures usually do not affect on other network technologies such as ZigBee in the same network. In order to understand the overall behavior of multi-technology networks, we believe that the relation of the utilized technologies should be considered together.

We use the *technology interdependence graph* defined in Section 3.2 as a graph to represent abstract interdependency of technology variants in a multi-technology environment such as smart homes and as a tool for mapping our multilayer home network to a monoplex network. In order to analize mulitlayer networks, most of the basic concepts and metrics should be redefined [120]. One way to avoid complex calculations of the multilayer network concepts is mapping them to a monoplex network when it is possible [126].

A technology interdependence graph is a monoplex network that shows the relationship among utilized technologies; however, it does not show that which nodes and links establish such relationships. In other words, a link between two particular nodes in a technology interdependence graph is the aggregation of links in the underlay graph connecting two technologies. The focus here is on the study of the interdependency of the technologies, we do not need the details about nodes connecting technologies. However, if the topological structure of each layer is under the study, the mulitlayer framework is the proper tool.

We can obtain the technology interdependence graph from a monoplex graph representing a network. The interdependence graph in a monoplex network is the result of *one-mode projection* of a bipartite graph illustrating the relationship between each node and the supported technologies in a particular network such as a smart home or city [100]. The technology interdependence graph considers two aspects, abstracted physical infrastructure and technology variants of a network as shown in Figure 5.4.

Assume that, in a smart home environment, we have nodes supporting various technologies including LAN, WLAN, and Bluetooth. Each group of nodes with a particular technology constructs a physical infrastructure. Some nodes such as a cell phone support various technologies including LTE and WLAN. Such nodes contribute in the physical infrastructure of many technologies connecting those technologies together and a *net* in the multilayer framework. If we consider the whole physical infrastructure of each technology as a single node in the technology interdependence graph and each connection between two different physical infrastructure as an edge between two corresponding nodes in the graph, we can obtain the technology interdependence graph for the corresponding multilayer network as shown in Figure 5.4. Each node in the technology interdependence graph is equivalent of one *net* in the mulilayer graph. The *access network* is considered as a node annotated with *WAN* and it is considered as one *net* in this example due to the abstraction process. This explanation confirms that we can obtain the same technology interdependence graph both from a monoplex and a multilayer graph. However, the multilayer graph is more intuitive and represents more details compared with a monoplex edge-colored graph.

In the following, Algorithm 1 shows the detail process of obtaining a technology interdependence graph from its corresponding multilayer graph. The algorithm generates a general mapping on a multilayer network to its corresponding monoplex network based on the utilized *nets* $n_n \in N$ in $\mathfrak{G}$. Therefore, if the intention is study of the interdependency among technologies in a smart home as we do in this chapter, $\mathfrak{G}$ should be abstracted to reflect only that particular part of the network as shown in Figure 5.4.

```
Data: $\mathfrak{G} = (\mathcal{G}, V_N, E_N, V, S, N, A)$
Result: A technology interdependence graph $G_T = (V_T, E_T)$ corresponding to
        graph $\mathfrak{G}$
for $n_n \in N$ do
    add $v_n$ to $V_T$ ;
end
for $(v_{e_i}, v_{e_j}) \in e_{i,j}$ and $e_{i,j} \in E_N$ do
    if $v_{e_i} \in V_{n_k}$ and $v_{e_j} \in V_{n_l}$ and $n_k \neq n_l$ then
        add $e_{n_l,n_k}$ to $E_T$ ;
    end
end
```

Algorithm 1: Obtaining a technology interdependence graph from a multilayer graph

In the following experiments, we study interdependence of technologies and how adding various links change the network resilience. We perform two groups of experiments. In the first group, we analyze the models against attacks on the most important nodes. In the second group, we add extra links between network technologies and study the behavior of the models. We consider our smart home instances in Chapter 4 for the the first group of experiments. We add extra links to the smart home and expanded smart home models for the second group of experiments and analyze the models when the new links are connected. Then, we compare the results with the original model when the extra links are not used. The instances with added links of the corresponding smart home graphs are illustrated in Figures 5.5 and 5.6. An edge color in the figures represents a particular technology as explained in the legends of the figures and the thickness of edges represents edge betweenness.

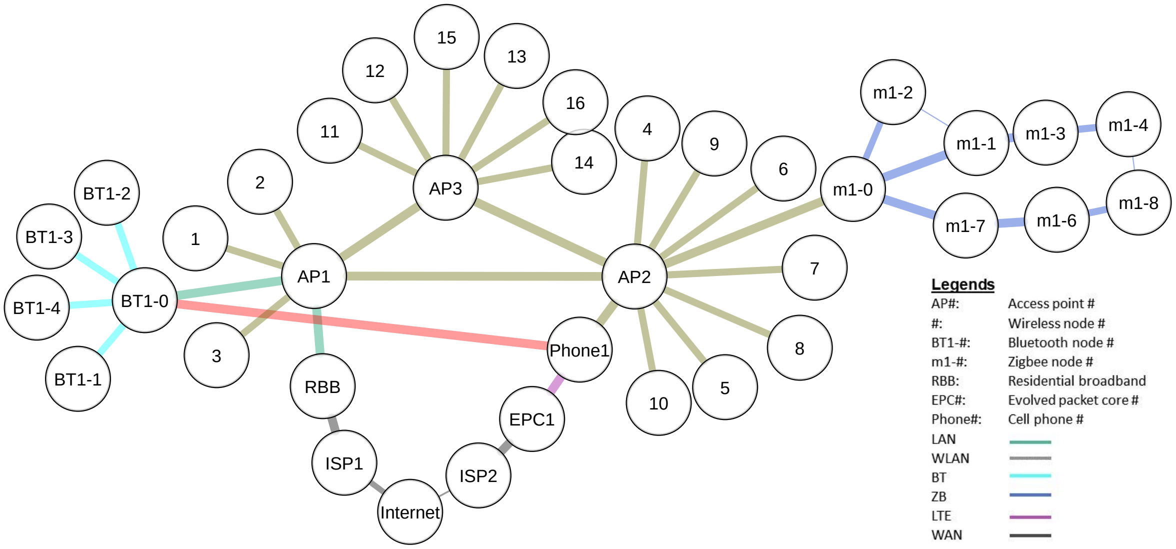


Figure 5.5: Smart home connectivity graph with a new Bluetooth connection

The graph illustrated in Figures 5.7 shows the technology interdependence graph of both home and expanded home when the *red* edge between *Phone1* and *BT-0* in Figures 5.5 and 5.6 is not connected.

It is worth to mention that both smart home and expanded smart home models have the same technology interdependence graphs; although the expanded smart home model have

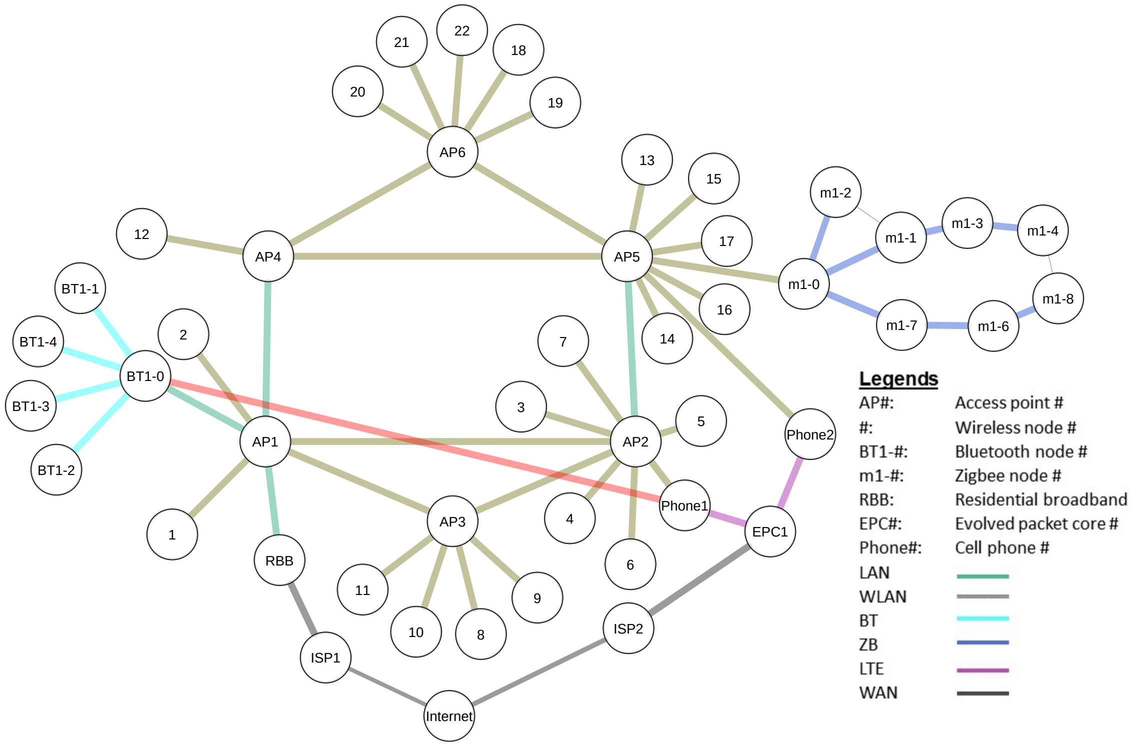


Figure 5.6: Expanded smart home connectivity graph with a new Bluetooth connection

more nodes and links and the 2-core graph (a k-core graph of G is a subgraph in which each vertex has at least degree k) of the model illustrated in Figure 4.12 is different compared to the 2-core graph of the smart home model in Figure 4.11. As a result, changing the structure of each network technology dose not modify the corresponding technology interdependence graph as long as connectivity among technologies stay intact. In other words, changing the structure of each network technology including k-connectivity improves robustness and consequently resilience of that particular technology network, but it does not improve the robustness of the overall network constructed by network of various network technologies.

As explained, k-connectivity is one of the prime factors to promote network resilience due to providing path redundancy. In a multi-technology networks such as smart homes and other smart environments, k-connectivity may promote not only path redundancy

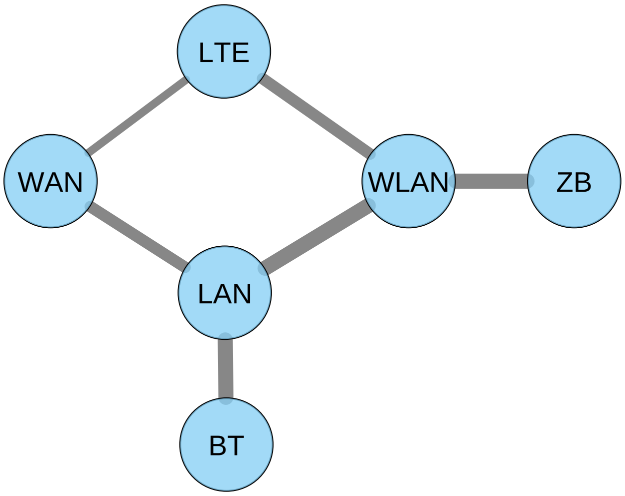


Figure 5.7: Home and expanded home technology interdependence graph

but also path diversity which even improves network resilience further compared to path redundancy alone. This is due to the fact that, diverse paths do not have the same characteristics as redundant paths. Therefore, they are less vulnerable to the similar challenges. This concepts leads us to the idea that k-connectivity should also be considered among technologies. While k-connectivity inside the network of each technology makes that particular network resilience, k-connectivity among network technologies improves the overall network resilience.

In conclusion, the technology interdependence graph can be used as a proper tool to represent connectivity among utilized technologies in a network by abstracting topological structure technological networks. As explained, k-connectivity among technologies can be obtained from this graph. In addition, path redundancy between two particular technologies is reflected on the corresponding edges in the technology interdependence graph. However, it is hard to infer the number of redundant paths between any two technologies and which nodes provide the paths. Therefore, when detail information about the number of redundant path in the underlying network is required the multilayer framework provides more accurate representation compared with a technology interdependence graph.

5.3.1 Framework of the Experiments

In this subsection, we explain our framework to perform targeted attack, i.e. taking the most important nodes offline, experiments and the effect of adding new links between technologies as explained above. We also analyze the results of the each experiment.

Targeted attacks on smart home models

For the first group of experiments, we use the smart home, expanded smart home, backup smart home, and backup expanded smart home models illustrated in Figures 4.3, 4.4, 4.8, and 4.9 in Chapter 4, respectively. We employ the graphs in Figures 5.5 and 5.6 for the second group of the experiments, adding a new link, when the red edges in the graphs of Figures 5.5 and 5.6 are available. From the connectivity graph of each model, we calculate the technology interdependence graph based on the technologies each node supports. We calculate various centrality metrics including degree, betweenness and eignvector before starting our experiments. We investigate the availability of technologies during nodes and links failure. The centrality metrics do not consider the type of each edge as explained in Chapter 4. For instance, degree centrality which considers the normalized number of connected edge to a node does not consider the type of each edge supporting a particular technology. Sometimes a high degree node is the right node to disrupt a network such as the master node in a Bluetooth network, or an access point in a WLAN. However, in other cases, a low degree node may have more effect on the connectivity of a network. For example, disabling a DSL modem with degree of two can disconnect the whole network from the Internet.

In a percolation process, nodes and edges are added to a network to increase robustness and resilience. The inverse process can be used to measure the robustness of an available network by removing nodes and edges and measure the network connectivity. In this experiment, a particular centrality metric such as degree centrality is calculated for all nodes. Then, we remove an available node with the highest centrality value as the most important node based on that particular centrality metric. During the experiment, we do not calculate the centrality metrics again. This is due to the fact that, a smart home is a relatively small-size network and it partitions quickly by removing a few nodes and edges. However, while the network is partitioned some network technologies may still remain functional. Therefore, we cannot eliminate partitioned nodes and consider those nodes dysfunctional because they are in the smaller component of the network. Furthermore, many distance-based centrality algorithms cannot calculate centrality metrics on a partitioned network. However, we eliminate nodes if they are not connected to any other nodes after each failure. We also assume that losing the ZigBee coordinator and the Bluetooth master node disrupts the corresponding network.

We use the following centrality metrics:

- Eignvector measures the importance of a node regarding its connectivity to other important nodes.

- Katz is an extension of eignvector considering a value to represent the importance of each node.

- Degree is the normalized number of connected edges to each node.

- Closeness is the inverse of the average shortest paths between a particular node v_i to other nodes in the network.

- Betweenness measures the fraction number of the shortest path between every node v_i and v_j traversing on a node v_k

- Edge betweenness uses the same measurement as betweenness for every edge e_{ij}

Figures 5.8, 5.9, 5.10, and 5.11 illustrate the results of targeted attacks based on centrality metrics analysis for various instances of the smart home models mentioned above. In each figure, the quantity of each bar represents the number of removed nodes and edges from the network until a particular network technology is completely disabled. When a node centrality metric is used for an experiment, an available node with the highest centrality value is removed from the network. If an edge centrality metric such as edge betweenness is used in the experiment, an available edge with highest centrality value is removed. Since both nodes and edges centrality metrics are shown in Figures 5.8 to 5.15, we use *removed nodes/edges* term on y-axis.

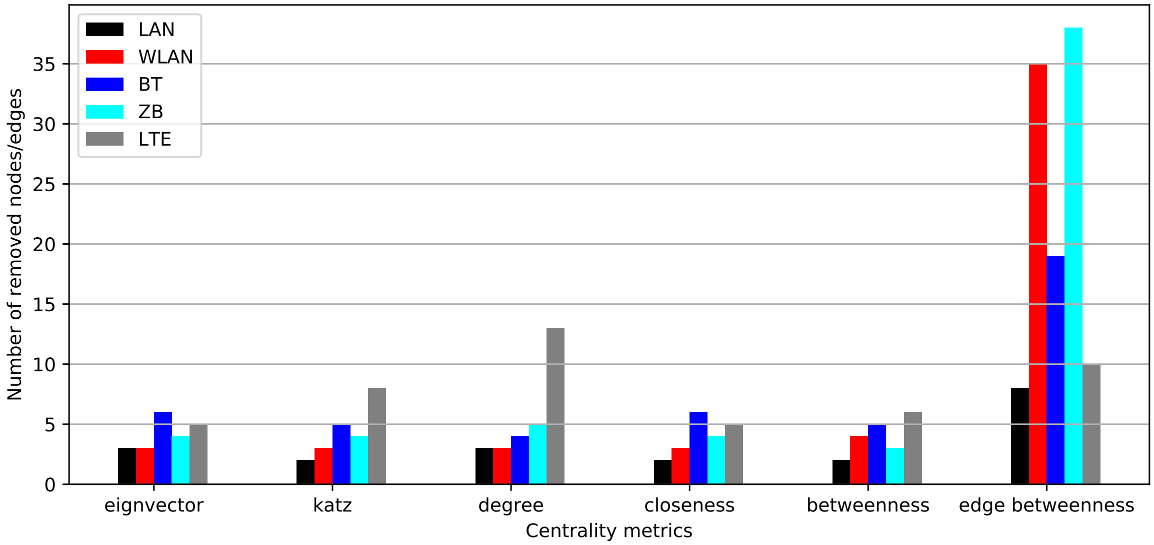


Figure 5.8: Smart homes Centrality - bars represent the number of removed nodes/edges until a network technology is disabled

One outcome of this experiment is that which centrality metric identifies the important nodes and consequently the network technologies adequately in a targeted attack. Each

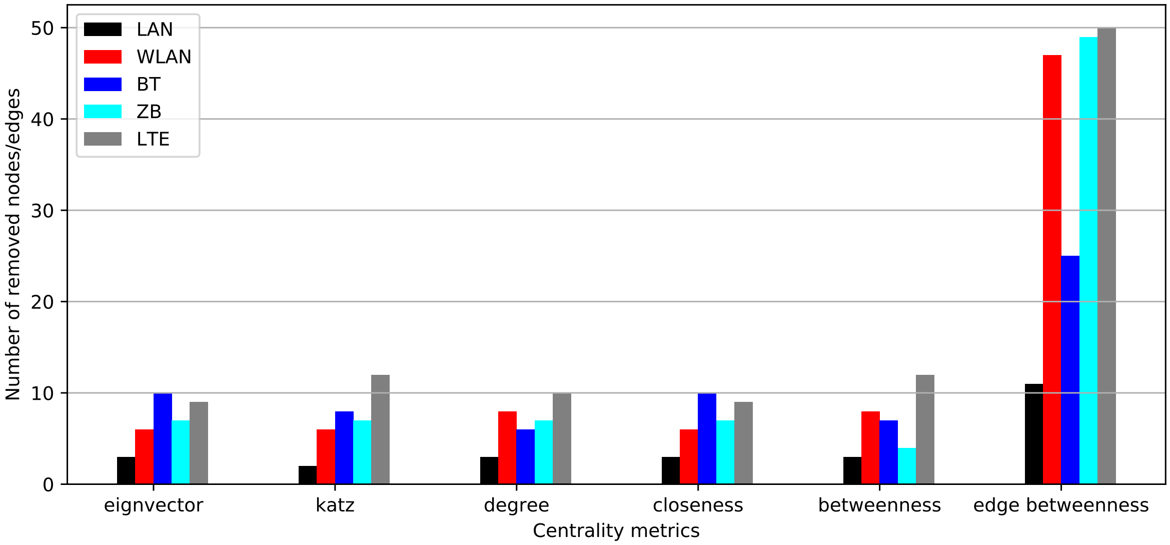


Figure 5.9: Expanded smart home centrality - bars represent the number of removed nodes/edges until a network technology is disabled

centrality metric has been designed for a specific goal. For example, the number of neighbors of each node is considered as the significant factor to identify the important nodes in degree centrality. However, since the conventional centrality metrics cannot identify the type of links and technologies, such metrics cannot consider link varieties in their calculation.

Most of the considered metrics are node-based centrality metrics with the exception of edge betweenness. Edge betweenness also provides the worst results compared to other node-based metrics under consideration. One reason is that when a node fails, all edges connected to the node fail as well. Therefore, the whole network fails faster than edge-based failures.

Since the expanded smart home model has more nodes and edges than the smart home model with the similar characteristics, we expect that the expanded smart home model fails after removing more nodes/edges compared to the smart home model. However, we observe some similarity in the order of the technology failures in Figures 5.8 and

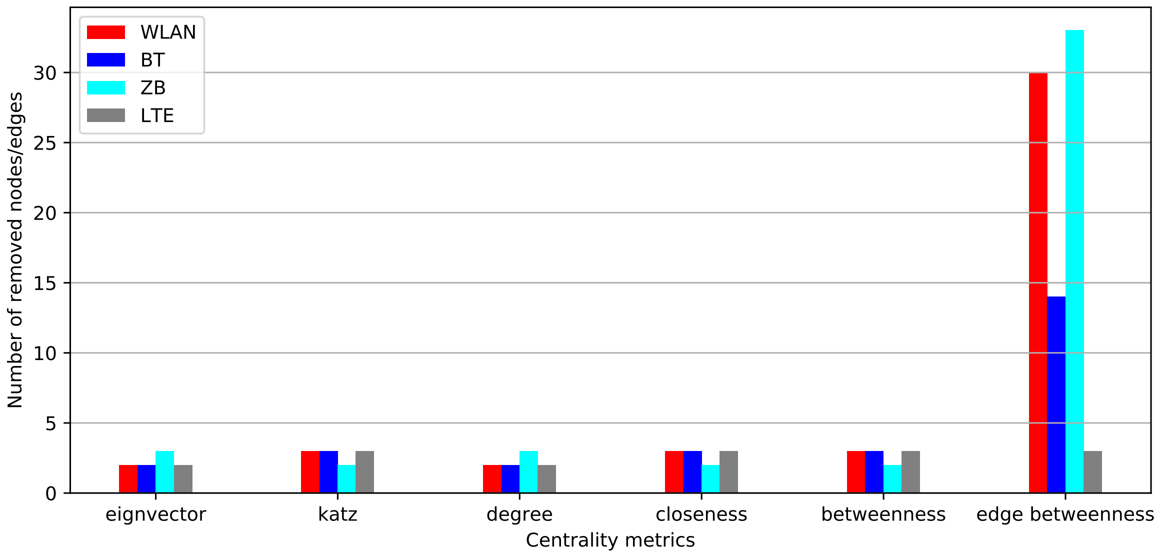


Figure 5.10: Backup smart home Centrality

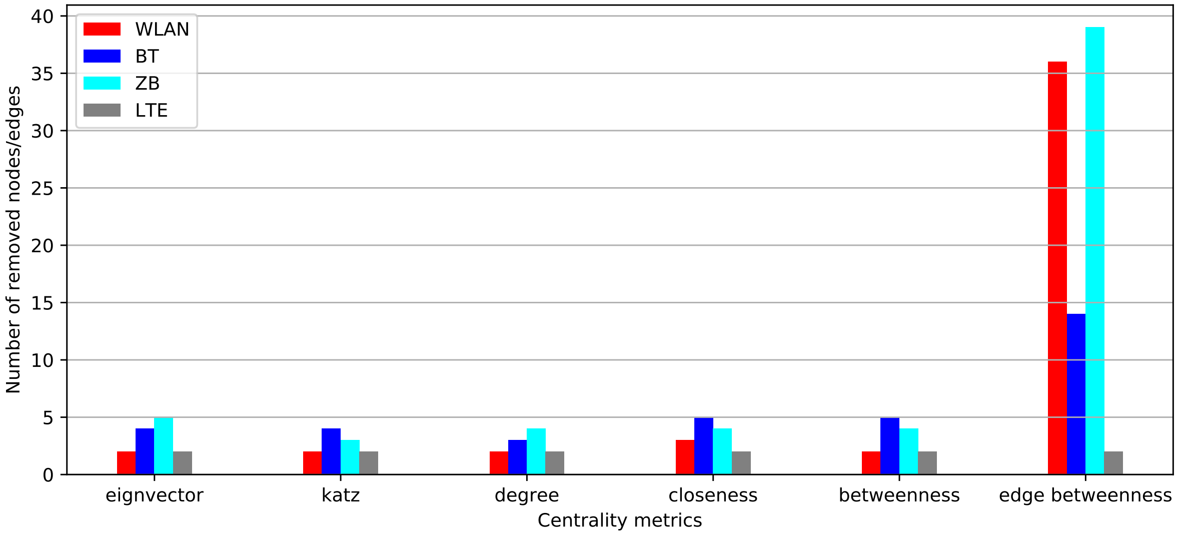


Figure 5.11: Backup expanded smart home centrality

5.9. This is the result of topological similarities of the two networks. For example, both networks have the same number of mesh and star networks connected the same way to the network backbone. However, we cannot achieve the same results regarding the similarity of the network failures from the backup models. As a reminder, the backup models are the results of the network failure in the main Internet connection. Therefore, it is not possible to design such networks with some particular characteristics. The outcome of the obtained models depends on the availability of technologies at the time of failure. For example, we do not have LAN technology anymore after failure. As a result, an available technology with better recovery mechanism during the failure offers more efficient solution. In other words, during a failure many recovery solutions may be available, but the results may not provide the same level of robustness.

In addition, the results in Figures 5.10, and 5.11 show that these two networks are not as resilient as the corresponding models in Figures 5.8, 5.9. Comparing the results of each metric in two corresponding models shows that backup models are more vulnerable to any subsequent attack.

The effect of adding new links between network technologies

In order to study the effect of adding a new link between technologies, we assume that *Phone1* makes a new Bluetooth connection to *BT1-0* indicated with *red edge* in Figures 5.5 and 5.6 as practical scenarios with current network technologies. For example, while Bluetooth and 802.11 are two common technologies utilized in cell phones, there is no cell phone in the current market that supports 802.11s or Zigbee. As observed in the figures, these edges connect two nodes. However, much more importantly they connect two technologies. This results in changes to the robustness of the overall technology interdependence graphs illustrated in Figures 5.12 and 5.13. We follow the same percolation process and use the same centrality metrics as the previous experiment.

Although similar to the previous experiment the technology interdependence graphs in Figures 5.12 and 5.13 are identical, a simple comparison shows that Bluetooth technology connects to more technologies. This new connectivity makes the whole network more robust to link failure. We observe that all technologies except ZigBee in Figure 5.12 are k-connected where $k \geq 2$. Calculating the network core for $k = 2$ confirms the result.

Therefore, any link failure between two particular technologies, except between ZigBee and WLAN, keeps the network connected. In addition, by comparing the thickness of the edges in both Figures 5.12 and 5.13 with their counterparts we observe that the edge betweenness among the technologies reduces. It confirms that the importance of edges has reduced. This is due to the improving path diversity leading to promoting network resilience against path failure.

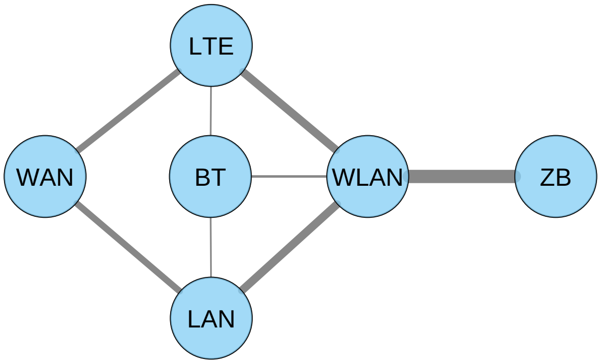


Figure 5.12: Smart Home technology interdependence graph with extra Bluetooth connectivity

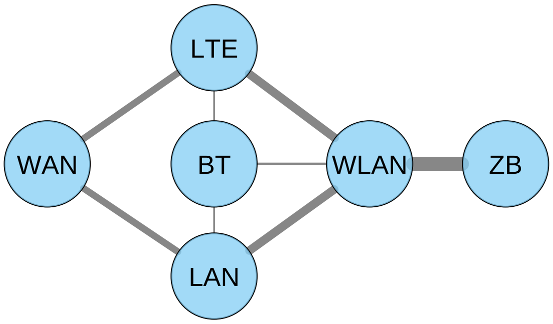


Figure 5.13: Expanded smart home technology interdependence graph with extra Bluetooth connectivity

Figures 5.14 and 5.15 illustrate the results of the targeted attacks on two improved networks with added links. Comparing Figures 5.8 and 5.14, we observe that in Figure 5.8, LTE technology provided by *Phone1* in the network with degree centrality two, fails after removing more nodes compared with the corresponding result in Figure 5.14. The reason is that the most number of nodes in both graphs have degree one or two. Activating Bluetooth in *Phone1* changes the node degree from two to three which makes the node more important in Figure 5.14. Since the smart home network has two paths to the Internet through WAN and LTE technologies, it requires more nodes to remove until the whole network is disconnected from the Internet. This is due to the fact that degree centrality does not consider the variety of the technologies represented by edges. It is significant to note that, this effect can not be observed in a monoplex network, but it is evident in a multilayer network. A node supporting multiple types of technologies works as a bridge among various network technologies and connects multiple layers in the corresponding multilayer network. Therefore, if the node provides the only connection among technologies, failure of such a node may disconnect many network technologies. As an example, if the only access point with many clients in a network fails, it disrupts WLAN; however, if a cell phone supporting two active technologies LTE and WLAN fails, the path between two technologies is disconnected. Therefore, we propose a new degree-based centrality metric considering variety of edges is Section 5.4 for confirmation.

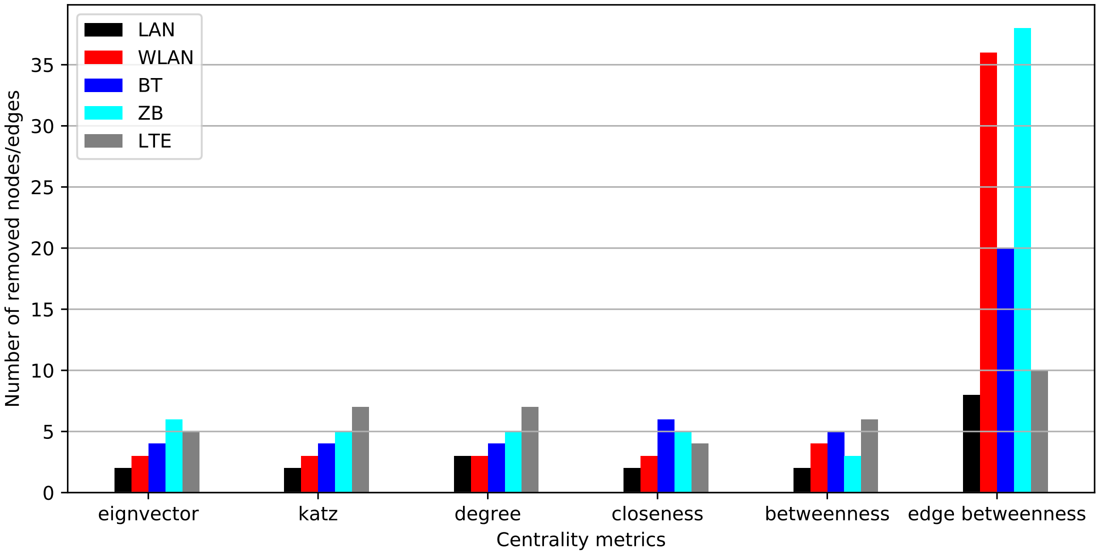


Figure 5.14: Smart home with a new Bluetooth link centrality analysis

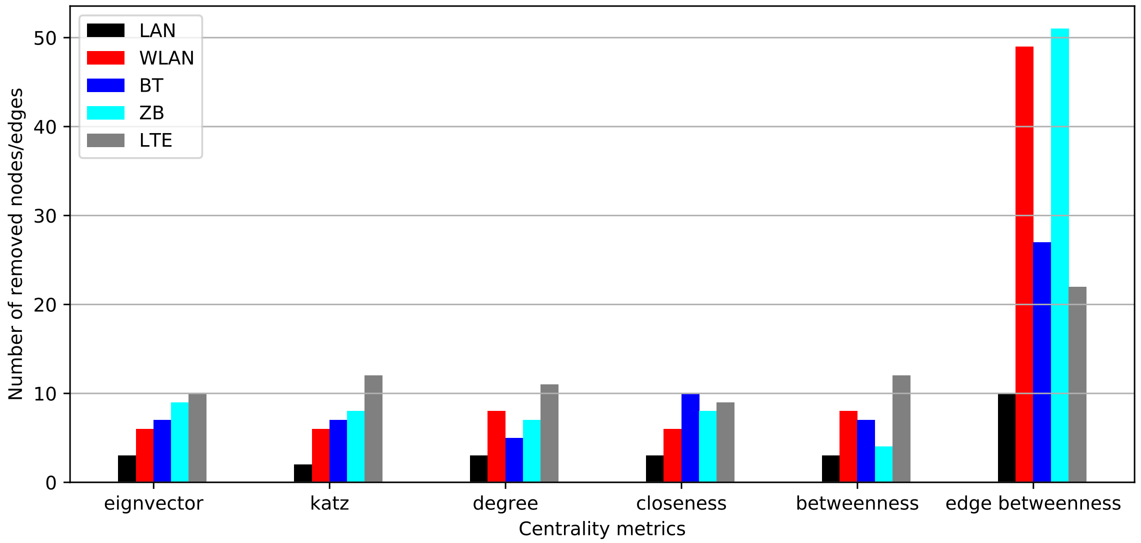


Figure 5.15: Expanded smart home with a new Bluetooth link centrality analysis

5.4 Proposed Degree-based Centrality Metrics

As discussed in Chapter 4 and illustrated in this chapter, the conventional centrality metrics fail to identify various type of edges in a multi-technology network such as smart homes. In some cases, assigning proper weights such as delay or bandwidth can resolve the problem, but in other cases such as the above experiments, assigning weights does not rectify the problem.

In this section, we propose four new degree-based centrality metric variants and compare them with the conventional *degree centrality metric* applied on the smart home instances. The results show that some of these variants, specifically *edge variant*, identify the important nodes more accurate compared to degree centrality. By important node, we mean that a node with a relatively high-degree value and variant technologies. The intention of proposing these new variants is that they consider both degree value and technology variants in the calculation.

As the first variant, called *edge variant*, we consider the degree centrality of each node

v_i as a fraction of the supporting technologies in a network. Given that, we propose *edge variant*, as:

$$d_{ei} = d_i \times (s_i/t)^{\alpha} \tag{5.1}$$

where t is the overall number of supporting technologies in a network, s_i is the number of technologies that node i supports, and d_i is the conventional degree centrality value of v_i. α is an optional exponent to magnify the effect of the various number of technologies. α increases differences among calculated centrality values. This metric assigns a higher centrality value to a node v_i with degree d_i supporting s_i technologies compared to another node with the same degree but $s_j < s_i$ supporting technologies.

We also propose three other degree centrality variants and illustrate their corresponding results in Figures 5.16 and 5.17 to manipulate the effect of technology variants in the calculation. *Boosted edge variant* calculates centrality as below:

$$d_{bi} = d_i + d_i \times (s_i/t)^{\alpha} \tag{5.2}$$

Similar to the above formula, t is the overall number of supporting technologies in a network, s_i is the number of technologies that node i supports, and d_i is the conventional degree centrality value of v_i. α is an optional exponent.

Exponential technology variant considers centrality as:

$$d_{ei} = d_i \times (s_i)^{\alpha} \tag{5.3}$$

We use different approach in *removed degree 1 variant*. First, we remove all nodes with one neighbor, and then we calculate degree centrality based on the new graph. We follow this approach to decrease the centrality value of nodes that increases by connecting to less important nodes; however, the result is not as promising as *edge variant*.

Figures 5.16 and 5.17 show the results of the targeted attacks based on the proposed degree centrality metrics for smart home and expanded smart home models and compared with the conventional *degree* centrality metric.

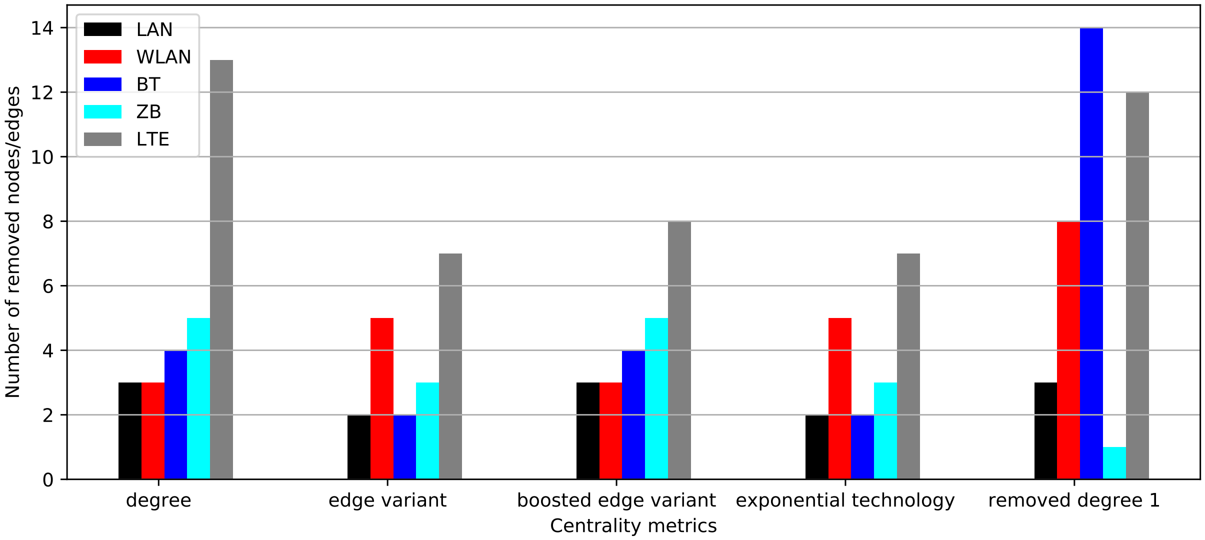


Figure 5.16: Smart homes degree variants centrality

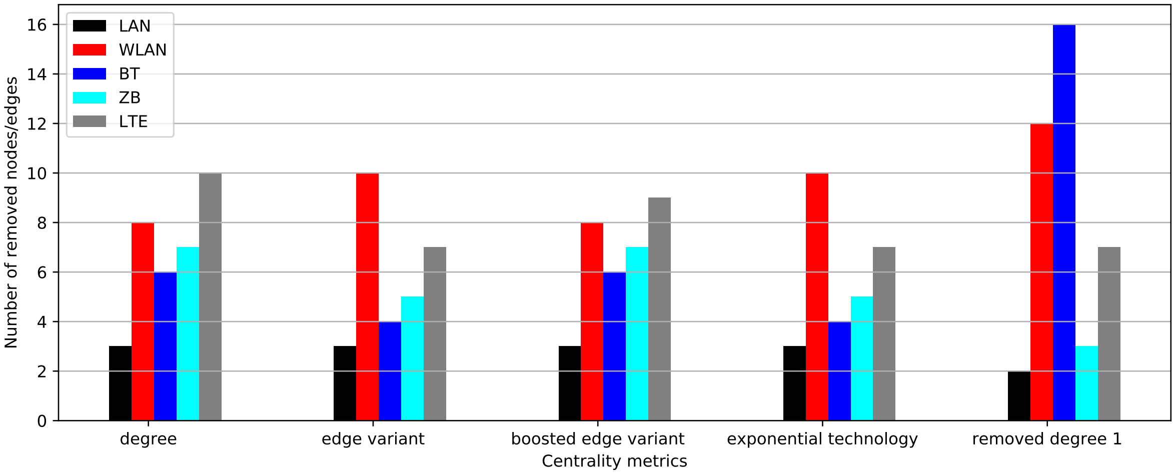


Figure 5.17: Expanded smart home degree variants centrality

As illustrated in Figures 5.16 and 5.17, *edge variant* shows better result with respect to identifying nodes with various links compared to the conventional degree centrality calculation. The result illustrates that the nodes with supporting more technology variants are targeted first, even if they have a lower degree centrality.

The results for the home and expanded home networks with an added new Bluetooth link are illustrated in Figures 5.18 and 5.19.

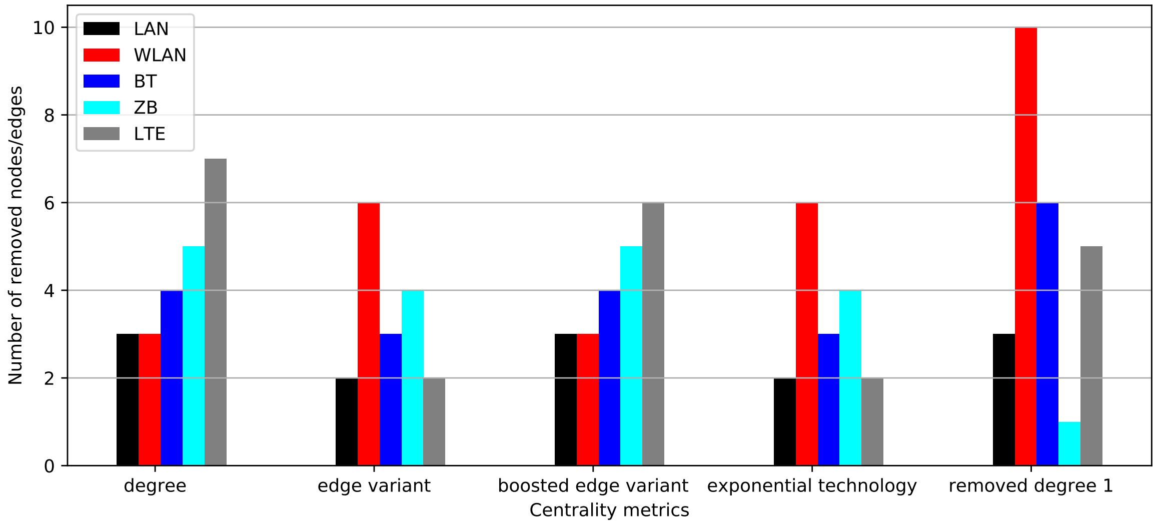


Figure 5.18: Smart home with a new Bluetooth link degree variant centrality

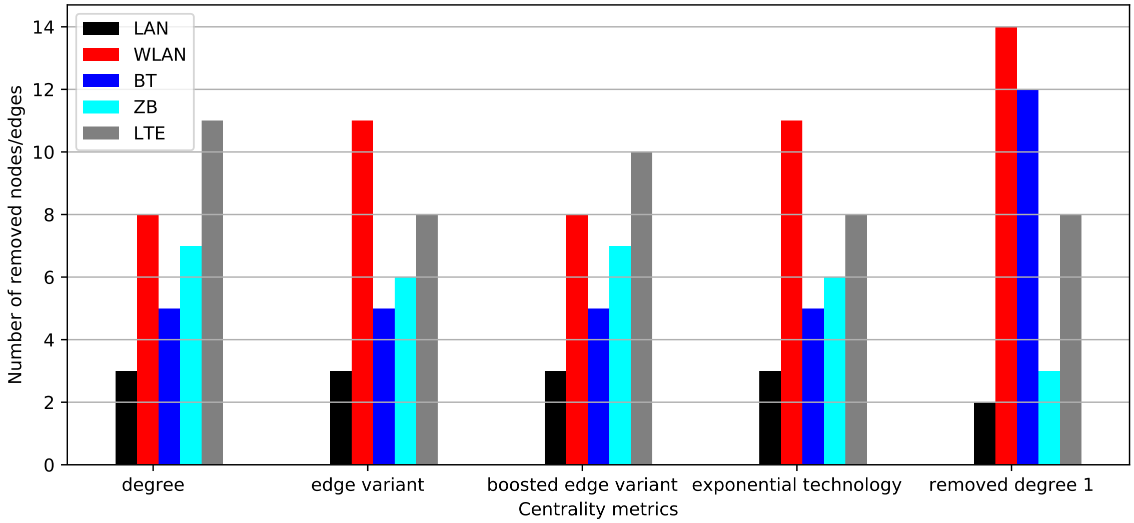


Figure 5.19: Expanded Smart home with a new Bluetooth link degree variant centrality

The conventional centrality metrics work on topological structure of a graph. When multiple type of interactions such as various network technologies among nodes are involved, such centrality metrics are not able to identify these interactions. Therefore, all kinds of interactions are treated similarly resulting in poor identification of the important nodes.

These interactions in a multilayer network appear as inter-layer edges. Considering the illustrated results for the degree centrality metric, we conclude that the conventional degree centrality metrics can not identify the important nodes in a multilayer network. More study on distance- and spectra-based centrality metrics in multilayer networks are required to confirm such results in other types of centrality metrics. We leave this study as our plan for future work.

5.5 Summary

In this chapter, we propose an instance of a smart home multilayer model to represent network technologies and functionalities in separate layers. This model provides valuable information about each layer and component of the system and it helps us to define the formal representation of the system. We also illustrate the connectivity of smart home components with the communication networks and the Internet in a comprehensive model compared to isolated smart home models. The idea can be used to model larger networks such as smart cities and the connectivity of smart homes in a city as future work.

In Section 5.2, we introduce a framework to formalize multi-technology systems with multilayer networks. This framework divides a network into various aspects of interest. The intersection of aspects in the network which has particular attributes is recognizable and can be formally defined. These intersections are called *slices* and *nets* in the framework. This framework not only offers a multilayer view from a complex network, but also has the ability to expand and shrink some part of the network for more detail information or abstraction. We utilize this framework to define a multilayer smart home model.

In Section 5.3, we define an algorithm to map a multilayer network to its corresponding technology interdependence graph and utilize the obtained graph to analyze interdependency among various technologies. The solution and mapping provide simpler calculation compared to direct calculation on a multilayer graph.

We introduce four new degree-based centrality metrics in Section 5.4. These variants consider supported technologies in a network to categorize the important nodes based on both conventional degree centrality values and the type of each edge. Edges with supporting multiple technologies establish connections between layers in a multilayer network and they act as a bridge in a monoplex network. These nodes have an important roles to establish connectivity between technologies and the overall resilience of a multi-technology network. Similar distance- or spectra-based centrality metrics can possibly be defined, which is left for future work.

Page left intentionally blank.

Chapter 6

Smart Home Topological Analysis

As presented in Chapters 3 and 4, smart home models are relatively small networks with various interactions caused by utilizing different network technologies. By considering nodes functionality typical centrality metrics, including degree-based centrality, are unable to identify the important nodes in the network adequately. We introduced four new variant degree-based centrality metrics in Chapter 5 to alleviate this deficiency. In this chapter, we analyze the topological structure of various smart home networks to show the value of the proposed new metrics.

As explained in previous chapters, using different network technologies to provide path redundancy and diversity to the Internet improves network resilience. In this chapter, we analyze how adding extra cell phones with 4G/LTE/5G and WiFi technologies affect the topological structure of the smart home models. This analysis is performed over many randomly generated smart home topologies with a different number of nodes in their backbone, resulting in networks of various sizes.

In Section 6.1, we explain our framework to construct a large set of smart home topologies to perform our experiments. In Section 6.2, we analyze the generated smart home topologies with conventional and our newly proposed centrality metrics in Chapter 5. In this chapter, we inspect the effect of size, the number of technology networks connected to the backbone, and the number of cell phones to understand the overall topological structure of a smart home network. In other words, we examine how several technologies incorporated into various nodes such as cell phones that improve path redundancy and technological diversity affect the smart home models and how conventional centrality metrics and our proposed metrics can capture such changes in the networks. The results of this chapter are under review for publishing in the *Journal of Ambient Intelligence and Humanized Computing*.

6.1 A Framework for Constructing Smart Home Variants

In this section, we explain our framework to construct randomly generated smart home topologies corresponding with the smart home abstract model proposed in Section 3.3. We use the topologies generated by this framework for further analysis of the topological structure of the smart home models. As explained in Section 3.3, each smart home topology has a backbone. The network technologies are connected to the backbone. Furthermore, the smart home network is connected to the Internet with RBB and 4G/LTE/5G technologies to provide diverse paths to the Internet. We construct smart home topologies with multiple integrated access points for the backbones. We consider three to six integrated access points for the backbones. After constructing the backbones, we connect network technologies to the backbone for two groups of experiments. In the first group, we add one star- (representing Bluetooth networks) and one mesh- (representing Zigbee/Z-Wave networks) networks to the backbones. In the second group, we connect two star and two mesh network technologies to each backbone. Each generated topology is integrated with one to three cell phones to provide redundant network access to the Internet.

6.1.1 Backbone structures

With three integrated access points we can construct only two different backbones, linear and complete graphs. As the number of integrated access points increases, the possible number of backbones increases accordingly. We construct a total of 25 different backbones manually in a way that we consider linear, partially completed, and bi-connected networks. For the backbones with more than three nodes, we add extra node(s) to the bi-connected graph obtained from the three-node backbone. We construct five different backbones with four nodes, including the linear network. The same process for adding nodes applies for five- and six-node backbones. The result is twelve different backbones for five nodes and six different backbones with six nodes. With six-node backbones, we construct two separate bi-connected components in the backbone, considering three nodes are the least number of nodes to construct one bi-connected component. Then, the bi-connected components are connected, similar to the expanded smart home network presented in Figure 4.4. The expanded smart home model is one of the six generated backbone topologies. In the backbones with four and five nodes, the new node is connected to one of the components of the bi-connected graph in the backbones with $n-1$ nodes. Figures 6.1 to 6.4 illustrate two samples from each group of backbones with a particular number of nodes among the generated networks. Nodes *AP1* to *AP6* construct the backbone graphs in Figures 6.1 to 6.4.

6.1.2 Network technology structures

The network technologies connect to the backbones through their gateways. In a star topology, the center of the star network is considered as the gateway. In a mesh topology, the first created node in the network is considered as the gateway labeled with 0 in Figures 6.1 to 6.4. We assume the number of nodes in both star and mesh topologies is fixed in all models to produce a controlled environment. However, the network technologies can connect to any nodes in the backbone randomly. We repeat this process ten times for each backbone to construct networks in a way that network technologies connect to different backbone nodes. Since the process of attaching the network technologies to the backbone nodes is random, it is possible that star and mesh networks connect to the same backbone node.

Adding or reducing the number of network technologies affect smart home networks in two ways. First, through the topology that each type of network technology utilizes to establish the network, second, by the number of nodes in each network. We use the same network topology for each particular network technology. It is more important for the mesh networks in which such networks can be constructed differently. Therefore, we form two groups of topologies. In the first group, we consider two mesh and two star networks in each topology and compare the results. In the second group, we add only one star and one mesh network to the topologies and compare the results with the corresponding topologies constructed in the first group. We use Python NetworkX library to construct both star and mesh topologies. As explained in Chapter 3, we use Caveman algorithm [108] to build the mesh topology.

In Section 6.2, all values presented in Tables 6.3 to 6.12 show the results for all topologies with two mesh and two star network technologies for each corresponding centrality metrics. Furthermore, all the figures in Section 6.2 illustrate the results of the comparison between the topologies with four network technologies (two star and two mesh networks) with the corresponding topologies with two network technologies.

6.1.3 Cell phones integration

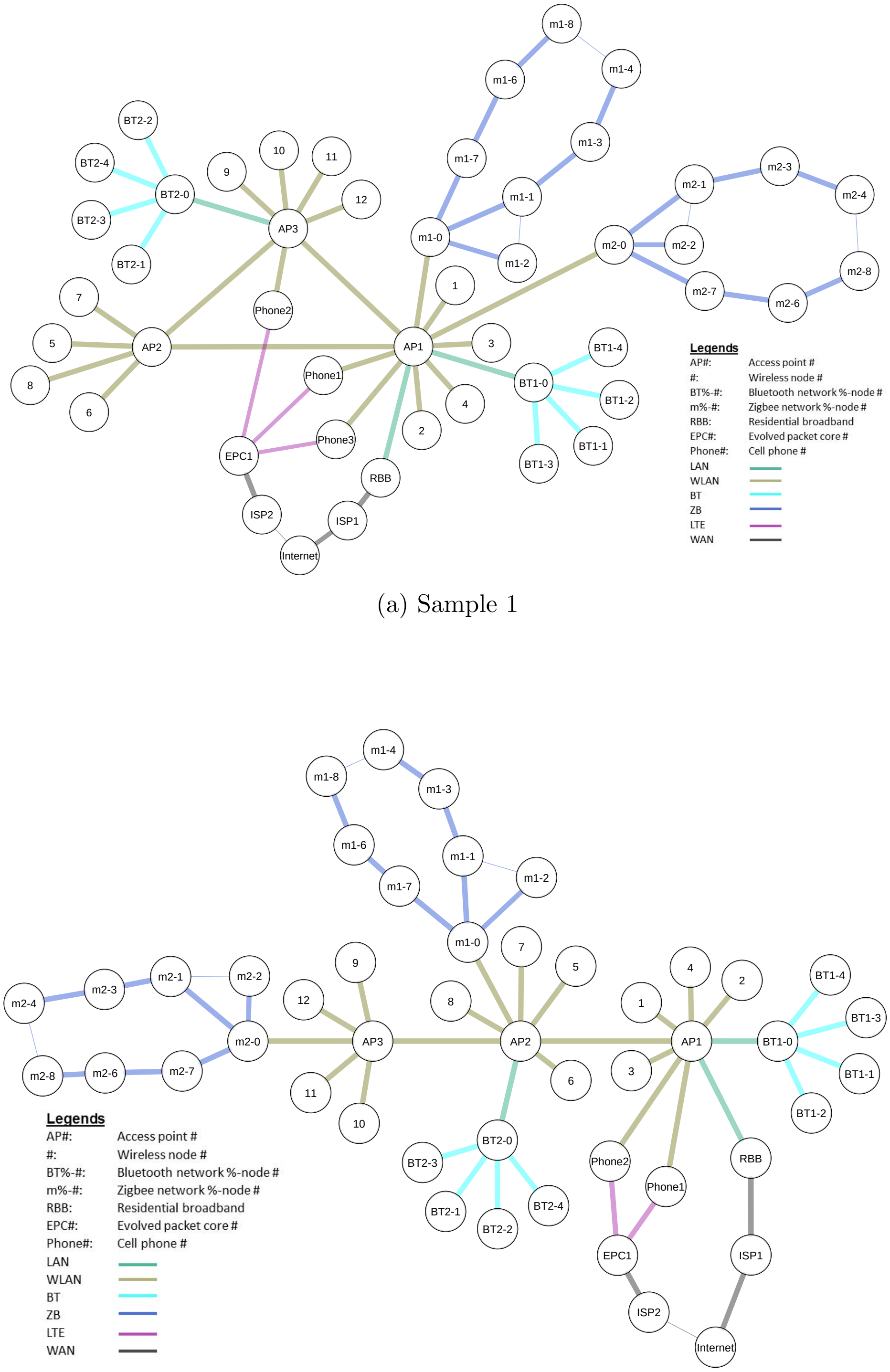
As explained in Chapter 4, cell phones provide additional paths to the Internet, improving network resilience against Internet connection failures. In order to study the effect of the number of cell phones on the topological structure of the networks, we connect one to three cell phones to each constructed topology after integrating the network technologies to the backbone. The cell phones are connected to the backbone nodes randomly. We also consider that all cell phones have the same provider; therefore, they connect to the same ISP through 4G/LTE/5G networks.

The generated topologies connect through *RBB* node to the Internet to establish another path. RBB nodes connect to a different *ISP* compared with the cell phones to improve path diversity and network resilience.

Considering the above process of constructing backbones, integrating network technologies, and cell phones, we obtain 750 different topologies with four network technologies randomly. Another group of 750 topologies is generated with two network technologies to compare with the first group.

6.2 Analysis of Smart Home Variants

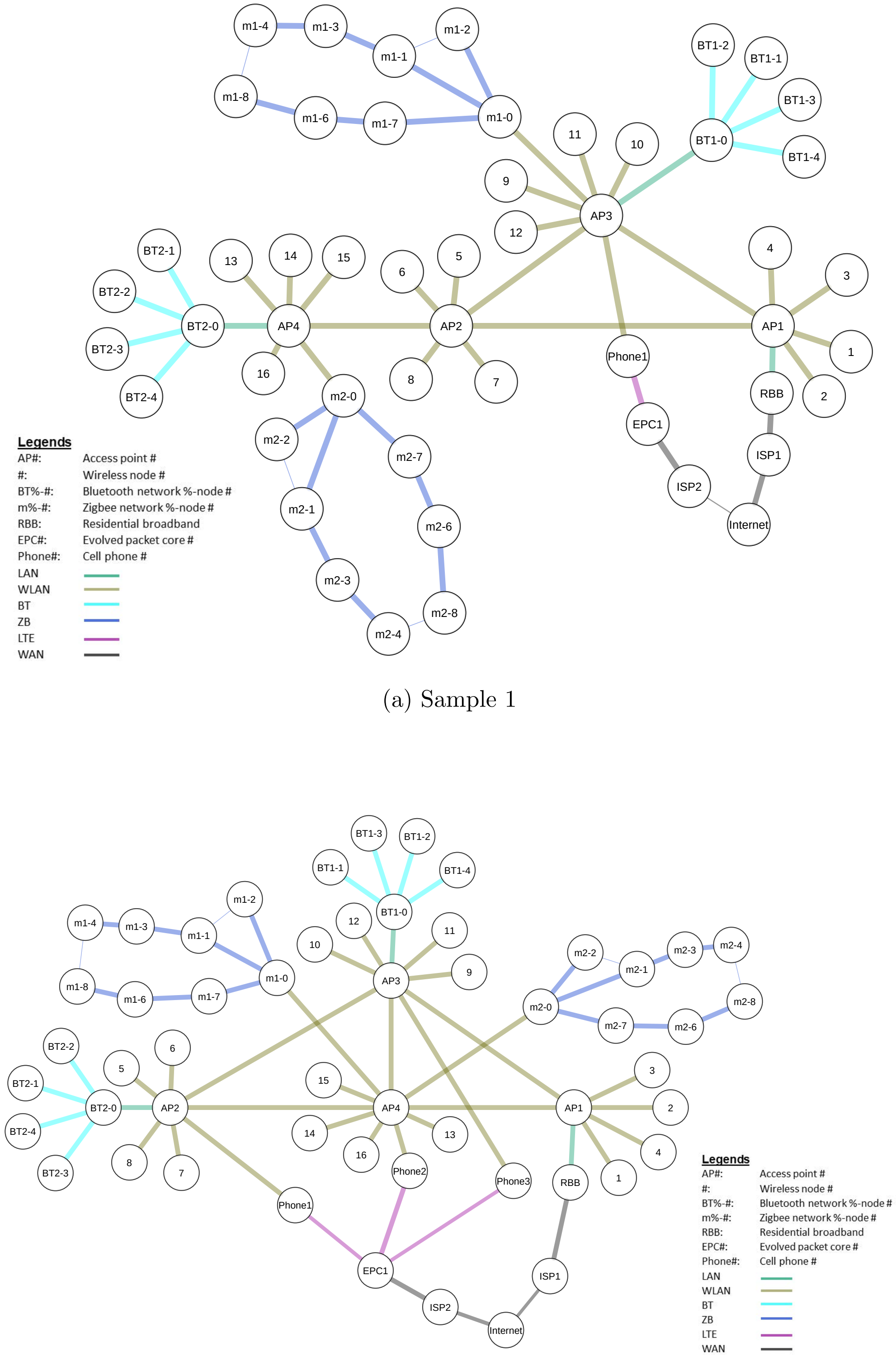
In this section, we calculate conventional graph centrality metrics and our proposed metrics introduced in Section 5.4 for all generated topologies from our framework explained in Section 6.1. During the analysis, we categorize all topologies with the same number of nodes in their backbones in one group and study the effect of adding cell phones to the topologies as nodes supporting multiple technologies and increasing path redundancy. In Tables 6.3 to 6.12, we calculate centrality metrics for each group of topologies per a particular number of cell phone. All topologies have the same number of network tech-



(a) Sample 1

(b) Sample 2

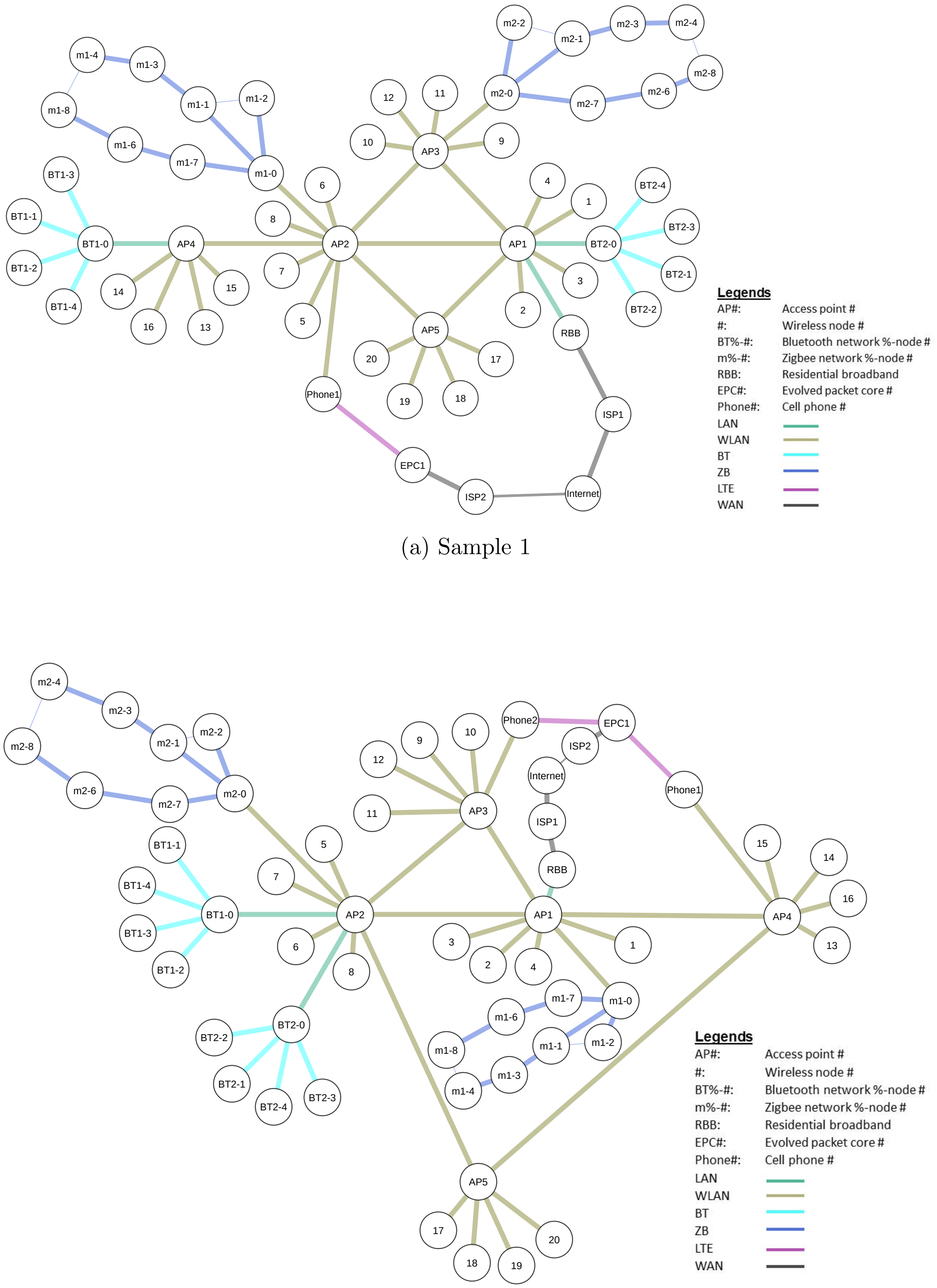
Figure 6.1: Smart home connectivity graphs with 3 Access points



(a) Sample 1

(b) Sample 2

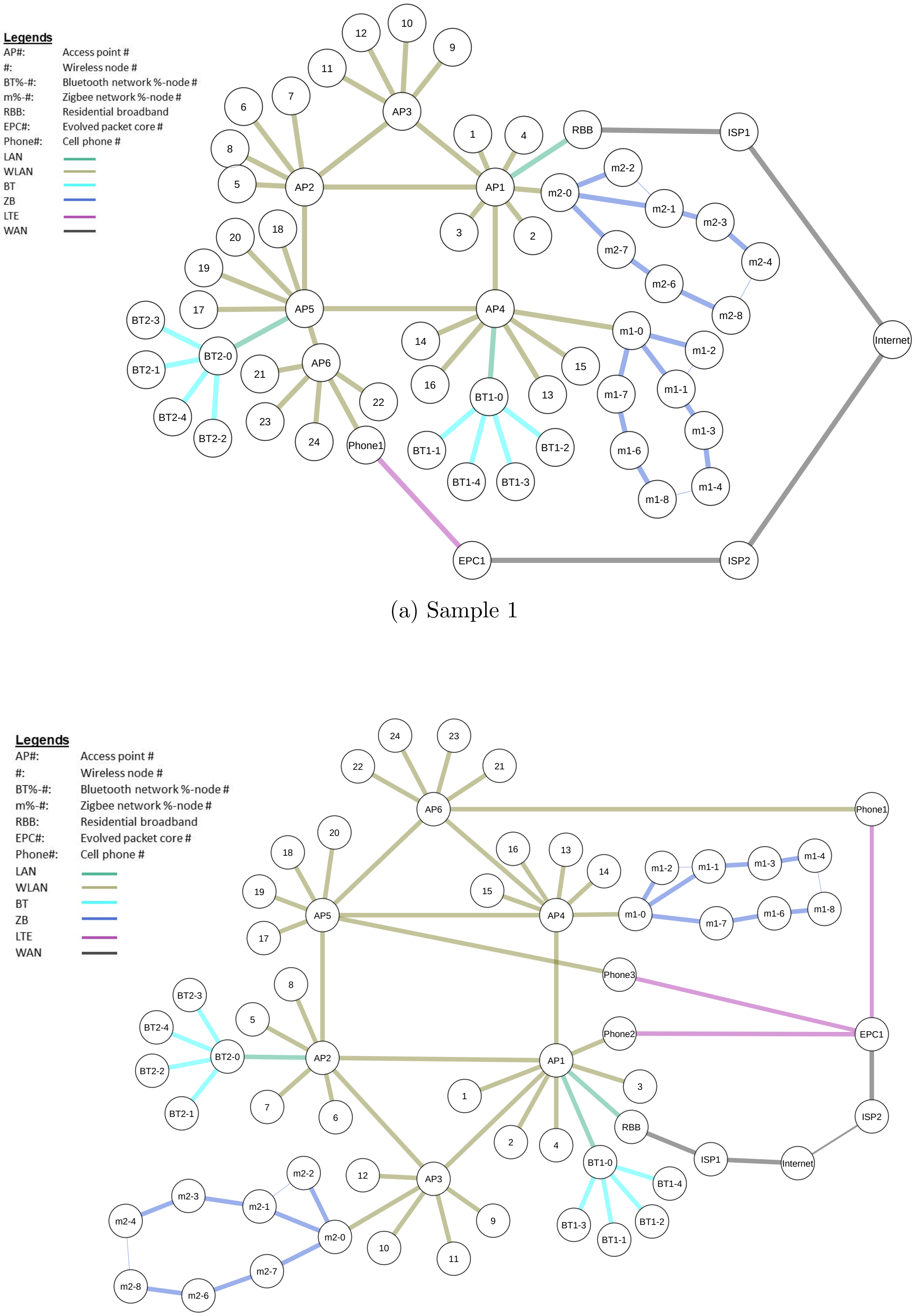
Figure 6.2: Smart home connectivity graphs with 4 Access points



(a) Sample 1

(b) Sample 2

Figure 6.3: Smart home connectivity graphs with 5 Access points



(a) Sample 1

(b) Sample 2

Figure 6.4: Smart home connectivity graphs with 6 Access points

nologies. For each group, the mean centrality value is calculated along with a 95 percent confidence interval.

Furthermore, we study the effect of the number of network technologies shown in Figures 6.1 to 6.4, in these figures, topologies with four network technologies (two mesh and two star networks) are compared with the corresponding topologies with two network technologies. Metrics are given with the mean values and a 95 percent confidence interval.

6.2.1 Analysis with conventional centrality metrics

In this section, we start our analysis by measuring general properties of the topologies. Tables 6.1 and 6.2 show values for the network diameter, average connectivity, algebraic connectivity, and efficiency of each group of topologies without categorizing the calculated values for a particular number of cell phones. Table 6.1 shows the results for topologies with two network technologies while Table 6.2 shows the corresponding results for topologies with four network technologies.

	Measurement							
No. APs	Diameter	±Δ	Connect.	±Δ	Algebra.	±Δ	Efficiency	±Δ
3 APs	8	0.13335	1.12019	0.00388	0.07716	0.00285	0.34604	0.00208
4 APs	8.16667	0.09931	1.10333	0.00276	0.0736	0.00219	0.33642	0.00156
5 APs	8.29722	0.05964	1.096	0.0017	0.07364	0.0013	0.32907	0.00105
6 APs	8.60556	0.12547	1.0908	0.00259	0.06956	0.00228	0.31928	0.00218

Table 6.1: Graph measurement for topologies with two network technologies

Figure 6.5 illustrates that the network diameters increase slowly when the number of nodes in the backbones increases; however, the increment is less than a unit. As expected, the topologies with two network technologies have shorter diameter compared with topologies with four network technologies; however, it shows that adding two network technologies with different topologies increases the network diameters nearly one

	Measurement							
No. APs	Diameter	±Δ	Connect.	±Δ	Algebra.	±Δ	Efficiency	±Δ
3 APs	8.8	0.16868	1.08989	0.00206	0.06341	0.00324	0.30853	0.00188
4 APs	9.02667	0.12209	1.08008	0.00144	0.06027	0.00208	0.30229	0.00141
5 APs	9.30278	0.08285	1.07492	0.00101	0.05953	0.0013	0.29785	0.00094
6 APs	9.54444	0.13544	1.07186	0.00155	0.05862	0.00203	0.2916	0.00183

Table 6.2: Graph measurement for topologies with four network technologies

unit. Diameter shows the longest shortest path in a network and can be utilized as an indicator to calculate delay. In small networks with the same size as the smart homes delay is negligible; however, when low-speed technologies are involved, each extra hop can add significant delay. Therefore, care should be taken in such networks that diameter cannot be a proper indicator for estimating delay.

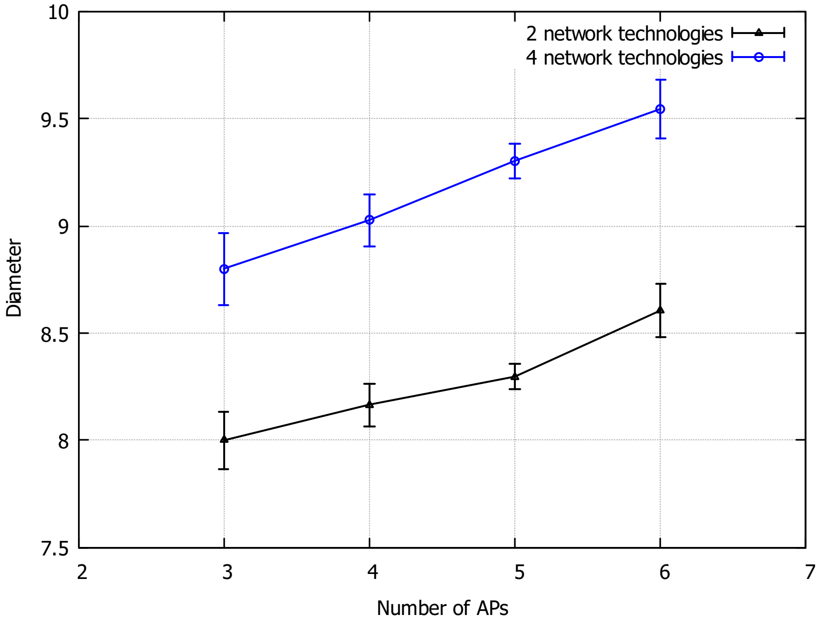


Figure 6.5: Network diameter vs access points

We take advantage of average connectivity to measure connectedness of our topologies instead of k-node connected used in Chapter 4. k-node connected is a lower bound for the average connectivity since k-node connected considers the worst case scenarios and most of the time it cannot reflect the connectedness of the whole network [127]. Figure 6.6

shows that the values of the average connectivity decrease when the number of nodes increases. Figure 6.6 also shows that topologies with more network technologies have smaller connectivity compared with topologies with fewer network technologies. The trend of decreasing network connectivity is slower when more access points are added to the network. These results show that the value of the average connectivity always stay above one since the topologies are connected. However, the connectivity results show that the topologies are partitioned approximately with one failure even if the backbones are bi-connected in most topologies. Another conclusion, specifically in our study, is that star networks are dominant in the topologies since most of the nodes in star networks have degree one.

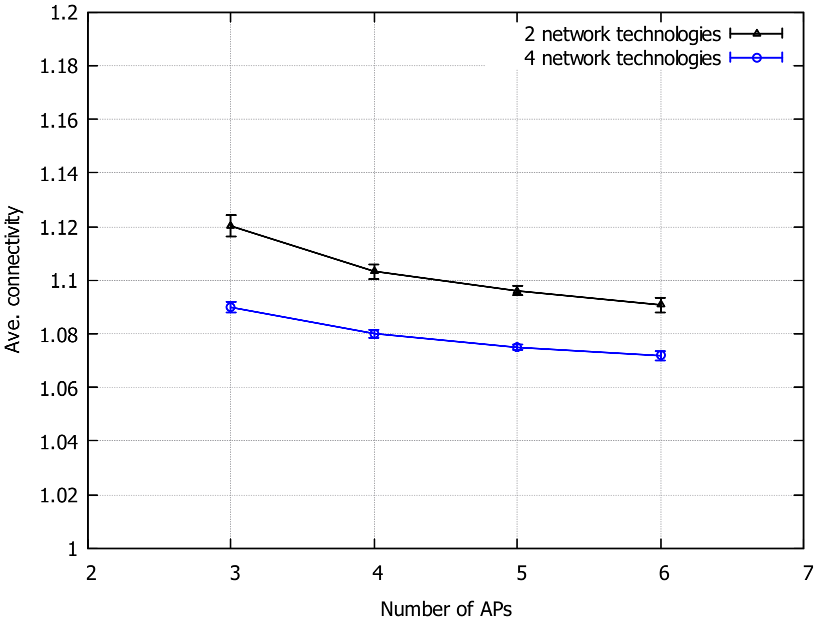


Figure 6.6: Average connectivity vs access points

Algebraic connectivity illustrated in Figure 6.7 follows a decreasing trend showing that the connectivity in the topologies is getting weaker. This is because the number of nodes with a small degree, mostly degree one (edge nodes), is increasing.

Figure 6.8 illustrates that the values of efficiency has a decreasing trend in both groups

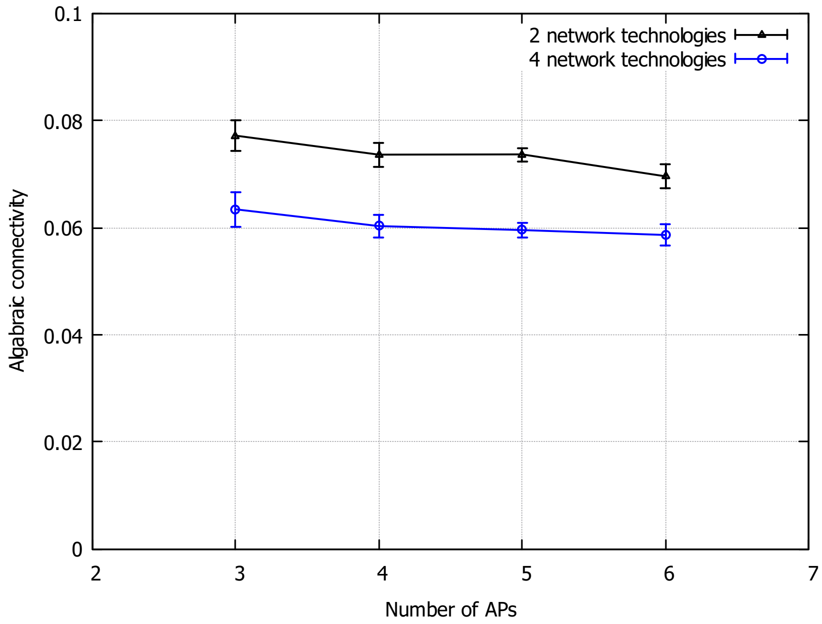


Figure 6.7: Algebraic connectivity vs access points

of topologies containing two and four network technologies. Efficiency shows that the average number of direct communication between each pair of nodes is decreasing. This is due to the fact that all nodes in any network technology connect to other nodes through their gateways. Therefore, there is no direct way for such nodes to communicate with other nodes outside their network.

Table 6.3 shows the mean values of the betweenness centrality for each group of topologies per number of cell phones. We observe that betweenness values decrease when both the number of nodes in the backbones and the number of cell phones in the topologies increase. However, in both cases, betweenness values decrease slowly.

Figure 6.9 illustrates the betweenness results for three-node-backbone topologies with two and four network technologies, and six-node-backbone topologies with two and four network technologies. We do not show the results for four and five-node-backbone topologies since the results follow the same trend as the results of three and six-node-backbone topologies. The results in Figure 6.9 show that the value of betweenness decreases for

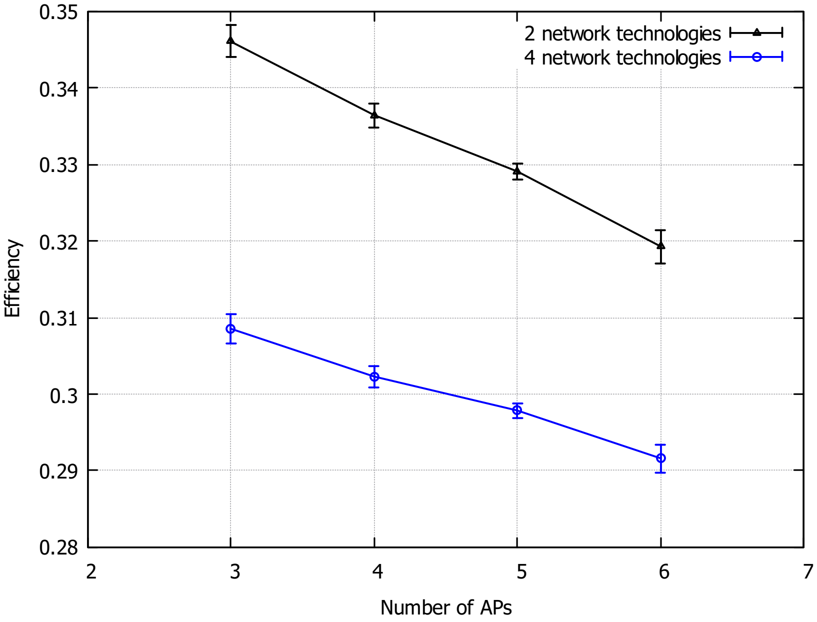


Figure 6.8: Efficiency vs access points

	Betweenness					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.06812	0.007	0.06574	0.00786	0.06348	0.00655
4 APs	0.06285	0.00382	0.06045	0.00323	0.05868	0.00246
5 APs	0.05776	0.0019	0.05583	0.00187	0.05435	0.00178
6 APs	0.05433	0.00431	0.05276	0.00466	0.05123	0.0039

Table 6.3: Betweenness centrality metrics for topologies

all topologies when the number of cell phones increases. Moreover, though the overall betweenness values for all topologies is small, we observe a distinct difference between three-node-backbone topologies with two network technologies, compared with the rest of the topologies. We can also observe that the slope in the betweenness plot for the three-node-backbone topologies with two network technologies is steeper compared with other topologies in Figure 6.9. We should emphasize that the values in Table 6.3 and Figure 6.9 indicate the mean betweenness for all nodes. The growth of the number of nodes in the backbones increases the probability of establishing new shortest paths between each node pair resulting in decreasing the mean betweenness value. However, for a fixed number of cell phones, the large values of betweenness belong to the three-node-backbone topologies due to the fewer number of nodes in the networks compared with the rest of the topologies. In other words, increasing the number of network technologies decreases the betweenness values due to integrating more nodes. Regardless of the number of network technologies, increasing the number of cell phones has a negligible effect on the betweenness values.

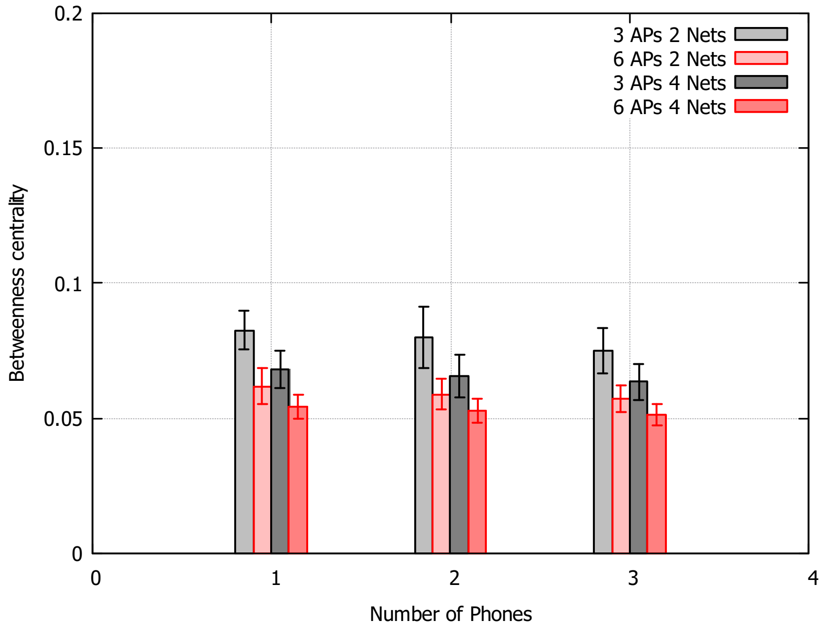


Figure 6.9: Betweenness results for topologies with two and four network technologies

Table 6.4 shows the closeness values for all the topologies per number of cell phones. Closeness shows the average shortest path values from any node v_i to other nodes. The larger value of closeness indicates that the nodes are closer to each other. The values in Table 6.4 indicate that adding a new node to the backbone or integrating a new cell phone has a negligible effect on the closeness values. However, reducing the number of network technologies illustrated in Figure 6.10 changes closeness values. The distance between the black plots and the distance between the red plots for each corresponding backbone in Figure 6.10 shows the increment of the closeness values due to changes in the number of network technologies.

	Closeness					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.25623	0.0209	0.25892	0.0243	0.26138	0.02164
4 APs	0.25176	0.0117	0.25531	0.01049	0.25706	0.00838
5 APs	0.24969	0.00604	0.25256	0.00623	0.25431	0.0061
6 APs	0.24477	0.01418	0.24729	0.01547	0.24947	0.01383

Table 6.4: Closeness centrality metrics for topologies

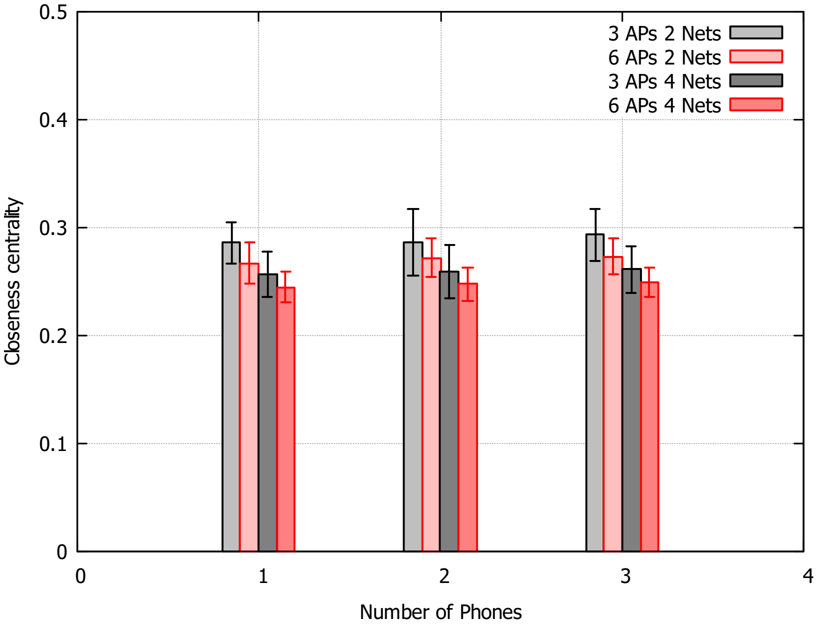


Figure 6.10: closeness results for topologies with two and four network technologies

Table 6.5 shows the degree centrality values for all topologies per number of cell phones. Degree centrality values are relatively small for all topologies. The results in Table 6.5 indicates that the three-node-backbone topologies have the highest and six-node-backbone topologies have the lowest values. Integrated cell phones change the degree centrality values very slightly since cell phones have degree 2 in the topologies. The reason for very low mean centrality values is the number of edge nodes with degree 1. All nodes in a star topology except the central node have degree 1. Several star topologies have been integrated in each network resulting in low mean degree values. Adding more network technologies with a star topology reduces degree centrality more.

In contrast, removing technologies with a star topology increases mean degree centrality. Figure 6.11 shows changes in the mean centrality values. Furthermore, the number of wireless stations connected to the backbone nodes of the three-node-backbone topologies is fewer than other topologies resulting in increasing the mean degree centrality values. Figure 6.11 also shows that adding one extra cell phone changes the mean centrality values slightly while adding a network such as a star with low degree centrality values changes the mean centrality values noticeably.

	Degree centrality					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.04764	0.0014	0.04743	0.00134	0.0472	0.0013
4 APs	0.04314	0.00065	0.04296	0.00063	0.04277	0.0006
5 APs	0.03958	0.00039	0.03942	0.00037	0.03926	0.00037
6 APs	0.0364	0.00083	0.03627	0.0008	0.03613	0.00078

Table 6.5: Degree centrality metrics for topologies

Table 6.6 presents the results of the edge betweenness centrality for all topologies per number of cell phones. Similar to the betweenness centrality results, reducing the number of network technologies increases the centrality values. Furthermore, adding more phones to the networks decreases the centrality values as well.

We observe larger variance for the three-node-backbone topologies both in Table 6.6 and Figure 6.12 compared with the rest of results. Figure 6.12 illustrates the results between two and four network technologies. The reason for larger variance is that there are only two possible connected solutions for the three-node-backbone topologies, linear and the complete graph. The intermediate edge betweenness values show that there is

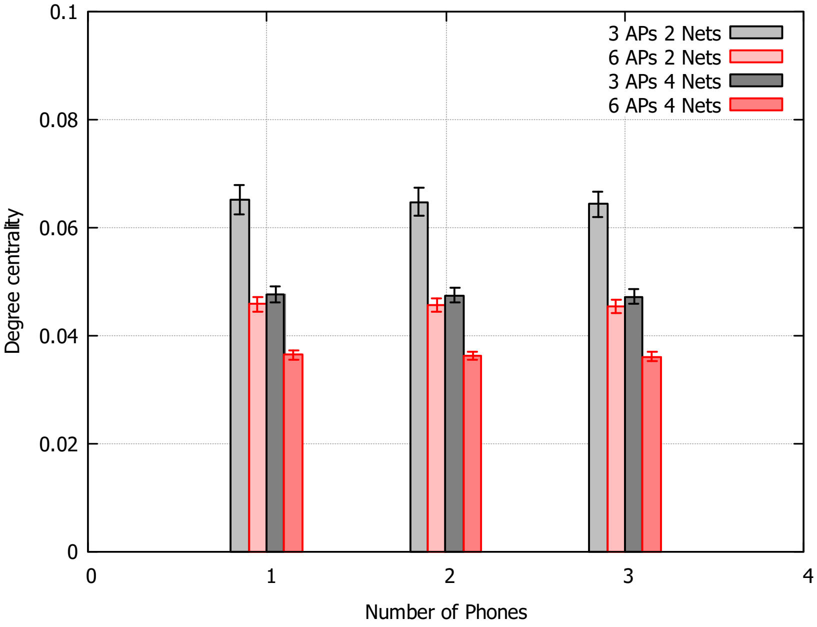


Figure 6.11: Degree results for topologies with two and four network technologies

a significant dispersion between results obtained from the linear models compared with the complete models resulting in larger variance.

	Edge betweenness					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.07896	0.00844	0.07525	0.0089	0.07181	0.00754
4 APs	0.07247	0.00443	0.06901	0.00376	0.06623	0.00304
5 APs	0.06618	0.00231	0.06337	0.00221	0.06106	0.00207
6 APs	0.062	0.00521	0.05967	0.00538	0.05743	0.0046

Table 6.6: Edge betweenness centrality metrics for topologies

The mean values of eigenvector centrality for all topologies per cell phones are presented in Table 6.7. Similar to the degree centrality results, the number of cell phones does not change the mean values of eigenvector centrality sharply. The amount of change is even slower when the number of nodes on the backbones increases. In addition, the distance between the values of each plot decreases from three-node-backbone to six-node-backbone topologies. The distances between plots in Figure 6.13 are much recognizable when

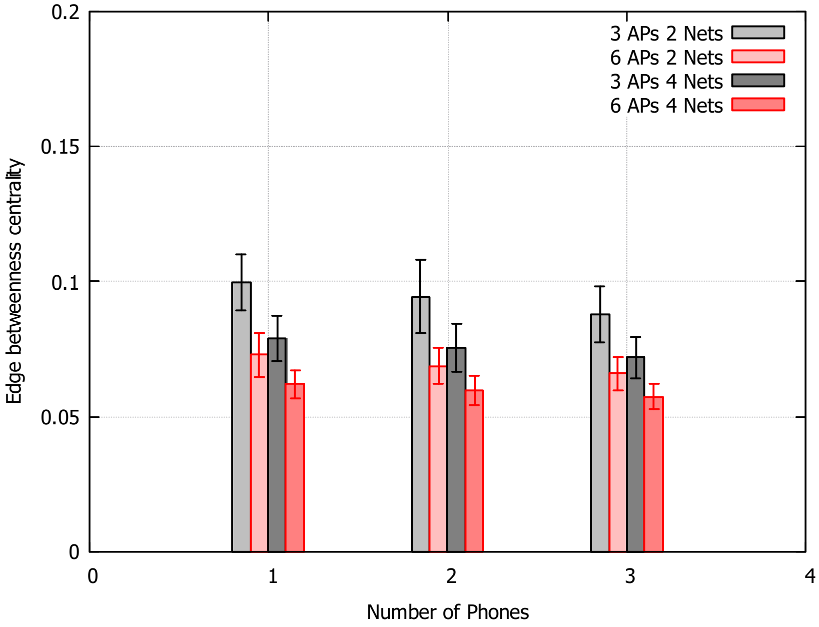


Figure 6.12: Edge betweenness results for topologies with two and four network technologies

the number of network technologies changes. Eigenvector centrality considers a node importance if the node connects to other important nodes. Cell phones in the topologies receive a relatively high eigenvector value because they connect to access points with high degree centrality; however, the assigned eigenvector values to the cell phones cannot be larger than the access points' eigenvectors; because, the access points are connected and each of which has relatively high degree centrality. Therefore, the amount that a single cell phone can contribute to the mean value of eigenvector centrality is not significant. On the other hand, when the number of network technologies decreases, it decreases the number of nodes in the topologies resulting in more significant value for the mean values of eigenvector centrality.

Katz centrality metric is an extension of the eigenvector centrality. The difference is that Katz centrality metric can accept wights for nodes. Table 6.8 presents the value of mean Katz centrality values. A noticeable change between the eigenvector and Katz centrality

	Eigenvector centrality					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.10284	0.0083	0.10208	0.00744	0.10146	0.00731
4 APs	0.09448	0.0035	0.09411	0.00376	0.09357	0.00266
5 APs	0.08758	0.0017	0.08721	0.0015	0.08714	0.00142
6 APs	0.0852	0.00258	0.08536	0.00302	0.08515	0.00293

Table 6.7: Eigenvector centrality metrics for models

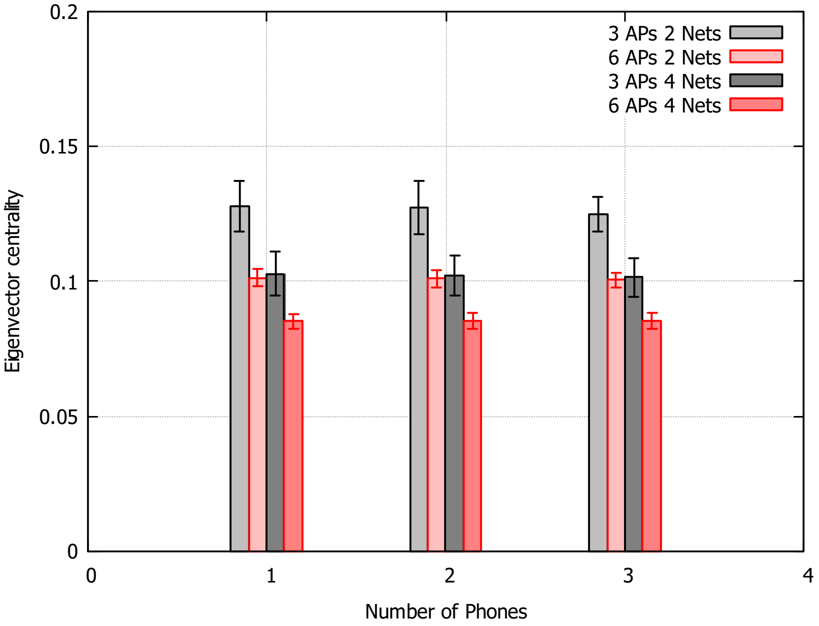


Figure 6.13: Eigenvector results for topologies with two and four network technologies

metric is the larger values for Katz centrality metric. Regardless of this change, the trends of the values in both Table 6.7 and Table 6.8 are identical. There is no significant change when the number of cell phones increases. However, the Katz centrality value for a particular node may be different compared with the eigenvector value of the same node, but the mean values does not reflect such changes.

	Katz					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.14327	0.00101	0.1416	0.00112	0.13998	0.0011
4 APs	0.13574	0.00054	0.13431	0.00054	0.13293	0.0005
5 APs	0.12915	0.00034	0.12793	0.00035	0.12671	0.00035
6 APs	0.12367	0.00074	0.12258	0.00076	0.1215	0.00075

Table 6.8: Katz centrality metric for topologies

6.2.2 Analysis with proposed centrality metrics

The results in Section 6.2.1 show that the typical centrality metrics are not very sensitive to adding a few cell phones to the topologies. The results using the existing metrics also show that distance-based centrality metrics identify important nodes with supporting multiple technologies better compared to degree-based and spectra-based centrality metrics. The results using the existing metrics also show that even distance-based centrality metrics cannot highlight the effect of adding a node supporting multiple technologies. A multi-technology node not only improves path diversity but also can work as a gateway to connect different components of a network. As shown in Section 5.3, targeting multi-technology nodes can disconnect the networks effectively compared to nodes with just high centrality values. Therefore, identifying such nodes to protect the networks and improve resilience is essential.

In this section, we use our proposed degree-based centrality metrics introduced in Section 5.4 for the analysis of the 1500 generated topologies. These new metrics consider the type of edges connected to each node to identify important nodes. In our study, nodes connect with various technologies; therefore, each technology is considered as a particular type for edges.

Edge variant centrality calculates the centrality value of each node proportion to the number of supported technologies. Therefore, the upper bound of edge variant centrality is degree centrality when a node supports all technologies in a system. As a result, the importance of a node decreases proportionally to the number of technologies not supported. The exponent α can increase or decrease the effect of the proportion s_i/t in the following equation:

$$d_{ei} = d_i \times (s_i/t)^{\alpha} \tag{6.1}$$

When $\alpha = 0$ Equation 6.1 returns degree centrality. Therefore, in order to consider various technologies supported by each node, α should be greater than zero. When $0 < \alpha \leq 1$ the value of $(s_i/t)^{\alpha}$ is in $[s_i/t, 1)$. For $\alpha > 1$, $(s_i/t)^{\alpha}$ is in $(0, s_i/t)$ when $\alpha \to \infty$.

If a system has only a few nodes supporting multiple technologies, choosing the α value closer to zero amplifies the importance of multi-technologies nodes. In addition, in a system containing nodes with high degree centrality supporting single technologies and nodes with low degree centrality and a few supporting multi-technologies, choosing α closer to zero decreases the importance of high-degree nodes with a single technology.

Figure 6.14 illustrates the values of edge variant metric for two network technology with three-node-backbone topologies when α varies. The plot corresponding $\alpha = 0$ shows degree value centrality. Although all bars for a particular value of α in Figure 6.14 look like having the same height, they are changing slightly. We observe these changes in Table 6.9. Furthermore, the distances between plots illustrate the effect of factor $(s_i/t)^{\alpha}$.

Table 6.9 presents the results of the edge variant metric for all topologies per number of cell phones. In contrast to the degree centrality results in Table 6.5 and Figure 6.11, the values in Table 6.9 are increasing, although the changes are not significant. The reason is that the effect of cell phones with two different types of links is strengthened with this metric. Figure 6.15 illustrates the edge variant results for three- and six-backbone topologies with two and four network technologies.

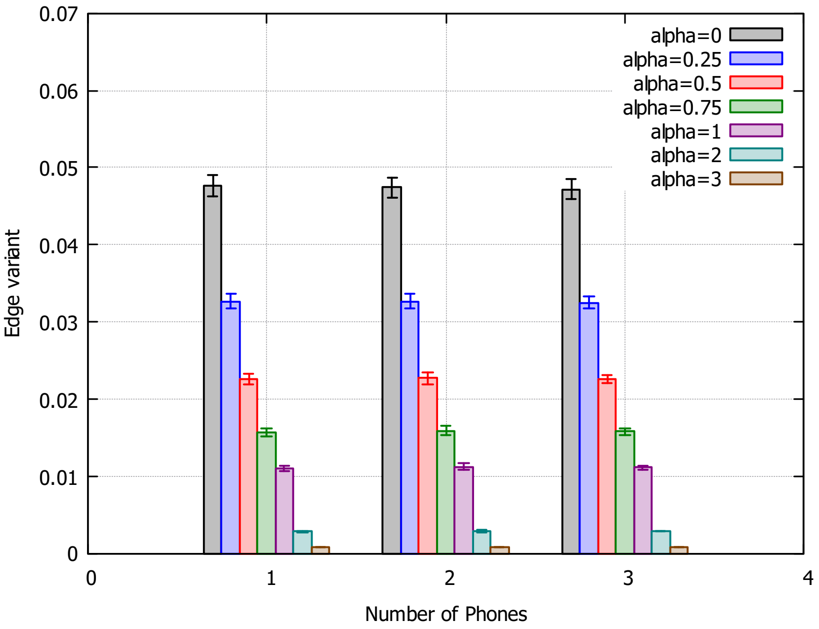


Figure 6.14: Edge variant for 3 node backbone, 2 network technologies

	Edge variant					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.00289	0.00012	0.00298	0.00014	0.00296	5E-05
4 APs	0.00256	4E-05	0.00258	2E-05	0.00266	6E-05
5 APs	0.00225	3E-05	0.00232	4E-05	0.00234	5E-05
6 APs	0.00201	0.00007	0.00205	4E-05	0.00207	5E-05

Table 6.9: Edge variant metric with $\alpha = 2$ for topologies

As explained in Section 5.4, *boosted variant centrality* is the sum of the degree centrality and *edge variant centrality* as:

$$d_{bi} = d_i + d_i \times (s_i/t)^{\alpha} \tag{6.2}$$

In Equation 6.2, when $\alpha = 0$, $d_{bi} = 2 \times d_i$ and it does not consider edge variations. When $0 < \alpha \leq 1$, d_{bi} is in $[d_i \times (1 + (s_i/t)^{\alpha}), 2d_i)$. For $\alpha > 1$, when $\alpha \to \infty$, then $d_{bi} \to d_i$, which is degree centrality. Therefore, the upper bound and lower bound of boosted edge variant is $2d_i$ and d_i, respectively.

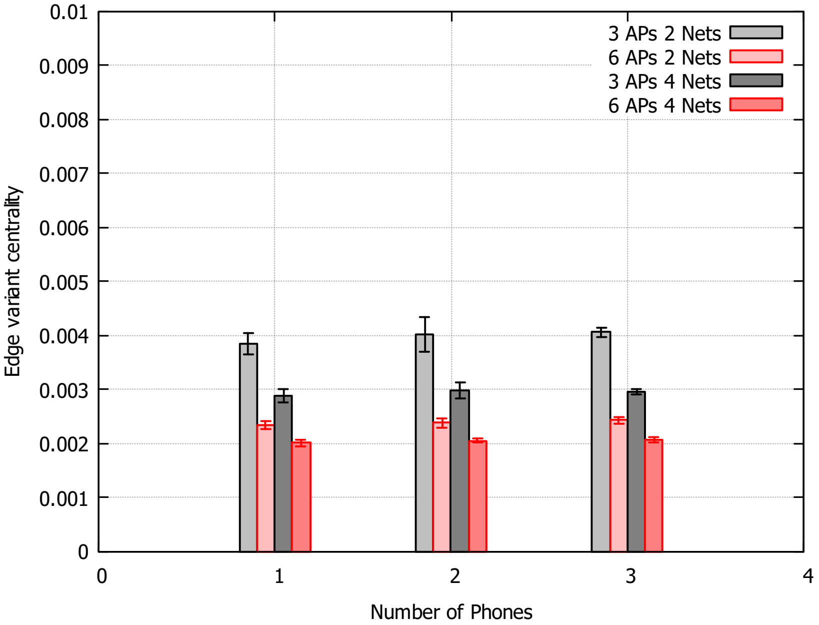


Figure 6.15: Edge variant results for $\alpha = 2$

Figure 6.16 illustrates the values of boosted edge variant metric for two network technologies with three-node-backbone topologies when α varies. Boosted edge variant returns relatively larger values compared with edge variant. Boosted edge variant is helpful when the difference between the largest and smallest degree centrality in a system is relatively high. In this case, the values of normalized degree centrality would be small, losing accuracy for further calculation. The comparison of Figures 6.14 and 6.16 shows improvement in values of boosted edge variant compared with edge variant.

Table 6.10 presents the values of the boosted variant metric for all topologies per cell phones. Observed in Tables 6.5 and 6.9, the degree centrality values are decreasing while the edge variant centrality values are increasing per number of cell phones. The sum of these values in the boosted variant centrality has a decreasing trend. The same result is observed in Figure 6.17 in which three-node-backbone and six-node-backbone topologies with two and four integrated network technologies are compared. The results in Table 6.10 explains that the mean number of nodes supporting multiple technologies in

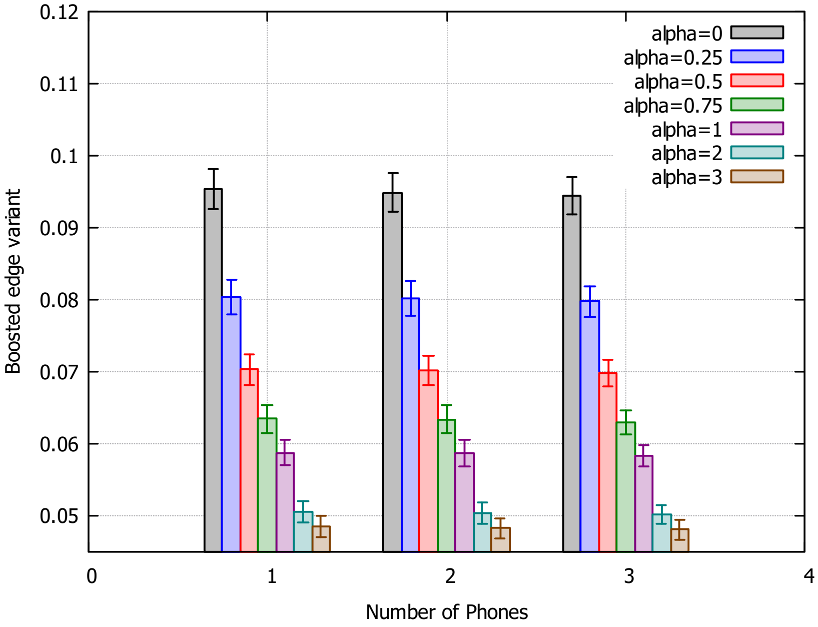


Figure 6.16: Boosted edge variant for 3 node backbone and 2 network technologies

the topologies are too scarce to compete with the decreasing result of degree centrality. In other words, most nodes in the topologies do not support multiple technologies. However, if we calculate lines with the values in Table 6.10, the amount of negative slops of lines for four-, five-, and six-node-backbone topologies are reducing. Two factors affect the negative slops of the calculated lines. The first and the most important factor is increasing degree centrality values for the backbone nodes, and the second factor is the new mesh network technology in these networks in which most of the nodes have degree 2. Furthermore, Figure 6.17 shows that reducing the number of network technologies increases the metric values per cell phone.

Exponential technology variant centrality metric, proposed in Section 5.4, amplifies the degree value of multi-technologies nodes based on the number of technologies they support and the value of exponent α. Compared with two centrality variants, edge variant and boosted edge variant, exponential technology variant is more aggressively amplifies the effect of multi-technology nodes. As shown in Equation 6.3, exponential technology

	Boosted variant					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	$\pm\Delta$	Mean	$\pm\Delta$	Mean	$\pm\Delta$
3 APs	0.05053	0.00152	0.05041	0.00151	0.05014	0.00135
4 APs	0.0457	0.00068	0.04554	0.00065	0.04543	0.00063
5 APs	0.04183	0.00041	0.04174	0.00041	0.04159	0.0004
6 APs	0.0384	0.00088	0.03832	0.00085	0.0382	0.00082

Table 6.10: Boosted variant metric with $\alpha = 2$ for topologies

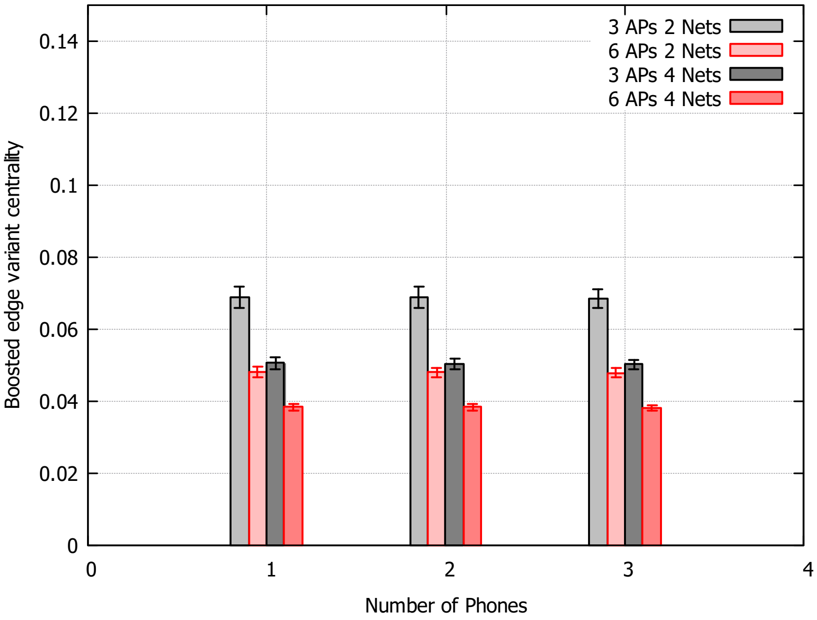


Figure 6.17: Boosted edge variant results with $\alpha = 2$

variant does not amplify the degree centrality values of nodes with a single technology.

$$d_{ei} = d_i \times (s_i)^{\alpha} \tag{6.3}$$

Another advantage of exponential technology variant is that this metric does not need to know the total number of network technologies in the system. The lower bound of exponential technology variant is degree value when $\alpha = 0$.

Figure 6.18 illustrates the comparison between the centrality values of edge variant, boosted edge variant, and exponential technology variant for $\alpha = 0.5$. The figure shows the centrality results for all topologies with the various number of nodes in the backbone. As observed, exponential technology variant returns the highest value among all compared variants.

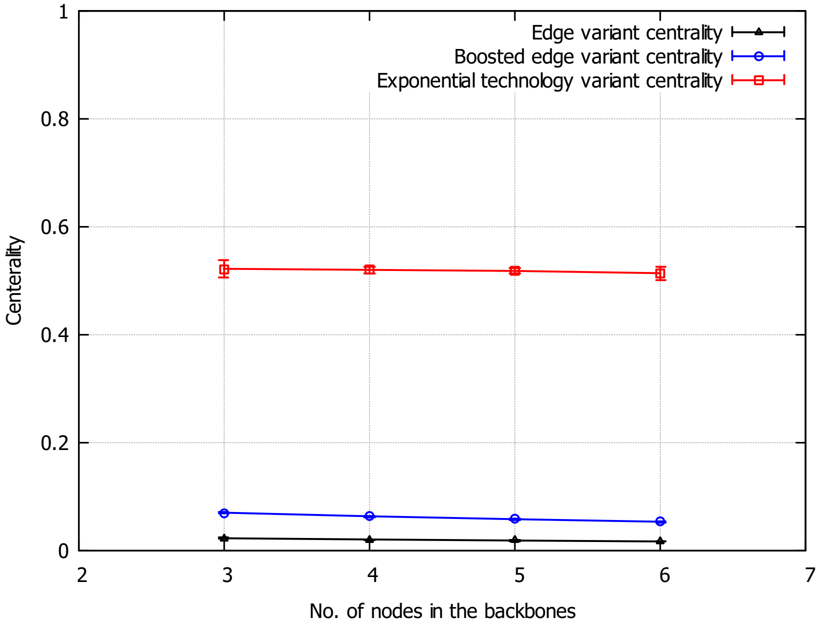


Figure 6.18: Variant results per number of nodes in the backbones for $\alpha = 0.5$

Figure 6.19 illustrates the results of exponential technology variant for topologies with three nodes in the backbone with two network technologies when the number of cell phones varies. The figure shows the results for different α values.

Table 6.11 shows the numerical results for the topologies with the various number of nodes in the backbone and four network technologies when the number of cell phones varies. The values in the table show an incremental trend when the number of cell phone increases. Though in conventional centrality metrics such as degree centrality, adding one low-degree node cannot change the centrality value, especially in a large network, this metric can highlight such changes if the node support multi-technology connections.

Figure 6.20 illustrates the effect of adding new cell phones as multi-technology nodes, related to the number of network technologies in the topologies. In Figure 6.20, three-

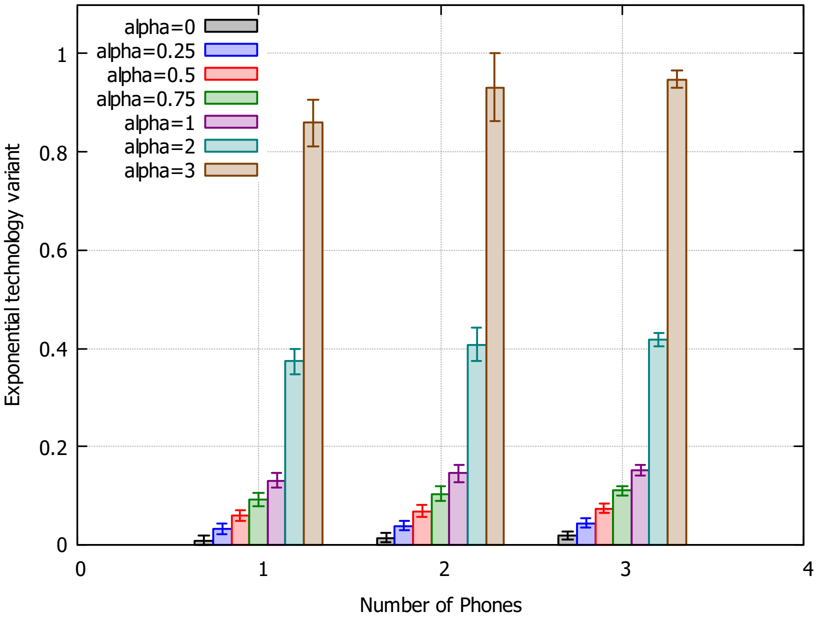


Figure 6.19: Exponential technology variant, 3 node backbone, 2 network technologies

node-backbone topologies are compared with six-node-backbone topologies with two and four network technologies. Similar to other centrality metrics, edge variant and boosted edge variant, three-node-backbone topologies have higher centrality values compared with six-node-backbone topologies. The reason is that, these new centrality metrics are sensitive to nodes supporting multi-technologies. When a new network technology is added to a topology, most of the nodes except the gateway support one technologies. Considering six-node-backbone topologies have more nodes compared with three-node-backbone topologies, the mean results are smaller. However, the relatively higher mean results calculated by exponential technology variant compared with degree centrality show that exponential variant is sensitive to multi-technology nodes.

Table 6.12 shows the result of the removed-degree-one metric explained in Section 5.4 for all topologies per cell phones. This metric does not consider the type of links; however, it removes any node with degree 1 that increases the importance of their neighbors. This process also reduces the importance of a neighbor node connected to nodes with degree

	Exponential technology variant					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.1915744	0.0072508	0.2012916	0.0097612	0.2041224	0.0036012
4 APs	0.1880156	0.002314	0.1932376	0.0019356	0.2030668	0.0043644
5 APs	0.1815672	0.0024612	0.190178	0.0031776	0.1950564	0.0036164
6 APs	0.175882	0.0056236	0.1832804	0.0040952	0.187698	0.0042172

Table 6.11: Exponential technology variant metric with $\alpha = 2$ for topologies

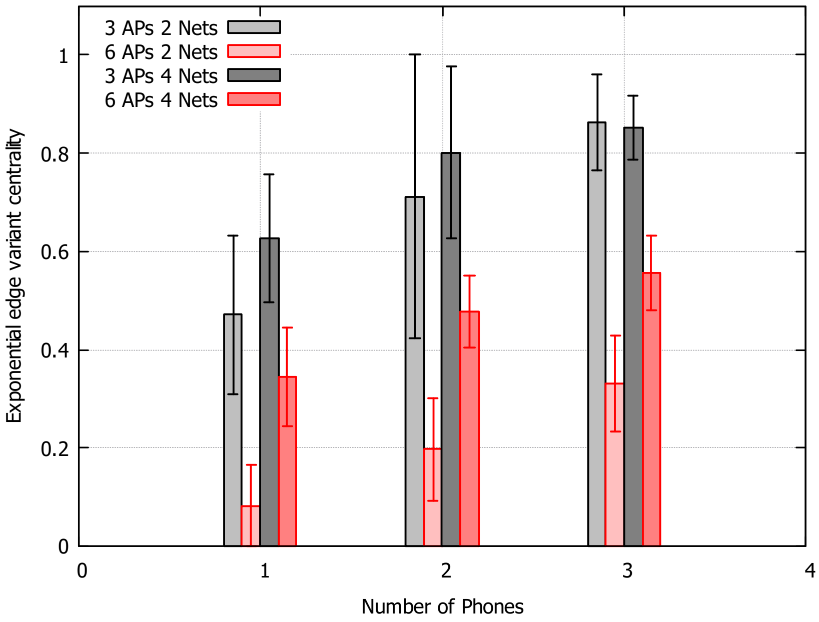


Figure 6.20: Exponential technology variant results with $\alpha = 2$

one. The phones in the topologies have degree two. Therefore, cell phones do not affect the process. However, integrating a new phone to a topology increases the number of nodes resulting in decreasing the metric values in Table 6.12.

Figure 6.21 illustrates the comparison results between three-node-backbone and six-node-backbone topologies with two and four network technologies. Since the number of nodes in the three-node-backbone topologies is lower than to other topologies, the three-node-backbone topologies have larger metric values compared with other topologies.

Using mean values in our calculation helps us to summarize the results since that are

	Removed degree 1					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.08974	0.00433	0.08862	0.00402	0.08744	0.00374
4 APs	0.08783	0.00228	0.0867	0.00212	0.08552	0.00198
5 APs	0.08662	0.00153	0.08544	0.00142	0.08423	0.00134
6 APs	0.08468	0.00362	0.08351	0.00338	0.08233	0.00317

Table 6.12: Removed-degree-one metric for topologies

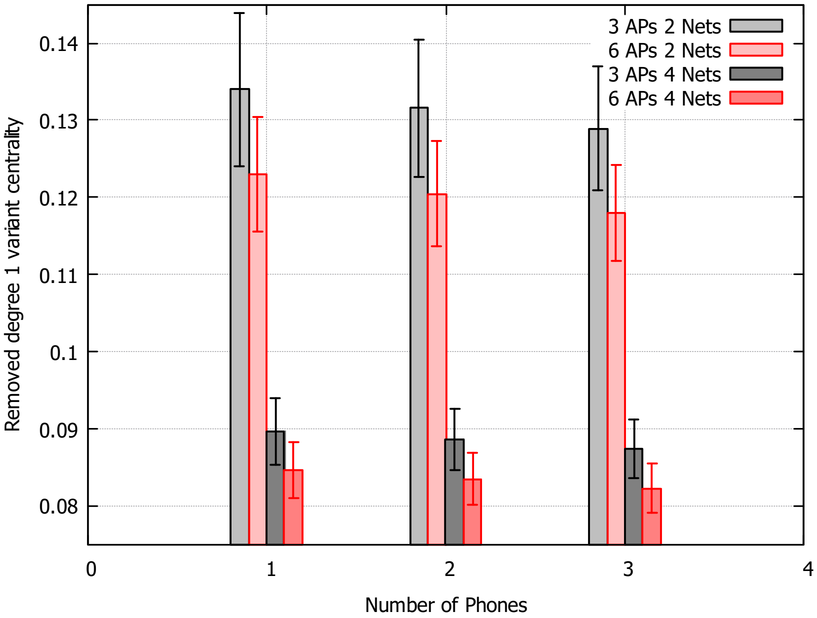


Figure 6.21: Removed-degree-one variant results

many nodes in each topology, especially when the number of nodes in the backbone and the network technologies increases. Furthermore, obtaining higher mean values in the figures and tables of Section 6.2.2 shows improvement in identifying nodes supporting multiple technologies such as phones. However, the mean values do not show the changes in the order of important nodes with each centrality metric. Tables 6.13 to 6.16 present the top 10 nodes measured by each metric. Tables 6.13 to 6.14 show the results of conventional and proposed metrics for three-node-backbone topologies while Tables 6.15 to 6.16 show the corresponding results for the six-node-backbone topologies. We move

	Centrality metrics					
Node's rank	betweenness	closeness	degree	eigenvector	katz	removed 1
1	AP2	AP2	AP1	AP2	AP1	AP1
2	AP1	AP1	AP2	AP1	AP2	m1-0
3	AP3	AP3	AP3	AP3	AP3	m2-0
4	m2-0	m1-0	BT1-0	m1-0	BT1-0	AP2
5	m1-0	m2-0	BT2-0	BT1-0	BT2-0	m1-1
6	BT2-0	BT1-0	m1-0	m2-0	m1-0	m2-1
7	BT1-0	BT2-0	m2-0	BT2-0	m2-0	AP3
8	m2-1	Phone1	m1-1	Phone1	m1-1	EPC1
9	m1-1	5	m2-1	Phone2	m2-1	m2-2
10	m2-7	RBB	EPC1	RBB	EPC1	m2-3

Table 6.13: Top 10 nodes per centrality metrics – three-node backbone, 3 phones

the results of removed degree 1 metric to the tables containing the results of conventional metrics. The reason is that removed degree 1 metric does not consider type of links.

Comparing the results in Tables 6.14 and 6.16 with corresponding results in Tables 6.13 and 6.15 shows that the order of nodes with supporting multiple technologies is changing. The changes in Table 6.15 is less obvious in the top 10 nodes, since the six APs with high degree values occupy six top places in the rank. However, checking the rank of other nodes in six-node-backbone topologies shows that nodes with multiple technologies such as EPC1 and Phones are moving toward the top of the rank.

Conventional centrality metrics consider a network as a single layer graph. However, as explained in Chapter 5, multilayer graphs can show networks with supporting multiple technologies better than a single-layer graph. This is because each network technology is represented explicitly in multilayer graphs. In such representations, nodes connecting layers are better highlighted compared to a single layer graph representation. Moreover, when the functionality of nodes is considered in topologies as proposed here, the importance of nodes connecting layers is observed. The result of studying over 1500 topologies in this Chapter shows that the conventional centrality metrics studied here are unable

	Varinat metrics								
	edge variant			boosted variant			exponential variant		
Node's rank	0.25	0.75	2	0.25	0.75	2	0.25	0.75	2
1	AP1	AP1	AP1	AP1	AP1	AP1	AP1	AP1	AP1
2	AP3	AP3	AP3	AP3	AP3	AP3	AP3	AP3	AP3
3	AP2	AP2	BT1-0	AP2	AP2	AP2	AP2	AP2	BT1-0
4	BT1-0	BT1-0	BT2-0	BT1-0	BT1-0	BT1-0	BT1-0	BT1-0	BT2-0
5	BT2-0	BT2-0	m1-0	BT2-0	BT2-0	BT2-0	BT2-0	BT2-0	m1-0
6	m1-0	m1-0	m2-0	m1-0	m1-0	m1-0	m1-0	m1-0	m2-0
7	m2-0	m2-0	EPC1	m2-0	m2-0	m2-0	m2-0	m2-0	EPC1
8	EPC1	EPC1	AP2	EPC1	EPC1	EPC1	EPC1	EPC1	AP2
9	m1-1	RBB	RBB	m1-1	m1-1	m1-1	m1-1	RBB	RBB
10	m2-1	Phone1	Phone1	m2-1	m2-1	m2-1	m2-1	Phone1	Phone1

Table 6.14: Top 10 nodes per variant metrics – three-node backbone, 3 phones

	Metrics					
Node's rank	betweenness	closeness	degree	eigenvector	katz	removed 1
1	AP2	AP2	AP1	AP2	AP2	AP1
2	AP1	AP4	AP2	AP1	AP1	AP2
3	AP5	AP5	AP5	AP5	AP5	m1-0
4	AP4	AP3	AP4	AP3	AP4	m2-0
5	AP3	AP1	AP3	AP4	AP3	AP5
6	AP6	AP6	AP6	AP6	AP6	m2-1
7	m1-0	m2-0	BT1-0	m2-0	BT1-0	m1-1
8	m2-0	m1-0	BT2-0	BT1-0	BT2-0	AP4
9	BT2-0	BT1-0	m1-0	BT2-0	m2-0	AP3
10	BT1-0	BT2-0	m2-0	m1-0	m2-0	AP6

Table 6.15: Top 10 nodes per centrality metrics – six-node backbone, 3 phones

to identify the correct nodes, while the results of the proposed metrics are better able to identify critical nodes in a multi technology network. Tables 6.14 and 6.16 explicitly confirm improvement in the process of identifying nodes with multiple technologies.

6.3 Summary

Smart home networks are set up by users who usually do not have technical knowledge of networking. In this chapter, we generated 1500 smart home topologies randomly

	Varinat metrics								
	edge variant			boosted variant			exponential variant		
Node's rank	0.25	0.75	2	0.25	0.75	2	0.25	0.75	2
1	AP1	AP1	AP1	AP1	AP1	AP1	AP1	AP1	AP1
2	AP2	AP2	BT1-0	AP2	AP2	AP2	AP2	AP2	BT1-0
3	AP5	AP5	BT2-0	AP5	AP5	AP5	AP5	AP5	BT2-0
4	AP4	AP3	m1-0	AP4	AP4	AP4	AP4	AP3	m1-0
5	AP3	BT1-0	m2-0	AP3	AP3	AP3	AP3	BT1-0	m2-0
6	AP6	BT2-0	EPC1	AP6	AP6	AP6	AP6	BT2-0	EPC1
7	BT1-0	AP4	AP5	BT1-0	BT1-0	BT1-0	BT1-0	AP4	AP5
8	BT2-0	AP6	AP2	BT2-0	BT2-0	BT2-0	BT2-0	AP6	AP2
9	m1-0	m1-0	AP3	m1-0	m1-0	m1-0	m1-0	m1-0	AP3
10	m2-0	m2-0	AP6	m2-0	m2-0	m2-0	m2-0	m2-0	AP6

Table 6.16: Top 10 nodes per variant metrics – six-node backbone, 3 phones

with the various number of backbone nodes. Then, we integrated new cell phones to the topologies as nodes to provide diverse paths to the Internet to improve resilience. We analyzed the topologies with conventional and our proposed centrality metrics. We observed that most degree-based centrality metrics such as degree centrality do not reflect the effect of adding one node such as a cell phone, though they are significant to improve resilience. On the other hand, the results from new proposed metrics, i.e., edge variant, boosted edge variant, and exponential technology variant show the changes adequately in Tables 6.9 to 6.11. The higher calculated mean centrality values compared to the corresponding degree centrality values confirm improvement in the process of identifying phones supporting multiple technologies.

The relatively low values of the mean calculated conventional metrics indicate that most centrality metrics consider the smart home topologies less important on average since most nodes receive low values for centrality metrics. However, smart environments, such as smart homes, contain many edge nodes that collect data, and some of them have an important role.

Page left intentionally blank.

Chapter 7

Conclusion and Future Work

In this section, we summarize the result of our study presented in this dissertation. We divide this chapter to Section 7.1 for concluding our study and Section 7.2 for future work.

7.1 Conclusion and Summary of the Results

Internet of things (IoT) has changed the structure of the edge networks by increasing the number of nodes and diversifying the number of technologies present as well as the topology of networks. These edge networks are now commonly referred to as smart homes and smart cities to show the integration of IoT. In this dissertation, we study heterogeneity and diversity of technologies on network resilience.

In the first step, we study the characteristics of typical network technologies used in smart home networks. Then, we introduce a reference model as a general instance following by an abstract model for smart home networks. Our abstract model shows the general structure, connectivity, and path diversity in smart home networks. Moreover, we use a graph representation of each smart home instance derived from the abstract model for further analysis. During the process of graph representation, we encounter new problems.

First, we realize that a simple graph representation does not express all characteristics of a multi-technology network, such as smart homes. Therefore, we choose an edge-colored graph to show link variants adequately. We also find out the way network technologies are connected to the home backbone has a substantial effect on the resilience of the network. To understand the connectivity of network technologies, we introduce our technology interdependence graph. This graph shows how various technologies are connected in a high-level representation.

We use graph centrality metrics to study smart home resilience. Centrality metrics can identify the importance of the nodes in a particular graph based on the topological structure of a network. We measure several centrality metrics on two smart home instances with different size and during the network failure. Then, we compare the results with two baseline topologies, star and mesh. The main result is that among centrality metrics under study many of them cannot identify important nodes in a multi-technology network such as a smart home adequately. Degree-based centrality metrics fail because these metrics cannot identify the type of network connection. We understand that a node with supporting multiple network technologies has a more important role compared with a similar node supporting only one technology. Distance-based centrality metrics fail because they cannot identify the important nodes at the edge of the network when the functionality of nodes are involved. For example, a vital sensor such as a smoke detector usually installed at the edge of the network. While such sensors are important, they receive lower centrality values compared with internal nodes, because they are usually end points on shortest paths and other paths do not pass over them.

Failure of centrality metrics to identify important nodes in multi-technology networks motivates us to propose four new degree-based centrality metrics. We compare the results from new metrics with typical centrality metrics under study over 1500 smart home instances. The results show that the new metrics can identify nodes regarding their functionality; while obtaining such results are not possible with typical centrality metrics. We use our new metrics in a targeted attack study and compare the results with typical centrality metrics under the study. The results show that utilizing new metrics can disconnect a smart home network through the node importance faster compared with typical centrality metrics.

Nodes supporting multiple technologies can provide path redundancy through the diversity of technologies. Such nodes have important roles in increasing the resilience of a network. For example, a cellphone supporting WLAN, LTE, and Bluetooth have such a characteristic. However, when such nodes are integrated into a network with low-degree connectivity, they cannot be identified as important nodes with typical centrality metrics. In contrast, our new centrality metrics are sensitive to multi-technology nodes compared with conventional centrality metrics. The result of the study over 1500 smart home instances confirms this claim.

We discovered that a single-layer graph cannot highlight the structure and connectivity of various technologies in a multi-technology network. We then determined that a multilayer framework can represent the detail characteristics of a multi-technology network more comprehensively compared with single-layer graphs. Our proposed multilayer framework can represent the topology of each network technology in a separate layer and the connectivity to other networks. This framework can be used as the first step to model smart cities. In addition, this framework can represent temporal networks.

7.2 Future Work

In this section, we introduce some of the problems we encounter during our study, which they need further attention as future work.

During our study and with the help of our technology interdependence graph, we realize that connecting non-IP technologies through a gateway creates a point of failure in the network. Even a well-designed network with capable network technologies and a mesh topology such as ZigBee and Z-Wave suffer from this deficiency. This problem makes any smart home network to a single-connected network even if the backbone of such networks and topology of each network technology are engineered. Designing new protocols for conventional network technologies such as ZigBee is necessary to connect such a network technology to the home backbone with a redundant path. Such protocols are available for IP networks to prevent network partitioning during a router or link failure.

Designing new spectra and distance-based centrality metrics can help to identify important nodes based on factors other than nodes degree. While each type of centrality metrics provide various understanding about the structure of the networks, centrality metrics based on distance and spectra sensitive to network functionality and link variance should be available for multi-technology networks.

Although smart home networks support multiple technologies and help us to understand the complexity of such systems, they are small in size and they cannot show the complexity of a large network through the increasing number of nodes, technologies, and connectivity. A similar study on more extensive networks such as smart cities is beneficial to increase our insight about multi-technology networks.

Though nodes with supporting multiple technologies can establish different types of connections, many of such links are not connected all the time. For example, When a cellphone in a home connected to the Internet through the home's WiFi network, the cellphone does not use its LTE connection at the same time. Study multi-technology networks with temporal multilayer graphs give us insight for network resilience during failures when other available technologies are activated.

In addition to typical factors such as topology to improve network resilience, the technologies available during the failure is a new factor involved in multi-technology networks. Considering which technologies are available during a network failure and what type of topology and characteristics they can provide will have an important effect on network resilience.

Many IoT services are cloud-based. This characteristic involves other hard to control network features such as delay or quality of service on the path from edge networks to the cloud. Study on the integration of other technologies such as fog computing and software-defined networking (SDN) and their effects on network resilience is another topic for future work.

While using multiple technologies in networks can improve resilience through heterogeneity, diversity of technologies, and path redundancy, they provide larger attack vectors for the adversaries. Security attacks such as Mirai botnet [128] use IoT end devices to initiate DDoS attacks. Improving security in multi-technology networks through the study of the traffic pattern and integrating technologies such as SDN to reroute the malicious traffic during an incident improves the resilience of networks. In addition, a study of attack penetrations to various technologies provides insight into the combination of technologies that should be considered for a particular network.

Page left intentionally blank.

Bibliography

[1] IEEE. IEEE standard for low-rate wireless networks. *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pages 1–709, April 2016.

[2] Zigbee Alliance. ZigBee IP Specification. `http://www.zigbee.org/download/standard-zigbee-ip-specification/`, March 2014.

[3] IEEE. IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 15.1a: Wireless medium access control (mac) and physical layer (phy) specifications for wireless personal area networks (wpan). *IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002)*, pages 1–700, June 2005.

[4] K. Townsend, R. Davidson, and C. Cufí. *Getting Started with Bluetooth Low Energy: Tools and Techniques for Low-Power Networking.* EBSCOhost ebooks online. O'Reilly, 2014.

[5] Dynastream Innovations. ANT message protocol and usage. Online, 2017.

[6] ITU. ITU, SERIES G:series g: Transmission systems and media, digital systems and networks, access networks – in premises networks. `https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12399`, February 2012.

[7] Jean-Jacques Deslise. What's the difference between ieee 802.11af and 802.11ah? http://mwrf.com/datasheet/what-s-difference-between-ieee-80211af-and-80211ah, 2015.

[8] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke. IEEE 802.11s: The WLAN mesh standard. *IEEE Wireless Communications*, 17(1):104–111, February 2010.

[9] LoRa Alliance Technical Marking Workgroup. What is LoRaWAN. https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf, November 2015.

[10] LoRa Alliance. LoRaWAN specification. https://www.lora-alliance.org/For-Developers/LoRaWANDevelopers, 2016.

[11] JC. Zuniga and B. Ponsard. SigFox system description. https://tools.ietf.org/html/draft-zuniga-lpwan-sigfox-system-description-01, October 2016.

[12] Peter R. Egli. LPWAN: Overview of Emerging Technologies for Low Power Wide Area Networks in Internet of Things and M2M Scenarios. http://www.slideshare.net/PeterREgli/lpwan, 2015.

[13] Roberto Minerva, Abyi Biru, and Domenico Rotondi. Toward a definition of the Internet of Things (IoT). https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf, May 2015.

[14] ITU. Overview of the Internet of Things. https://www.itu.int/rec/T-REC-Y.2060-201206-I, June 2012.

[15] Joachim W. Walewski. Internet-of-Things Architecture IoT-A. `http://www.meet-iot.eu/deliverables-IOTA/D1_3.pdf`, July 2012.

[16] Cisco. The Internet of Things reference model. `http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf`, 2014.

[17] OpenFog Consortium Architecture Working Group. OpenFog reference architecture for fog computing. `https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf`, 2017.

[18] James P. G. Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, and Paul Smith. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245–1265, 2010.

[19] Wikipedia. Bluetooth. `https://en.wikipedia.org/wiki/Bluetooth#Bluetooth_1.1`, Nov 2015.

[20] Marta Gaia Zanchi. Bluetooth low energy. `http://www.litepoint.com/wp-content/uploads/2014/02/Bluetooth-Low-Energy_WhitePaper.pdf`, 2012.

[21] Chad Boutin. The internet's next big idea: Connecting people, information, and things, 2014.

[22] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[23] Mark Roberti. The history of RFID technology. *RFID Journal*, 2005.

[24] Special report: The internet of things. *The Institute, IEEE*, 2014.

[25] ITU. Terms and definitions for the internet of things. `https://www.itu.int/rec/T-REC-Y.2069-201207-I/en`, July 2012.

[26] David Lake, Ammar Rayes, and Monique Morrow. The internet of things. *The Intrnet Protocol Journal*, 2012.

[27] Egemen K. Çetinkaya, Andrew M. Peck, and James P. G. Sterbenz. Flow Robustness of Multilevel Networks. In *Proceedings of the 9th IEEE/IFIP International Conference on the Design of Reliable Communication Networks (DRCN)*, pages 274–281, Budapest, March 2013.

[28] Bob Violino. What is RFID? `http://www.rfidjournal.com/articles/view?1339`, 2005.

[29] Ken Traub, Felice Armenio, Henri Barthel, Paul Dietrich, John Duker, Christian Floerkemeier, John Garrett, Mark Harrison, Bernie Hogan, Jin Mitsugi, Josef Preishuber-Pfluegl, Oleg Ryaboy, Sanjay Sarma, KK Suen, and John Williams. The GS1 EPCglobal architecture framework, 2015.

[30] Belal Alsinglawi, Mahmoud Elkhodr, Quang Vinh Nguyen, Upul Gunawardana, Anthony Maeder, and Simeon J Simoff. Rfid localisation for internet of things smart homes: a survey. *International Journal of Computer Networks and Communications*, 9(1):81–99, 2017.

[31] Son Minh Huynh, David Parry, Alvis Cheuk M Fong, and Jie Tang. Novel rfid and ontology based home localization system for misplaced objects. *IEEE Transactions on Consumer Electronics*, 60(3):402–410, 2014.

[32] Ehsan Ahvar, Nafiseh Daneshgar-Moghaddam, Antonio M Ortiz, Gyu Myoung Lee, and Noel Crespi. On analyzing user location discovery methods in smart homes: A taxonomy and survey. *Journal of Network and Computer Applications*, 76:75–86, 2016.

[33] NFC Forum. NFC and contactless technologies. online, 2015.

[34] ISO. Information technology – telecommunications and information exchange between systems – near field communication – interface and protocol (nfcip-1). ISO/IEC 18092, March 2013.

[35] ISO. Identification cards – contactless integrated circuit cards – proximity cards – part 1: Physical characteristics. ISO/IEC 14443-1, June 2008.

[36] ISO. Identification cards – contactless integrated circuit cards – proximity cards – part 2: Radio frequency power and signal interface. ISO/IEC 14443-2, September 2010.

[37] ISO. Identification cards – contactless integrated circuit cards – proximity cards – part 3: Initialization and anticollision. ISO/IEC 14443-3, April 2011.

[38] ISO. Identification cards – contactless integrated circuit cards – proximity cards – part 4: Transmission protocol. ISO/IEC 14443-4, July 2008.

[39] ZigBee Alliance. Zigbee document 053474r17. *ZigBee Specification, ZigBee Alliance*, 2008.

[40] ZigBee. ZigBee Alliance. `http://www.zigbee.org/`, May 2015.

[41] Bluetooth Special Interest Group. Bluetooth Core Specification v5.0. `https://www.bluetooth.com/specifications/bluetooth-core-specification`, 2016.

[42] Bluetooth Special Interest Group. Bluetooth. `http://www.bluetooth.com/what-is-bluetooth-technology/bluetooth`, 2015.

[43] Dynastream Innovations. ANT website. `https://www.thisisant.com/`, 2017.

[44] Sigma Design. Z-wave. `http://z-wave.sigmadesigns.com/`, 2018.

[45] N. T. Johansen (editor). Z-Wave Plus Device Type Specification. `http://zwavepublic.com/specifications`, 2017.

[46] Niels Thybo Johansen. Z-Wave Plus Role Type Specification. `http://zwavepublic.com/specifications`, 2018.

[47] C. Paetz. *Z-Wave Essentials.* Christian Paetz, 2018.

[48] IEEE. Status of project IEEE 802.11ah. `http://www.ieee802.org/11/Reports/tgah_update.htm`, 2016.

[49] Wi-Fi Alliance. Wi-Fi HaLow. `http://www.wi-fi.org/discover-wi-fi/wi-fi-halow`, 2016.

[50] Weiping Sun, Munhwan Choi, and Sunghyun Choi. Ieee 802.11 ah: A long range 802.11 wlan at sub 1 ghz. *Journal of ICT Standardization*, 1(1):83–108, 2013.

[51] Eric Wong, Matthew Fischer, ChaoChun Wang, Yong Liu, and Minyoung Park. Two-hop relay function. `https://mentor.ieee.org/802.11/dcn/12/11-12-1330-00-00ah-two-hop-relaying.pptx`, 2012.

[52] IEEE. IEEE draft standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. *IEEE P802.11-REVmb/D12, November 2011 (Revision of IEEE Std 802.11-2007, as amended by IEEEs 802.11k-2008, 802.11r-2008, 802.11y-2008, 802.11w-2009, 802.11n-2009, 802.11p-2010, 802.11z-2010, 802.11v-2011, 802.11u-2011, and 802.11s-2011)*, pages 1–2910, Nov 2011.

[53] G. R. Hiertz, S. Max, R. Zhao, D. Denteneer, and L. Berlemann. Principles of IEEE 802.11s. In *2007 16th International Conference on Computer Communications and Networks*, pages 1002–1007, Aug 2007.

[54] S. M. Faccin, C. Wijting, J. Kenckt, and A. Damle. Mesh wlan networks: concept and system design. *IEEE Wireless Communications*, 13(2):10–17, April 2006.

[55] Elizabeth M Royer and Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE personal communications*, 6(2):46–55, 1999.

[56] Charles E Perkins et al. *Ad hoc networking*, volume 1. Addison-wesley Reading, 2001.

[57] C Siva Ram Murthy and BS Manoj. *Ad hoc wireless networks: Architectures and protocols, portable documents*. Pearson education, 2004.

[58] Alliance LoRa. LoRa Alliance. `https://www.lora-alliance.org/What-Is-LoRa/Technology`, 2016.

[59] Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melia-Segui, and Thomas Watteyne. Understanding the limits of LoRaWAN. *IEEE Communications Magazine*, 55(9):34–40, 2017.

[60] Ludovic Le Moan. Sigfox Website. `https://www.sigfox.com/en`, 2017.

[61] LinkLabs. A Comprehensive Look at Low Power, Wide Are Networks for Internet of Things Engineers and Decision Makers. `https://www.link-labs.com/lpwan`, 2016.

[62] ETSI. ETSI Technical Committee on EMC and Radio Spectrum Matters (ERM) TG28 Low Throughput Networks (LTN). https://portal.etsi.org/tb.aspx?tbid=584&SubTB=584, 2015.

[63] ETSI. ETSI EN 300-220: Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz. http://www.etsi.org/deliver/etsi_en/300300_300399/30033002/01.06.01_60/en_30033002v010601p.pdf, May 2016.

[64] 3GPP. Standardization of NB-IoT Completed. http://www.3gpp.org/news-events/3gpp-news/1785-nb_iot_complete, 2016.

[65] Y. P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi. A primer on 3GPP narrowband internet of things. *IEEE Communications Magazine*, 55(3):117–123, March 2017.

[66] GSMA. 3GPP Low Power Wide Area Technologies. https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf, 2016.

[67] Wikipedia. Narrowband IoT. https://en.wikipedia.org/wiki/Narrowband_IoT#cite_ref-8, 2018.

[68] IEEE. IEEE Standard Association, P2413. https://standards.ieee.org/develop/project/2413.html, May 2015.

[69] Cisco. Cisco fog computing: Unleash the power of the internet of things. White paper, 2015.

[70] IETF. The Internet of Things concept and problem statement. http://tools.ietf.org/id/draft-lee-iot-problem-statement-00.txt, 2010.

[71] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, and M. Dohler. Standardized protocol stack for the Internet of (important) Things. *Communications Surveys Tutorials, IEEE*, 15(3):1389–1406, 2013.

[72] Dave Evans. The internet of things - how the next evolution of the internet is changing everything. https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, 2011.

[73] OpenFog Consortium Architecture Working Group. OpenFog. https://www.openfogconsortium.org/, 2017.

[74] Luis M. Vaquero and Luis Rodero-Merino. Finding your way in the fog: Towards a comprehensive definition of fog computing. *SIGCOMM Comput. Commun. Rev.*, 44(5):27–32, October 2014.

[75] Niroshinie Fernando, Seng W. Loke, and Wenny Rahayu. Mobile cloud computing: A survey. *Future Generation Computer Systems*, 29(1):84 – 106, 2013. Including Special section: AIRCC-NetCoM 2009 and Special section: Clouds and Service-Oriented Architectures.

[76] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing*, 13(18):1587–1611, 2013.

[77] Eugene E Marinelli. Hyrax: cloud computing on mobile devices using mapreduce. Technical report, DTIC Document, 2009.

[78] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies. The case for vm-based cloudlets in mobile computing. *IEEE Pervasive Computing*, 8(4):14–23, Oct 2009.

[79] Michael Till Beck, Martin Werner, Sebastian Feld, and S Schimper. Mobile edge computing: A taxonomy. In *Proc. of the Sixth International Conference on Advances in Future Internet*, pages 48–54. IARIA, 2014.

[80] Nokia. Nokia website. `https://networks.nokia.com/solutions/multi-access-edge-computing`, 2017.

[81] James P.G. Sterbenz, Egemen K. Çetinkaya, Mahmood A. Hameed, Abdul Jabbar, Qian Shi, and Justin P. Rohrer. Evaluation of network resilience, survivability, and disruption tolerance: Analysis, topology generation, simulation, and experimentation (invited paper). *Springer Telecommunication Systems*, 52(2):705–736, February 2011. published online 2011.

[82] James P. G. Sterbenz, David Hutchison, Egemen K Çetinkaya, Abdul Jabbar, Justin P Rohrer, Marcus Schöller, and Paul Smith. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245–1265, 2010.

[83] James P. G. Sterbenz and David Hutchison. Resilinets: Multilevel resilient and survivable networking initiative wiki. `http://wiki.ittc.ku.edu/resilinets`, April 2006.

[84] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing. Technical Research Report TR 2004-47, Institute for Systems Research, the University of Maryland, 2004.

[85] Egemen K. Çetinkaya and James P. G. Sterbenz. A Taxonomy of Network Challenges. In *Proceedings of the 9th IEEE/IFIP International Conference on the Design of Reliable Communication Networks (DRCN)*, pages 322–330, Budapest, March 2013.

[86] Ulrik Brandes. *Network analysis: methodological foundations*, volume 3418. Springer Science & Business Media, 2005.

[87] Javier Martın Hernández and Piet Van Mieghem. Classification of graph metrics. *Delft University of Technology: Mekelweg, The Netherlands*, pages 1–20, 2011.

[88] Vito Latora and Massimo Marchiori. Efficient behavior of small-world networks. *Physical review letters*, 87(19):198701, 2001.

[89] Vito Latora and Massimo Marchiori. A measure of centrality based on network efficiency. *New Journal of Physics*, 9(6):188, 2007.

[90] Per Hage and Frank Harary. Eccentricity and centrality in networks. *Social networks*, 17(1):57–63, 1995.

[91] Thomas W Valente and Robert K Foreman. Integration and radiality: Measuring the extent of an individual's connectedness and reachability in a network. *Social networks*, 20(1):89–105, 1998.

[92] Alfonso Shimbel. Structural parameters of communication networks. *The bulletin of mathematical biophysics*, 15(4):501–507, 1953.

[93] Linton C Freeman. A set of measures of centrality based on betweenness. *Sociometry*, pages 35–41, 1977.

[94] Sergei Maslov and Kim Sneppen. Specificity and stability in topology of protein networks. *Science*, 296(5569):910–913, 2002.

[95] Mahdi Jalili, Ali Salehzadeh-Yazdi, Yazdan Asgari, Seyed Shahriar Arab, Marjan Yaghmaie, Ardeshir Ghavamzadeh, and Kamran Alimoghaddam. CentiServer: a comprehensive resource, web-based application and R package for centrality analysis. *PloS one*, 10(11):e0143111, 2015.

[96] Dirk Koschützki, Katharina Anna Lehmann, Leon Peeters, Stefan Richter, Dagmar Tenfelde-Podehl, and Oliver Zlotowski. *Centrality Indices*, pages 16–61. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[97] Wikipedia. k-edge-connected graph. `https://en.wikipedia.org/wiki/K-edge-connected_graph`, 2018.

[98] Mark Newman. *Networks: An introduction*. Oxford university press, 2010.

[99] Ted G Lewis. *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons, 2014.

[100] Amir Modarresi and James P. G. Sterbenz. Towards a model and graph representation for smart homes in the IoT. In *2018 IEEE International Smart Cities Conference (ISC2) (ISC2 2018)*, Kansas City, USA, September 2018.

[101] Justin P. Rohrer, Abdul Jabbar, and James P. G. Sterbenz. Path Diversification: A Multipath Resilience Mechanism. In *Proceedings of the IEEE 7th International Workshop on the Design of Reliable Communication Networks (DRCN)*, pages 343–351, Washington, DC, October 2009.

[102] Yufei Cheng, M. Todd Gardner, Junyan Li, Rebecca May, Deep Medhi, and James P.G. Sterbenz. Optimised Heuristics for a Geodiverse Routing Protocol. In *Proceedings of the IEEE 10th International Workshop on the Design of Reliable Communication Networks (DRCN)*, pages 1–9, Ghent, Belgium, April 2014.

[103] Mohammed J.F. Alenazi and James P. G. Sterbenz. Comprehensive comparison and accuracy of graph metrics in predicting network resilience. In *2015 / 11th International Conference on Design of Reliable Communication Networks (DRCN 2015)*, Kansas City, USA, March 2015.

[104] Egemen K. Çetinkaya, Mohammed J. F. Alenazi, Justin P. Rohrer, and James P. G. Sterbenz. Topology Connectivity Analysis of Internet Infrastructure Using Graph Spectra. In *Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 752–758, St. Petersburg, October 2012.

[105] Paul Shannon, Andrew Markiel, Owen Ozier, Nitin S Baliga, Jonathan T Wang, Daniel Ramage, Nada Amin, Benno Schwikowski, and Trey Ideker. Cytoscape: a software environment for integrated models of biomolecular interaction networks. *Genome research*, 13(11):2498–2504, 2003.

[106] NetworkX developers. NetworkX: Software for complex networks. `https://networkx.github.io/`, May 2018.

[107] Amir Modarresi and John Symons. Modeling and graph analysis for enhancing resilience in smart homes. *Procedia Computer Science*, 160:197–205, 2019.

[108] Duncan J Watts. Networks, dynamics, and the small-world phenomenon. *American Journal of sociology*, 105(2):493–527, 1999.

[109] NetworkX Developers. NetworkX website. `https://networkx.github.io/documentation/stable/index.html`, 2018.

[110] The 802.11 Working Group. Ieee standard for information technology—telecommunications and information exchange between systems local and metropolitan area networks—specific requirements - part 11: Wireless lan medium

access control (mac) and physical layer (phy) specifications. *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pages 1–3534, Dec 2016.

[111] Wikipedia. Gateway (telecommunications). `https://en.wikipedia.org/wiki/Multidimensional_network`, 2019.

[112] Jordi Torrents and Fabrizio Ferraro. Structural cohesion: visualization and heuristics for fast computation. *arXiv preprint arXiv:1503.04476*, 2015.

[113] Michael Joseph Holroyd. *Synchronizability and connectivity of discrete complex systems*. PhD thesis, College of William and Mary, 2006.

[114] Ginestra Bianconi. *Multilayer Networks: Structure and Function*. Oxford university press, 2018.

[115] Amir Modarresi and John Symons. Modeling technological interdependency in IoT - a multidimensional and multilayer network model for smart environments. In *2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM) (RNDM 2019)*, Nicosia, Cyprus, October 2019.

[116] Michele Berlingerio, Michele Coscia, Fosca Giannotti, Anna Monreale, and Dino Pedreschi. Multidimensional networks: Foundations of structural analysis. *World Wide Web*, 16(5-6):567–593, November 2013.

[117] Stefano Boccaletti, Vito Latora, Yamir Moreno, Martin Chavez, and D-U Hwang. Complex networks: Structure and dynamics. *Physics reports*, 424(4-5):175–308, 2006.

[118] Wikipedia. Complex networks. `https://en.wikipedia.org/wiki/Complex_network`, 2019.

[119] Mikko Kivelä, Alex Arenas, Marc Barthelemy, James P Gleeson, Yamir Moreno, and Mason A Porter. Multilayer networks. *Journal of complex networks*, 2(3):203–271, 2014.

[120] Rushed Kanawati. Multiplex network mining: A brief survey. *IEEE Intelligent Informatics Bulletin*, 16(1):24–27, 2015.

[121] Antonios Garas. *Interconnected networks*. Springer, 2016.

[122] Sergey V Buldyrev, Roni Parshani, Gerald Paul, H Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025, 2010.

[123] Egemen K. Çetinkaya, Mohammed J. F. Alenazi, Andrew M. Peck, Justin P. Rohrer, and James P. G. Sterbenz. Multilevel resilience analysis of transportation and communication networks. *Telecommunication Systems*, 60(4):515–537, Dec 2015.

[124] Wikipedia. Multidimensional network. `https://en.wikipedia.org/wiki/Multidimensional_network`, 2018.

[125] John Symons. Supervenience. *Encyclopedia of Neuroscience*, pages 3901–3903, 2009.

[126] T. Murata. Comparison of inter-layer couplings of multilayer networks. In *2015 11th International Conference on Signal-Image Technology Internet-Based Systems (SITIS)*, pages 448–452, Nov 2015.

[127] Lowell W Beineke, Ortrud R Oellermann, and Raymond E Pippert. The average connectivity of a graph. *Discrete mathematics*, 252(1-3):31–45, 2002.

[128] Wikipedia. Mirai (malware). https://en.wikipedia.org/wiki/Mirai_(malware), 2017.

Appendix A

Centrality Metrics Results

This appendix contains the centrality metrics results for the baseline models, star and mesh, smart home, expanded smart home, and their corresponding backup models in Chapter 4.

A.1 Star Model

This section contains the centrality metric analysis for the star model explained in Subsection 4.1.1. Tables A.1 shows the results for distance-based centrality and Table A.2 presents corresponding results for degree and spectra-based centrality metrics.

Nodes	**Shortest path**	**Eccentricity**	**Closeness**	**Betweenness**	**Radiality**	**Stress**
AP	1.16	3	0.86	0.98	0.96	336
RBB	1.89	2	0.53	0.20	0.78	68
ISP1	2.69	3	0.37	0.11	0.57	36
Internet	3.67	4	0.27	0	0.33	0
1	2.11	4	0.48	0	0.72	0
2	2.11	4	0.48	0	0.72	0
3	2.11	4	0.48	0	0.72	0
4	2.11	4	0.48	0	0.72	0
5	2.11	4	0.48	0	0.72	0
6	2.11	4	0.48	0	0.72	0
7	2.11	4	0.48	0	0.72	0
8	2.11	4	0.48	0	0.72	0
9	2.11	4	0.48	0	0.72	0
10	2.11	4	0.48	0	0.72	0
11	2.11	4	0.48	0	0.72	0
12	2.11	4	0.48	0	0.72	0
13	2.11	4	0.48	0	0.72	0
14	2.11	4	0.48	0	0.72	0
15	2.11	4	0.48	0	0.72	0
16	2.11	4	0.48	0	0.72	0

Table A.1: The results of distance-based centrality metrics for the star model

The results of distance and spectra-based metrics for the star model studied in Subsection 4.1.1 is shown in Table A.2.

Nodes	**Degree**	**Neighborhood**	**Core No.**	**Cluster coeff**	**Eigenvector**	**Katz**
AP	16	1.06	1	0	0.71	0.59
RBB	2	9.5	1	0	0.18	0.36
ISP1	2	1.5	1	0	0.05	0.14
Internet	1	2	1	0	0.01	0.11
1	1	17	1	0	0.18	0.25
2	1	17	1	0	0.18	0.15
3	1	17	1	0	0.18	0.15
4	1	17	1	0	0.18	0.15
5	1	17	1	0	0.18	0.15
6	1	17	1	0	0.18	0.1
7	1	17	1	0	0.18	0.15
8	1	17	1	0	0.18	0.15
9	1	17	1	0	0.18	0.15
10	1	17	1	0	0.18	0.25
11	1	17	1	0	0.18	0.15
12	1	17	1	0	0.18	0.15
13	1	17	1	0	0.18	0.15
14	1	17	1	0	0.18	0.15
15	1	17	1	0	0.18	0.25
15	1	17	1	0	0.18	0.15

Table A.2: The results of degree and spectra-based centrality metrics for the star model

A.2 Mesh Model

This section contains the centrality metric analysis for the mesh model explained in Subsection 4.1.1. Tables A.3 presents the results for distance-based centrality while Table A.4 shows corresponding results for degree and spectra-based centrality metrics.

Nodes	**Shortest path**	**Eccentricity**	**Closeness**	**Betweenness**	**Radiality**	**Stress**
AP1	1.71	3	0.58	0.55	0.85	232
AP2	1.76	4	0.57	0.50	0.86	210
AP3	1.76	4	0.57	0.50	0.85	210
RBB	2.48	3	0.40	0.18	.70	76
ISP1	3.33	4	0.30	0.09	0.52	40
Internet	4.29	5	0.23	0	0.34	0
1	2.67	4	0.38	0	0.67	0
2	2.67	4	0.38	0	0.67	0
3	2.67	4	0.38	0	0.67	0
4	2.67	4	0.38	0	0.67	0
5	2.71	5	0.37	0	0.66	0
6	2.71	5	0.37	0	0.66	0
7	2.71	5	0.37	0	0.66	0
8	2.71	5	0.37	0	0.66	0
9	2.71	5	0.37	0	0.66	0
10	2.71	5	0.37	0	0.60	0
11	2.71	5	0.37	0	0.66	0
12	2.71	5	0.37	0	0.66	0
13	2.71	5	0.37	0	0.66	0
14	2.71	5	0.37	0	0.66	0
15	2.71	5	0.37	0	0.66	0
16	2.71	5	0.37	0	0.66	0

Table A.3: The results of distance-based centrality metrics for the mesh model

The results of degree and spectra-based metrics for the star model studied in Subsection 4.1.1 is shown in Table A.4.

Nodes	Degree	Neighborhood	Core No.	Cluster coeff	Eigenvector	Katz
AP1	7	3.14	2	0.05	0.45	0.44
AP2	8	2.63	2	0.04	0.49	0.43
AP3	8	2.63	2	0.04	0.49	0.43
RBB	2	4.50	1	0	0.12	0.32
ISP1	2	1.50	1	0	0.04	0.13
Internet	1	2	1	0	0.01	0.10
1	1	7	1	0	0.11	0.22
2	1	7	1	0	0.11	0.13
3	1	7	1	0	0.11	0.13
4	1	7	1	0	0.15	0.13
5	1	8	1	0	0.15	0.13
6	1	8	1	0	0.15	0.13
7	1	8	1	0	0.15	0.13
8	1	8	1	0	0.15	0.13
9	1	8	1	0	0.15	0.13
10	1	8	1	0	0.15	0.13
11	1	8	1	0	0.14	0.13
12	1	8	1	0	0.14	0.13
13	1	8	1	0	0.14	0.13
14	1	8	1	0	0.14	0.13
15	1	8	1	0	0.14	0.13
16	1	8	1	0	0.14	0.13

Table A.4: The results of degree and spectra-based centrality metrics for the mesh model

A.3 Smart Home Model

This section contains the centrality metric analysis for the smart home instance introduced in Subsection 4.1.2. Tables A.5 shows the results for distance-based centrality and Table A.6 presents corresponding results for degree and spectra-based centrality metrics.

Beging of Table A.5

Nodes	Shortest path	Eccentricity	Closeness	Betweenness	Radiality	Stress
AP1	2.27	5	0.44	0.47	0.84	660
AP2	2.08	4	0.48	0.68	0.86	946
AP3	2.41	5	0.42	0.30	0.82	402
RBB	3.08	6	0.32	0.09	0.74	148
ISP1	3.89	7	0.26	0.05	0.64	88
ISP2	4.51	7	0.22	0.02	0.56	28
Phone1	2.89	5	0.35	0.10	0.76	162
EPC1	3.70	6	0.27	0.06	0.66	102
Internet	4.70	8	0.21	0.01	0.53	28
1	3.24	6	0.31	0	0.72	0
2	3.24	6	0.31	0	0.72	0
3	3.24	6	0.31	0	0.72	0
4	3.05	5	0.33	0	0.74	0
5	3.05	5	0.33	0	0.74	0
6	3.05	5	0.33	0	0.74	0
7	3.05	5	0.33	0	0.74	0
8	3.05	5	0.33	0	0.74	0
9	3.05	5	0.33	0	0.74	0
10	3.05	5	0.33	0	0.74	0
11	3.79	6	0.30	0	0.70	0
12	3.79	6	0.30	0	0.70	0
13	3.79	6	0.30	0	0.70	0
14	3.79	6	0.30	0	0.70	0
15	3.79	6	0.30	0	0.70	0
16	3.79	6	0.30	0	0.70	0
m1-0	2.68	5	0.37	0.32	0.79	446
m1-1	3.49	6	0.29	0.10	0.69	136
m1-2	3.57	6	0.28	0	0.68	0
m1-3	4.32	7	0.23	0.05	0.58	72
m1-4	5.16	8	0.19	0.01	0.48	8
m1-5	4.35	7	0.23	0.05	0.58	70
m1-6	3.51	6	0.28	0.10	0.69	134
m1-7	5.19	8	0.19	0	0.48	6
BT1-0	3.03	6	0.33	0.21	0.75	0

Continuation of Table A.5						
Nodes	**Shortest path**	**Eccentricity**	**Closeness**	**Betweenness**	**Radiality**	**Stress**
BT1-1	4	7	0.25	0	0.63	0
BT1-2	4	7	0.25	0	0.63	0
BT1-3	4	7	0.25	0	0.63	0
BT1-4	4	7	0.25	0	0.63	284

Table A.5: The results of distance-based centrality metrics for the smart home instance

The results of degree and spectra-based metrics for the smart home instance introduced in Subsection 4.1.2 and analyzed Section 4.2 is shown in Table A.6.

Beging of Table A.6

Nodes	**Degree**	**Neighborhood**	**Core No.**	**Cluster coeff**	**Eigenvector**	**Katz**
AP1	7	4.14	2	0.05	0.39	0.34
AP2	11	2.54	2	0.02	0.56	0.38
AP3	8	3	2	0.04	0.41	0.32
RBB	2	4.5	2	0	0.11	0.23
ISP1	2	2	2	0	0.03	0.09
ISP2	2	2	2	0	0.01	0.08
Phone1	2	6.5	2	0	0.16	0.17
ECP1	2	2	2	0	0.04	0.09
Internet	2	2	2	0	0.01	0.08
1	1	7	1	0	0.10	0.16
2	1	7	1	0	0.10	0.10
3	1	7	1	0	0.10	0.10
4	1	11	1	0	0.14	0.10
5	1	11	1	0	0.14	0.10
6	1	11	1	0	0.14	0.10
7	1	11	1	0	0.14	0.10
8	1	11	1	0	0.14	0.10
9	1	11	1	0	0.14	0.10
10	1	11	1	0	0.14	0.16
11	1	8	1	0	0.11	0.09
12	1	8	1	0	0.11	0.09
13	1	8	1	0	0.11	0.09
14	1	8	1	0	0.11	0.09
15	1	8	1	0	0.11	0.16
16	1	8	1	0	0.11	0.09
m1-0	4	4.5	2	0.17	0.20	0.28
m1-1	3	2.67	2	0.33	0.07	0.18
m1-2	2	3.5	2	1	0.07	0.17
m1-3	2	2.5	2	0	0.02	0.09
m1-4	2	2	2	0	0.01	0.09
m1-5	2	2	2	0	0.02	0.09
m1-6	2	3	2	0	0.05	0.16
m1-7	2	2	2	0	0.01	0.14
BT1-0	5	2.2	1	0	0.14	0.26
BT1-1	1	5	1	0	0.04	0.15
BT1-2	1	5	1	0	0.04	0.09
BT1-3	1	5	1	0	0.04	0.09

Continuation of Table A.6						
Nodes	**Degree**	**Neighborhood**	**Core No.**	**Cluster coeff**	**Eigenvector**	**Katz**
BT1-4	1	5	1	0	0.04	0.09

Table A.6: The results of degree and spectra-based centrality metrics for the smart home instance

A.4 Backup Smart Home Model

This section contains the centrality metric analysis for the backup smart home instance explained in Subsection 4.1.2. Tables A.7 shows the results for distance-based centrality.

Beging of Table A.7						
Nodes	**Shortest path**	**Eccentricity**	**Closeness**	**Betweenness**	**Radiality**	**Stress**
ISP1	5.22	8	0.19	0	0.47	0
ISP2	3.43	6	0.30	0.12	0.71	120
Phone1	1.72	4	0.58	0.91	0.91	904
EPC1	2.5	5	0.40	0.18	0.81	174
Internet	4.25	7	0.24	0.07	0.59	62
1	2.69	5	0.37	0	0.79	0
2	2.69	5	0.37	0	0.79	0
3	2.69	5	0.37	0	0.79	0
4	2.69	5	0.37	0	0.79	0
5	2.69	5	0.37	0	0.79	0
6	2.69	5	0.37	0	0.79	0
7	2.69	5	0.37	0	0.79	0
8	2.69	5	0.37	0	0.79	0
9	2.69	5	0.37	0	0.79	0
10	2.69	5	0.37	0	0.79	0
11	2.69	5	0.37	0	0.79	0
12	2.69	5	0.37	0	0.79	0
13	2.69	5	0.37	0	0.79	0
14	2.69	5	0.37	0	0.79	0
15	2.69	5	0.37	0	0.79	0
m1-0	2.25	5	0.44	0.36	0.84	362
m1-1	3.03	6	0.33	0.11	0.75	112
m1-2	3.13	6	0.32	0	0.73	0
m1-3	3.84	7	0.26	0.06	0.64	60
m1-4	4.66	8	0.21	0.01	0.54	8
m1-5	3.88	7	0.26	0.06	0.64	58
m1-6	3.06	6	0.33	0.11	0.74	110
m1-7	4.69	8	0.21	0.01	0.54	6
BT1-0	2.44	5	0.41	0.24	0.82	236
BT1-1	3.41	6	0.29	0	0.70	0
BT1-2	3.41	6	0.29	0	0.70	0
BT1-3	3.41	6	0.29	0	0.70	0
BT1-4	3.41	6	0.29	0	0.70	0

Table A.7: The results of distance-based centrality metrics for the backup smart home instance

The results of degree and spectra-based metrics for the backup smart home instance introduced in Subsection 4.1.2 and analyzed in Section 4.2 is shown in Table A.8.

Beging of Table A.8						
Nodes	**Degree**	**Neighborhood**	**Core No.**	**Cluster coeff**	**Eigenvector**	**Katz**
ISP1	1	2	1	0	0.01	0.08
ISP2	2	2	1	0	0.04	0.09
Phone1	18	1.44	1	0	0.70	0.50
EPC1	2	10	1	0	0.17	0.13
Internet	2	1.5	1	0	0.01	0.09
1	1	18	1	0	0.16	0.19
2	1	18	1	0	0.16	0.12
3	1	18	1	0	0.16	0.12
4	1	18	1	0	0.16	0.12
5	1	18	1	0	0.16	0.12
6	1	18	1	0	0.16	0.12
7	1	18	1	0	0.16	0.12
8	1	18	1	0	0.16	0.12
9	1	18	1	0	0.16	0.12
10	1	18	1	0	0.16	0.19
11	1	18	1	0	0.16	0.12
12	1	18	1	0	0.16	0.12
13	1	18	1	0	0.16	0.12
14	1	18	1	0	0.16	0.12
15	1	18	1	0	0.16	0.19
16	1	18	1	0	0.16	0.12
m1-0	4	6.25	2	0.17	0.20	0.32
m1-1	3	2.67	2	0.33	0.06	0.20
m1-2	2	3.50	2	1	0.06	0.19
m1-3	2	2.50	2	0	0.02	0.10
m1-4	2	2	2	0	0.01	0.10
m1-5	2	2	2	0	0.01	0.10
m1-6	2	3	2	0	0.05	0.18
m1-7	2	2	2	0	0.01	0.16
BT1-0	5	4.4	1	0	0.20	0.31
BT1-1	1	5	1	0	0.05	0.17
BT1-2	1	5	1	0	0.05	0.10
BT1-3	1	5	1	0	0.05	0.10
BT1-4	1	5	1	0	0.05	0.10

Table A.8: The results of degree and spectra-based centrality metrics for the backup smart home instance

A.5 Expanded Smart Home Model

This section contains the centrality metric analysis for the expanded smart home instance explained in Subsection 4.1.2. Tables A.9 shows the results for distance-based centrality and Table A.10 presents corresponding results for degree and spectra-based centrality metrics.

Beging of Table A.9						
Nodes	**Shortest path**	**Eccentricity**	**Closeness**	**Betweenness**	**Radiality**	**Stress**
AP1	2.62	6	0.38	0.37	0.80	1150
AP2	2.38	5	0.42	0.41	0.83	1110
AP3	2.91	6	0.34	0.16	0.76	404
AP4	2.62	5	0.38	0.18	0.80	596
AP5	2.36	4	0.42	0.56	0.83	1534
AP6	2.87	5	0.35	0.20	0.77	500
RBB	3.47	7	0.29	0.06	0.69	182
ISP1	4.30	8	0.23	0.03	0.59	76
ISP2	4.40	7	0.23	0.02	0.57	66
Phone1	3.21	6	0.31	0.03	0.72	90
Phone2	3.17	5	0.31	0.07	0.73	128
EPC1	3.55	6	0.28	0.06	0.68	148
Internet	4.81	8	0.21	0.01	0.53	28
1	3.60	7	0.28	0	0.68	0
2	3.60	7	0.28	0	0.68	0
3	3.60	6	0.30	0	0.70	0
4	3.60	6	0.30	0	0.70	0
5	3.60	6	0.30	0	0.70	0
6	3.60	6	0.30	0	0.70	0
7	3.60	6	0.30	0	0.70	0
8	3.89	7	0.26	0	0.64	0
9	3.89	7	0.26	0	0.64	0
10	3.89	7	0.26	0	0.64	0
11	3.89	7	0.26	0	0.64	0
12	3.60	6	0.28	0	0.68	0
13	3.34	5	0.30	0	0.71	0
14	3.34	5	0.30	0	0.71	0
15	3.34	5	0.30	0	0.71	0
16	3.34	5	0.30	0	0.71	0
17	3.34	5	0.30	0	0.71	0
18	3.85	6	0.26	0	0.64	0
19	3.85	6	0.26	0	0.64	0
20	3.85	6	0.26	0	0.64	0

Continuation of Table A.9						
Nodes	**Shortest path**	**Eccentricity**	**Closeness**	**Betweenness**	**Radiality**	**Stress**
21	3.85	6	0.26	0	0.64	0
22	3.85	6	0.26	0	0.64	0
m1-0	3.04	5	0.33	0.26	0.74	712
m1-1	3.89	6	0.26	0.08	0.64	212
m1-2	3.96	6	0.25	0	0.63	0
m1-3	4.77	7	0.21	0.04	0.53	110
m1-4	5.64	8	0.18	0	0.42	8
m1-5	4.79	7	0.21	0.04	0.53	108
m1-6	3.91	6	0.26	0.08	0.64	210
m1-7	3.65	8	0.18	0	0.42	6
BT1-0	3.43	7	0.29	0.16	0.70	484
BT1-1	4.40	8	0.23	0	0.57	0
BT1-2	4.40	8	0.23	0	0.57	0
BT1-3	4.40	8	0.23	0	0.57	0
BT1-4	4.40	8	0.23	0	0.57	0

Table A.9: The results of distance-based centrality metrics for the expanded smart home instance

The results of degree and spectra-based metrics for the expanded smart home instance introduced in Subsection 4.1.2 and analyzed in Section 4.2 is shown in Table A.10.

Beging of Table A.10						
Nodes	**Degree**	**Neighborhood**	**Core No.**	**Cluster coeff**	**Eigenvector**	**Katz**
AP1	7	4	2	0.05	0.33	0.22
AP2	9	3.33	2	0.03	0.43	0.25
AP3	6	3.33	2	0.07	0.25	0.20
AP4	4	6.25	2	0.17	0.28	0.18
AP5	10	3.10	2	0.02	0.46	0.26
AP6	7	2.71	2	0.05	0.27	0.20
RBB	2	4.50	2	0	0.09	0.14
ISP1	2	2	2	0	0.03	0.13
ISP2	2	2.5	2	0	0.02	0.14
Phone1	2	6	2	0	0.12	0.31
Phone2	2	6.5	2	0	0.13	0.31
EPC1	3	2	2	0	0.07	0.19
Internet	2	2	2	0	0.02	0.13
1	1	7	1	0	0.08	0.14
2	1	7	1	0	0.08	0.14
3	1	9	1	0	0.11	0.14
4	1	9	1	0	0.11	0.14
5	1	9	1	0	0.11	0.14
6	1	9	1	0	0.11	0.14
7	1	9	1	0	0.11	0.14
8	1	6	1	0	0.06	0.14
9	1	6	1	0	0.06	0.14
10	1	6	1	0	0.06	0.14
11	1	6	1	0	0.06	0.14
12	1	4	1	0	0.07	0.14
13	1	10	1	0	0.12	0.14
14	1	10	1	0	0.12	0.14
15	1	10	1	0	0.12	0.14
16	1	10	1	0	0.12	0.14
17	1	10	1	0	0.12	0.14
18	1	7	1	0	0.07	0.14
19	1	7	1	0	0.07	0.14
20	1	7	1	0	0.07	0.14
21	1	7	1	0	0.07	0.14
22	1	7	1	0	0.07	0.14
m1-0	4	4.25	2	0.17	0.15	0.19
m1-1	3	2.67	2	0.34	0.05	0.16

Continuation of Table A.10						
Nodes	**Degree**	**Neighborhood**	**Core No.**	**Cluster coeff**	**Eigenvector**	**Katz**
m1-2	2	3.50	2	1	0.05	0.15
m1-3	2	2.50	2	0	0.01	0.14
m1-4	2	2	2	0	0.01	0.14
m1-5	2	2	2	0	0.01	0.14
m1-6	2	3	2	0	0.04	0.14
m1-7	2	2	2	0	0.01	0.14
BT1-0	5	2.2	1	0	0.11	0.20
BT1-1	1	5	1	0	0.03	0.13
BT1-2	1	5	1	0	0.03	0.13
BT1-3	1	5	1	0	0.03	0.13
BT1-4	1	5	1	0	0.03	0.13

Table A.10: The results of degree and spectra-based centrality metrics for the expanded smart home instance

A.6 Backup Expanded Smart Home Model

This section contains the centrality metric analysis for the backup expanded smart home instance explained in Subsection 4.1.2. Tables A.11 shows the results for distance-based centrality and Table A.12 presents corresponding results for degree and spectra-based centrality metrics.

Beging of Table A.11

Nodes	**Shortest path**	**Eccentricity**	**Closeness**	**Betweenness**	**Radiality**	**Stress**
ISP2	3.28	6	0.30	0.51	0.71	76
Phone1	2.51	6	0.40	0.65	0.81	956
Phone2	2.36	4	0.42	0.71	0.83	1046
EPC1	2.36	5	0.42	0.56	0.83	828
Internet	4.26	7	0.23	0	0.59	0
1	3.49	7	0.29	0	0.69	0
2	3.49	7	0.29	0	0.69	0
3	3.49	7	0.29	0	0.69	0
4	3.49	7	0.29	0	0.69	0
5	3.49	7	0.29	0	0.69	0
6	3.49	7	0.29	0	0.69	0
7	3.49	7	0.29	0	0.69	0
8	3.49	7	0.29	0	0.69	0
9	3.49	7	0.29	0	0.69	0
10	3.49	7	0.29	0	0.69	0
11	3.49	7	0.29	0	0.69	0
12	3.33	5	0.30	0	0.71	0
13	3.33	5	0.30	0	0.71	0
14	3.33	5	0.30	0	0.71	0
15	3.33	5	0.30	0	0.71	0
16	3.33	5	0.30	0	0.71	0
17	3.33	5	0.30	0	0.71	0
18	3.33	5	0.30	0	0.71	0
19	3.33	5	0.30	0	0.71	0
20	3.33	5	0.30	0	0.71	0
21	3.33	5	0.30	0	0.71	0
22	3.33	5	0.30	0	0.71	0
m1-0	2.97	5	0.34	0.31	0.75	460
m1-1	3.79	6	0.26	0.09	0.65	140
m1-2	3.87	6	0.26	0	0.64	0
m1-3	4.64	7	0.22	0.05	0.54	74
m1-4	5.49	8	0.18	0.01	0.43	8
m1-5	4.67	7	0.21	0.05	0.54	72

Continuation of Table A.11						
Nodes	**Shortest path**	**Eccentricity**	**Closeness**	**Betweenness**	**Radiality**	**Stress**
m1-6	3.82	6	0.26	0.09	0.65	138
m1-7	5.51	8	0.18	0	0.44	6
BT1-0	3.28	7	0.30	0.20	0.71	292
BT1-1	4.26	8	0.23	0	0.60	0
BT1-2	4.26	8	0.23	0	0.60	0
BT1-3	4.26	8	0.23	0	0.60	0
BT1-4	4.26	8	0.23	0	0.60	0

Table A.11: The results of distance-based centrality metrics for the backup expanded smart home instance

The results of degree and spectra-based metrics for the backup expanded smart home instance introduced in Subsection 4.1.2 and analyzed in Section 4.2 is shown in Table A.12.

Beging of Table A.12

Nodes	**Degree**	**Neighborhood**	**Core No.**	**Cluster coeff**	**Eigenvector**	**Katz**
ISP2	2	2	1	0	0.08	0.14
Phone1	13	1.46	1	0	0.49	0.31
Phone2	13	1.38	1	0	0.49	0.31
EPC1	3	9.33	1	0	0.28	0.19
Internet	1	2	1	0	0.02	0.13
1	1	13	1	0	0.13	0.14
2	1	13	1	0	0.13	0.14
3	1	13	1	0	0.13	0.14
4	1	13	1	0	0.13	0.14
5	1	13	1	0	0.13	0.14
6	1	13	1	0	0.13	0.14
7	1	13	1	0	0.13	0.14
8	1	13	1	0	0.13	0.14
9	1	13	1	0	0.13	0.14
10	1	13	1	0	0.13	0.14
11	1	13	1	0	0.13	0.14
12	1	13	1	0	0.13	0.14
13	1	13	1	0	0.13	0.14
14	1	13	1	0	0.13	0.14
15	1	13	1	0	0.13	0.14
16	1	13	1	0	0.13	0.14
17	1	13	1	0	0.13	0.14
18	1	13	1	0	0.13	0.14
19	1	13	1	0	0.13	0.14
20	1	13	1	0	0.13	0.14
21	1	13	1	0	0.13	0.14
22	1	13	1	0	0.13	0.14
m1-0	4	5	2	0.17	0.18	0.19
m1-1	3	2.67	2	0.34	0.07	0.16
m1-2	2	3.50	2	1	0.06	0.15
m1-3	2	2.50	2	0	0.02	0.14
m1-4	2	2	2	0	0.01	0.14
m1-5	2	2	2	0	0.01	0.14
m1-6	2	3	2	0	0.05	0.14
m1-7	2	2	2	0	0.01	0.14
BT1-0	5	3.40	1	0	0.18	0.20
BT1-1	1	5	1	0	0.05	0.13

Continuation of Table A.12						
Nodes	**Degree**	**Neighborhood**	**Core No.**	**Cluster coeff**	**Eigenvector**	**Katz**
BT1-2	1	5	1	0	0.05	0.13
BT1-3	1	5	1	0	0.05	0.13
BT1-4	1	5	1	0	0.05	0.13

Table A.12: The results of degree-based centrality metrics for the backup expanded smart home instance