Resilience Evaluation and Enhancement in Mobile Ad Hoc Networks

By

Dongsheng Zhang

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. James P.G. Sterbenz

Prof. Victor S. Frost

Prof. Fengjun Li

Prof. Gary J. Minden

Prof. Dr. Bernhard Plattner

Prof. Caterina Scoglio

Prof. John Symons

Date Defended: 21-September-2015

The Dissertation Committee for Dongsheng Zhang certifies that this is the approved version of the following dissertation:

Resilience Evaluation and Enhancement in Mobile Ad Hoc Networks

Chairperson: Prof. James P.G. Sterbenz

Date approved: 21-September-2015

Abstract

Understanding network behavior that undergoes challenges is essential to constructing a resilient and survivable network. Due to the mobility and wireless channel properties, it is more difficult to model and analyze mobile ad hoc networks under various challenges. We provide a comprehensive model to assess the vulnerability of mobile ad hoc networks in face of malicious attacks. We analyze comprehensive graph-theoretical properties and network performance of the dynamic networks under attacks against the critical nodes using both synthetic and real-world mobility traces. Motivated by Minimum Spanning Tree and small-world networks, we propose a network enhancement strategy by adding long-range links. We compare the performance of different enhancement strategies by evaluating a list of robustness measures. Our study provides insights into the design and construction of resilient and survivable mobile ad hoc networks.

Page left intentionally blank.

Acknowledgments

I would like to sincerely thank my advisor, Prof. James P.G. Sterbenz for his support during my doctoral studies. I have been tremendously motivated and inspired by his eruditeness within the technical fields and also by his infinite passion for knowledge and his curiosity about the world. I thank the committee members: Prof. Victor S. Frost, Prof. Fengjun Li, Prof. Gary J. Minden, Prof. Dr. Bernhard Plattner, Prof. Caterina Scoglio, and Prof. John Symons for their valuable feedback in improving this dissertation.

I would like to thank Justin P. Rohrer and Egemen Çetinkaya for their help during my early stages in the ResiliNets group. Santosh Ajith Gogi and Kamakshi Sirisha Pathapati have helped me greatly in the ANTP project. I also would like to thank Mohammed J.F. Alenazi, Andrew Peck, Yufei Cheng, Siddharth Gangadhar, and Truc Anh N. Nguyen for their suggestions and discussions about my research work.

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

I received support during my doctoral studies partially through my advisor's grants by the NSF grant CNS-1050226 (Multilayer Network Resilience Analysis and Experimentation on GENI). I was also supported by teaching assistantship at the Department of Electrical Engineering and Computer Science, the University of Kansas.

Finally, I am grateful to my family for their trust in all my decisions during these years, and for cultivating me into a person with curiosity and free spirit. I would have never gotten so far without their endless support.

Page left intentionally blank.

Contents

1 Introduction and Motivation **1**

1.1 Thesis Statement 3

1.2 Proposed Solution 4

1.3 Contributions 5

1.4 Relevant Publications 6

1.5 Additional Publications 8

1.6 Organization 9

2 Background and Related Work **11**

2.1 Graph Theoretical Background 11

2.1.1 Time-Varying Graphs 12

2.1.2 Random Geometric Graphs 14

2.1.3 Small-World Networks 16

2.1.4 Centrality Metrics 17

2.1.5 Robustness Metrics 20

2.2 Modeling and Analyses of MANETs 23

2.2.1 Network and Challenge Modeling 23

2.2.2 Network Vulnerability 24

2.3 Connectivity Management in MANETs 25

2.3.1 Mobile-Agent-Based Improvement 25

2.3.2 Topology Control 26

2.4 Quantifying Network Resilience 27

3 Modeling Approach **31**
3.1 Attack Modeling . . . 32
3.1.1 Constructing Link Availability Graphs . . . 33
3.1.2 Determining the Window Size . . . 34
3.1.3 Applying Malicious Attacks . . . 35
3.2 Enhancement Modeling . . . 39
3.2.1 Bridging Disconnected Components . . . 39
3.2.2 Enhancement Strategies . . . 42

4 MANET Robustness Analysis **45**
4.1 Synthetic Trace Analysis . . . 45
4.1.1 Synthetic Scenarios . . . 46
4.1.2 Attacks Based on Aggregation . . . 50
4.1.3 Real-Time Attacks . . . 54
4.1.4 Simulations in ns-3 . . . 56
4.2 Real-World Trace Analysis . . . 59
4.2.1 Data Set . . . 60
4.2.2 Topological Analysis . . . 65
4.2.3 Simulations in ns-3 . . . 80

5 Evaluation of Enhancement Strategies **85**
5.1 Synthetic Trace Enhancement . . . 86
5.1.1 Enhancement Strategies Evaluation . . . 86
5.1.2 Sum of Flow Robustness Evaluation . . . 94
5.2 Real-World Trace Enhancement . . . 95
5.2.1 Enhancement Strategies Evaluation . . . 95
5.2.2 Sum of Flow Robustness Evaluation . . . 115

6 Conclusions and Future Work **119**
6.1 Conclusions . . . 120
6.2 Future Work . . . 124

A Plots for Additional Scenarios **147**

List of Figures

2.1 Resilience $\mathbb{R}$ measured in the state space 28

3.1 MANET topologies at six consecutive time steps 33
3.2 Weighted link availability graph and its adjacency matrix 34
3.3 Adaptive node attacks based on degree centrality 37
3.4 Disconnected graph consisting of fully-connected components 38
3.5 A minimum spanning tree to bridge the disconnected components 40

4.1 Normalized giant component size 47
4.2 Flow robustness 48
4.3 Probability of being 1-connected 48
4.4 MANETs under simultaneous node attacks 51
4.5 Sum of flow robustness with varying mobility coefficient 53
4.6 20 nodes MANETs under real-time simultaneous node attacks 55
4.7 50 nodes MANETs under real-time simultaneous node attacks 55
4.8 20 nodes MANETs under real-time simultaneous node attacks 57
4.9 50 nodes MANETs under real-time simultaneous node attacks 57
4.10 ns-3 vs. topological analysis with 20 nodes 59
4.11 CCDF of average node velocities 62
4.12 Snapshots of Statefair trace with tr = 250 63
4.13 Snapshots of NCSU trace with tr = 1000 64
4.14 Snapshots of KAIST trace with tr = 500 64
4.15 Statefair 67
4.16 NCSU 68
4.17 KAIST 69
4.18 Change of high centrality nodes over time in StateFair with tr = 250 . . . 70

4.19 Change of high centrality nodes over time in NCSU with tr = 1000 . . . 71
4.20 Change of high centrality nodes over time in KAIST with tr = 500 71
4.21 Centrality-based attacks using different window sizes for StateFair trace . 73
4.22 Centrality-based attacks using different window sizes for NCSU trace . . 74
4.23 Centrality-based attacks using different window sizes for KAIST trace . . 75
4.24 Giant component size under centrality-based attacks with 30 s window size 76
4.25 Resilience space using different routing protocols 82

5.1 Algebraic connectivity in the enhanced networks 87
5.2 Inverse of network diameter in the enhanced networks 88
5.3 Inverse of path length in the enhanced networks 89
5.4 Network criticality in the enhanced networks 91
5.5 Clustering coefficient in the enhanced networks 93
5.6 A snapshot of Statefair trace with 20 added links based on long-path strategy 96
5.7 Algebraic connectivity of Statefair with an increased number of added links 97
5.8 Inverse of diameter of Statefair with an increasing number of added links 97
5.9 Inverse of path length of Statefair with an increasing number of added links 98
5.10 Clustering coefficient of Statefair with an increasing number of added links 98
5.11 Network criticality of Statefair with an increasing number of added links 99
5.12 A snapshot of NCSU trace with 20 added links based on long-path strategy 100
5.13 Algebraic connectivity of NCSU with an increased number of added links 101
5.14 Inverse of diameter of NCSU with an increased number of added links . . 101
5.15 Inverse of path length of NCSU with an increased number of added links 102
5.16 Network criticality of NCSU with an increased number of added links . . 102
5.17 A snapshot of Orlando trace with 20 added links based on long-path strategy 103
5.18 Algebraic connectivity of Orlando with an increased number of added links 104
5.19 Inverse of diameter of Orlando with an increased number of added links . 105
5.20 Inverse of path length of Orlando with an increased number of added links 105
5.21 Network criticality of Orlando with an increased number of added links . 106
5.22 Clustering coefficient of Orlando with an increased number of added links 106
5.23 A snapshot of NewYork trace with 20 added links based on long-path strategy 108
5.24 Algebraic connectivity of NewYork with an increased number of added links 109

5.25 Network criticality of NewYork with an increased number of added links 109
5.26 Inverse of diameter of NewYork with an increased number of added links 110
5.27 Inverse of path length of NewYork with an increased number of added links 110
5.28 Clustering coefficient of NewYork with an increased number of added links 111
5.29 A snapshot of KAIST trace with 20 added links based on long-path strategy 112
5.30 Algebraic connectivity of KAIST with an increased number of added links 113
5.31 Inverse of diameter of KAIST with an increased number of added links . 113
5.32 Inverse of path length of KAIST with an increased number of added links 114
5.33 Clustering coefficient of KAIST with an increased number of added links 114

Page left intentionally blank.

List of Tables

3.1 $\mathcal{F}$ of time-varying graphs under node attacks 36

4.1 Synthetic scenario parameters 46
4.2 Graph metrics of selected transmission ranges 49
4.3 Windows sizes for different scenarios with MC = 0.1 and 0.5 50
4.4 Simulation parameters of synthetic traces in ns-3 58
4.5 Five sites of real-world mobility traces 60
4.6 The Statistics of all sites 63
4.7 $\Delta\mathbb{R}$ between random node failures and malicious attacks 79
4.8 Simulation parameters of real-world traces in ns-3 80
4.9 Resilience of MANET routing in Two Sites 81

5.1 $\sum$F of the enhanced synthetic traces under attacks 94
5.2 $\sum\mathcal{F}$ of the enhanced real-world traces under attacks 116

Page left intentionally blank.

Chapter 1

Introduction and Motivation

In a MANET (mobile ad hoc network) environment, nodes communicate with each other without infrastructure. Networks can be established quickly in a decentralized and self-organized manner. Communication between node pairs relies on multihop traffic forwarding from other nodes. Historically, the original goal of MANETs was to provide military communication in battlefields where the network cannot rely on a fixed infrastructure [1]. In the past decade, MANETs have begun to be widely utilized in many real-world scenarios [2], such as VANETs (vehicular ad hoc networks) [3], WSNs (wireless sensor networks) [4], and PANs (personal area networks) [5]. With the exponential growth of wireless devices, commercial and educational MANET applications have become more attractive in our daily lives such as ad hoc communications during conferences, wireless sensor networks, vehicular ad hoc networks, and social movements [2, 6, 7]. With the emergence of driverless cars, using ad hoc networking for communications between auto-piloted vehicles could be an emerging application in the near future. In addition, with the fast growth of tablets, cellphones, and wearable devices in recent years, people use wireless networks in their daily lives to an unprecedented level. Two companies (Open Garden [8] and TextMe [9]) recently teamed up so that Android devices without cellular or 802.11 access can text and make voice calls. When there is no direct access to

the Internet, devices can access the Internet through a multihop chain of other devices that have Internet access. MANETs have also been used in social movements, in which the smart phone apps including FireChat [10, 11] and TwiMight [12, 13] allow ad hoc communications without Wi-Fi or cellular connection.

However, due to the properties of wireless channels, the potential attacks and challenges are tremendously high [14]. Wireless networks are vulnerable due to the unreliable medium and their open channels that have them subject to attacks such as eavesdropping and jamming interference [15]. In addition, they have hidden/exposed-terminal problems due to shared channels among the wireless devices.

Due to the dynamics and channel properties of mobile wireless networks, techniques used to improve the disruption tolerance and network reliability for wired networks are not sufficient in the wireless context [14]. The non-infrastructure, multihop, and mobile aspects of MANETs pose an even greater challenge to reliable communications within the network [2]. Dynamically changing topologies could lead to route change and packet loss. Battery-powered devices used as transceivers and relayers of packets in ad hoc networks have energy constraints. A resilient and survivable MANET needs to be established so that network performance can remain above a certain level even under malicious attacks or node failures. Traditional security approaches address the problem by protecting each individual layer of the whole network stacks [16] and defending the network against known and unknown security threats [16, 17]. Instead of designing intrusion protection mechanisms to secure network stacks, we focus on the fault tolerance, resilience, and survivability of MANETs from a topological perspective by assuming the existence of network failures caused by all possible reasons.

The connectivity of underlying topologies of MANETs is essential to the normal functioning of the entire network. Intelligent attackers intend to destroy the network using a

minimum amount of resources. The key players in the network are more prone to be the target of the attack. One of the problems is how to identify critical nodes in dynamically changing mobile wireless networks. The roles of nodes are associated with routing mechanism used in the network. Communications in MANETs require a relatively high network connectivity so that there are stable end-to-end paths between node pairs. MANETs are different from delay-tolerant networks [18] that are usually sparsely-connected and use store-and-forward and ferrying mechanisms to deliver packets. In this work, we propose a model to address the problem of resilience assessment and enhancement of MANETs from the perspective of networking science and graph theory. The detailed attack mechanisms are out of the scope of this work. We assess the critical points of MANETs which are more likely be chosen as the attack target by intelligent attackers. Network structure resilience can be improved by providing a certain level of diversity and redundancy. We propose mechanisms to enhance the network topological structure which can mitigate the impact of node attacks on the overall network performance.

1.1 Thesis Statement

In order to construct MANETs that are robust to network attacks, we need to understand network behavior under intelligent node attacks. Nodes whose removal could result in high impact on network performance are more likely to be the target of an attack. Identification of the critical node set is known as $\mathcal{NP}$-hard on general graphs [19]. Furthermore, due to the dynamics of network topologies, it is nontrivial to identify the critical nodes within the mobile networks. We exploit weighted centrality metrics as node significance indicators for MANETs within a certain time window. Inspired by the short path lengths in small-world networks, long-range links can be added to intermittent MANETs using directional antennas. Simulations of critical node attacks against

MANETs in both improved and unimproved networks and analysis of corresponding network performance would guide the design and construction of more resilient and survivable MANETs. Therefore, our thesis statement is:

> *Modeling of critical node attacks against mobile ad hoc networks leads to a better understanding of the potential network vulnerabilities under intelligent attacks. The evaluation of network enhancement strategies that can improve the robustness in mobile ad hoc networks provides guidance to the design and construction of resilient mobile wireless networks.*

The goal of this dissertation is fivefold:

1. Present methods to model dynamic topologies and malicious attacks in MANETs;
2. Examine the impact of different centrality-based attacks on MANETs' robustnesss;
3. Propose network topology enhancement mechanisms for MANETs;
4. Investigate the robustness of MANETs enhanced by using different strategies;
5. Gain understanding of how to design and construct resilient and survivable MANETs.

1.2 Proposed Solution

We propose a graph-theoretical model to simulate and analyze mobile wireless networks under critical node attacks. In order to represent dynamic topologies abstractly, we model the dynamic topologies of MANETs as time-varying graphs. Each snapshot of dynamic topologies can be represented as an adjacency matrix. Pairwise node interaction within a certain time window size is aggregated as a weighted graph, in which the weights denote link availabilities. Based on our representation of dynamic topologies, centrality

metrics are computed to indicate relative significance of each node in the network. We simulate critical node attacks using both synthetic mobility models and real-world mobility traces. Various network performance and graph theoretical measures are employed to evaluate network resilience. A cross comparison between topological connectivity and network throughput in the application layer is conducted. Next, we propose the network enhancement strategy motivated by small-world network characteristics and evaluate various network robustness metrics of MANETs enhanced by link additions using different strategies. We compare how the enhanced MANETs using different strategies survive the centrality-based malicious attacks. We show how link additions to the MANETs transforms the random geometric graphs to the small world networks. Our analyses provide insight into the design of resilient MANETs.

1.3 Contributions

The main contributions of this dissertation are to:

1. Present a novel approach to model time-varying graphs. We aggregate network topologies within certain time windows into a weighted graph.

2. Study the impact of centrality-based attacks on network robustness. Degree, closeness, betweenness, and eigenvector centrality are utilized for this study. We propose a new flexible centrality metric that combines the advantages of both degree and betweenness.

3. Contribute to the understanding of the network properties of dynamic mobile networks. This reveals the inherent characteristics of time-varying graphs.

4. Measure network robustness using graph metrics such as algebraic connectivity and network criticality. Different resilience metrics are used to compare network performance under attacks from different aspects.

5. Assess vulnerabilities in MANETs that lead to a better understanding of how to improve the resilience of MANETs.

6. Propose and evaluate topology enhancement mechanisms by adding long-range links between longest-distance node pairs.

7. Evaluate network robustness of improved MANET topologies using both synthetic and real-world mobility traces.

8. Provide a better understanding of how link addition transform the geometric random network to small-world networks.

1.4 Relevant Publications

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

Peer-Reviewed Proceedings

6. **Dongsheng Zhang** and James P.G. Sterbenz, "Measuring the Resilience of Mobile Ad Hoc Networks with Human Walk Patterns," in *Proceedings of the 7th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, Munich, Germany, October 2015.

5. **Dongsheng Zhang** and James P.G. Sterbenz, "Robustness Analysis of Mobile Ad Hoc Networks Using Human Mobility Traces," in *Proceedings of the 11th IEEE/IFIP*

International Conference on Design of Reliable Communication Networks (DRCN), Kansas City, MO, March 2015.

4. **Dongsheng Zhang** and James P.G. Sterbenz, "Analysis of Critical Node Attacks in Mobile Ad Hoc Networks," in *Proceedings of the 6th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, Barcelona, Spain, November 2014.

3. **Dongsheng Zhang**, Egemen K. Çetinkaya, and James P.G. Sterbenz, "Robustness of Moible Ad Hoc Networks Under Centrality-Based Attacks," in *Proceedings of the 5th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, Almaty, Kazakhstan, September 2013.

2. **Dongsheng Zhang**, Egemen K. Çetinkaya, and James P.G. Sterbenz, "Modelling Critical Node Attacks in MANETs," in *In Self-Organizing Systems, Lecture Notes in Computer Science, Springer Berlin Heidelberg*, vol. 8221, pp. 127–138, 2014.

1. **Dongsheng Zhang**, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. Çetinkaya, and James P.G. Sterbenz, "Modelling Attacks and Challenges to Wireless Networks," in *Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, St. Petersburg, Russia, October 2012 (**best paper award**).

Extended Abstracts

1. **Dongsheng Zhang**, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. Çetinkaya, and James P.G. Sterbenz, "Modelling Wireless Challenges," in *Proceedings of the 18th ACM International Conference on Mobile Computing and Networking (MobiHoc)*, Istanbul, Turkey, August 2012.

1.5 Additional Publications

Other publications that have resulted from the work during my Ph.D. studies are listed as follows:

5. Mohammed J.F. Alenazi, **Dongsheng Zhang**, Yufei Cheng, and James P.G. Sterbenz, "Epidemic Routing Protocol Implementation in ns-3," *to appear in Workshop on ns-3 (WNS3)*, Spain, Barcelona, March 2015.

4. Mohammed J.F. Alenazi, Santosh Ajith Gogi, **Dongsheng Zhang**, Egemen K. Çetinkaya, Justin P. Rohrer, and James P.G. Sterbenz, "Implementation of Aeronautical Network Protocols," in *Proceedings of the AIAA Infotech@Aerospace Conference*, Boston, MA, August 2013.

3. Santosh Ajith Gogi, **Dongsheng Zhang**, Egemen K. Çetinkaya, Justin P. Rohrer, and James P.G. Sterbenz, "Implementation of the AeroTP Transport Protocol in Python," in *Proceedings of the 48th International Telemetering Conference (ITC)*, San Diego, CA, October 2012.

2. Mohammed Alenazi, Santosh Ajith Gogi, **Dongsheng Zhang**, Egemen K. Çetinkaya, Justin P. Rohrer, and James P.G. Sterbenz, "ANTP Protocol Suite Software Implementation Architecture in Python," in *Proceedings of the 47th International Telemetering Conference (ITC)*, Las Vegas, NV, October 2011.

1. Egemen K. Çetinkaya, Justin P. Rohrer, Abdul Jabbar, Mohammed J.F. Alenazi, **Dongsheng Zhang**, Dan S. Broyles, Kamakshi Sirisha Pathapati, Hemanth Narra, Kevin Peters, Santosh Ajith Gogi, and James P.G. Sterbenz, "Protocols for Highly-Dynamic Airborne Networks," in *Proceedings of the 18th ACM International Conference on Mobile Computing and Networking (MobiHoc)*, Istanbul, Turkey, August 2012.

1.6 Organization

In this chapter, we provide the overview and motivation for this dissertation. The remainder of the dissertation is organized as follows: Chapter 2 presents the background and related work for this dissertation, which includes time-varying graphs, random geometric graphs, small-world networks, centrality metrics, network challenge modeling, network vulnerability, and network resilience quantification. In Chapter 3, we present our modeling of dynamic topologies in MANETs and how we evaluate the impact of different centrality metrics on the network flow robustness. We also introduce the two-step enhancement model that starts with adding bridging links to make a 1-connected network, and then adds long-range links to further improve network resilience. In Chapter 4, an in-depth topological analysis of synthetic and real-world mobility traces is presented. In addition, we show the relationship between topological connectivity and network throughput by running MANET routing protocols in ns-3. Two layers of resilience analysis are presented so that resilience optimization could be addressed in each layer. In Chapter 5, we propose a network enhancement mechanism by adding long-range links. Several enhancement mechanisms are compared by evaluating various graph robustness metrics of both synthetic and real-world mobility traces. Finally, we conclude this dissertation and discuss future works in Chapter 6.

Page left intentionally blank.

Chapter 2

Background and Related Work

In this chapter, we first present the graph theoretical background for this work, which includes time-varying graphs, random geometric graphs, small-world networks, centrality, and network robustness metrics in Section 2.1. Related work about the modeling and analysis of MANETs is given in Section 2.2, including network challenge modeling, network vulnerability, and critical node problems. In Section 2.3, we discuss connectivity management in MANET by using additional mobile agents nodes and applying topology control techniques. Finally, we present resilience quantification model that can measure MANET resilience based on a range of network operational states in Section 2.4. For the consistency of variable representation, we use $\mathcal{G} = (\mathcal{N}, \mathcal{L})$ to represent a graph, where $\mathcal{N}$ represents the set of nodes, and $\mathcal{L}$ to represent the set of links in a graph.

2.1 Graph Theoretical Background

TVGs (Time-varying graphs) have been used to model dynamic complex systems [20]. The mobile topologies of MANETs can be represented as TVGs. A RGG (random geometric graph) is a spatial graph model in which nodes are connected if the distance between nodes are less than a threshold value [21]. It is natural to model a snapshot of mobile topologies as a RGG due to its limited radio transmission range. Inspired by the

short average path length in small-world networks [22], short-cuts could be introduced to MANETs to improve network connectivity. Centrality metrics were originally used to describe relative significance of each individual in social network analysis [23]. They can be used to the identify the significant nodes in MANETs. Various robustness metrics will be introduced to measure MANET resilience from different perspectives.

2.1.1 Time-Varying Graphs

The notion of TVG is the natural means to represents a MANET. A TVG is defined as:

$$\mathcal{G} = (\mathcal{N}, \mathcal{L}, \mathcal{T}, \rho, \zeta) \tag{2.1}$$

where $\mathcal{N}(\mathcal{G})$ and $\mathcal{L}(\mathcal{G})$ denote nodes and links that evolve over time [20]. $\mathcal{T} \subseteq \mathbb{T}$ is called the *lifetime* of the system; $\rho\colon \mathcal{L} \times \mathcal{T} \to \{0, 1\}$, is the link presence function that indicates the availability of a specified link at a given time; $\zeta\colon \mathcal{L} \times \mathcal{T} \to \mathbb{T}$, is the latency function that indicates the time needed to traverse a certain link $\mathcal{L}$. Since both nodes and links could be up or down, we added an additional parameter $\nu\colon \mathcal{N} \times \mathcal{T} \to \{0, 1\}$ as a counterpart of ρ, which denotes the availability of a specified *node*; therefore, we have a new TVG model represented as [24]:

$$\mathcal{G} = (\mathcal{N}, \mathcal{L}, \mathcal{T}, \rho, \zeta, \nu) \tag{2.2}$$

In wireless environments, information propagates at a speed that is close to the velocity of light and is far higher than the speed of mobile nodes; hence, the latency function ζ is negligible in MANET scenarios. The *footprint* of a TVG $\mathcal{G}$ from t_1 to t_2 can be represented as a static graph:

$$\mathcal{G}^{[t_1,t_2)} = \left(\mathcal{N}, \mathcal{L}^{[t_1,t_2)}\right) \tag{2.3}$$

such that $\forall l \in \mathcal{L}, l \in \mathcal{L}^{[t_1,t_2)} \Leftrightarrow \exists t \in [t_1, t_2), \rho(l,t) = 1$ [20]. Fundamentally, the footprint denotes an aggregation of node interactions within a certain time window $[t_1, t_2)$. A weighted static graph, representing node interactions during each time interval, can be obtained by aggregating node interactions. The time interval between two instants t_i and t_j can be denoted as $\tau_{i,j} = [t_i, t_j) \subseteq \mathcal{T}$. The link availability during interval $\tau_{i,j}$ between pairwise nodes can be represented as the ratio of τ_{a} to the time window length $\tau_{i,j}$, where $\tau_{\mathrm{a}} \subseteq \tau_{i,j}$ is the time during which two nodes are within the transmission range of each other and are able to communicate directly. By considering all pairs of nodes, the availability matrix for each time window can be obtained, in which each element in the matrix denotes the link availability of a certain pair of nodes with a value ranging from 0 to 1. Availability matrices of varying granularities can be calculated based on the different sizes of time windows. Traditional atemporal metrics such as centrality for a static weighted graph can then be applied on the availability matrix. Temporal reachability graphs have been introduced as time-varying directed graphs that can capture the correlations between successive snapshots of dynamic topologies [25]. A combinatorial model has been developed to capture time-varying characteristics of TVGs [26]. In SNA (social network analysis) and DTNs (delay-tolerant networks), temporal graph metrics have been used to capture temporal characteristics [27, 28]. However, they are not applicable to real-time MANETs since traditional MANET routing protocols require stable end-to-end paths and do not allow data transmission if there is no route between source and destination at the time of sending. This makes metrics such as temporal path ineffective. In this work, we model dynamic networks as an aggregation of time-varying topologies using traditional MANETs routing protocols.

2.1.2 Random Geometric Graphs

In MANETs, when all nodes transmit with the same power, it is usually assumed that their transmission ranges are similar. A snapshot of MANETs' topologies can be represented as random nodes distributed in a two or three dimensional Euclidean space, and there is a link between a pair of nodes if they stay within the transmission range of each other. This model is identical to the RGG [29] and the continuum percolation model [30]. A dynamic RGG model has been developed to analytically study a variation of the Random Walk model for MANETs [31]. Percolation theory deals with the clusters with the groups of neighboring occupied sites [30]. Basically, it describes the behavior of connected clusters in a random graph. The percolation probability is the probability that an arbitrary node belongs to a cluster of infinite size with nodes distributed with Poisson intensity λ. Continuum percolation theory extends discrete percolation theory to N-dimensional Euclidean continuous space. Continuum percolation has been used to develop stochastic geometry models of MANETs, such as the coverage and connectivity of mobile wireless sensor networks [32]. Threshold density in continuum percolation determines where there exists a giant component in random systems, which can be calculated numerically from simulations with no known analytical derivation [32]. This is the identical to the determination of critical transmission range in a MANET. It has been shown, assuming each node in a MANET has constant power, there is a phase-transitioning critical transmission power required to ensure with a high probability that two nodes in the network can communicate with each other via multi-hop paths [33]. An accurate estimation for the smaller value of radius r can be made at which, a RGG becomes connected with a high probability. This happens at the critical value r_c for a

RGG under the Euclidean distance in $[0,1)^2$,

$$\pi r_c^2 = \frac{\log(n) + \mathcal{O}(1)}{n} \tag{2.4}$$

where n is the number of nodes and in particular, r_c is a sharp threshold for the connectivity of RGGs. The phase transitions for several graph metrics, including network connectivity, multi-path reliability, and neighbor count, have also been observed along with the critical density threshold [34]. This is important for the configuration of wireless transmission range in MANETs to maintain network connectivity while reducing energy consumption. A simulation-based study has shown that the minimum value for the transmission range can be calculated to maintain full connectivity in ad hoc networks with no strong dependence on mobility models [35]. However, in order to have a well-connected network with multiple paths form one node to the other, the node density has to be far above the critical threshold [36]. The critical density threshold provides a guideline for the selection of transmission range of MANETs. The transmission range can be set higher than the critical threshold to achieve a high connectivity with a greater number of multi-hop paths between node pairs, or it can be relaxed with a lower-than-critical density to satisfy energy constraints but with added links to bridge the disconnected component. An asymptotic distribution of the critical transmission radius and upper bound on the critical neighbor number for k-connectivity has been obtained by modeling MANETs as a uniform n-point process over a unit disc or square [37]. The above theoretical analysis assumes a Poisson node distribution in a unit space; whereas, in many real-world cases, node distribution does not necessarily follow a certain probabilistic pattern. In this dissertation, in addition to the analysis of synthetic mobility models that generate traces with probabilistic distributions, we investigate a set of mobility traces collected in real-world scenarios with irregular node distributions.

2.1.3 Small-World Networks

In a small-world network, most nodes are not neighbors of one another, but can be reached from every other via a small number of hops or steps. A small-world network is characterized by a high average clustering coefficient as in regular networks, and a low average path length as in random graphs. The WS (Watts-Strogatz) model constructs a small-world network by rewiring the links in a regular graph with a probability p, which allows for tuning the network between regularity and disorder [22]. Another method to construct small-world networks is to add long-range links with a certain probability to avoid the possible disconnection of the network in WS model arising from rewiring process [38]. Decentralized algorithms to find paths between nodes have been proposed with a new way to construct small-world networks by starting from a grid network and then adding long-range links with a probability inversely proportional to the Euclidean distance between two nodes [39].

A short average path length facilitates the quick transfer of information. The addition of long-range links provides alternative short paths between some node pairs, which could mitigate the reliability on the original central nodes before link additions. It has been shown that the network connectivity and efficiency of international airline alliances can be improved by providing complementary alliances of carriers as shortcut links [40]. Due to the geographical constraints in MANETs, nodes are locally clustered with a high average path length compared to random graphs. The structure of MANETs is more like that of regular networks with a relatively high average clustering coefficient. While most of the small-world networks in the real world are relational such as hyperlinks in the web, MANETs fall into a different category. MANETs are categorized as the spatial networks in which the existence of a link depends on the distance between a pair of nodes. However, small-world effects have been exploited to improve connectivity in MANETs

by assuming that each node is equipped with multiple radios [41]. More related work about applying small-world networks characteristics to MANETs will be discussed in Section 2.3.

2.1.4 Centrality Metrics

Centrality metrics (degree, closeness, and betweenness) can be traced back to applications in human communications [42]. They have been used as important structural attributes of social networks and later extended to many other fields [43]. Centrality metrics have been utilized as the routing criteria in opportunistic network scenarios [28, 44]. Each of these three metrics plays a different role in the network. Degree centrality is a measure of node communication ability. Both closeness and betweenness centrality are related to the shortest paths between all pairs of nodes. The closeness of a node is the inverse of the sum of the shortest paths from that node. A node's closeness is a measure of the extent to which its communication capabilities are independent of the functioning (or malfunctioning) of other nodes [43]. Betweenness is defined as the frequency that a node falls on the shortest paths between pairwise nodes [43] and is a measure of the degree to which it enables communication between other node pairs.

The unweighted centrality metrics represent the relationship between nodes as a binary measure. However, a more accurate method might be required to describe fine-grained relation between nodes. Generalized centrality definitions that can take into account weighted graphs have been proposed to describe node relationship in a more accurate way [45]. In these definitions, a tuning factor α is introduced to describe the relative significance of link weights as compared to the number of links. Degree centrality of node n_i in a weighted graph is formally defined as:

$$C_{\mathrm{D}}^{w\alpha}\left(n_i\right) = k_i^{(1-\alpha)} \times \left(\sum_{j=1}^{N} w_{ij}\right)^{\alpha} \tag{2.5}$$

where α is a non-negative tuning factor that can be set based on network scenarios, k_i is the number of neighbors, and w_{ij} represents the link weight between n_i and n_j [45]. With a network represented by an adjacency list, degrees of all nodes in the network can be computed in $\mathcal{O}(|\mathcal{N}| + |\mathcal{L}|)$ time both for a weighted and unweighted graph by breadth-first or depth-first traversing the graph once.

The calculation of betweenness and closeness relies on the identification and length of the shortest paths. Similar to the adaptation for weighted degree centrality, both the number of internal nodes on the shortest paths and the weight of these links are important to identify a weighted shortest path. The weights are inverted to represent link cost instead of link strength [46]. Hence, the shortest paths between two nodes j and k is defined as:

$$d^{w\alpha}(n_j, n_k) = \min\left(\frac{1}{(w_{jh})^{\alpha}} + \cdots + \frac{1}{(w_{hk})^{\alpha}}\right) \tag{2.6}$$

where h represents the internal nodes between n_j and n_k, and α is the tuning factor that controls the tendency towards link weights or the number of internal nodes [45]. A weighted version of closeness of node i is calculated as:

$$C_{\mathrm{C}}^{w\alpha}(n_i) = \left[\sum_{j=1}^{n} d^{w\alpha}(n_i, n_j)\right]^{-1} \tag{2.7}$$

One major deficiency of this definition is that the distance between two nodes in different disconnected components would be infinite. Instead of calculating the inverse of the sum, the inverse of the distance can be calculated before summing them up. The inverse of the distance between two nodes in different components will be 0. An improved definition of closeness centrality is defined as

$$C_{\mathrm{C}}^{w\alpha}(n_i) = \sum_{j=1}^{n} d^{w\alpha}(n_i, n_j)^{-1} \tag{2.8}$$

Similarly, by applying the adapted shortest path algorithm, the measure of weighted

betweenness of node i can be obtained as:

$$C_{\mathrm{B}}^{w\alpha}(n_i) = \sum_j \sum_k \frac{g_{jk}^{w\alpha}(n_i)}{g_{jk}^{w\alpha}} \tag{2.9}$$

where $j < k$ and $j \neq i \neq k$, $g_{jk}^{w\alpha}$ is the total number of shortest paths between n_j and n_k, and $g_{jk}^{w\alpha}(n_i)$ is the number of shortest paths that include n_i [45]. The calculation of both closeness and betweenness is based on all-pair shortest paths algorithms. They can be computed with $\mathcal{O}(|\mathcal{N}||\mathcal{L}| + |\mathcal{N}|^2 \log |\mathcal{N}|)$ time for weighted graph by augmenting Dijkstra's short path algorithm and $\mathcal{O}(|\mathcal{N}||\mathcal{L}|)$ time for unweighted graph using modified breadth-first search, both with a space cost of $\mathcal{O}(|\mathcal{N}| + |\mathcal{L}|)$ [47].

Different from degree, closeness, and betweenness centrality metrics that weight every node equally, the eigenvector centrality of a node not only depends on the number of its neighbors but also the value of the neighbors' centrality [48, 49]. The eigenvector centrality $C_{\mathrm{E}}(n_i)$ of a node n_i is defined as:

$$\lambda C_{\mathrm{E}}(n_i) = \sum_{j=1}^{N} w_{ij} C_{\mathrm{E}}(n_j) \tag{2.10}$$

where w_{jk} represents the link weight between n_i and n_j and λ is the largest eigenvalue. With a matrix notation of C_E, Equation 2.10 yields $\lambda C_E = A C_E$ and this type of equation can be solved by the eigenvalues and eigenvectors of A. The eigenvector can be computed using power method [50]. PageRank is considered a variant of eigenvector centrality [51].

Even though centrality metrics capture how central a node is from various perspectives, they might not always be effective to indicate structural importance of each node, as it has been shown that those nodes whose removal could cause the most damage to the network are not necessarily the nodes with high centrality values [52]. Section 2.2.2 introduces more background regarding the identification of the critical node set. We propose a *flexible* metric based on dynamically selected centrality metrics in Chapter 3.

2.1.5 Robustness Metrics

Algebraic connectivity, denoted as $a(\mathcal{G})$, is defined as the second smallest eigenvalue of the Laplacian matrix [53]. The Laplacian matrix of a graph $\mathcal{G}$ with n nodes is a $n \times n$ matrix $L(\mathcal{G}) = D(\mathcal{G}) - A(\mathcal{G})$, where $D(\mathcal{G})$ is the diagonal matrix of node degrees and $A(\mathcal{G})$ is the symmetric adjacency matrix with no self-loops. The normalized Laplacian matrix $L(\mathcal{G})$ can be represented as:

$$L(\mathcal{G})(i,j) = \begin{cases} 1, & \text{if } i = j \text{ and } d_i \neq 0 \\ -\dfrac{1}{\sqrt{d_i d_j}}, & \text{if } v_i \text{ and } v_j \text{ are adjacent} \\ 0, & \text{otherwise} \end{cases}$$

The algebraic connectivity of a complete graph is n for a n-node graph, and is 0 for a disconnected graph. Algebraic connectivity has been widely used for topological optimizations and shown as more informative and accurate than the average node degree when characterizing network resilience [54–56]. Different types of synthetically generated topologies, including WS small-world, Gilbert random, and Barabási-Albert scale-free networks, have been improved by rewiring links with the objective of increasing the algebraic connectivity [56]. It has been shown that algebraic connectivity increases the most when links are rewired between weakly-connected nodes. Another study improved synthetically generated random ER (Erdős-Rényi) and BA (Barabási-Albert) graphs by adding links to the existing topology [54].

Network criticality, denoted as $\tau(\mathcal{G})$, is a graph metric that measures the robustness of networks against topological changes [57]. A smaller value of τ indicates higher network robustness. We note that this metric is also called *total resistance distance* [58]. The

normalized value of $\hat{\tau}$ is calculated as:

$$\hat{\tau}(\mathcal{G}) = \frac{2}{|\mathcal{N}| - 1}\text{Trace}(L^{+}) \tag{2.11}$$

where n is the number of nodes in a given graph, $\text{Trace}(L^{+})$ is the trace of the Moore-Penrose inverse of Laplacian matrix of the given graph [57].

Flow robustness, denoted as $\mathcal{F}(\mathcal{G})$, captures the maximum possible paths for a given topology [59]. It is computed as the ratio of the number of reliable flows to the maximum number of flows in the network. Let $\mathcal{C}$ be the set of components in graph $\mathcal{G}$ and the size of ith $(1 \leq i \leq k)$ component is denoted as c_i. The flow robustness of a graph $\mathcal{G}$ is calculated as:

$$\mathcal{F}(\mathcal{G}) = \frac{\sum_{i=1}^{k} c_i(c_i - 1)}{|\mathcal{N}|(|\mathcal{N}| - 1)}, \qquad 0 \leq \mathcal{F}(\mathcal{G}) \leq 1 \tag{2.12}$$

A flow is considered reliable if there exists at least one path between the source and destination. The maximum number of traffic flows for a connected n-node network is $n(n-1)$. The algorithm to compute flow robustness is based on the computation of connected components, the complexity of which is $\mathcal{O}(|\mathcal{N}| + |\mathcal{L}|)$ by running a breadth-first or depth-first search. Noting that the same approach has also been used to measure network connectivity in [35, 60]. An important feature of flow robustness is that it can capture network connectivity in disconnected networks; however, it cannot accurately distinguish the connectivity level in connected networks. In contrast, graph metrics such as k-connectedness, algebraic connectivity, and network criticality can be exploited to evaluate connected networks with varying levels of connectivity; whereas, they are ineffective to identify critical nodes in disconnected networks.

Average path length, denoted as $\overline{l(\mathcal{G})}$, is the average length of the shortest paths between all node pairs. Let $d(n_i, n_j)$ be the shortest path length between node n_i and n_j, and the

average path length is calculated as:

$$\overline{l(\mathcal{G})} = \frac{\sum_{i \neq j} d(n_i, n_j)}{|\mathcal{N}|(|\mathcal{N}| - 1)} \tag{2.13}$$

A small average path length has been observed in random networks such as ER graphs, as well as in partially random networks such as WS small-world networks, which scales as $\overline{l(\mathcal{G})} \propto \log(|\mathcal{N}|)$ [22, 61]. The estimation of average path length is of great importance for network studies as it delivers basic information on a type of network geometry [62]. A small average path length indicates a small degree of separation between nodes in the network, which allows for an efficient exchange of information among the network as mentioned in Section 2.1.3.

Clustering coefficient of a node n_i is given by the proportion of links between the neighboring nodes divided by the number of links that could possibly exist between them. Let k_i be the number of neighbors of node n_i and l_i be the number of links among those k_i nodes [22]. The local clustering coefficient C_i of the node n_i can be calculated as:

$$C_i = \frac{2l_i}{k_i(k_i - 1)} \tag{2.14}$$

The global clustering coefficient $\overline{C(\mathcal{G})}$ of the whole network is the average of all individual clustering coefficients, which can be represented as:

$$\overline{C(\mathcal{G})} = \frac{1}{|\mathcal{N}|} \sum_{i=1}^{|\mathcal{N}|} \frac{2l_i}{k_i(k_i - 1)} \tag{2.15}$$

It has been observed that many real-world networks, such as social networks, have a higher average clustering coefficient than random networks [63]. The small-world networks generated by rewiring links of regular networks retain the characteristic of the high clustering coefficient of regular graphs [22].

2.2 Modeling and Analyses of MANETs

Various approaches have been proposed to model wired and wireless communication networks [64–66]. Network robustness and vulnerability assessment have been studied for different types of real-world networks [19, 67].

2.2.1 Network and Challenge Modeling

Ideas that are similar to dynamic topology modeling have been pursued in the sociology literature [68, 69]. Weighted graphs represent social interactions between people, and the strength of weight describes the intensity of the relationship between people. The longer duration of time individuals commit to others or the more frequently people interact with each other, the stronger the ties or the friendship between these people tends to be. In the communications network context, simulation framework that models area-based network challenges in wired backbone communication networks has been developed [64, 70]. Due to the dynamics and channel properties of wireless networks, techniques used to improve the disruption tolerance and network dependability, reliability, and availability for wired networks are insufficient for wireless scenarios [14, 15].

For wireless networks, a toolkit to represent obstacle presence and disaster scenarios has been introduced in the ns-2 simulator [71, 72]. A preliminary model of wireless challenges have been presented [64, 70]. Fundamental mathematical properties of MANETs have been studied with networks being modeled using a realistic log-normal shadowing radio model [65, 73]. The graph connectivity of wireless multihop networks has been investigated, and a mathematical derivation between node density and desired k-connectedness has been shown [66]. The impact of the number of placement sources and node density on the performance of WSNs using data centric routing has been examined [74]. Energy saving techniques have been proposed to conserve energy in MANETs without sacrificing

connectivity [75]; however, they have not considered network behavior under the potential challenges of malicious attacks or network element failures. Random spatial models have been applied to various types of wireless networks that allow for standardized rapid benchmarking of wireless network protocols [76]. It has been showed the transmitting power can be adjusted to maintain a region-based connectivity in the presence of region failure [77, 78]. A grid partition technique has been used to identify the vulnerable zones of wireless mesh networks, which can guide network designers to initiate proper network protection against probabilistic region failures [79].

2.2.2 Network Vulnerability

Vulnerability assessment in case of potential malicious attacks is critical to network resilience design. A general graph-theoretical formulation of this problem is removing a certain number of nodes in a graph to maximize the impairment against overall network connectivity, which falls under the class of CNPs (critical node problems). The CNPs are known to be $\mathcal{NP}$-hard on general graphs [19]. Heuristics, branch and cut algorithms, and dynamic programming algorithms have been proposed to solve CNPs; nonetheless, all of them put certain constraints on graph structures such as trees, series-parallel graphs, or sparse graphs [19, 80, 81]. As far as we know, no effective approximation algorithms for weighted graph CNPs have been proposed.

Several localized algorithms has been proposed to detected critical links and nodes whose removal would disconnect the graph [82–84]. However, they only consider whether or not disconnect graph, but ignore how fragmentary the graph becomes. A framework that models the network as a connected directed graph can evaluate network vulnerability by investigating how many nodes are required to be removed so that network connectivity can be degraded to a desired level [67]. Geographic vulnerabilities in networks are evaluated by using 2- and all-terminal methods [85]. It should be noted that the definition of

2- and all-terminal is different from the flow robustness metric. Critical node behavior has been studied using network simulations by only considering discrete static connected topologies [86, 87]. Temporal network robustness is used to measure how communication of a given time-varying network is affected by random attacks [88]; however, it does not address the impact of critical node attacks that could result in higher degradation of network performance.

2.3 Connectivity Management in MANETs

Considering the dynamic and intermittent connectivity of MANETs, there have been various approaches proposed to maintain network performance in MANETs. Critical network service and data can be buffered or replicated at multiple nodes and these nodes can deliver data for each disconnected network component autonomously by manual deployment [89–92]. Node trajectory modification has been used to avoid network partition and ensure the packet delivery [82, 93]. Additional mobile nodes and topology control techniques in MANETs have been widely used to reduce energy cost and improve network connectivity.

2.3.1 Mobile-Agent-Based Improvement

Forwarding nodes with GPS capability that can adjust their locations are deployed to assist network partitions in MANETs [94]. Connectivity of a disconnected ground MANET can be improved by dynamically placing unmanned air vehicles (UAVs) as relay nodes [95]. A gradient-based algorithm to determine the location of a single-UAV has been defined to maximize various network connectivity measures [96]. A connectivity management model has been proposed to conceptualize an autonomous topology optimization for MANETs using multiple mobile agents [60]. A flocking-based dynamic

MANET management system has been proposed to maintain and augment network connectivity by using controlled mobile agent nodes [97]. One of the key challenges of improving network connectivity by using mobile agents is how to determine the positions where mobile agents should be deployed. Due to the dynamic topologies in MANETs, it is critical that mobile agents be deployed to the designated area in a fast and accurate manner. This requires a both fast algorithm to compute optimal positions to deploy mobile agents and also a well-calculated placement of mobile agents while they are waiting for the deployment.

2.3.2 Topology Control

Topology control is one of the most important techniques in MANETs to reduce energy consumption and radio interference while maintaining network connectivity [98]. A distributed topology control algorithm that leverages on location information provided by low-power GPS receivers to build a topology has been proven to minimize the energy required to to communicate with a given master node [99]. Topology control algorithms to adjust transmit power have been proposed to achieve 1-connectedness and biconnectivity in multihop wireless networks [100]. There are two main topology control approaches in wireless networks, homogeneous and non-homogeneous [98]. In the homogeneous cases, nodes are assumed to have the same transmission range, and the topology control problem is reduced to the determination of a transmission range to achieve certain graph properties. In the non-homogeneous cases, different transmission ranges can be assigned to each node as far as they do not exceed the maximum radio power. One of most important topological feature in MANETs is connectivity, and many topology control techniques have been proposed to maintain a connected network. The problem of assigning a transmission range to each node such that the resulting network is connected with minimum energy cost is called range assignment problem [101]. It has been shown that

this problem is $\mathcal{NP}$-hard in both two- and three-dimensional cases with an approximated optimal solution generated from MST [101]. Imposing a topology that is too connected would cause radio interference to occur, which could decrease the capacity of the network. Hence, it is important that the network density is not too high while preserving connectivity. A self-organizing small-world framework for MANETs has been proposed to achieve better performance by rewiring existing omni-directional antennas as randomized long-range directional links [102]. Small-world benefits in wireless networks have been studied by adding long links between randomly chosen node pairs [41,103,104]. Nodes in wireless networks are assumed to be equipped with multiple radios. Directional antennas in wireless networks have been shown feasible to implement [105–108]. In this work, we will also employ the small-world effects to enhance network connectivity by adding links between long-path-length node pairs.

2.4 Quantifying Network Resilience

An evaluation framework has been developed to quantify network resilience in the presence of challenges using functional metrics [15, 109, 110]. We will exploit this framework to evaluate network resilience for various MANET scenarios under attacks based on different graph metrics in Chapter 4. Resilience $\mathbb{R}$ is characterized as the mapping between network operational state $\mathbb{N}$ and service state $\mathbb{P}$. Instead of evaluating the impact of different network scenarios and attack measures separately, which would result in an intractable number of cases, the service can be quantified based on varying operational conditions.

Let the system $\mathcal{S}$ be represented by ℓ operational metrics $N_{\mathcal{S}} = \{N_1, \ldots, N_\ell\}$ with each operational metric N_i $(1 \leq i \leq \ell)$ being a set of m values for all possible settings of the particular operational metric, $N_i = \{n_{i,1}, \ldots, n_{i,m}\}$. The service state space is

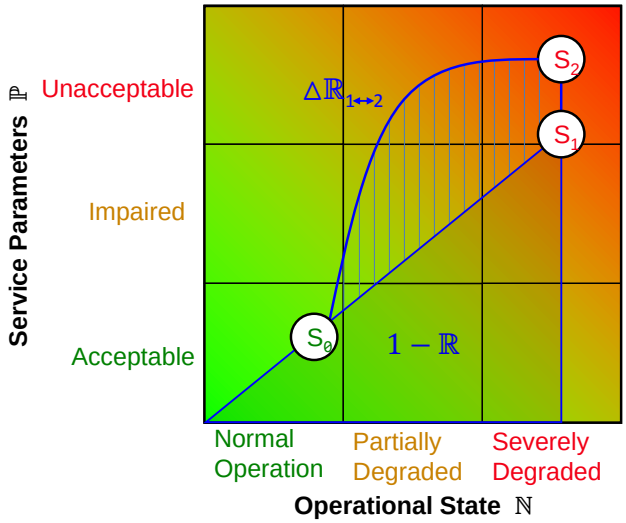


Figure 2.1: Resilience $\mathbb{R}$ measured in the state space

orthogonal to the operational state space. Let service parameters $P_{\mathcal{S}} = \{P_1, \ldots, P_\ell\}$ represent the system $\mathcal{S}$. Each service parameter P_i $(1 \leq i \leq \ell)$ is in itself a set of m values (representing all possible values of the particular service parameter), $P_i = \{p_{i,1}, \ldots, p_{i,m}\}$. The operational state space comprises all possible combinations of the operational metrics and so does the service state space. An *operational state* $\mathbb{N}$ or *service state* $\mathbb{P}$ can be defined as a subset of the complete operation or service state space. Since both operational state space and the service state space could be multivariate, they can be projected to one dimension via objective functions. The objective function could be weighted linear combination or logical function (e.g., AND, OR) [110].

Network resilience can be evaluated in terms of network state transitions under various network challenges. The network operational space $\mathbb{N}$ is divided into *normal operation*, *partially degraded*, and *severely degraded* regions. The service space $\mathbb{P}$ is divided into *acceptable*, *impaired*, and *unacceptable* regions. The resilience for a particular scenario can be quantified as the total area of the square deducted by the area under resilience trajectory. A service state transits when the state of a network is degraded by adverse

events such as malicious attacks. In Figure 2.1, a network service state may take a trajectory $S_0 \rightarrow S_1$ if an adverse event occurs. The resilience value for $S_0 \rightarrow S_1$ can be calculated as the 1 minus the shaded area. Some adverse events could degrade network states more severely than others. The trajectory $S_0 \rightarrow S_2$ exhibits a state transition worse than trajectory $S_0 \rightarrow S_1$. The variance of network resilience under the impact of different network events is denoted as $\Delta\mathbb{R}$. The striped area in Figure 2.1 illustrates that $S_0 \rightarrow S_2$ results in heavier service degradation than $S_0 \rightarrow S_1$, and the difference is $\Delta\mathbb{R}_{1\leftrightarrow 2}$.

Page left intentionally blank.

Chapter 3

Modeling Approach

In this Chapter, we introduce our modeling approach of malicious attacks in MANETs and enhancement strategies to improve MANET resilience. We first introduce the representation of dynamic topologies as an aggregation of topological snapshots within a certain time window size into a weighted static graph. We define a measure, *mobility coefficient*, to determine the window size used for aggregation. We present a network attack example that adaptively applies the node attacks based on centrality metrics. The sum of flow robustness after each node attack is used to measure network robustness under attacks. Next, we introduce the enhancement strategies to mitigate the intermittent connectivity of MANETs and potential attacks against high centrality nodes. The first step is to bridge the disconnected graph components. We propose a MST-based algorithm that can combine disconnected graph components into a connected network with minimum total energy cost. The network is still vulnerable in face of attacks against the articulation points. Motivated by the robust network structure of small-world networks, we further enhance the network by adding long-range links among those node pairs with the largest hop count, which could mitigate the dependence of the global network connectivity on the originally high betweenness nodes.

3.1 Attack Modeling

In real-time MANET communications, it is pivotal that nodes are available as transceivers or relay nodes for each other. A network with a set of fixed nodes and links can be modeled as a static graph. Two nodes are adjacent if they are within the transmission range of each other (with no interference) and are connected if they can be reached via a multi-hop path. We assume node pair communication is symmetric to simplify the graph model for malicious attacks; therefore, undirected graphs are sufficient to model our network. Empirical human contact networks have been shown to be predictable [111], which could be utilized by malicious attackers to disrupt the normal operation of MANETs. Various approaches are possible to obtain or predict network topologies in MANETs [16, 17, 112–114]. For the attacks based on the aggregated graphs, we assume that the future positions of nodes are known in advance for application scenarios such as pre-programmed networks.

A snapshot of dynamic topologies can be represented as a adjacency matrix. We construct a weighted graph to represent network topologies within a certain range of time. Node attacks can be exerted based on centrality metrics, that is, links incident to the node of the highest centrality will be removed from the network, and the next node to be attacked is identified based on centrality values of the updated network.

In this section, we first present the model to construct weighted link availability graphs within certain time windows. Next, we present a metric to determine the aggregation window size by taking into account transmission range and average node velocities. Finally, with an aggregated graph within a selected time window, weighted centrality metrics can be calculated adaptively after the attack of each node. We measure the effects of different centrality-based attacks by evaluating how much degradation of flow robustness with a

varying percentage of node attacks, and the sum of flow robustness after the attack of each node.

3.1.1 Constructing Link Availability Graphs

In a MANET environment, all the nodes are mobile and the pairwise node connectivity is dynamic. The evolution of the network topologies can be described as a sequence of static graphs. We aggregate all the interactions between nodes given a time range into a static weighted graph, in which the link weights represent link availability between node pairs. Figure 3.1 presents a scenario of MANET topologies at six consecutive time steps and Figure 3.2 shows the aggregated graph and its representation as in a matrix. The weight that denote link availability is computed as the ratio of the time duration of being directly connected to the window size. For example, node 1 and 2 are only adjacent at time t_2 out of six time steps; hence, in the aggregated graph, the link weight between them is 0.17. In contrast, node 5 and 6 are connected in all six time steps; therefore, the

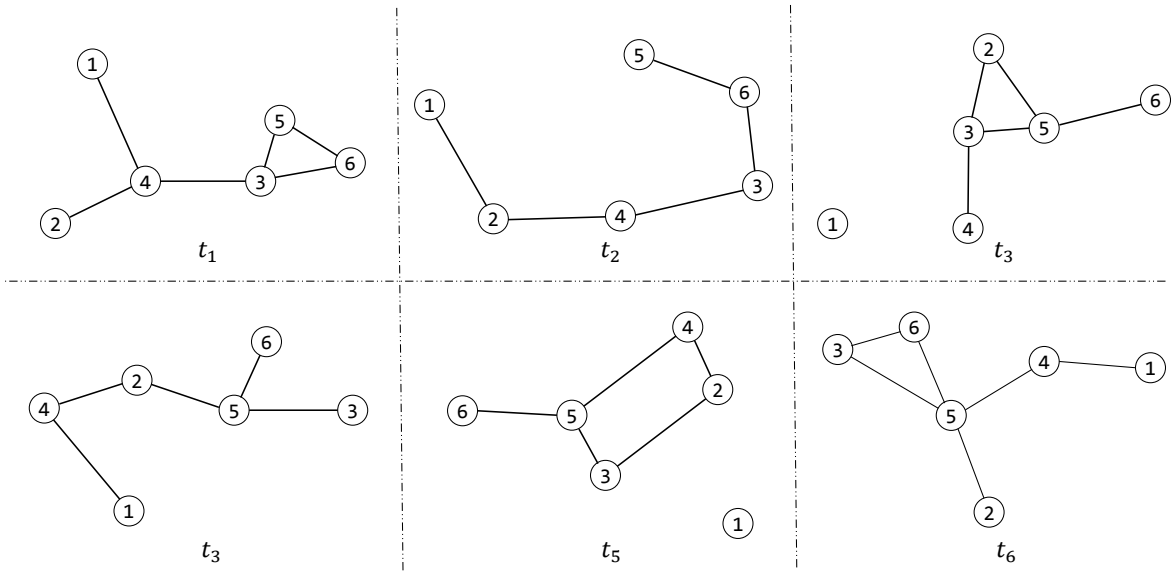


Figure 3.1: MANET topologies at six consecutive time steps

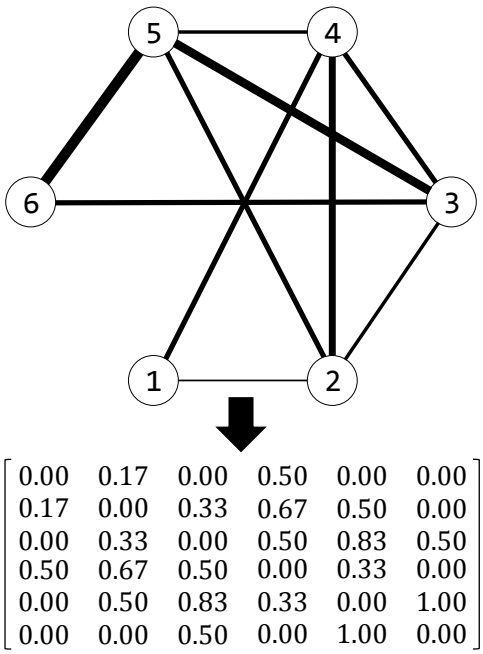


Figure 3.2: Weighted link availability graph and its adjacency matrix

link weight between them is 1.

Our aggregation model differs from many existing aggregation approaches when dealing with dynamic networks. Instead of having a binary weighted graph resulting from the aggregation, our model uses the link availability to represent weights that takes into account not only the existence of links between node pairs but also the intensity of node interactions. Next, we describe how to determine the window size for aggregation.

3.1.2 Determining the Window Size

Dynamic topologies of MANETs can be modeled by aggregating time-varying graphs within a certain time window into a static weighted graph. Based on differing number of nodes, transmission range, and node velocities, the rate of topology changing varies. For network topologies that change at different rates, a uniform aggregation window size is inappropriate. Too small a window size for a low mobility topology results in redundancy

and overhead of calculation; while too large a window size for a high mobility topology leads to the inaccuracy of node significance measured by weighted centrality metrics. Instead of using a uniform window size to aggregate, we compute the average time interval during which the dynamic topologies stay relatively stable. For a given MANET scenario, we define a new measure MC (*mobility coefficient*) as follows:

$$\mathrm{MC} = \frac{\overline{V} \times W_a}{r} \tag{3.1}$$

where $\overline{V}$ is the mean velocity of mobile nodes, W_a is the window size selected for aggregation, and r is the transmission range of the scenario. The product $\overline{V} \times W_a$ provides the average distance traveled by a node within a given time window. Hence, the MC defines the distance change within a given time window relative to the transmission range. Based on a given MC, the window size W_a can be determined as:

$$W_a = \frac{\mathrm{MC} \times r}{\overline{V}} \tag{3.2}$$

A small value of MC results in a small aggregation time window, which provides more accurate identification of critical nodes within the aggregated time than a large value of MC. In Section 4.1.3, our results show that different centrality metrics demonstrate dissimilar behavior with increasing mobility coefficients.

3.1.3 Applying Malicious Attacks

We have established a reference to determine aggregation window size. Given an aggregated graph, attacks are applied adaptively against the important nodes. For each attack target, the graph metrics will be recalculated. It has been shown that node attacks based on recalculated centrality metrics cause more network damage than based on

initial node centrality metrics [115]. We use flow robustness $\mathcal{F}$ to measure the effects of different centrality-based attacks. We provide two perspectives to measure network flow robustness. First, we use a fixed window size and apply node attacks against up to 50% of the total number of nodes. We evaluate how network flow robustness is impacted by varying percentage of node failures caused by malicious attacks using different centrality metrics. As centrality metrics play different roles depending on the network connectivity, they could cause different effects in terms of degrading network robustness. The second method to measure network robustness is to calculate the sum of flow robustness under increasing number of node attacks until there is no path available. We use an example in Figure 3.3 to illustrate a simple scenario of attacking nodes in the topologies shown in Figure 3.2 based on degree centrality. Node 5 is the original highest degree node. After the attack of node 5, all the incident links are removed as shown in Step 1. Then, we calculate the sum of flow robustness $\sum \mathcal{F}$ for each of the six topologies during this time window as shown in Table 3.1. Each column represents the step-by-step flow robustness change for each topology snapshot. We use the mean value $\overline{\sum \mathcal{F}}$ to measure the damage on MANETs caused by a particular type of malicious attacks, and in this case $\overline{\sum \mathcal{F}}$ is 1.311.

Table 3.1: $\mathcal{F}$ of time-varying graphs under node attacks

Step	Attacked nodes	$\mathcal{F}_{t_1}$	$\mathcal{F}_{t_2}$	$\mathcal{F}_{t_3}$	$\mathcal{F}_{t_4}$	$\mathcal{F}_{t_5}$	$\mathcal{F}_{t_6}$
0	None	1.0	1.0	0.667	1.0	0.667	1.0
1	5	0.667	0.667	0.2	0.2	0.2	0.133
2	5, 4	0.067	0.133	0.067	0	0.067	0.067
3	5, 4, 3	0	0.067	0	0	0	0
4	5, 4, 3, 1	0	0	0	0	0	0
$\sum \mathcal{F} = 1.131$		1.733	1.867	0.933	1.200	0.933	1.200

The above attack scenario assumes that we can accurately obtain the node positions in the next time window. In many real-world scenarios, it might be impractical to predict

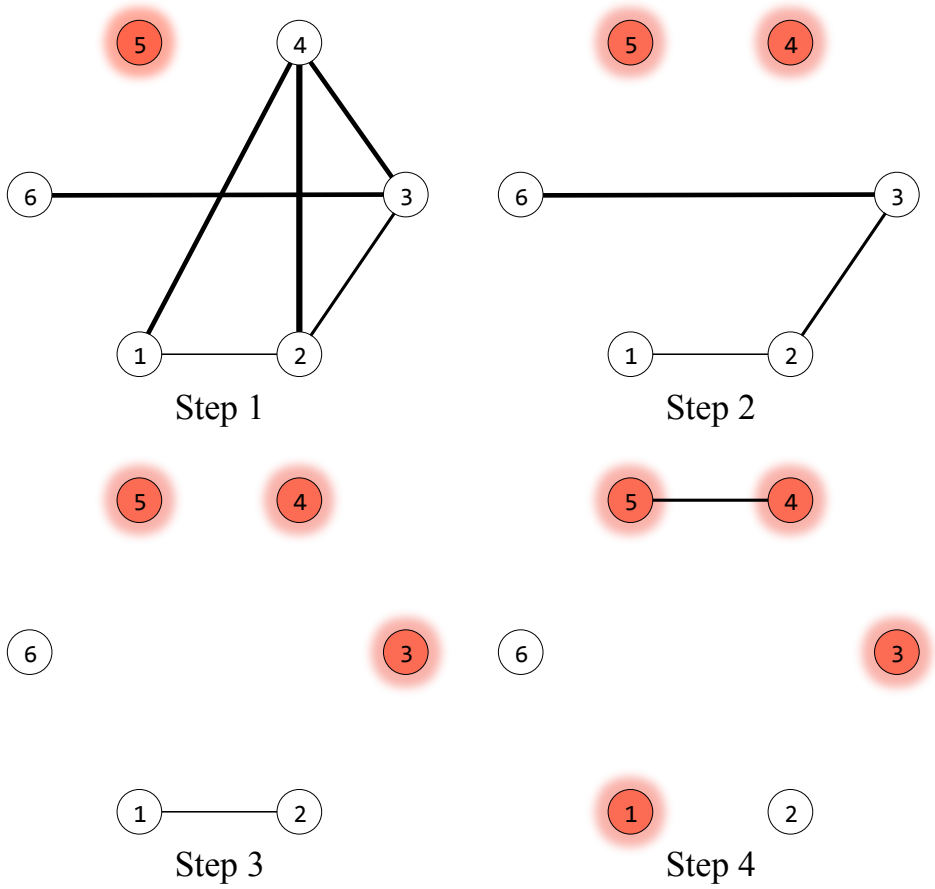


Figure 3.3: Adaptive node attacks based on degree centrality

node positions in the future accurately. By utilizing the correlation of dynamic topologies, we can apply attacks to high centrality nodes in current topological snapshot for the next time window. In this case, we attack the nodes iteratively for all six time steps based on degree centrality of the topology $\mathcal{G}_{t_1}$. We call this strategy real-time attacks in this work. In Chapter 4, we compare the attacks based on the aggregated graphs with attacks using current topology for the next time window that is considered as real-time attack. Our result will show that real-time attacks based on the centrality metrics of current topology perform differently than using varying window sizes.

As mentioned in Section 2.1.4, each centrality metric has its advantages and disadvan-

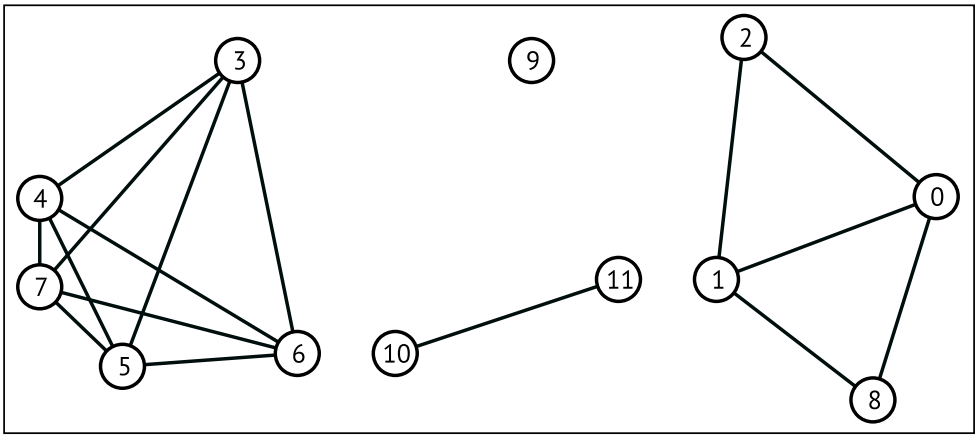


Figure 3.4: Disconnected graph consisting of fully-connected components

tages. We define a new *flexible* attack model that applies attacks against significant nodes based on dynamically selected centrality metrics. In contrast to malicious attacks using a single centrality metric, the *flexible* attack model intelligently chooses centrality metrics to identify nodes with key roles based on global connectivity. In the case of Figure 3.4, all nodes have the same 0 betweenness values. Betweenness-based attacks will randomly select one node; whereas, attacks against one of the highest degree nodes have the greatest impact on the network. The flexible attack strategy can overcome the shortage of betweenness-based attacks in such scenarios. If we calculate the highest betweenness node as n_b and the highest degree node as n_d, attacks will be applied against node n_b if $\mathcal{C}_{\mathrm{B}}(n_b) + \mathcal{C}_{\mathrm{D}}(n_b) > \mathcal{C}_{\mathrm{D}}(n_d)$ and vice versa. The removal of node n_d will impact $\mathcal{C}_{\mathrm{D}}(n_d)$ pairs of nodes; while the removal of node n_b, if resulting in component partition, will impact $\mathcal{C}_{\mathrm{B}}(n_b) + \mathcal{C}_{\mathrm{D}}(n_b)$ pairs of nodes. The node whose removal impacts more pairs of nodes will be selected as the attack target. The complexity of computing attack target using *flexible* strategy is bounded by the computation complexity of node betweenness.

3.2 Enhancement Modeling

Our enhancement modeling is established upon homogeneous MANETs with a uniform transmission range assigned to each node. In addition, we assume that each mobile node carries multiple unidirectional wireless antennas in addition to the omnidirectional radio used for original MANET communications. It has been shown that directional beamforming antennas have tremendous potential of being deployed in ad hoc networks to improve network throughput and reduce end-to-end delay [116,117]. Routing strategies and topology control techniques have been proposed in multi-radio wireless networks to enhance network performance [118, 119]. The enhancement scheme is composed of two steps. Due to the node mobility, the dynamic networks might be partitioned in certain time instants even though the network is well-connected most of the time. We first add the links to bridge the disconnected components of MANETs whenever network partition occurs. The bridging links are computed based on the MST algorithm with minimized total energy cost. Next, we add long-range links to MANETs to further improve the resilience and survivability of networks in presence of malicious attacks. We present four enhancement strategies including two random-based strategies, the longest-path-based enhancement, and a heuristic that adding links to lowest degree nodes to optimize algebraic connectivity.

3.2.1 Bridging Disconnected Components

In our MST model that bridges the disconnected graph components, the goal is to add links to connect all graph components with a minimum sum of energy cost. We exploit a widely used energy model [120–128] to assign the link weight based on the component pair distance. The measurement of energy consumption of a wireless network interface

when transmitting a unit message depends on the range of the emitter u:

$$E(u) = r(u)^{\alpha} \tag{3.3}$$

where α is a real constant usually between 2 and 4, and $r(u)$ is the transmission range of the wireless node. In reality, however, it has a constant to be added in order to take into account the overhead due to signal processing, minimum energy needed for successful reception and MAC control messages [129]

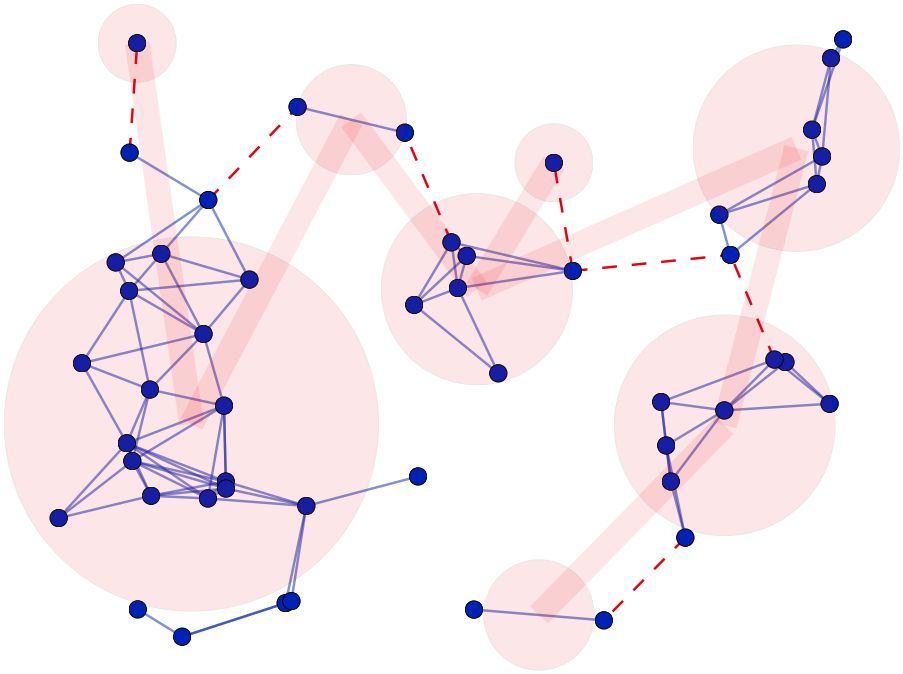


Figure 3.5: A minimum spanning tree to bridge the disconnected components

Figure 3.5 provides an example to using our MST-based approach to bridge a disconnected network consisting of 8 graph components. Each graph component can be represented as a node in the MST graph and the distance between two disconnected graph components is measured by the shortest distance between any nodes in different graph components. Assuming that $\alpha = 2$ in Equation 3.3 and all receivers have the same power

threshold for signal detection, the weight in our MST model is represented as the square of the component-pair distance. The MST algorithm can be run on the fully-connected weighted graph with 8 nodes, and the red dash lines in Figure 3.5 are the actual added bridging links computed based on the MST algorithms.

There are two well-known greedy algorithms for the calculation of MSTs:

Kruskal's algorithm [130] starts with a list of links, sorted by cost, adding one link of the least cost at a time to the constructed MST, if the newly added link does not create a loop in the current MST. Otherwise, the link is skipped. The *Kruskal*'s algorithm can be implemented using a disjoint-set data structure to maintain several disjoint sets of elements. Each set contains the nodes in one tree [131]. The running time of *Kruskal*'s algorithm is $\mathcal{O}(|\mathcal{L}| \log |\mathcal{N}|)$.

Prim's algorithm [132] starts from an arbitrary node in the constructed MST. It constructs the MST by adding one new link of at a time. The new link is selected as the shortest link from nodes in the current version of the MST to nodes not currently in the MST. The algorithm terminates when the constructed MST spans all the nodes. The running time of *Prim*'s algorithm is $\mathcal{O}(|\mathcal{L}| + |\mathcal{N}| \log |\mathcal{N}|)$ by using a Fibonacci heap to implement the min-priority queue [131].

The addition of long links to bridge disconnected components results in a 1-connected network. The network is still vulnerable in face of node attacks or failures as it suffers from single point-of-failure. All the nodes that are incident to the bridging links (red dash lines in Figure 3.5) are the articulation points whose removal would immediately partition the network. As mentioned in Section 2.1.3, the short characteristic path length in small-world network has been applied to wireless networks to improve network reliability. We propose a network enhancement strategy by adding links between the longest-distance node pairs along with two random enhancement strategies and one

heuristic that optimizes the algebraic connectivity by adding links to the lowest degree nodes. Our enhancement strategies assume that each mobile device carries multiple directional radios in addition to the omni-directional antennas used for normal MANET communications.

3.2.2 Enhancement Strategies

We provide four MANET connectivity enhancement strategies by adding long-range links to mitigate the reliance on the high betweenness nodes. Except for the *PR (Pure random)* strategy, the other three enhancement strategies start by adding bridging links, and once the network becomes 1-connected, they select the links based on respective algorithms.

- *PR (Pure random)* enhancement strategy iteratively adds a link between a randomly selected node pair if there is no direct link between them. Otherwise, next random node pair is selected.

- *MR (MST random)* enhancement strategy first adds links to bridge disconnected graph components using MST algorithms. Then, it selects random links in the same way as in *pure random* strategy.

- *LD (Lowest degree)* enhancement strategy is a heuristic that iteratively selects links whose addition would result in the highest algebraic connectivity [133]. The random adding heuristic can be simplified by only considering links that are incident to the lowest degree nodes, as the network connectivity is bounded by minimum node degree $P(\mathcal{G} \text{ is } k\text{-connected}) \leq P(d_{\min} \geq k)$ [134]. Before applying the lowest degree heuristics, we first add the bridging links to obtain a connected network. As network algebraic connectivity needs to be computed once for each heuristic adding, this algorithm is much costly than other strategies.

- *LP (Long path)* enhancement strategy also first adds links to bridge disconnected graph components. Once the network becomes connected, this strategy selects the node pair with the largest hop count (i.e. diameter). If there are multiple node pairs having the same largest hop count, we randomly select one node pair. The complexity of *long path* strategy depends on the cost to find the diameter, which can be obtained by running all-pair-shortest-paths algorithm.

In Chapter 5, we will apply the four enhancement strategies to both synthetic and real-world traces and compare how each strategy performs by evaluating various robustness measures.

Page left intentionally blank.

Chapter 4

MANET Robustness Analysis

In this Chapter, we apply the proposed attack model to both synthetic and real-world mobility traces. We first examine the graph-theoretical properties of synthetic mobility traces generated using different parameters. We investigate the flow robustness of a variety of MANET scenarios under various centrality-based attacks. We run ns-3 [135] simulations to evaluate network performance by sending constant bit rate traffic on top of MANET routing protocols. Finally, we employ the resilience quantification approach mentioned in Section 2.4 to evaluate network resilience under a range of operational states.

4.1 Synthetic Trace Analysis

In this section, we first evaluate a set of graph metrics for MANETs generated using different combinations of network parameters. Then, we select a transmission range for each node number as baseline scenarios. We analyze the sum of flow robustness using a range of window sizes determined by node velocity, transmission range, and mobility coefficient. We evaluate centrality-based attacks using both aggregated and real-time topologies, and compare how the performance of different centrality metrics is affected by the aggregation window size. Finally, we evaluate MANET routing protocols

in ns-3 simulations and compare the PDR (packet delivery ratio) with flow robustness of underlying topologies. The steps of modeling malicious attack in MANETs are shown as follows:

1. Selecting a proper window size for aggregation according to average node velocities
2. Calculating node significance based on aggregated or current time network topology
3. Attacking nodes of high significance for the next time window iteratively
4. Measuring network flow robustness and other graph metrics under malicious attacks

4.1.1 Synthetic Scenarios

Without loss of generality, we choose a simulation area of 1000×1000 m^2 with a node number of 20, 50, and 100. Node velocities are set as a uniform distribution between $[0, 2]$, $[5, 10]$, and $[10, 20]$ m/s, which corresponds to the walking speed of pedestrians, the speed of bicycles, and the city speed of automobiles respectively.

Table 4.1: Synthetic scenario parameters

Simulation area	1000×1000 m^2
Mobility trace duration	1000 s
Mobility model	Gauss-Markov
Number of seeds	10
Number of nodes	20, 50, 100
Node velocity	[0, 2], [5, 10], [10, 20] m/s

As it has been shown that the minimum transmission range to maintain full connectivity in ad hoc networks can be calculated with no strong dependence on mobility models [35], we concentrate our work on the impact of different attack strategies on the network robustness and use the Gauss-Markov mobility model [136, 137] to simulate node movements. Mobility traces are generated for every 0.1 s time interval. We will start with a

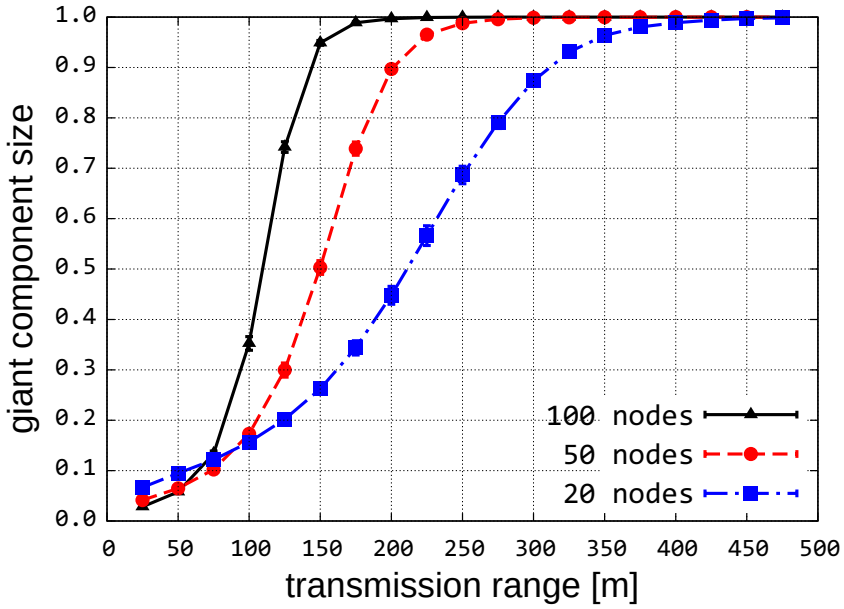


Figure 4.1: Normalized giant component size

MANET of decent connectivity. As mentioned in Section 2.1.2, there is a critical transmission range for MANETs that the network becomes connected with a high probability, which is defined by Equation 2.4. Based on this equation, the critical transmission ranges for 20, 50, and 100 nodes networks are 685, 495, and 380 m respectively in a 1000×1000 m^2 area. This guarantees an almost fully-connected MANET during the entire simulation time by assigning long transmission ranges. One of the issues with using a large transmission range is that it could cause a high wireless radio interference that degrades network capacity. We first study the connectivity metrics of MANETs using varying transmission ranges and select a value that is less than critical transmission range but can still provide a decent network connectivity for MANETs. All the results are provided as an average of 10 different runs with a 95% confidence interval.

Figure 4.1, 4.2, and 4.3 provide normalized giant component size, flow robustness, and probability of MANETs being 1-connected with the transmission range between 25 and 475 m. For the metric of 1-connected probability, each snapshot of dynamic topologies are

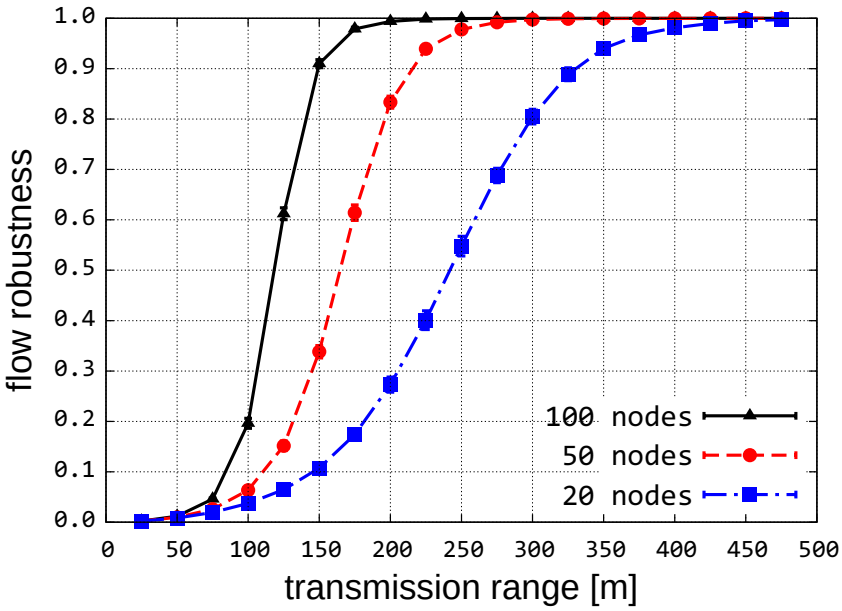


Figure 4.2: Flow robustness

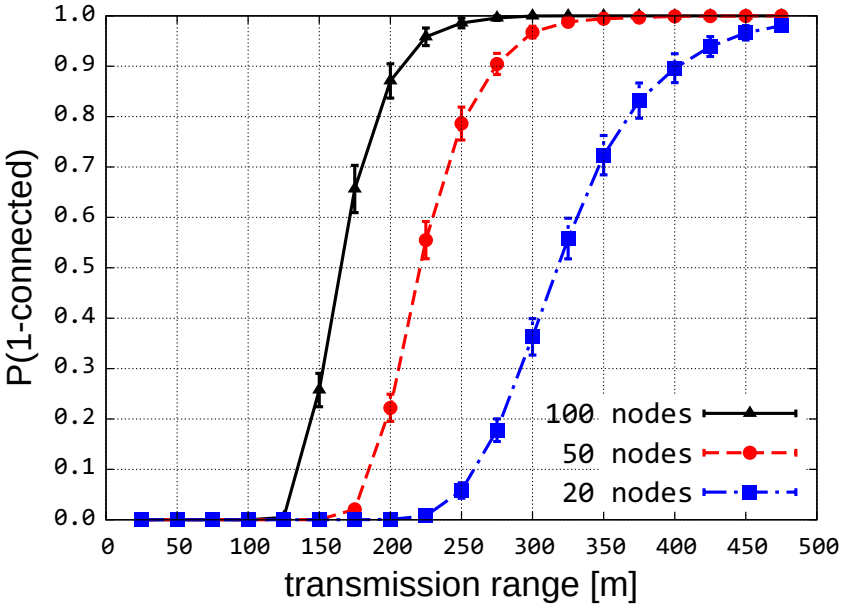


Figure 4.3: Probability of being 1-connected

measured in a binary way, either connected or disconnected. The other two metrics, flow robustness and giant component size, measure MANET connectivity in a more gradated way. With 100 nodes, all three graph metrics increase from 0 to 1 more sharply than 50 and 20 nodes. Within a confined area, MANETs with a larger number of nodes are more sensitive to the change of uniform transmission range. The probability of being 1-connected is a more strict measure than flow robustness and giant component size. For example, with a transmission range of 150 m for 100-node networks, the probability of being 1-connected is approximately 25%; however, both the normalized giant component size and flow robustness are higher than 0.9. This indicates that the majority of nodes are clustered in a connected component, with a small number of nodes disconnected from the giant component. The sacrifice of flow robustness from these small portion of disconnected nodes is trivial if we care about robustness for the entire network.

Table 4.2: Graph metrics of selected transmission ranges

# of nodes	critical tr. range [m]	selected tr. range [m]	avg. node degree	# of components	flow robustness	giant component	prob. of 1-connected
20	685	**350**	5.53	1.31	0.94	0.96	0.72
50	495	**225**	6.67	1.60	0.94	0.97	0.56
100	380	**150**	6.50	2.42	0.91	0.95	0.26

Hence, we select a transmission range for each node number that can provide a higher than 90% flow robustness. We also present average node degrees, average number of graph components for the network scenarios using selected transmission ranges shown in Table 4.2. The normalized giant component sizes of all three scenarios are all above 95%, while there is a large difference in terms of 1-connectedness probability. There is higher chance for nodes being isolated from the giant component with a large number of node numbers. The average node degrees for three scenarios are close to each other, which indicates the levels of potential wireless interference among neighboring nodes.

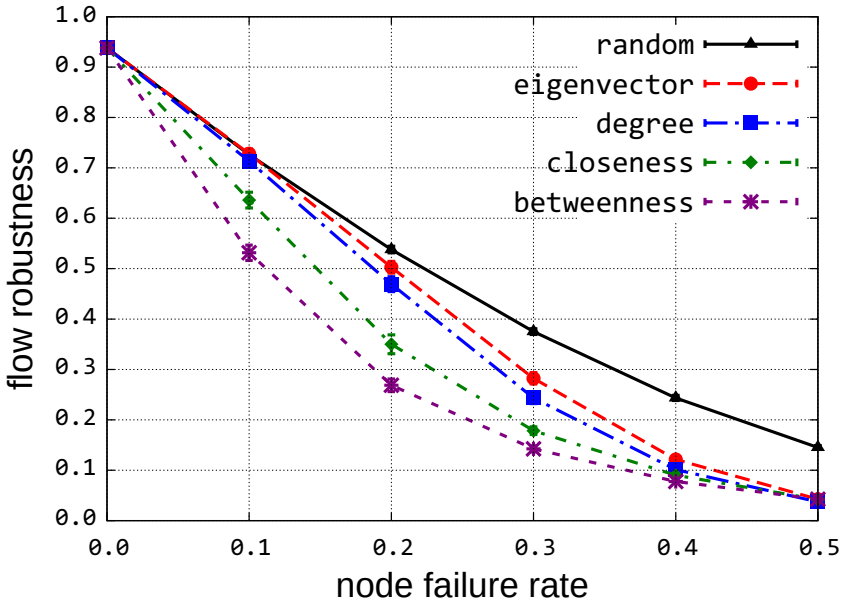
Table 4.3: Windows sizes for different scenarios with MC = 0.1 and 0.5

	Window size [s] (MC = 0.1)			Window size [s] (MC = 0.5)		
Node number	[0, 2] m/s	[5, 10] m/s	[10, 20] m/s	[0, 2] m/s	[5, 10] m/s	[10, 20] m/s
20	35.0	4.7	2.3	175.0	23.3	11.7
50	22.5	3.0	1.5	112.5	15.0	7.5
100	15.0	2.0	1.0	75.0	10.0	5.0

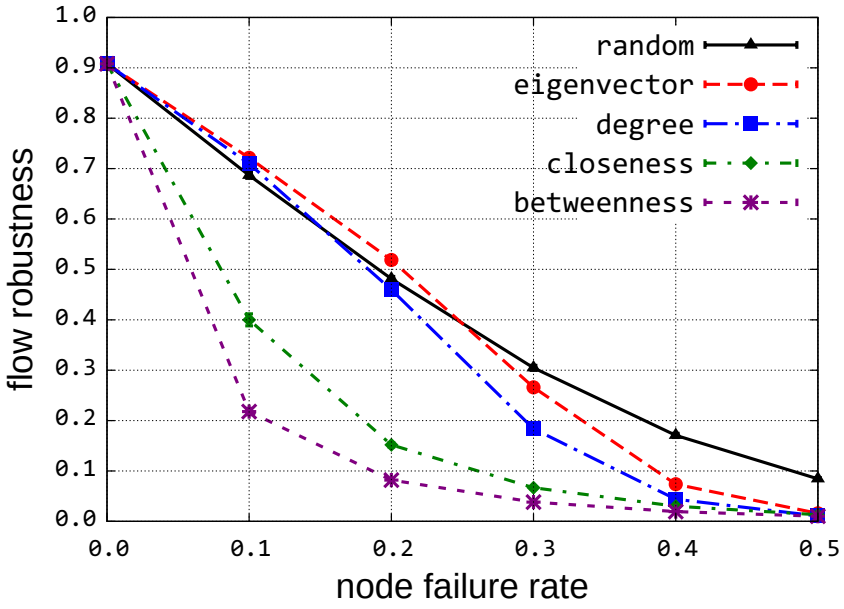
The selection of a window size for aggregation is esentially a tradeoff between computation complexity and the accuracy of identifying significant nodes. According to the transmission ranges suggested in Table 4.2, we examine how MANETs are affected by various malicious attacks for all combined scenarios with MC values ranging from 0.1 to 0.5. Table 4.3 provides the window sizes for MC = 0.1 and MC = 0.5 computed using Equation 3.2. We can observe that there is large variation of the window sizes for different scenarios, which could be as small as 1 s for 100 nodes with [10, 20] m/s; the window size could also be as large as 175 s for 20 node with [0, 2] m/s velocity.

4.1.2 Attacks Based on Aggregation

We first examine the flow robustness change under an increasing number of node attacks using MC = 0.1. In Figure 4.4, we provide average network flow robustness under random failures and various centrality-based attacks for 20 and 100 nodes scenarios. We apply node attacks up to 50% of the total number of nodes. The betweenness-based attacks result in the highest degradation of network flow robustness with node attacks up to 40% in both 20 and 100 nodes scenarios. When there are 50% of node being attacked, all the centrality-based attacks converge to a similar value; however, they still have a greater impact on the network than random node failures. Closeness-based attacks degrade network flow robustness less than betweenness but cause greater damage than others. It is worth mentioning that with 10% node attacks that cause relatively slight



(a) 20 nodes

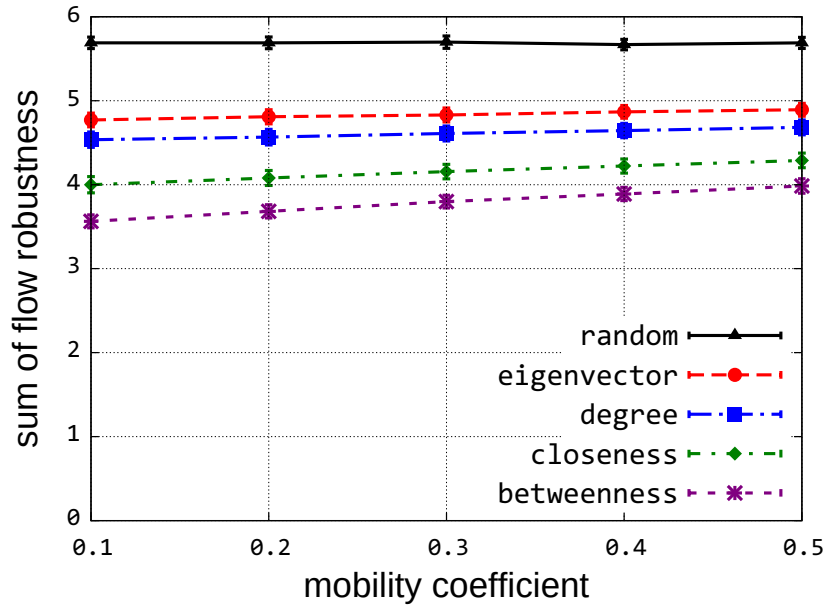


(b) 100 nodes

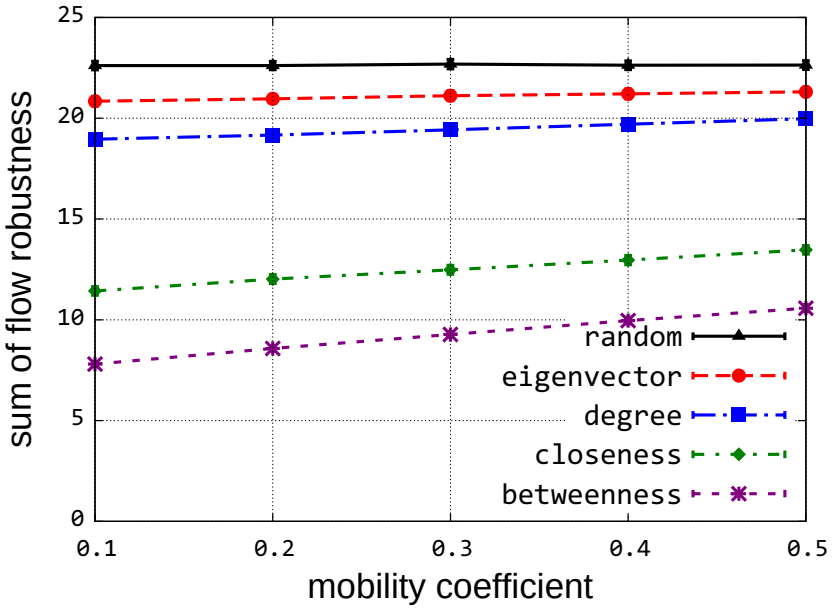
Figure 4.4: MANETs under simultaneous node attacks

damage in the networks, degree and eigenvector-based attacks have no greater impact than random node failures. Especially, in 100 nodes networks, the removals of high degree and eigenvector nodes result in even less damage on the network connectivity than random nodes failures. With a small percentage of nodes being attacked, the nodes with more neighbors play trivial roles in terms of its contribution to the global network connectivity. This observation becomes more obvious in a larger network. In comparison, the high-betweenness nodes play a more vital roles than other other centrality metrics. Particularity, node betweenness can identify the most significant nodes better in the 100 nodes networks than in 20 nodes networks. This is because the calculation of node betweenness relies on the all-shortest-paths in the network.

Figure 4.5 provides the sum of flow robustness that is equivalent to the area under each curve in Figure 4.4 by extending to 100% of node attacks in x-axis. We use a varying mobility coefficient that reflects a range of aggregation window sizes. In both Figure 4.4a and Figure 4.4b, the sum of flow robustness increases slightly with MC increasing from 0.1 to 0.5. As expected, with a larger aggregation window size, the high centrality nodes become less accurate. The degree-based attacks are less affected by the window size, which indicates from another perspective that the high degree nodes are less affected by the change of dynamic topologies. All centrality-based attacks result in a lower sum of flow robustness than random node failures. In 100 nodes scenarios, degree- and eigenvector-based attacks are closer to random node failures than in 20 nodes networks, while the gap between degree-based and betweenness-based attack are larger in 100 nodes networks. This again demonstrates that all-shortest-paths based centrality metrics including betweenness and closeness provide a more accurate identification of significant nodes than other centrality metrics in terms of the nodes' contribution to the global connectivity.



(a) 20 nodes



(b) 100 nodes

Figure 4.5: Sum of flow robustness with varying mobility coefficient

4.1.3 Real-Time Attacks

As we have already understood the relative effect of centrality metrics on the degradation of flow robustness, we select degree, closeness, and betweenness centrality metrics to compare real-time attacks to the attacks based on aggregation. We aslo include the flexible attacks for real-time scenarios. Figure 4.6 and 4.7 presents the comparison of flow robustness between real-time attacks and complete information attacks with 20 and 50 nodes. The results for 100 nodes scenarios are shown in the Appendix A. For real-time attacks, the priority of nodes to be attacked is determined according to the centrality metrics of the initial topology of each time window, and for attacks with complete information, the attack priority is computed based on the aggregated weighted graph of the entire time window. As shown in Figure 4.6 and 4.7, flow robustness under complete information centrality-based attacks is slightly lower than real-time attacks for the same metric as expected, since attacks with complete information can identify significant nodes more precisely by taking into account all the topological information within the time window. It is worth noting that degree-based attacks using real-time topology information cause almost the same damage as using aggregated topologies. This indicates that the highest degree nodes are less affected by the topology change. In contrast, the closeness- and betweenness-based attacks based on real-time information cause less damage than based on the aggregated graphs. In particular, in the 50 nodes networks, the difference between real-time and complete information attacks using closeness and betweenness is greater than in the 20 nodes networks.

Figure 4.8 and 4.9 compare the sum of flow robustness $\sum \mathcal{F}$ based on real-time and aggregated topologies for 20 and 50 nodes information. The 100 nodes results are shown in the Appendix A. Of all the curves shown in the two Figures, we compare the degree-, closeness-, and betweenness-based attacks for both real-time and aggregated approach.

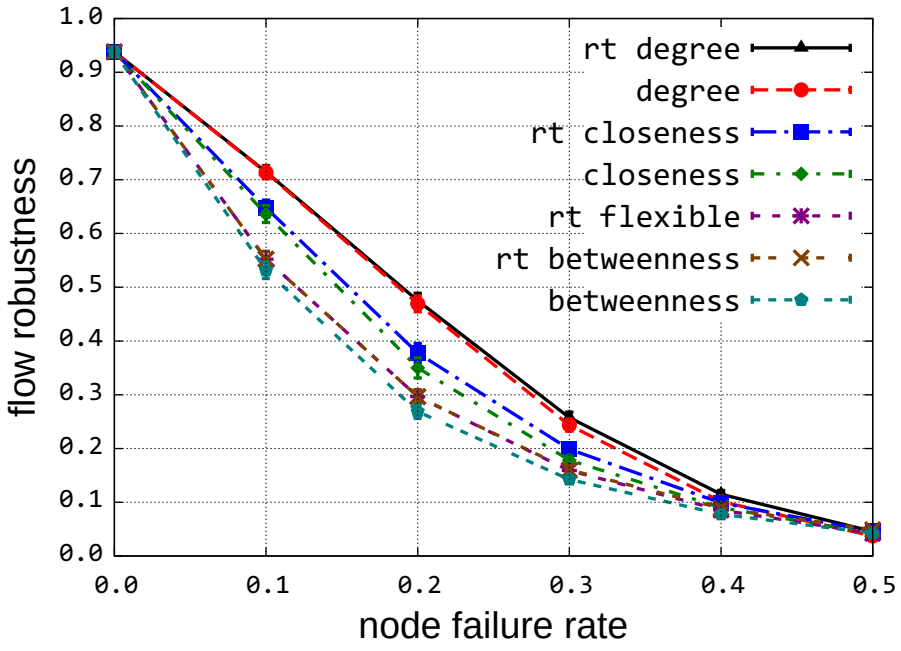


Figure 4.6: 20 nodes MANETs under real-time simultaneous node attacks

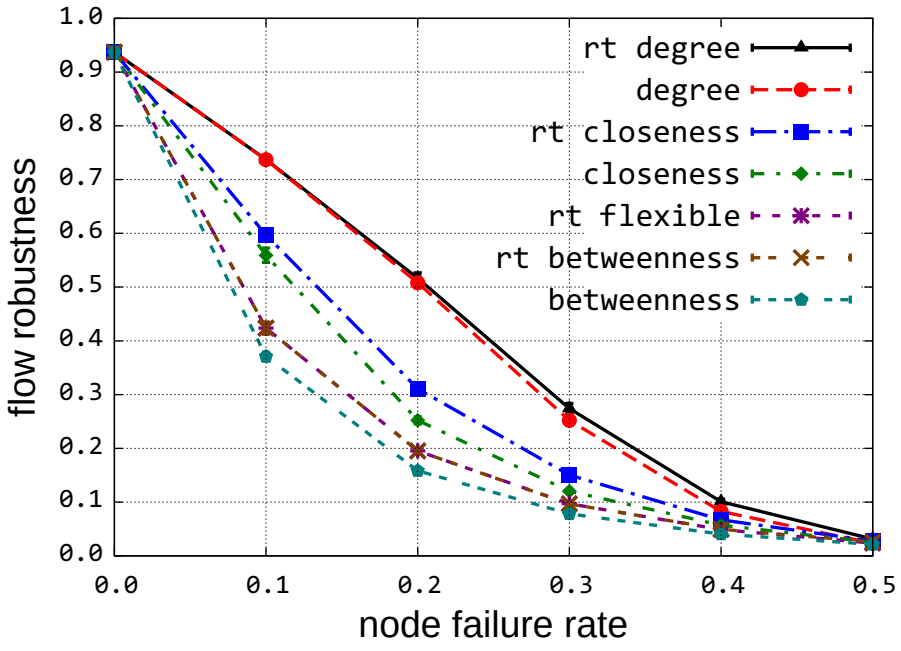


Figure 4.7: 50 nodes MANETs under real-time simultaneous node attacks

In addition, we include the flexible centrality metric that overcomes the inefficiency of betweenness in disconnected networks. The MC in the x-axis reflect the window

sizes. With the increase of MC, the $\sum \mathcal{F}$ for all attack strategies increases as expected. The $\sum \mathcal{F}$ increases faster in real-time closeness, betweenness, and flexible attacks than in other scenarios. This means that aggregated approach can provide more accurate identifications of high centrality nodes than using the real-time approach with a larger window size. With MC = 0.1, *closeness* > rt-betweenness > rt-flexible > betweenness; when MC increase to 0.5, rt-betweenness > rt-flexible > *closeness* > betweenness. It is worth noting that the rt-flexible curve is always lower that rt-betweenness curve although the difference is slight. The real-time centrality metrics based computed based on all-paths-shortest-paths algorithms are more sensitive to the increase of window sizes. The high closeness and betweenness nodes change faster than high degree nodes when the global topological structure changes. Even though nodes are moving constantly within the certain simulation area, the local structure of the entire network remains relatively stable in that nodes with the highest degree centrality do not vary much within each time window. The difference of flow robustness under real-time and complete information attacks is slight with a small MC, which means that historical mobility trace information can be exploited by malicious attackers to understand network topological structures and then determine the most vital nodes to be attacked.

4.1.4 Simulations in ns-3

In this section, we select a list of network parameters shown in Table 4.4 to study the network performance running MANET routing protocols. In the simulation, every node sends constant bit rate traffic to every other node and we only select 20 nodes for ns-3 simulation since a high number of nodes results in severe network traffic collisions when all of them attempt to send packets to other nodes at the same time. We use PDR (packet delivery ratio) to measure network performance in the application level, which is computed as the ratio of delivered packets to the total number of packets being sent

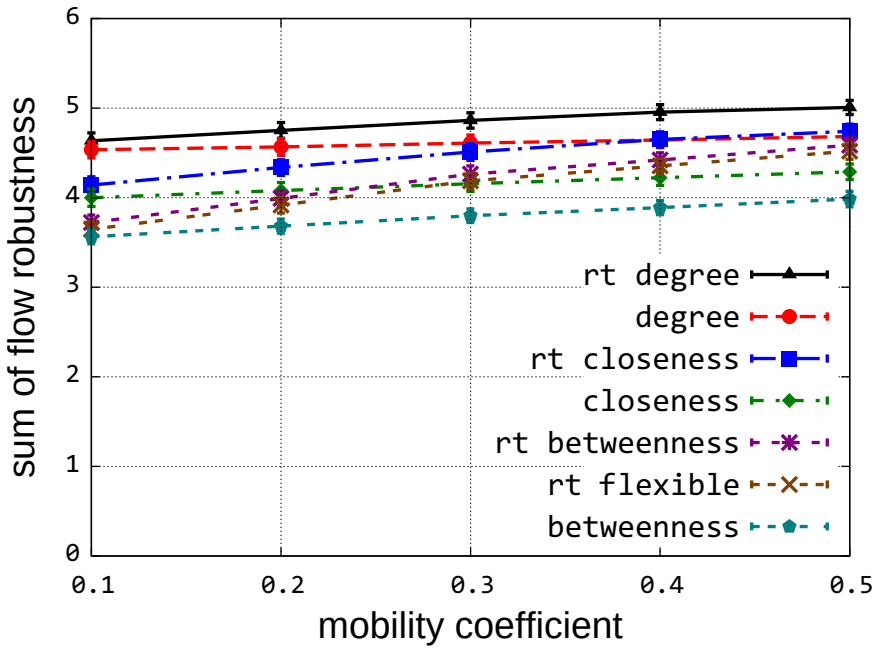


Figure 4.8: 20 nodes MANETs under real-time simultaneous node attacks

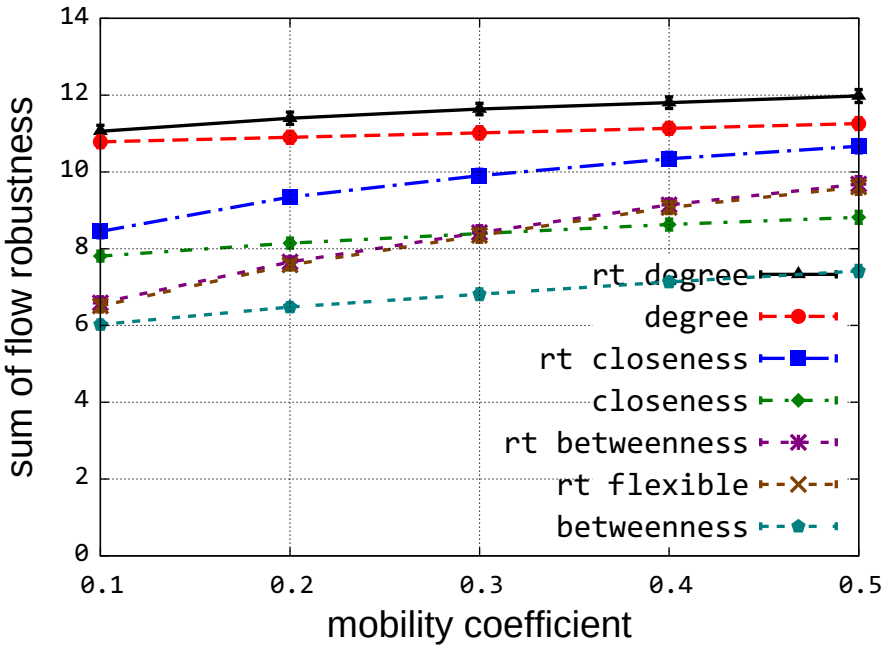


Figure 4.9: 50 nodes MANETs under real-time simultaneous node attacks

out. We use AODV as the routing protocols as it provides the highest baseline PDRs without being attacked.

Table 4.4: Simulation parameters of synthetic traces in ns-3

Number of iterations	10
Traffic generation time	1000 s
Transmission range	350 m
Simulation area	1000×1000 m^2
Mobility model	Gauss-Markov
Number of nodes	20
Window size	35 s (MC = 0.1)
Physical channel	802.11g (54 Mb/s)
Routing protocol	AODV
Node velocity	[0, 2] m/s
Traffic model	CBR (constant bit rate)
Traffic type	UDP
Traffic flows	380 (20×19)

We compute the window size based on MC = 0.1. The simulation results present PDRs of networks under different centrality-based attacks. Many factors could lead to the variation of end-to-end throughput, such as AODV routing table updates, hidden terminals, and network congestion, even though we try to minimize the impact of these factors in our simulation. We compare PDR with flow robustness that provide the underlying theoretically highest network performance under attacks. In order to display each curve in the plots clearly, we only select random, degree, and betweenness centrality for the comparison. As shown in Figure 4.10, the analytical flow robustness is always slightly higher than the PDR as expected, since flow robustness is a theoretical upper limit for PDR if all packets can be delivered with no delay whenever there is an available path. For both PDR and flow robustness, the relationship for network performance under attacks always follows as: random > degree > betweenness.

It is apparent that centrality metrics based on either aggregated graph or instant topology become less precise if we increase the window size. Flow robustness of underlying topologies is essential to the quality of service in the application layer. Ideally, if all the packets can be delivered across different layers instantly, PDR under the same types of

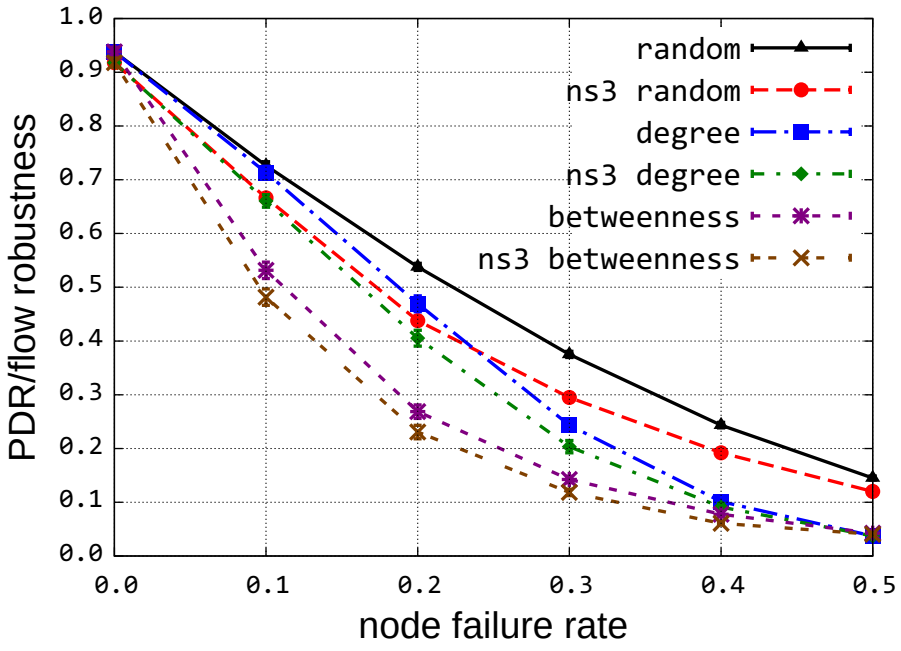


Figure 4.10: ns-3 vs. topological analysis with 20 nodes

attacks should be almost equal to flow robustness. In theory, flow robustness provides the best network performance under certain types of attacks. As network density increases, wireless channel effects and packet loss/drop during transmission could degrade network performance more heavily in the application layer.

4.2 Real-World Trace Analysis

The synthetic trace analysis provides insights into how MANETs are affected by centrality-based attacks in general cases. In the real-world scenarios, network parameters such as moving areas and distribution of node positions might be more case-specific. For example, the simulation area are usually not in regular shapes in the real-world sites. In addition, the positions of all nodes might not follow a Poisson distribution and the movement of nodes might not follow a Gauss-Markov pattern. In this section, we employ human mobility traces collected from five different sites [138] to evaluate our malicious

attack model. These traces were originally used to study the statistics of human mobility pattern and the similarity between humans' walking and Lévy Walks [139]. The data sets provided are 30 seconds average of GPS coordinates recorded using Garmin 60CSx handhold devices. Table 4.5 presents basic information regarding the five traces.

Table 4.5: Five sites of real-world mobility traces

	KAIST	Orlando	NewYork	NCSU	StateFair
# of traces	83	41	39	35	19
Min. duration [s]	15180	7860	4440	6180	5340
Pause-time [s]	5440	1546	1382	2490	380
# of clean traces	72	26	21	25	19

4.2.1 Data Set

The five real-world mobility traces provide a range of network sizes and connectivity levels for us to investigate a variety of realistic MANET scenarios. Before exploiting theses real-world traces for our attack analysis, we need to first clean the recordings of node positions in the trace files. There are occasional cases that GPS signals cannot be received when GPS holders move indoors in the original data sets. In addition, the average speed during a 30-second window for some nodes is calculated as high as 200 m/s based on the original trace. We remove the traces from the data sets if there is any occurrence of velocity higher than 20 m/s during a 30-second time window. The number of traces after the removal of corrupted data in each site in shown in Table 4.5. The NewYork traces were collected from volunteers living in the Manhattan NY area, and they traveled by cars and buses. The KAIST and NCSU traces were collected in two campuses, one in Korea Advanced Institute of Science and Technology and the other in North Carolina State University. The Orlando traces were obtained from volunteers who spent their holidays in the Disney World. The StateFair traces were obtained from

participants who went to the North Carolina State Fair. This set of traces were collected outdoors, and the size of the StateFair site is the smallest of all. As each trace in the same site lasts for different durations of time, we truncate all traces based on the minimum trace time for each site. The trace duration used for each site is listed in the third row of Table 4.5. The second row provides the number of traces collected for each site.

In real-world MANET scenarios including the five sites used here, the actual network density depends on the number of nodes and transmission range of each node. In this work, the number of nodes in MANETs is based on the number of traces provided in the data sets even though the node number in a real case could be significantly higher since only a small portion of people are selected as candidates for trace collection. Theoretically, the transmission range can be adjusted by increasing the radio power of handhold devices. Noting that handheld devices are mostly battery-powered, the transmission range cannot be increased infinitely. We choose 250 m to 1000 m as an acceptable range.

In Table 4.5, we also present the average pause-time of all nodes for each site. Pause-time is the duration a person halts before moving to another location. The StateFair site has the smallest average pause-time, which accounts for about 7% (380/5340) of the entire trace duration. In contrast, the pause-time of KAIST and NCSU account for a very high percentage of entire trace duration, which indicates the dynamic topologies remain stable most of the time.

We analyze the distribution of node velocities for all 30-second windows. The CCDF (Complementary Cumulative distribution function) of node velocities are presented in Figure 4.11. Both x and y axes use log-scale. It is apparent that node velocities follow a non-linear distribution. For the NCSU and StateFair sites, almost 90 percent of velocities are distributed below 1 m/s while the maximum velocity for NCSU is around 20 m/s. The velocity of the New York site is generally higher than the other 4 sites, and probability of

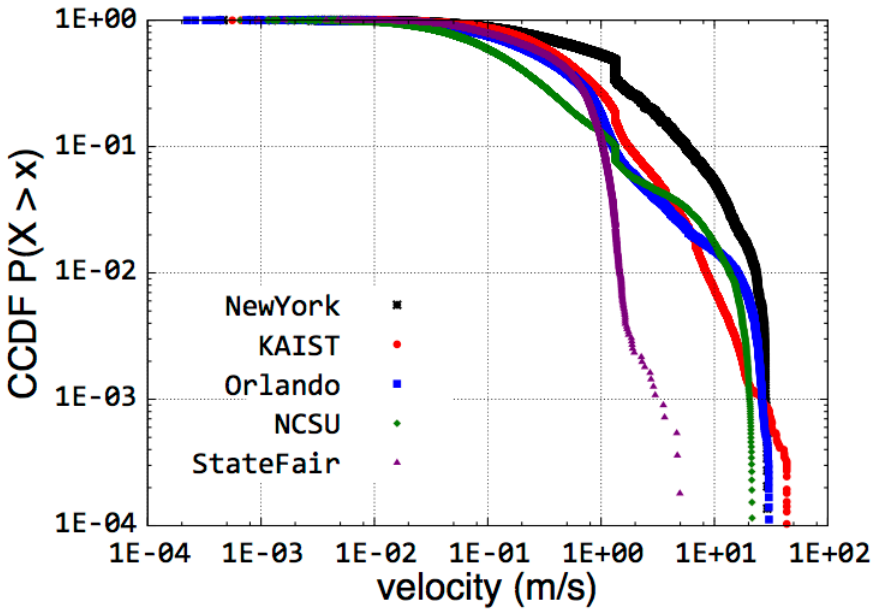


Figure 4.11: CCDF of average node velocities

velocity higher than 5 m/s is approximately 0.1. About 80% of velocities in the KAIST site is less than 1 m/s while the maximum velocity could be as high as 50 m/s. The non-uniform distribution of node velocities cannot be captured by synthetic mobility models such as Gauss-Markov. This also poses a big challenge for MANET robustness as whenever nodes start moving with a high speed, the network performance cannot be guaranteed.

We also present average flow robustness, node degree, average giant component size of each site using 3 different transmission ranges in Table 4.6. With the same transmission range, the StateFair site has the highest average flow robustness of all. When the transmission range is 1000 m, the network becomes a full-mesh as the average giant component size is equal to the total number of nodes. The NewYork site has the lowest average flow robustness. Even when the transmission range is set to 1000 m, the average node degree is 2.8 noting that there are 39 nodes in total. The average flow robustness of the Orlando site is slightly higher than NewYork but still presents a very low network

connectivity. The average giant component size of the KAIST site with 500 and 1000 m transmission range are 73.1 and 75.2, while the average degree almost doubles from 27.8 to 53.9. This means that there are several nodes moving far apart from the largest node clusters, and the increase of transmission range only leads to a higher connectivity within a local cluster with other nodes still isolated from the giant component.

Table 4.6: The Statistics of all sites

Site name	Avg. flow robustness			Avg. node degree			Avg. giant comp. size		
	tr(250)	tr(500)	tr(1000)	tr(250)	tr(500)	tr(1000)	tr(250)	tr(500)	tr(1000)
KAIST	0.509	0.777	0.822	15.6	27.8	53.9	56.6	73.1	75.2
Orlando	0.167	0.208	0.233	3.8	7.1	8.5	12.1	13.0	14.0
NewYork	0.022	0.041	0.190	0.8	1.2	2.8	4.2	5.6	14.6
NCSU	0.112	0.238	0.488	3.5	4.8	9.5	9.5	13.7	23.9
StateFair	0.825	0.993	1.000	6.8	13.9	17.9	16.6	18.9	19.0

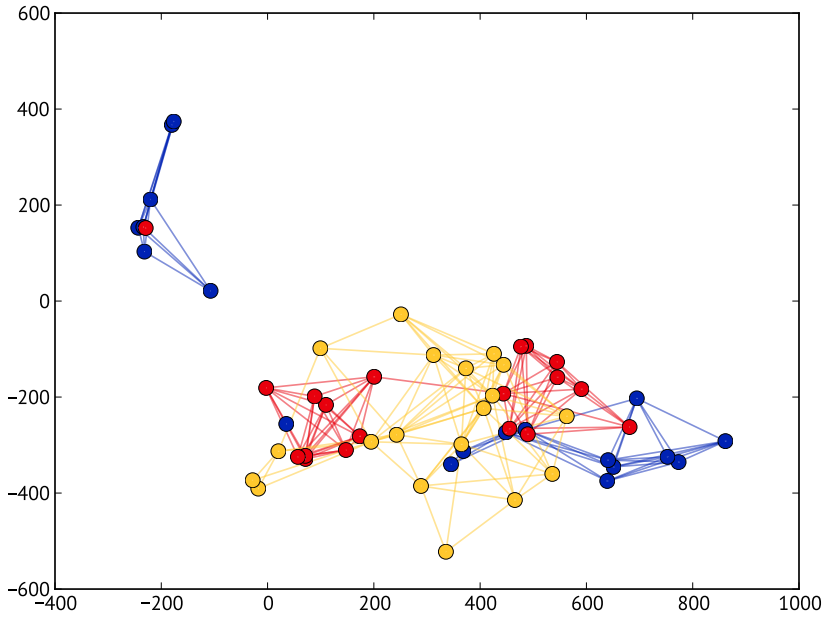


Figure 4.12: Snapshots of Statefair trace with tr = 250

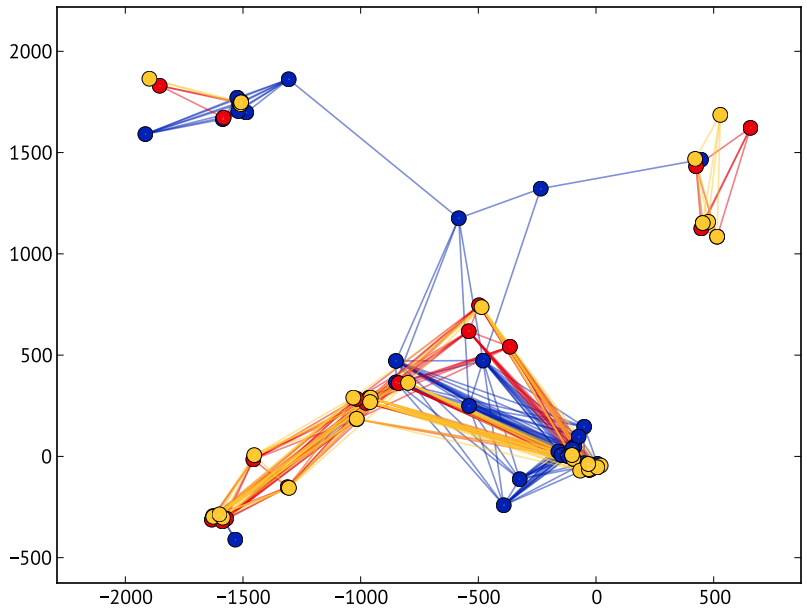


Figure 4.13: Snapshots of NCSU trace with tr = 1000

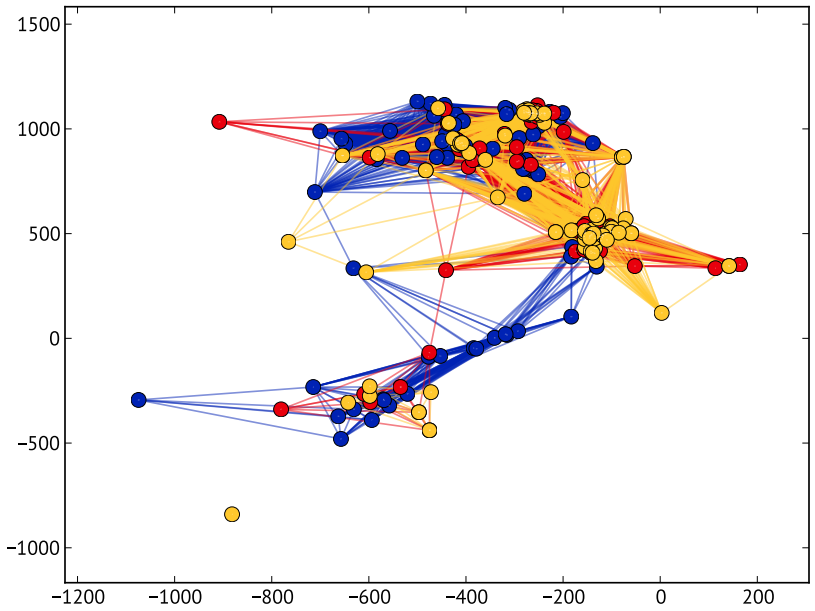


Figure 4.14: Snapshots of KAIST trace with tr = 500

The normal functioning of MANETs requires network connectivity to remain above a certain level since all routes are established in real time. For the flow robustness analysis, we will focus on StateFair, NCSU, and KAIST. In the original data set, both the x and y coordinates are recorded as the distance from a reference point in meters. We present the snapshots of the selected three sites. Each color represents the snapshot of start (blue), middle (red), and end point (yellow) of the traces respectively. In Figure 4.12, it can be observed that the StateFair traces are confined within a relatively small area (1200×1000 m^2). Both NCSU and KAIST site span a large area with most nodes clustering around a particular part of the map, as shown in Figures 4.13 and 4.14.

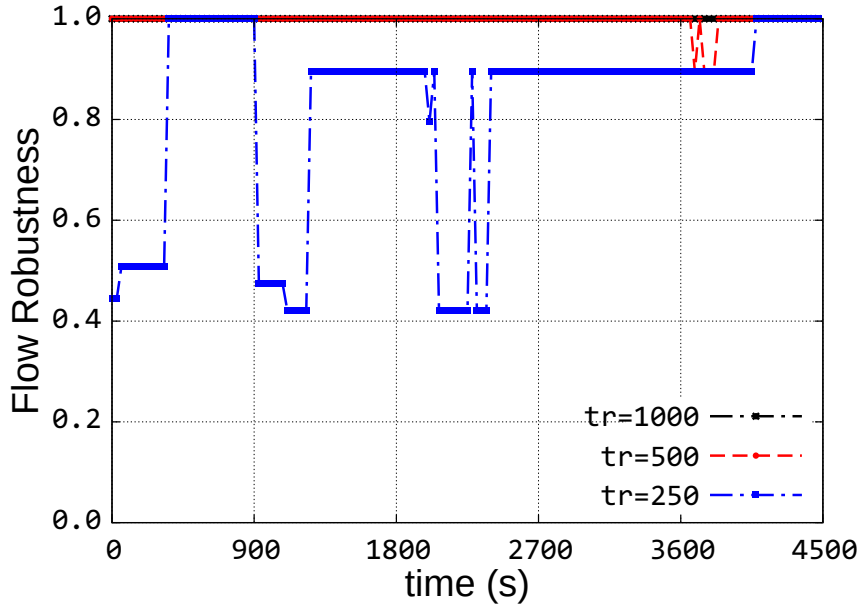
4.2.2 Topological Analysis

Network robustness changes over time as nodes disconnect and reconnect to others constantly. We compute the flow robustness for each 30 s topology snapshot, and then calculate the autocorrelation between time-varying flow robustness. In order to compare fairly among three different sites, we only analyze first 4500 s trace data. Figure 4.15, 4.16, and 4.17 present time-varying flow robustness and the corresponding autocorrelation coefficient $R_{\text{StateFair}}$, R_{NCSU}, and R_{KAIST} for the StateFair, NCSU, and KAIST sites using different transmission ranges. For the StateFair site, flow robustness is always 1 for 1000 m transmission range; hence, we do not provide the autocorrelation for this scenario as the variance is 0. For 500 m transmission range, StateFair flow robustness falls below 100% for a short period of time after 3600 s and remains at 100% for the rest of time. This indicates a very high network connectivity as we can also see that average giant component size is 18.9 from Table 4.6. For StateFair traces with 250 m transmission range, flow robustness fluctuates between 50% and 100%. $R_{\text{StateFair}}$ displays a linear decrease to 0 within 300 s, and certain levels of periodicity are observed since participants of North Carolina State Fair are moving in a relatively confined area. Flow

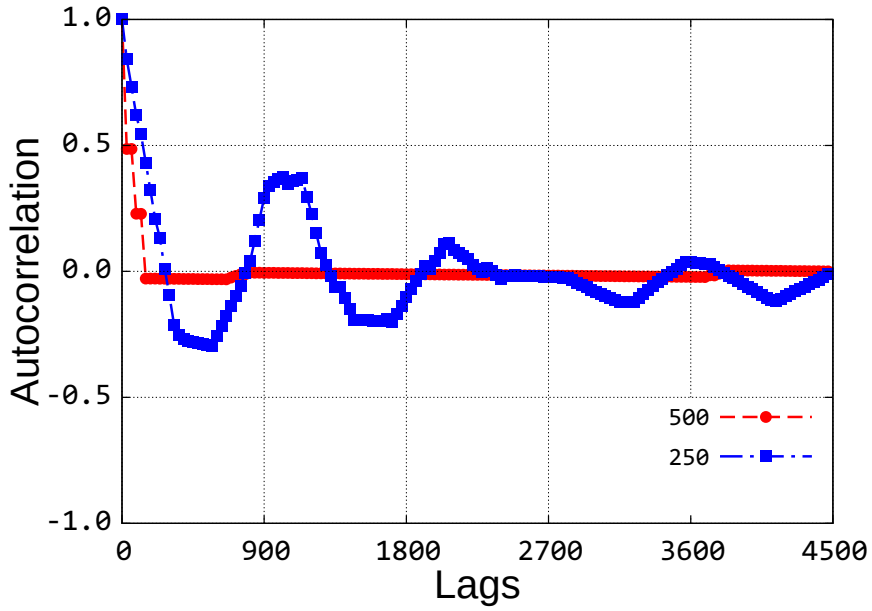
robustness of the NCSU site increases during specific short time windows as shown in Figure 4.16a. R_{NCSU} with a 250 m transmission range is weaker than 500 and 1000 m transmission ranges. As shown in Figure 4.13, the majority of nodes move slowly within a small area in the map, and a smaller transmission range causes the nodes to disconnect from others more frequently.

Flow robustness of the KAIST site shows the strongest autocorrelation of all three sites. Similar to R_{NCSU}, R_{KASIT} is higher with a longer transmission range. R_{KASIT} with 500 and 1000 m transmission ranges presents a more linear decrease, and time-varying flow robustness is strongly correlated within 1800 s. R_{KAIST} with 250 m transmission range decreases to 0 significantly faster than with 500 and 1000 m transmission ranges. As shown in Figure 4.17a, flow robustness oscillates far more frequently between 0.35 and 0.7 with 250 m transmission range. The giant component gets partitioned into half of the original size. Whenever flow robustness goes up or down to a new state, the network connectivity remains for a certain period of time. Remediation measures can be taken to improve network connectivity, such as adjusting transmission power of certain nodes or adding extra static or mobile nodes to bridge the network if there is a repeated pattern of network disconnection.

Next ,we evaluate how the high centrality nodes change over time. We compute the top 20% highest centrality nodes for each 30 s snapshot and round it up to an integer value. Node centrality metrics are calculated adaptively after the removal of each node [115]. We compare how many high-centrality nodes in common between two different snapshots. For example, in the StateFair trace, we calculate a set of 4 nodes with the highest degree, closeness, and betweenness respectively. We compare the node sets with a range of time differences and then calculate the average number of common nodes for each range. In Figure 4.18, for two snapshots of 30 s time difference, the average number of common nodes between them is approximately 3 for all three centrality metrics, which indicates

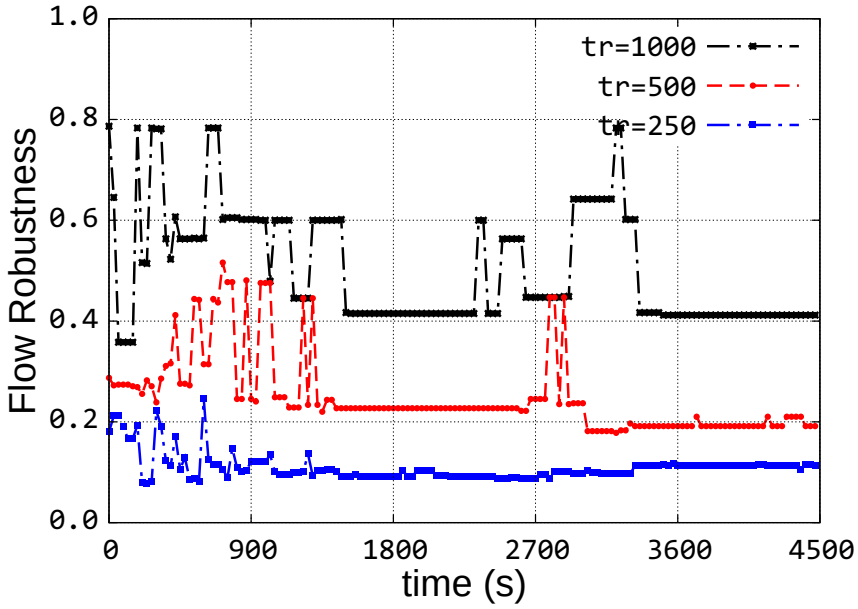


(a) Time-varying flow robustness

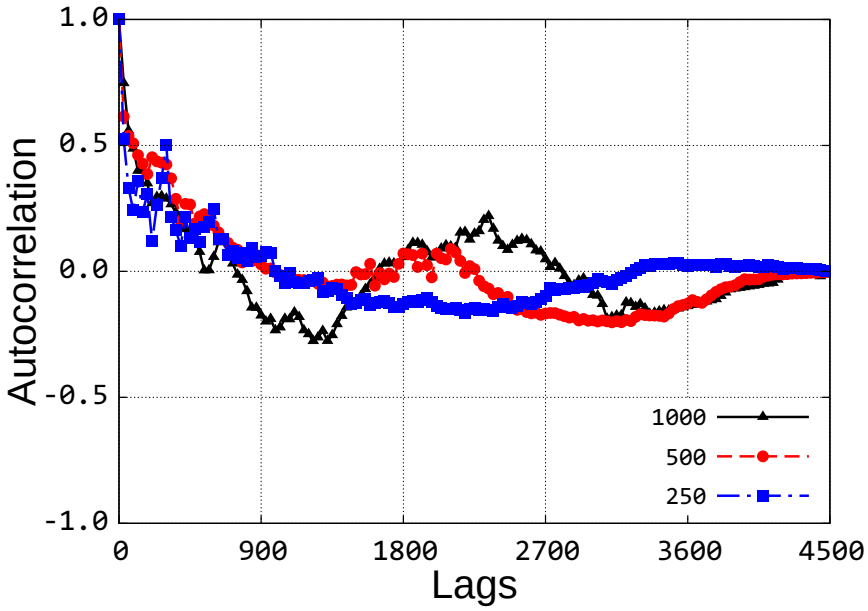


(b) Autocorrelation

Figure 4.15: Statefair

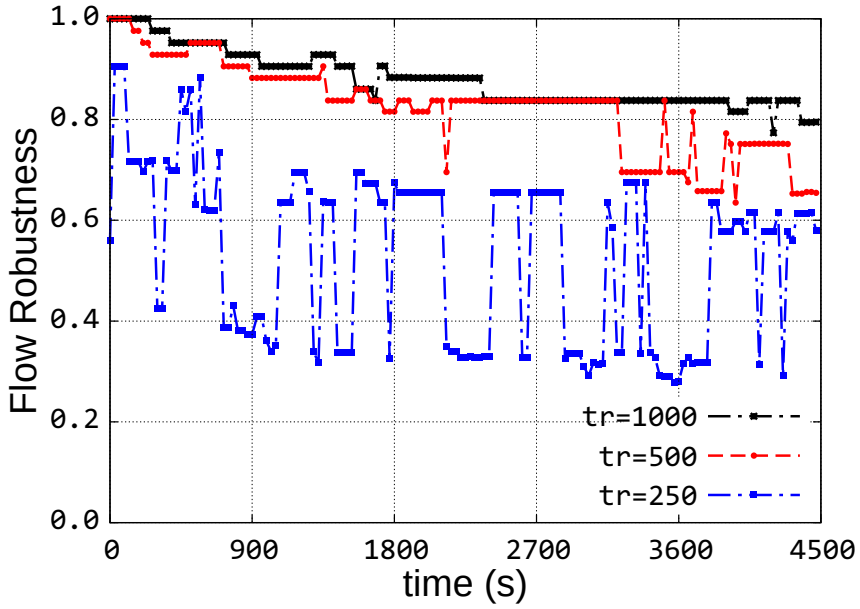


(a) Time-varying flow robustness

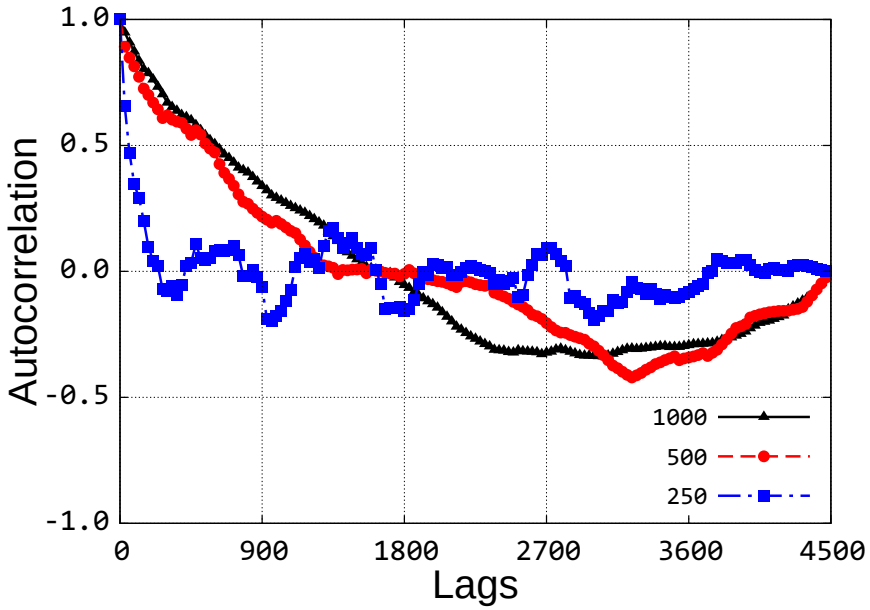


(b) Autocorrelation

Figure 4.16: NCSU



(a) Time-varying flow robustness



(b) Autocorrelation

Figure 4.17: KAIST

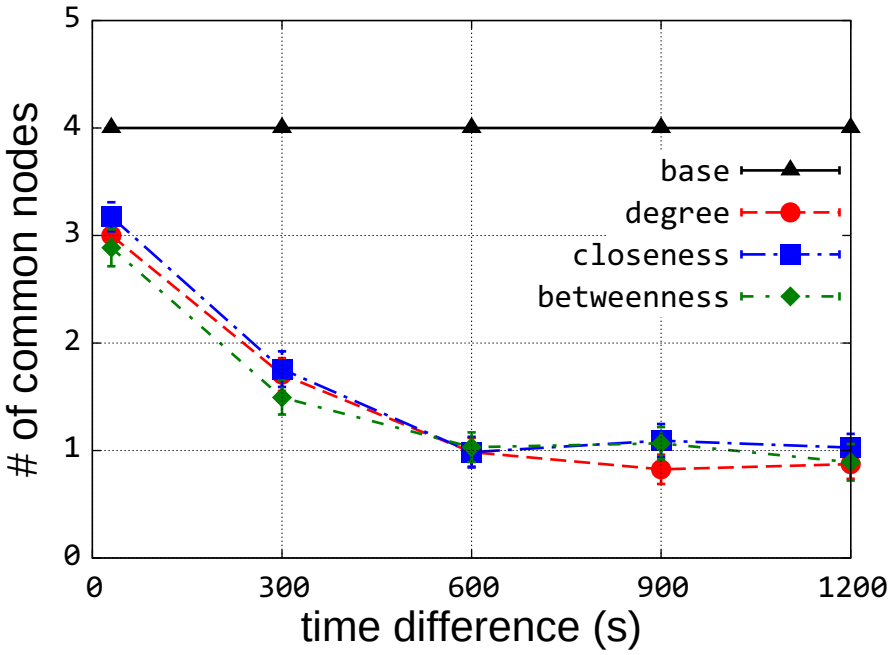


Figure 4.18: Change of high centrality nodes over time in StateFair with tr = 250

a relatively high similarity. It is apparent that with the increase of time difference, each node has a larger deviation from the original position. When window size is increased to 300 s, the average number of common nodes decreases to less than 2. For window sizes that are larger than 600 s, the average common nodes is approximately 1 with no more decrease. This can be explained as nodes in StateFair site move within a confined area and have a high chance to meet each other repeatedly after a certain period of time.

For the NCSU site, the top 7 nodes with the highest centrality are compared across different time window sizes as shown in Figure 4.19. There are more than 6 nodes shared between the top centrality nodes with 30 s window size, which indicates extremely slight change of topology structure. Even with a window size of 900 s, an average 5 out of 7 nodes are the same. This would explain the difference of centrality-based attacks using different window sizes.

The average number of common high centrality nodes within a 30 s window size for

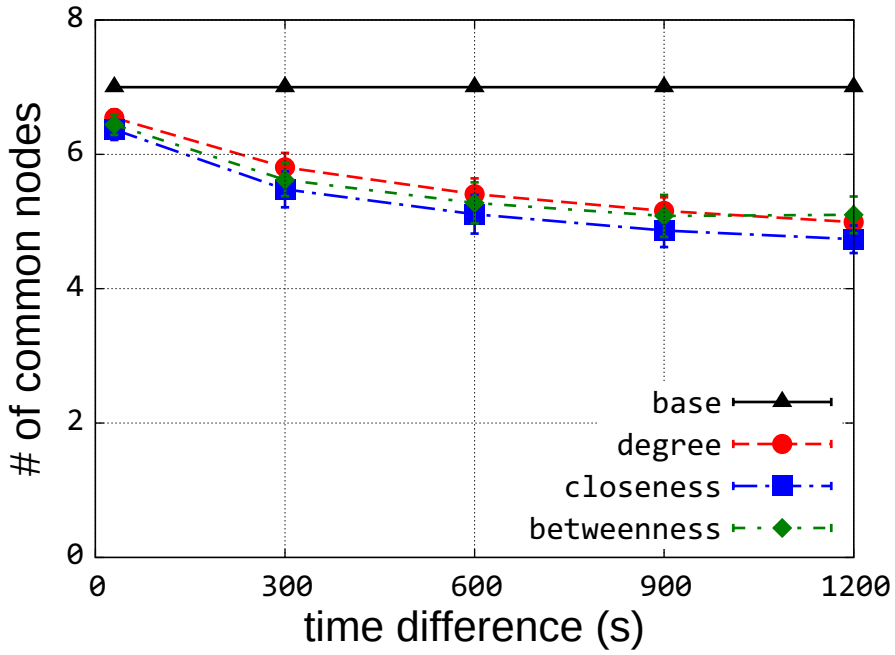


Figure 4.19: Change of high centrality nodes over time in NCSU with tr = 1000

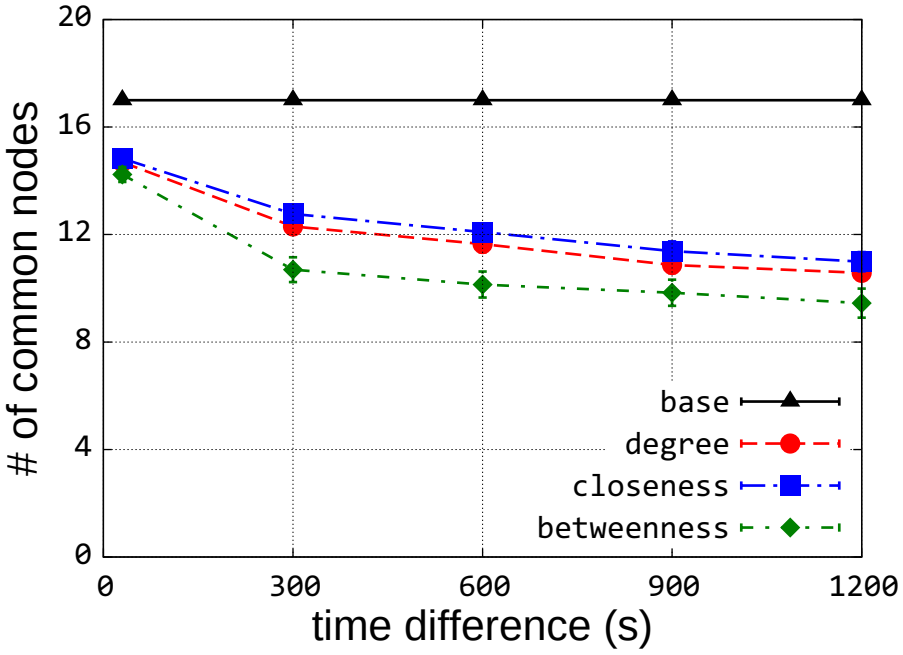
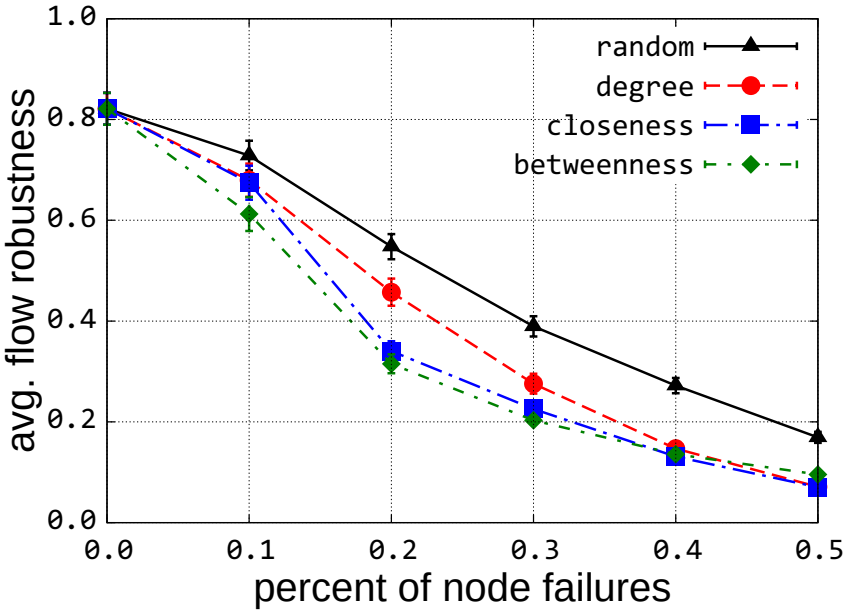


Figure 4.20: Change of high centrality nodes over time in KAIST with tr = 500

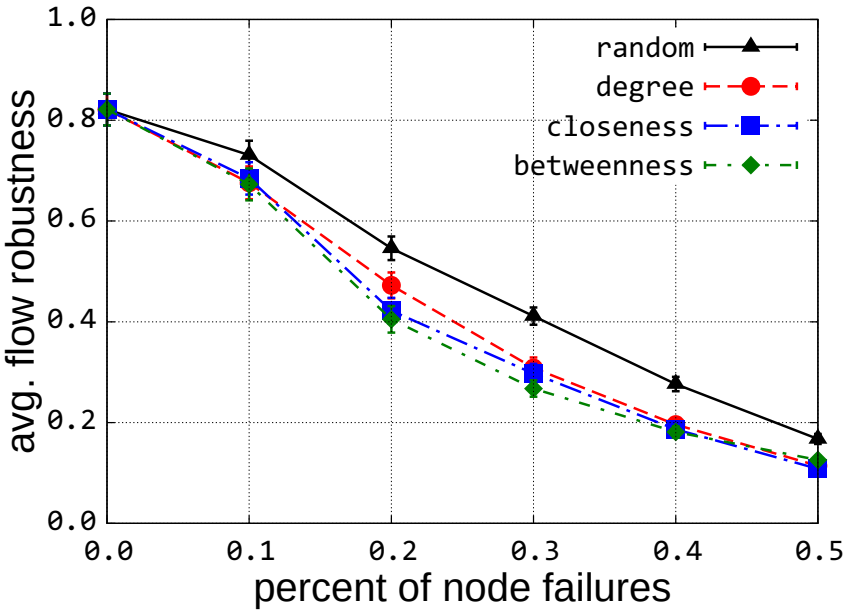
the KAIST site is about 15 out of 17 for all centrality metrics, which also shows a high correlation within a 30 s window as shown in Figure 4.20. When the window size increases, the common nodes with high betweenness decreases faster. This is because shortest paths between all node pairs are more sensitive to the change of node positions in a comparatively larger network and node betweenness highly relies on the count of shortest paths. When the window size is increased to 900 s, an average of approximately 10 of 17 nodes are in common for two snapshots of topologies.

We apply centrality-based attacks against the above three scenarios using window sizes of 30, 300, and 900 s. We compare the average network flow robustness of centrality-based attacks against random node failures. Five different levels of damage are applied adaptively with up to 50% of the total number of nodes being removed in each scenario.

For StateFair scenarios, betweenness-based attacks have the heaviest impact on network flow robustness. With a 300 s window size, the gap between random failures and centrality-based attacks decreases compared to attacks using 30 s window size. With a 900 s window size, the difference between random failures and centrality-based attacks becomes even smaller. However, for 20% and 30% node removals, betweenness-based attacks degrade the flow robustness slightly higher than the others. With 10% of nodes being removed, attacks based on degree and closeness have similar impact on the network as random failures. In Figure 4.22, the baseline flow robustness is only 50% for the NCSU site with 1000 m transmission range. As shown in Figures 4.13 and 4.14, nodes in this site span a large campus area, while the majority of them construct a connected component with the rest being isolated most of the time. The difference between the impact of each centrality-based attack on the network is modest for 30, 300, and 900 window sizes. This is because network structure remains relatively stable within the giant components of the NCSU site as shown in Figure 4.19. In addition, with failure rate higher than 0.3, betweenness-based attacks have less impact on the network than

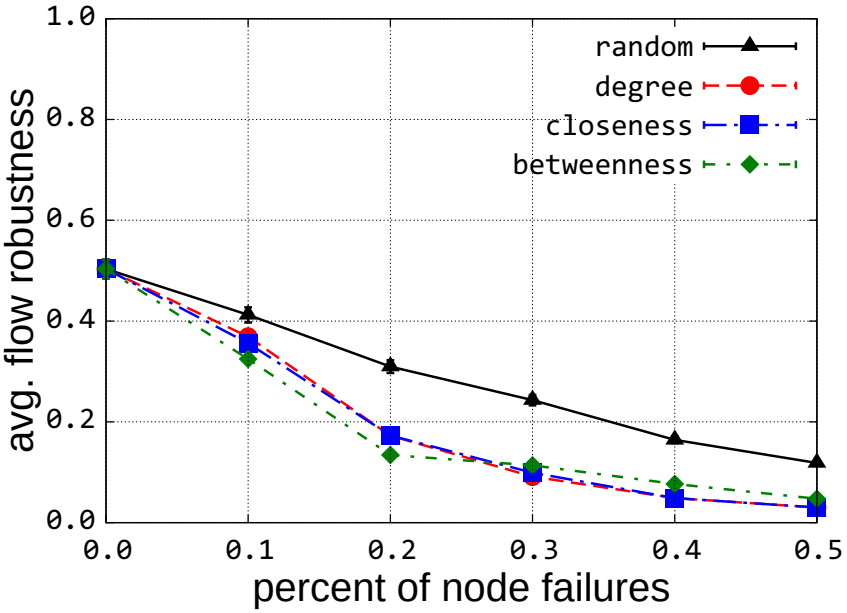


(a) Window size of 30 s

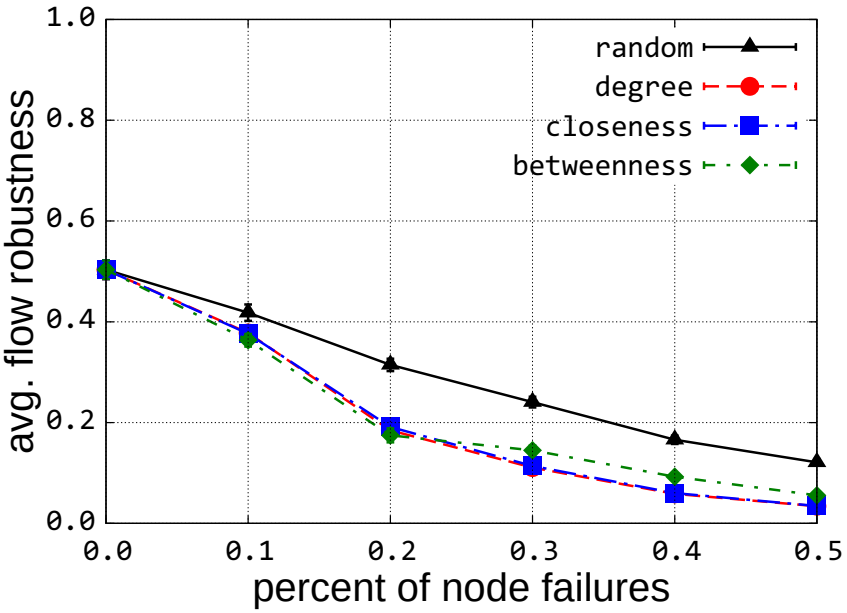


(b) Window size of 300 s

Figure 4.21: Centrality-based attacks using different window sizes for StateFair trace

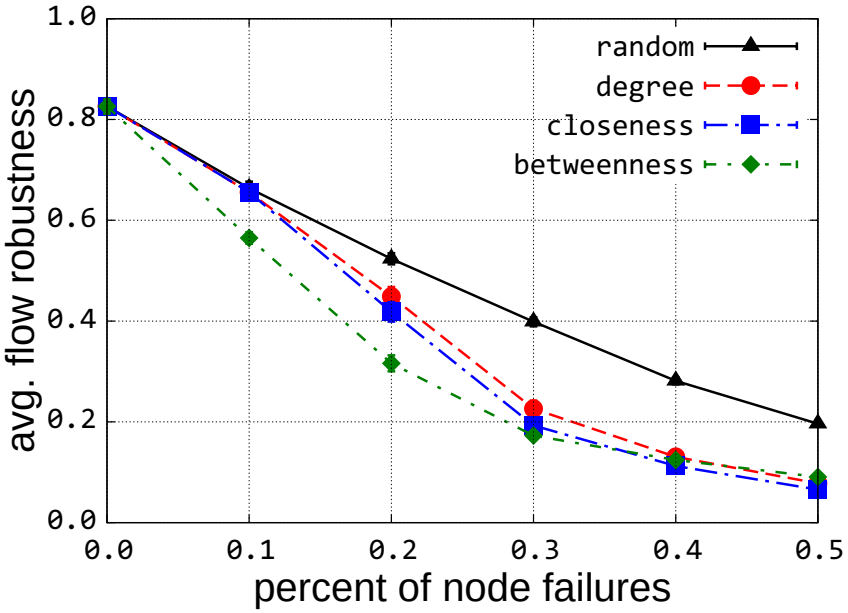


(a) Window size of 30 s

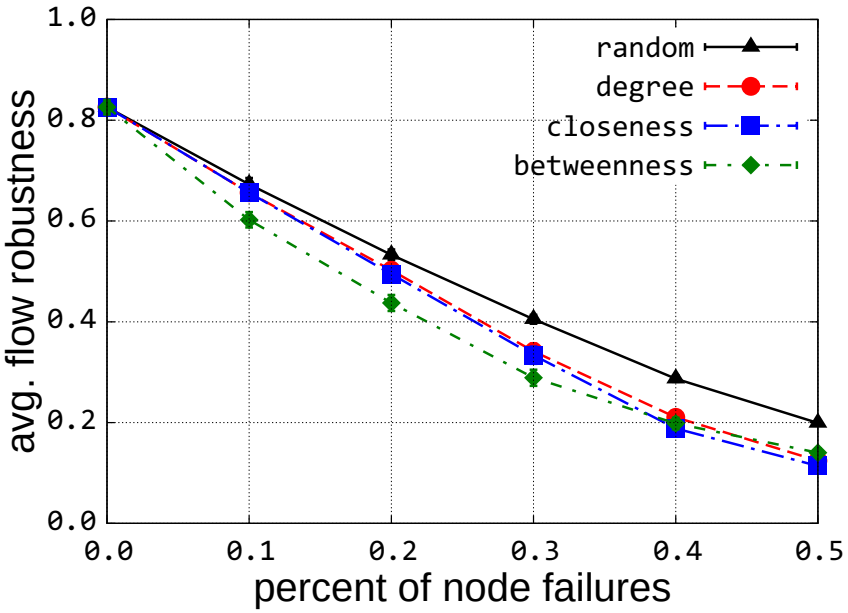


(b) Window size of 300 s

Figure 4.22: Centrality-based attacks using different window sizes for NCSU trace

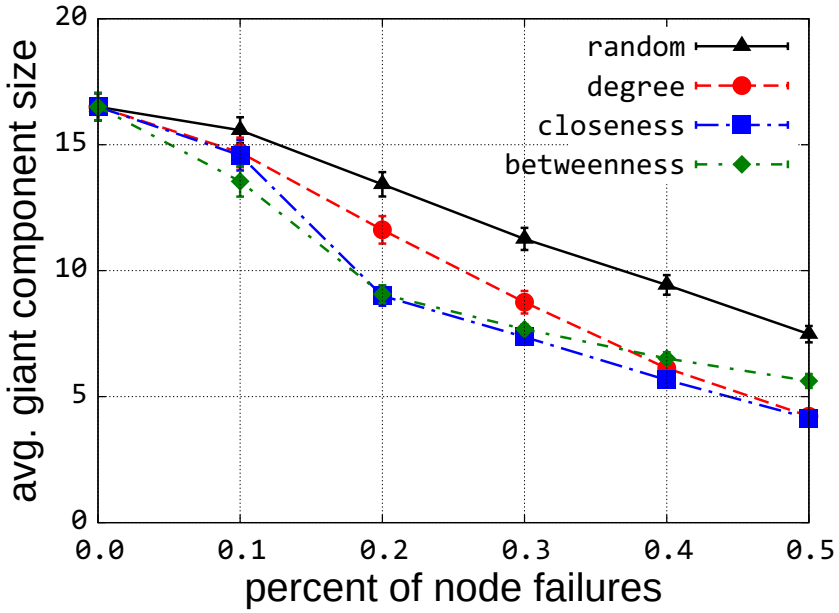


(a) Window size of 30 s

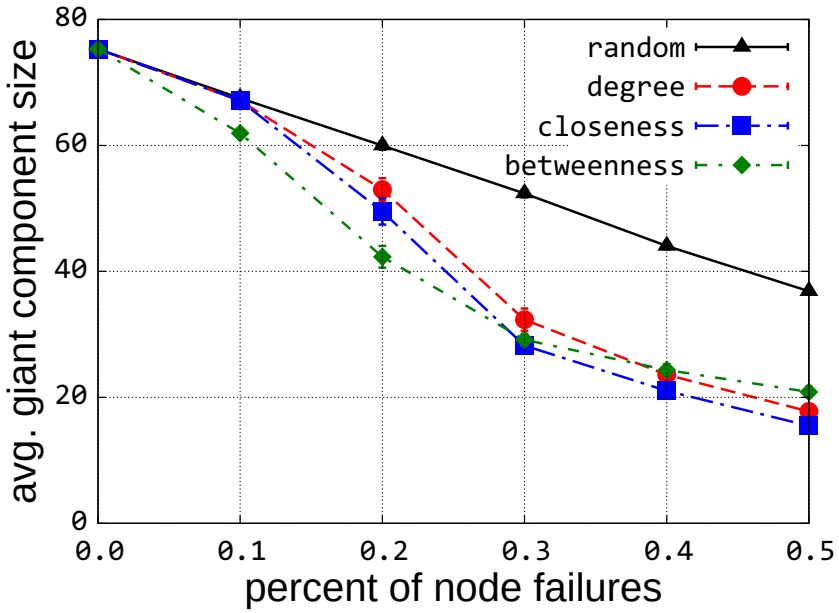


(b) Window size of 300 s

Figure 4.23: Centrality-based attacks using different window sizes for KAIST trace



(a) StateFair



(b) KAIST

Figure 4.24: Giant component size under centrality-based attacks with 30 s window size

attacks based on degree and closeness. When the network is partitioned into small fully-connected components, all the remaining nodes have the same betweenness of 0, which makes them indistinguishable from each other. With a total of 83 nodes in the KAIST site, a significant difference among betweenness-based attacks and other metrics for 10% and 20% node removal is observed in Figure 4.23a. Degree and closeness become better node significance indicators when there are more than 30% of nodes removed from the network. As the calculation of node degree is based on its neighborhood, it makes sense that local network structural change becomes dominant in overall connectivity of a more partitioned network. Both betweenness and closeness metrics are calculated based on the global shortest paths of the entire network. However, the betweenness metric provides more accurate indication of node significance in terms of providing connectivity of the entire network. The global influence of node closeness is less than node betweenness because the sum of the inverse of farness to every other node also takes into account the impact of all local nodes within the neighbors.

Figure 4.24 presents the giant component component sizes under centrality-based attacks with a 30 s window size. The relationship among giant component sizes under different centrality attacks are similar to the corresponding flow robustness under attacks. When the percentage of nodes being attacks reaches 0.3, the slope of the curve for betweenness-based attacks becomes less sharp than the degree- and closeness-based attacks. Even though average giant component size is more than 20 as shown in Figure 4.24b, nodes in each fully-connected component have the same betweenness value of 0.

For the above analysis, certain parameters must be fixed so that we can study the impact of a specific parameter on the network performance. It is not feasible to plot the individual result for each one of all the combinations of parameters such as time window size and transmission range. Next, we use our two dimensional state space resilience quantification framework [110] to evaluate how different types of attacks impact network

flow robustness for a range of network operational states that include all combinations of various parameters.

First of all, we need to establish objective functions for the operational and service dimensions of the state space. In the topological level of a given site's traces, parameters that affect network flow robustness are the number of node failures/attacks, network node density, and time window size chosen for malicious attacks. Centrality metrics within a smaller time window size provide more accurate identification of significant nodes over time [140]. Transmission range determines the average number of neighbors of each node. Neighbor count reflects network density independent of number of nodes, transmission range, and size of area covered by mobility traces. Hence, we represent operational state $N_{\mathcal{S}}$ as an objective function with three parameters: neighbor count, node failure rate, and time window size, denoted by N_1, N_2, and N_3 respectively. In order to obtain the x-axis value based on these three metrics, we calculate n_1^*, n_2^*, and n_3^* corresponding to n_1, n_2, and n_3 on a piecewise linear scale. Let n_1^* be within the range of the n_1 regions, which can be represented as:

$$n_1^* = \begin{cases} \frac{n_1 - \underline{n}_1}{\overline{n}_1 - \underline{n}_1}, & \text{if } n_1 \text{ positively affects operation} \\ \\ 1 - \frac{n_1 - \underline{n}_1}{\overline{n}_1 - \underline{n}_1}, & \text{if } n_1 \text{ negatively affects operation} \end{cases} \tag{4.1}$$

where $\underline{n}_1$ and $\overline{n}_1$ represent the lower and upper limit of the n_1 operational metric respectively. For example, the possible range of a 10-node network's neighbor count is between 0 and 9. With other parameters being fixed, the higher the neighbor count, the higher the flow robustness. Hence an average neighbor count of 4.5 results in 0.5 for n_1^*. Therefore, the projected state $N_{\mathcal{S}}^* = f(N_1, N_2, N_3)$ can be calculated using the following objective function: $n^* = \alpha n_1^* + \beta n_2^* + \gamma n_3^*$ where α, β, and γ are the weights assigned to each metric. The weights are determined based on the degree to which the network is

Table 4.7: $\Delta\mathbb{R}$ between random node failures and malicious attacks

Site	Random	Degree	Close	Between	Flexible	$\Delta\mathbb{R}_{\mathrm{R}\leftrightarrow\mathrm{D}}$	$\Delta\mathbb{R}_{\mathrm{R}\leftrightarrow\mathrm{C}}$	$\Delta\mathbb{R}_{\mathrm{R}\leftrightarrow\mathrm{B}}$	$\Delta\mathbb{R}_{\mathrm{R}\leftrightarrow\mathrm{F}}$
KAIST	0.5623	0.5388	0.5322	0.5284	0.5235	0.0236	0.0302	0.0339	0.0388
Orlando	0.3499	0.3373	0.3371	0.3451	0.3369	0.0126	0.0128	0.0048	0.0130
NCSU	0.4090	0.3786	0.3786	0.3835	0.3780	0.0304	0.0304	0.0255	0.0310
StateFair	0.6527	0.6362	0.6322	0.6247	0.6233	0.0165	0.0205	0.0280	0.0294

affected by each metric. However, it is difficult to set weights as all the metrics affect the flow robustness of each site differently. We experimentally set α, β, and γ to be 0.45, 0.5, and 0.05 to obtain an approximately linear mapping. The range of n^* is between $[0, 1]$, where 0 indicates the most degreded operational state with n_1^*, n_2^*, and n_3^* all being 0, and 1 indicates the best operational state with n_1^*, n_2^*, and n_3^* all being 1.

We provide the resilience value $\mathbb{R}$ for each site in the face of different attack strategies along with $\Delta\mathbb{R}$ to represent the difference between random node failures and centrality-based attacks in Table 4.7. Each resilience value represents aggregated service states from 450 different combinations of operational states. With the same attack strategy across different sites, the StateFair site has the highest resilience for all attack strategies. In addition, we present how network resilience under each centrality-based attack degrades compared with under random node failures. Networks under flexible attacks have the lowest resilience among all malicious attacks. Betweenness-based attacks result in lower resilience than degree- and closeness-based attacks for the KAIST and StateFair sites; however, in the Orlando and NCSU sites, betweenness-based attacks produce higher resilience than degree- and closeness-based attacks. Since the operational states in the Orlando and NCSU sites are more degraded than in KAIST and StateFair sites, betweenness fails to provide a favorable indication of node significance in relatively poorly-connected networks such as Orlando and NCSU. Again, the flexible metric provides the best measurement of node significance across varying network connectivities.

4.2.3 Simulations in ns-3

In this section, we evaluate network resilience in the application level using different routing protocols given a topological connectivity measured by flow robustness, as it is necessary to improve network resilience at multiple layers in the protocol stack. The two metrics used to measure service states are PDR (packet delivery ratio) and average network delay. The operational state is a single flow robustness value, and the service state objective function is composed by the logic AND, which means that both PDR and delay have to meet a certain threshold in order to characterize the state as acceptable, impaired, or unacceptable. Network delay less than 10 ms is considered as normal, and network delay is considered unacceptable if it is greater than 250 ms. PDR is already in the range of $[0, 1]$, and all the network delay values also need to be projected into $[0, 1]$ range. The calculation of projected service state values is based on the smaller value of PDR and projected delay as both of them are necessary conditions for acceptable services.

Table 4.8: Simulation parameters of real-world traces in ns-3

Transmission range	250, 500, 1000 meters
Number of nodes	19 (StateFair), 25 (NCSU)
Simulation time	4500 s
Physical channel	802.11g 54 Mb/s
Data rate	1 packet/s
Routing protocol	DSDV, AODV, DSR, OLSR
Window size	30, 300, 600, 900, 1200
Node removal rate	0, 0.1, 0.2, 0.3, 0.4, 0.5
Attack strategy	random, degree, closeness, betweenness, flexible

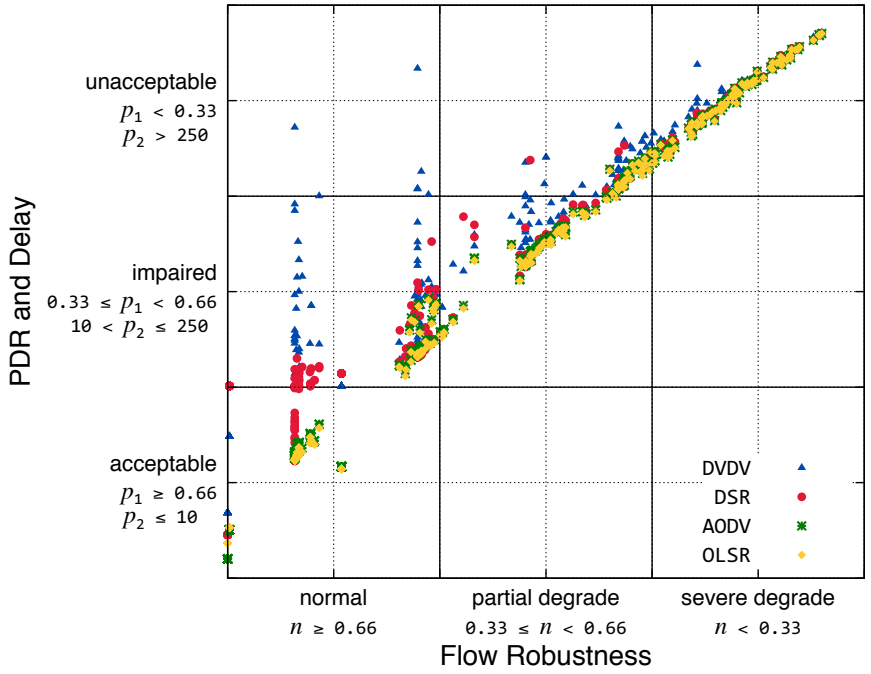
We use the open source network simulator ns-3 [135] as our simulation tool. Constant bit rate UDP traffic is generated every second. The data rate is set as 1 packet/s to minimize potential network congestion. We convert the original humans' walking traces to ns-2 format, so that traces can be imported using `Ns2MobilityHelper` model, which is the only

way to import traces from files in the latest version of ns-3. The four routing protocols used in the simulations are DSDV (Destination-Sequenced Distance Vector) [141, 142], DSR (Dynamic Source Routing) [143, 144], AODV (Ad hoc On-Demand Distance Vector) [145], and OLSR (Optimized Link State Routing) [146]. In order to guarantee a fair evaluation of nodes' roles, each node sends traffic to every other node. With 72 nodes in the KAIST scenario, there are 5112 packets generated in the network simultaneously every second, which could cause serious network contention in the MAC layer. The flow robustness of the Orlando site is within the unacceptable range that provides a narrow range of operational states to evaluate routing protocols. Hence, here we only evaluate the resilience of StateFair and NCSU sites. The other parameters used in our simulation are listed in Table 4.8.

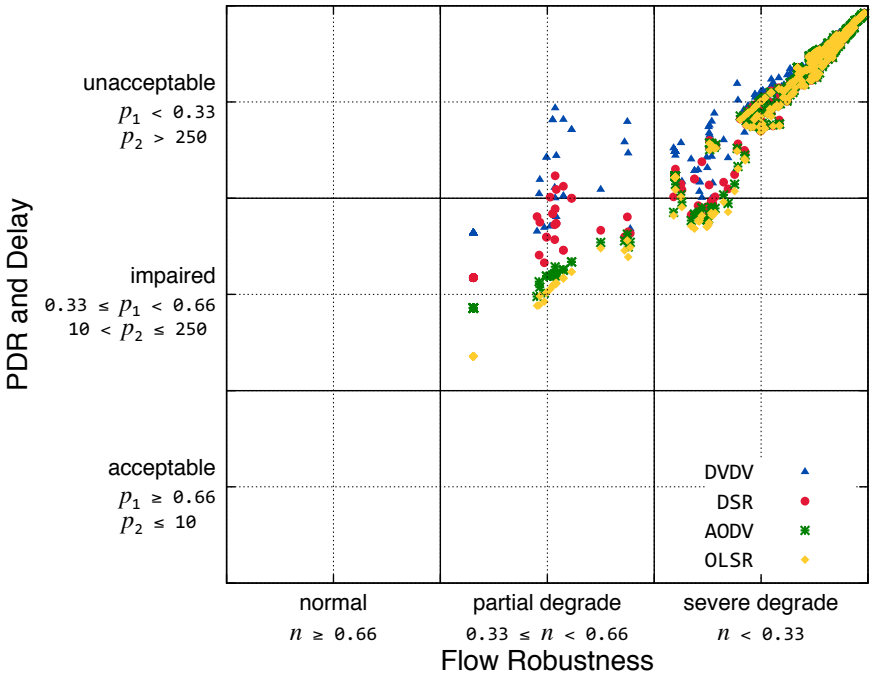
Table 4.9: Resilience of MANET routing in Two Sites

	StateFair			NCSU		
	$\overline{\text{PDR}}$	$\overline{\text{Delay}}$	$\mathbb{R}$	$\overline{\text{PDR}}$	$\overline{\text{Delay}}$	$\mathbb{R}$
DSDV	0.468	64.36	0.472	0.144	85.76	0.358
DSR	0.486	50.15	0.488	0.164	57.76	0.384
AODV	0.488	3.35	0.526	0.169	7.76	0.400
OLSR	0.494	1.62	0.527	0.177	1.25	0.421

Figure 4.25 presents resilience state space for the StateFair and NCSU sites using four different routing protocols. Each resilience value $\mathbb{R}$ in Table 4.9 is calculated based on 450 flow robustness values that are generated using different combinations of parameters. The operational states of the StateFair site have a relatively even distribution between normal operation and severely degraded operation, while the operational states of NCSU are mostly distributed around the degraded and severely degraded regions. By evaluating services under a list of operational states, OLSR has the highest resilience among the four routing protocols, since OLSR has the lowest connection setup time with up-to-date routes. Both DSDV and OLSR are table-driven proactive routing protocols. The interval



(a) StateFair



(b) NCSU

Figure 4.25: Resilience space using different routing protocols

of `Hello` message in OLSR is set as 1 s in our simulation. Due to the high overhead of routing update in DSDV, the periodic update interval in DSDV is set as 5 s. Another reason why DSDV has the lowest resilience is that the routes in DSDV might not always be accurate as it only depends on periodic triggering messages to update the routes. The relatively low resilience of DSDV and DSR arises from their high delay as shown in Table 4.9; the delay value are presented in ms. Network resilience using AODV is slightly higher than using DSR. Both DSR and AODV are reactive routing protocols. The stale route cache in DSR could result in route inconsistencies when constructing the route. In constrast, the periodic beacons in AODV consumes extra bandwidth but can fix the stale entries faster than DSR, and multiple routes are maintained between source and destination in the AODV routing table. Extensive dependence on the route cache information in DSR during the route discovery phase could lead to high setup delay. When the operational states are severely degraded, there are no apparent difference among service states by using four different routing protocols.

Service states for different routing protocols become close to each other under severely degraded operations, since with more nodes being attacked, route convergence of existing nodes becomes faster with few available paths between node pairs if two nodes are reachable from each other. For a range of network operational states in both sites, the OLSR protocol provides the highest PDRs and lowest delays among the four different routing protocols. However, noting that the interval of `Hello` message is set as 1 s, OLSR achieves this performance with a high routing overhead.

Page left intentionally blank.

Chapter 5

Evaluation of Enhancement Strategies

In Chapter 4, we have investigated the potential vulnerability of MANET topologies in face of malicious attacks. As shown in the our results, the attacks against the high betweenness nodes could cause severe performance degradation of MANETs. In this chapter, we first address the issue of network partition caused by node mobility. The CTR (critical transmission range) could guarantee that the network in a unit disc area is connected with a probability of 1 asymptotically; however, it is impractical to assign an exorbitantly long transmission range that could result in high power consumption and interference among neighboring mobile devices. We propose an approach to use a smaller-than-CTR transmission range, and maintain a connected network by exploiting directional antenna to bridge the disconnected components with minimum energy cost based on MST (Minimum Spanning Tree). A great number of existing studies focus on the minimization of local and global energy consumption by reassigning the radio power of each participating device in MANETs. Our work builds upon homogeneous MANETs with a uniform transmission range and adds additional long-range links to enhance network connectivity.

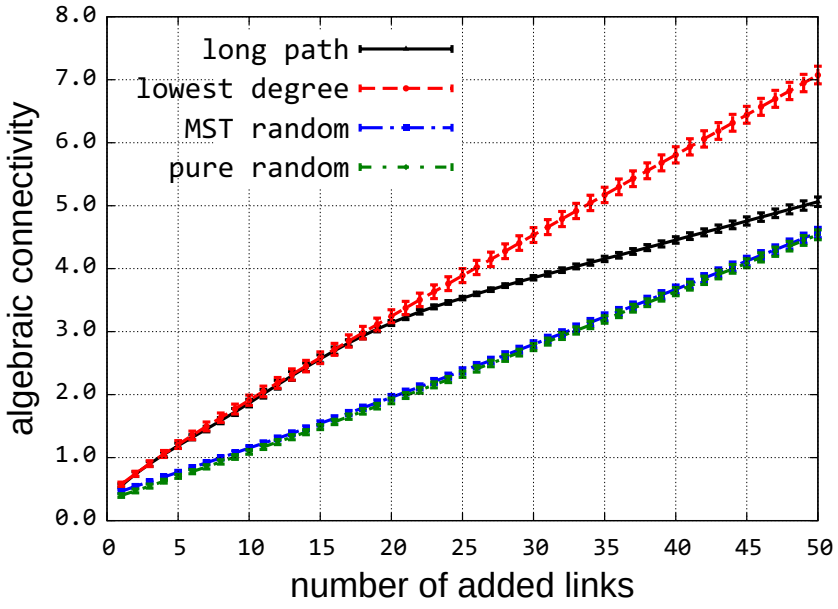
5.1 Synthetic Trace Enhancement

We use the same network parameters as in the evaluation of the impact of centrality-based attacks in synthetic networks. A set of network robustness measures are evaluated for each enhancement strategy. In addition, we evaluate the sum of flow robustness under iterative attacks based on different centrality metrics.

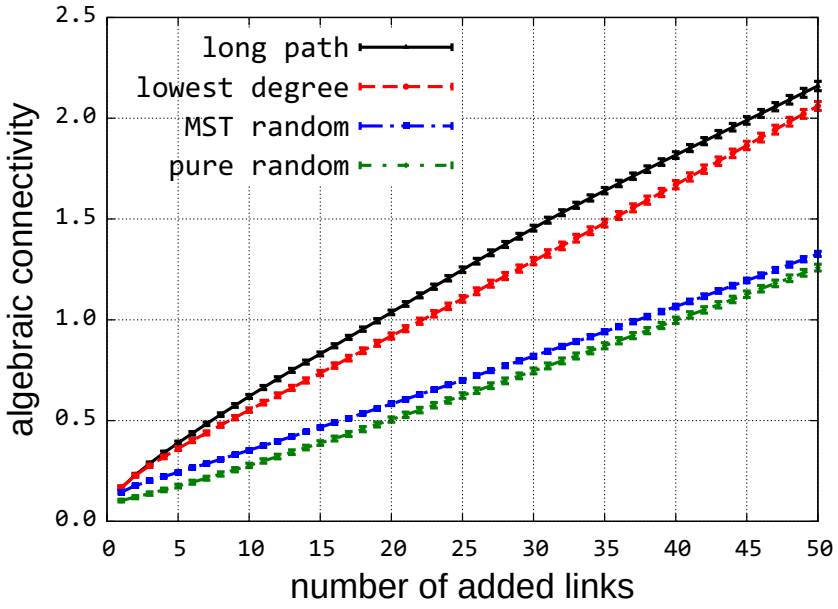
5.1.1 Enhancement Strategies Evaluation

We add up to 50 links for each scenarios in Table 4.1, and investigate several graph robustness measures of the enhanced networks using different enhancement strategies. The measures are algebraic connectivity, network criticality, clustering coefficient, the inverse of path length, and the inverse of diameter. Since it is possible that the MANETs are disconnected which results in an infinite path length and diameter, we take the inverse of these two measures so that they can be calculated for all possible cases. As mentioned in Section 3.2, the four enhancement strategies are: PR (pure random), MR (MST random), LD (lowest degree), and LP (longest path).

Figure 5.1 provides the average algebraic connectivity in enhanced networks using the strategies mentioned above. For 20-node networks, the algebraic connectivity of networks using LD-based improvement heuristic remains the highest among all after there are more than 20 link additions. Whereas, with less than 20 links being added, LD-based strategy has almost the same performance with LP-based strategy. The MR-based strategy improves algebraic connectivity slightly higher than PR-based strategies, although both of them stay the lowest of all. Different from 20-node networks, the LP-based enhancement strategy in 50-node networks provide the highest performance consistently among all strategies in terms of algebraic connectivity in the improved networks. This indicates that in a network of a relatively small size, the link additions to those lowest degree nodes

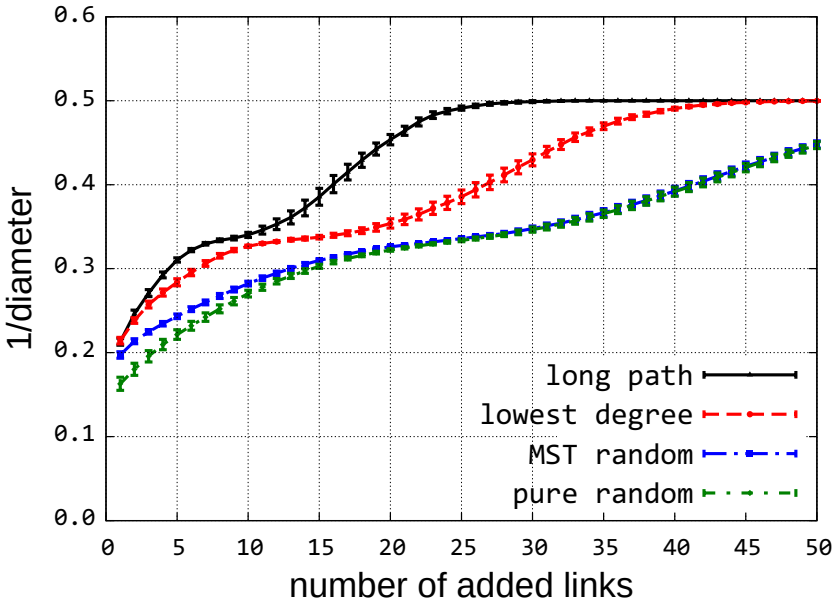


(a) 20 nodes

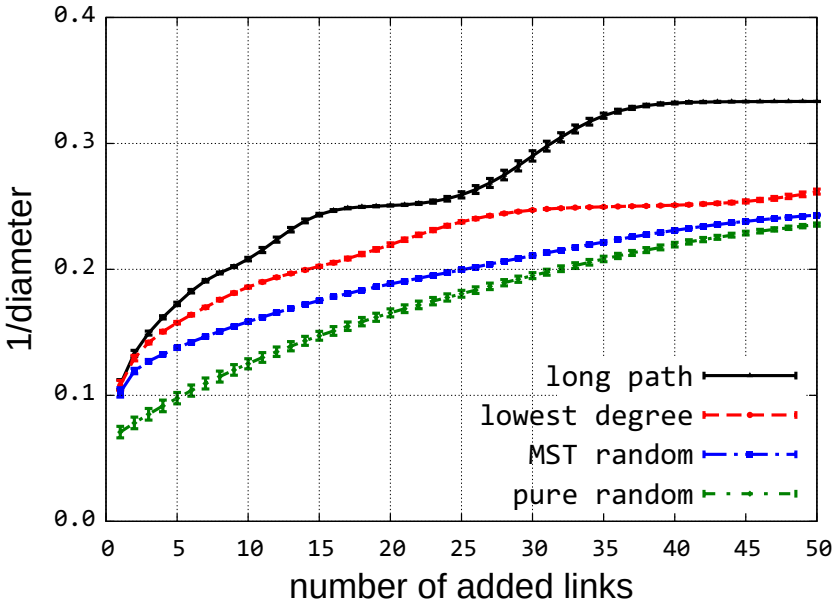


(b) 50 nodes

Figure 5.1: Algebraic connectivity in the enhanced networks

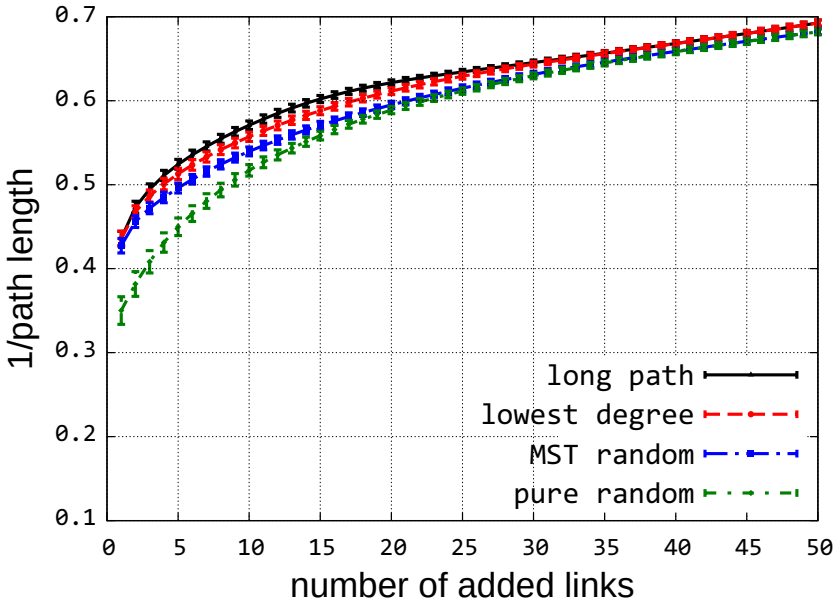


(a) 20 nodes

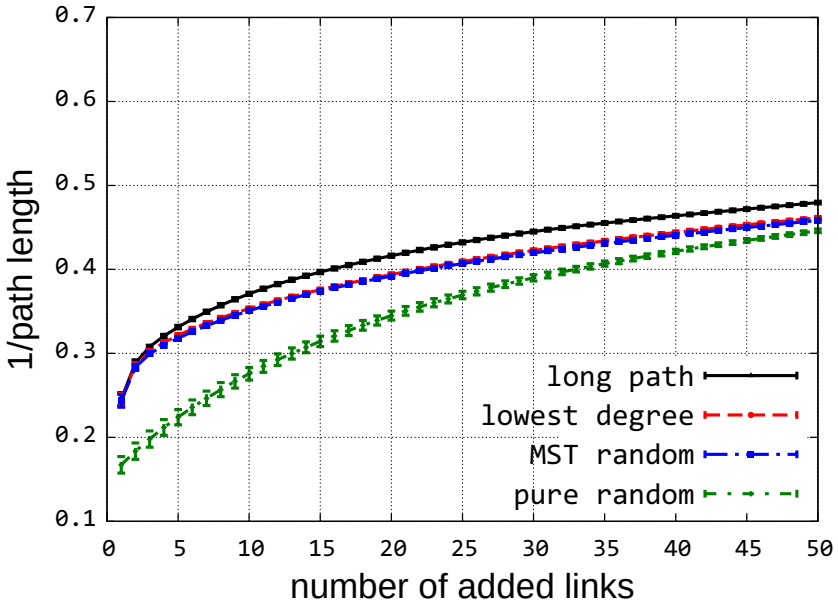


(b) 50 nodes

Figure 5.2: Inverse of network diameter in the enhanced networks



(a) 20 nodes



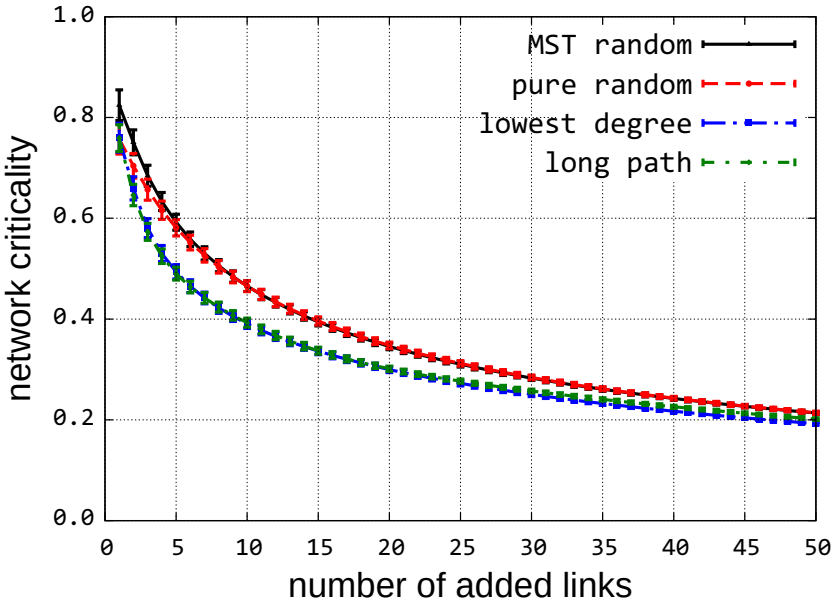
(b) 50 nodes

Figure 5.3: Inverse of path length in the enhanced networks

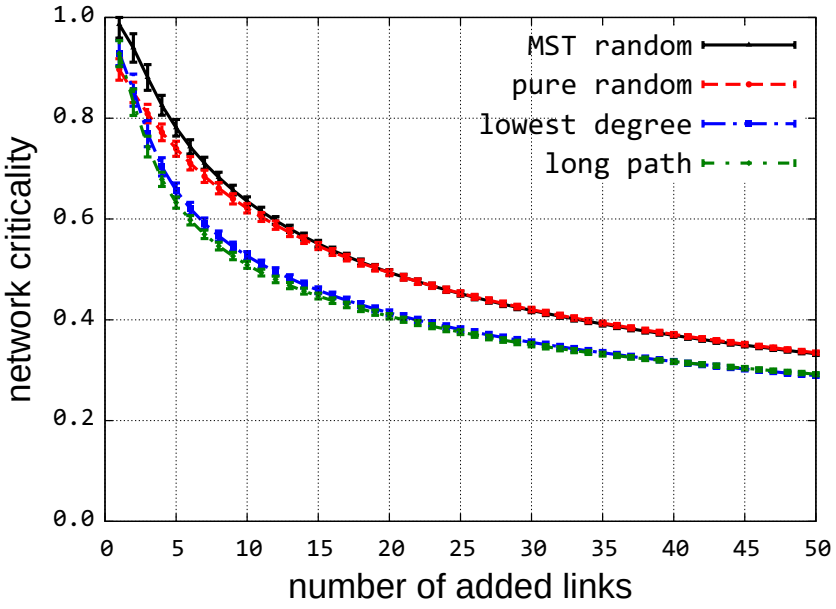
increase the network robustness better than in a relatively-large size network. We can observe in Figure 5.2a that the average network diameter get close to 2 (1/0.5) and barely changes after adding 25 links using LP-based strategy to a 20-node network. This means that the link selection based on the longest node-pair distance has trivial advantage over random selection. The inverse of the diameter gets close to saturation with almost 25 link additions in the 20-node networks. With an increasing number of added links, the MANET topologies becomes more like small-world networks. The average path length in 50-node networks remains at 3 (1/0.33), which indicates that all nodes can reach each other via no more than 3 hops.

Figure 5.3 shows that the average path length keeps increasing in both 20-node and 50-node networks. With more links being added to 20-node networks, the average path length become close to each other for all enhancement strategies. In 50-node network scenarios, LP-based strategy results in the largest inverse of network diameter of all strategies, while there are almost no difference between the LD-based an MR-based strategy. Since the links in the complementary graph that are incident lowest degree node could possibly connect to another local node, the improvement heuristic based on link additions to the lowest degree nodes might not contribute to the reduction of average path length, particularly in a relatively large network.

Network criticality values in both 20-node and 50-node networks are similar by using LD-based and LP-based strategies. However, it is interesting to observe that MR-based strategy has the highest network criticality (worst robustness) with few added links. This means that by measuring network criticality, PR-based strategy could improve network robustness better than MR-based strategy, which seems counter-intuitive since network are not necessarily connected by adding a few random links. This exposes an disadvantage of using network criticality to measure robustness and connectivity. By investigating the original definition of network criticality, this metric captures the effect of topology and



(a) 20 nodes

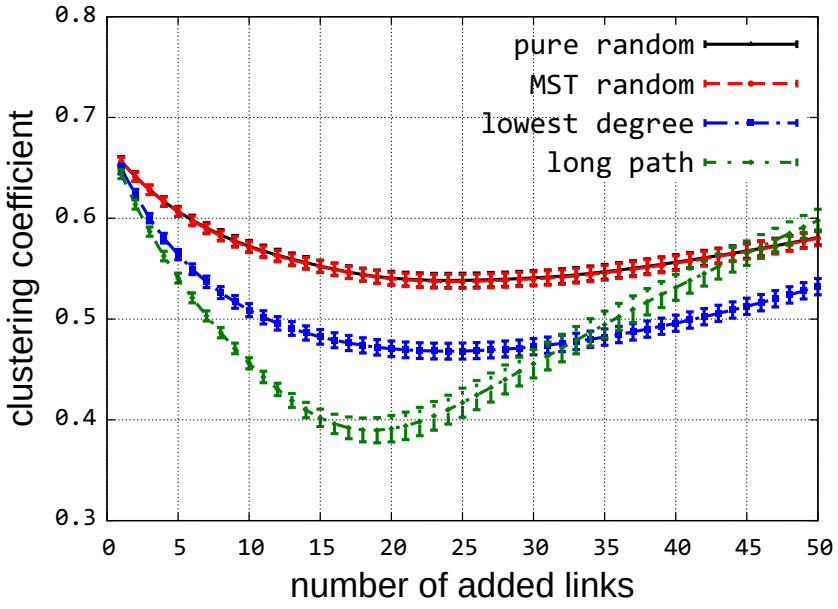


(b) 50 nodes

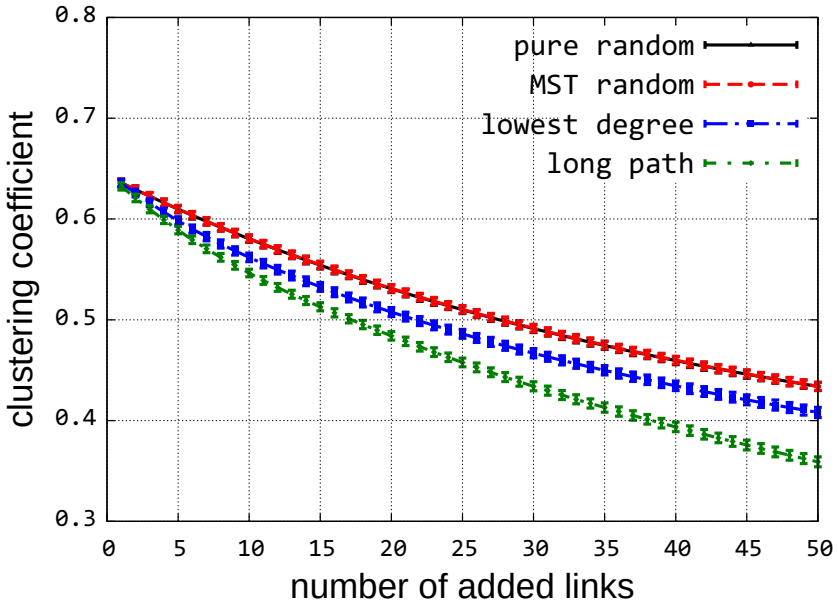
Figure 5.4: Network criticality in the enhanced networks

community of interest via Markov chain random-walk betweenness. This metric notes that the higher the betweenness of a node, the higher the risk of using the node. After adding the bridging links using the MST algorithm, more articulation points are exposed due to the bridging links. Hence, the addition of bridging links increases the random-walk betweenness of these nodes. By adding more links, this effect will be compensated by shorter and more alternative paths between node pairs.

Figure 5.5 provides how network average clustering coefficient changes with an increasing number of added links. The characteristic path length and high average clustering coefficient are two major properties of small-world networks as mentioned in [22]. A small-world network can be constructed by rewiring links in a regular graph. Each link is rewired with a probability p. Small-world characteristics appear when $0.01 \leq p \leq 0.1$. Here, we are investigating the relationship between adding long links to MANETs and the small-world networks. As shown in Figure 5.2 and 5.3, the average path length keeps decreasing with bounded distance between any pair of nodes indicated by the inverse of the diameter, the variation of clustering coefficient with an increasing number of added links presents a non-linear trend as shown in Figure 5.5. The short average path length is a phenomenon that can be observed in random networks. The high clustering in small-world network comes from the characteristic of regular networks. In a 20-node network scenario, the change of clustering coefficient with increasing number of link is a convex function, in particular for LP-based strategy. The clustering coefficient of the LP-based strategy hits the minimum when there are about 20 links being added. After that, the clustering coefficient increases to the highest of all when there are 50 links being added. In contrast, the change of clustering coefficient in the 50-node networks is always non-increasing with less than 50 links being added. This can be explained as, in the initial stage of link additions, the long links are added between node pairs of long hop counts; therefore, the added links contribute to no triangles among neighboring nodes but only



(a) 20 nodes



(b) 50 nodes

Figure 5.5: Clustering coefficient in the enhanced networks

triplets for the calculation of clustering coefficient. After more than 20 links being added, the network becomes more connected and the addition of links results in a high number of triangles. This saturation point for LP-based strategy is also observed in the diameter change of the network in Figure 5.2. For 50-node networks, since it takes more link additions to reach the saturation point, the clustering coefficient has not hit the nadir with 50 link additions.

5.1.2 Sum of Flow Robustness Evaluation

Table 5.1: $\sum$F of the enhanced synthetic traces under attacks

	Unimproved	Pure random	MST random	Lowest degree	Longest path
$\sum \mathcal{F}_{20}^{d}$	4.546	6.080	6.099	**6.399**	6.264
$\sum \mathcal{F}_{20}^{c}$	4.001	5.928	5.943	**6.303**	6.212
$\sum \mathcal{F}_{20}^{b}$	3.563	5.517	5.534	**6.044**	5.943
$\sum \mathcal{F}_{20}^{f}$	3.463	5.509	5.528	**6.043**	5.948
$\sum \mathcal{F}_{50}^{d}$	10.785	13.179	13.296	14.163	**14.302**
$\sum \mathcal{F}_{50}^{c}$	7.808	11.329	11.409	12.223	**12.653**
$\sum \mathcal{F}_{50}^{b}$	6.026	9.433	9.504	10.292	**10.918**
$\sum \mathcal{F}_{50}^{f}$	5.992	9.400	9.471	10.263	**10.887**
$\sum \mathcal{F}_{100}^{d}$	18.961	23.075	23.558	24.936	**26.047**
$\sum \mathcal{F}_{100}^{c}$	11.429	16.955	17.211	18.119	**20.236**
$\sum \mathcal{F}_{100}^{b}$	7.802	12.390	12.526	13.211	**14.820**
$\sum \mathcal{F}_{100}^{f}$	7.788	12.347	12.484	13.169	**14.780**

We evaluate how the enhanced networks survive malicious attacks measured by sum of flow robustness $\sum \mathcal{F}$ using different centrality metrics. We fix the number of added links to be 20. We use the four centrality metrics, degree, closeness, betweenness, and flexible, that could cause the most damage to the network robustness. For 20 nodes scenarios, using the same centrality-based attacks, the LD-based enhancement strategy provides the highest $\sum \mathcal{F}$, and the $\sum \mathcal{F}$ using the LP-based enhancement strategy is slightly lower than enhancement strategy. However, in 50 and 100 nodes scenarios, our proposed LP-based enhancement strategy provides the highest $\sum \mathcal{F}$ of all. This set of results match

the algebraic connectivity results shown in Figure 5.1, that is, the LD-based strategy provide a better improvement than LP-based strategy in 20 nodes networks and vice verse in networks with 50 and 100 nodes. Under the most damaging flexible attacks, the difference between the LD- and LP-based strategy is negligible in 20-node network scenarios; the LP-based strategy provides a far better enhancement of network robustness than LD-based strategy in 50- and 100-node networks. Moreover, considering that the computational complexity of the LP-based strategy for adding each link is far less than the LD-based heuristic, our LP-based link addition strategy is more efficient and effective in enhancing network robustness.

5.2 Real-World Trace Enhancement

In this section, we apply the enhancement strategies to the real-world data set mentioned in Section 4.2.1. For the synthetic trace analysis in the previous section, we evaluate network scenarios with decent connectivity. In the analysis of real-network, we investigate MANETs with varying network connectivity levels, which present diverse perspectives to evaluate our enhancement strategies. We evaluate the cleaned mobility traces shown in Table 4.5 and investigate the robustness of five sites by applying different enhancement strategies.

5.2.1 Enhancement Strategies Evaluation

Figure 5.6 provides a snapshot of mobility traces in the *StateFair* site with 20 links added using LP-based strategy. We select 250 m as the transmission range resulting in an average node degree of 6.8 and an average flow robustness of 0.825. Nodes in this site are moving in a relatively confined area. In Figure 5.7, the algebraic connectivity almost increases linearly with the growing number of added links. The MANETs enhanced by

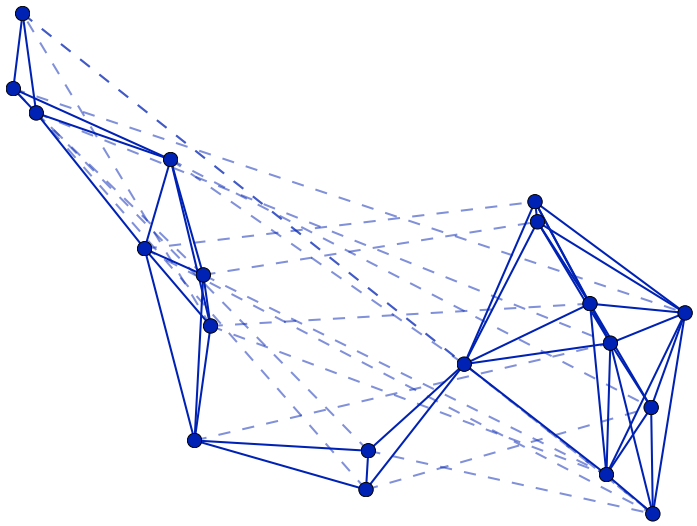


Figure 5.6: A snapshot of Statefair trace with 20 added links based on long-path strategy

the LP-based strategy have the highest algebraic connectivity with less than 20 links being added. The LD-based strategy intersects the LP-based strategy at the point of 20 added links. From Figure 5.8, we can observe that the average network diameter hits 2 (1/0.5) after adding 20 links based on LP strategy, which means that any node pairs can be reach within 2 hops. After that, the LP-based strategy becomes more like a random addition of links between any node pairs. The LD-based heuristic outperforms other strategies after more than 20 links being added. After adding 50 links, the average diameters of all enhancement strategies are approximately 2. Both the average diameters and path lengths of different enhancement strategies increase quickly with up to 20 links being added. The LP-based strategy converges to an average diameter of 2 much faster

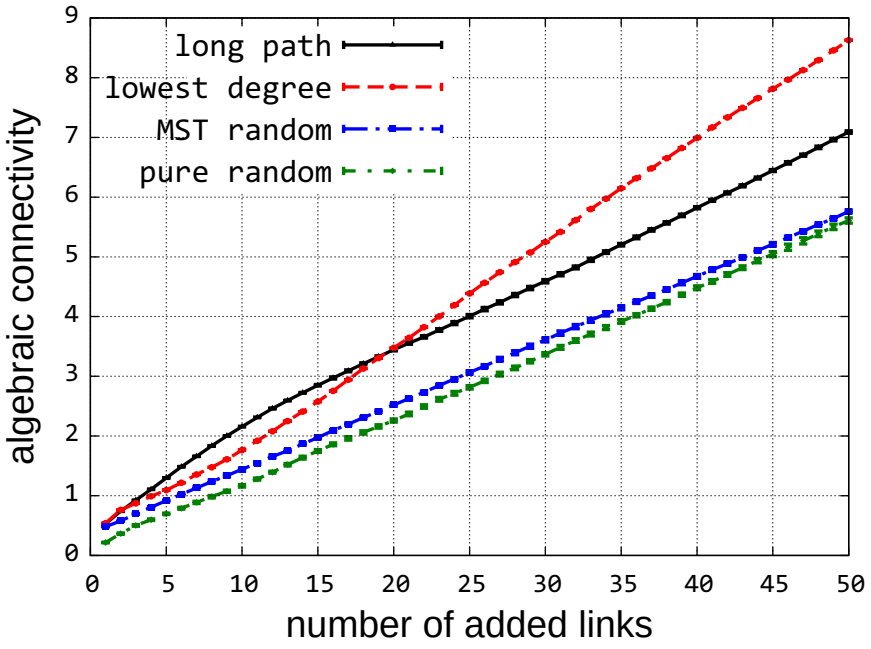


Figure 5.7: Algebraic connectivity of Statefair with an increased number of added links

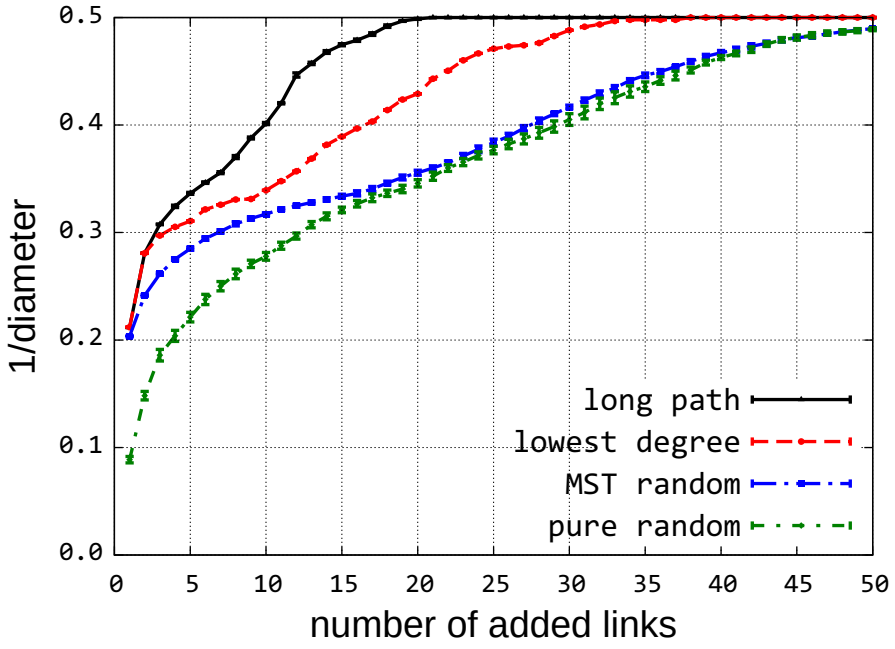


Figure 5.8: Inverse of diameter of Statefair with an increasing number of added links

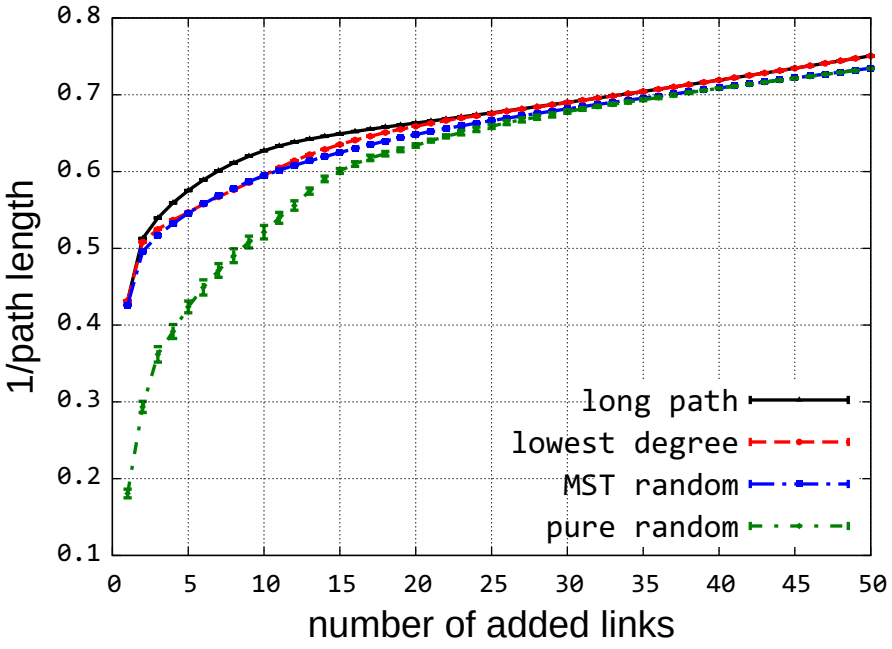


Figure 5.9: Inverse of path length of Statefair with an increasing number of added links

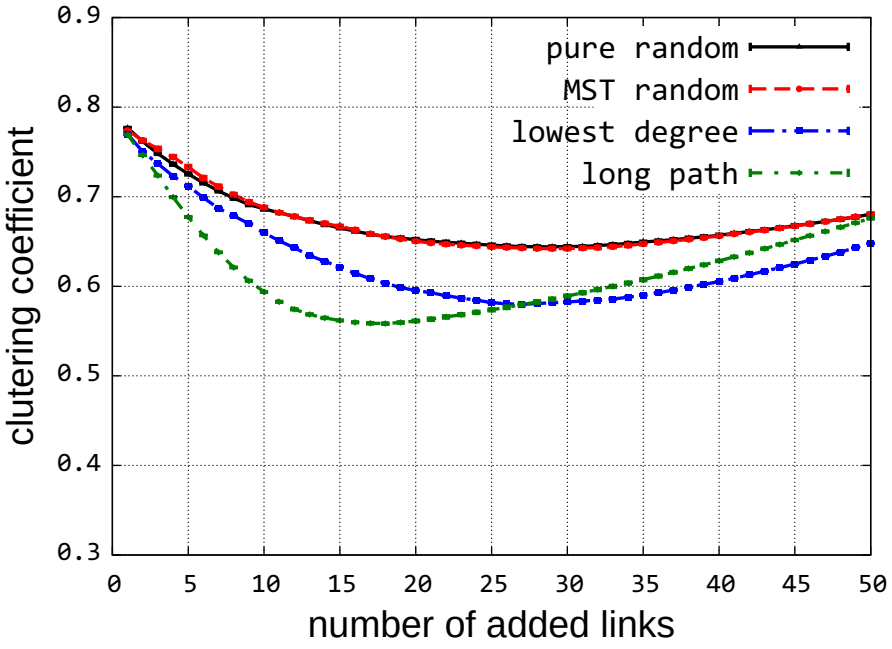


Figure 5.10: Clustering coefficient of Statefair with an increasing number of added links

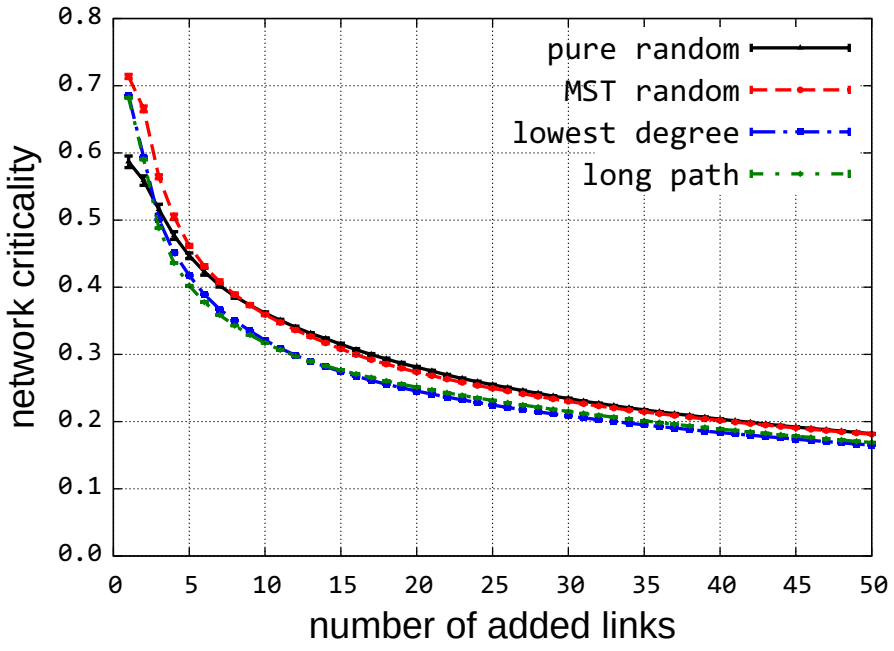


Figure 5.11: Network criticality of Statefair with an increasing number of added links

than other strategies, while the average path lengths of all strategies are getting close to each other after adding 20 links including two random strategies, which indicates that the MANETs become more like small-world networks that have short path lengths. Increasing random additions of links to random geometric graphs will gradually reduce the path lengths, while our LP-based link addition strategy expedites the decrease of path length at the initial stage.

The average network criticality of different enhancement strategies are closer to each other with an increasing number of link additions as shown in Figure 5.11. The addition of links between long distance node pairs first causes the clustering coefficient of the network to decrease to a value where the inverse of average network diameter just becomes 0.5. Then, the clustering coefficient of LP-based strategy quickly increases to the same value as the random strategies with 50 links being added.

Figure 5.12 presents a snapshot of NCSU site improved by 20 links using LP-based strat-

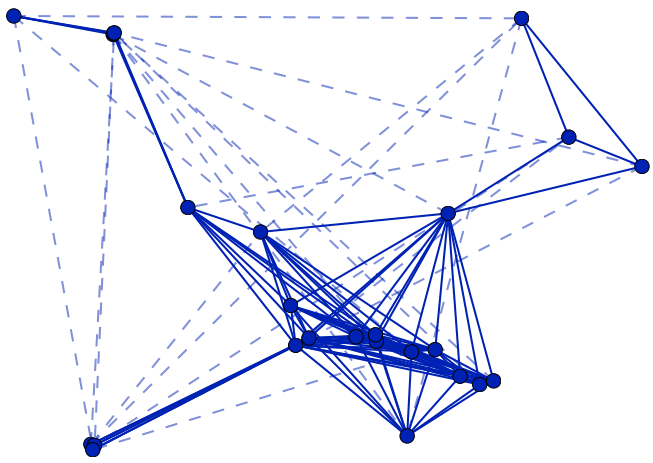


Figure 5.12: A snapshot of NCSU trace with 20 added links based on long-path strategy

egy. In this site, the network consists of a few disconnected components during most of the trace time and a small portion of nodes span a wide range of area . The LD-based strategy results in the highest algebraic connectivity of all strategies as shown in Figure 5.13. Similar to the StateFair site, LP- and LD-based strategies produce similar algebraic connectivity, after 17 links being add, the LP-based strategy behaves like random strategies, since the network diameter almost hits the saturated value as shown in Figure 5.14. With the addition of long links using LP-based strategy, whenever the diameter reduces by one hop, it remains at the same value for a while and quickly moves down to one hop less. The addition of initial 10 links significantly reduces the path length as shown in Figure 5.15.

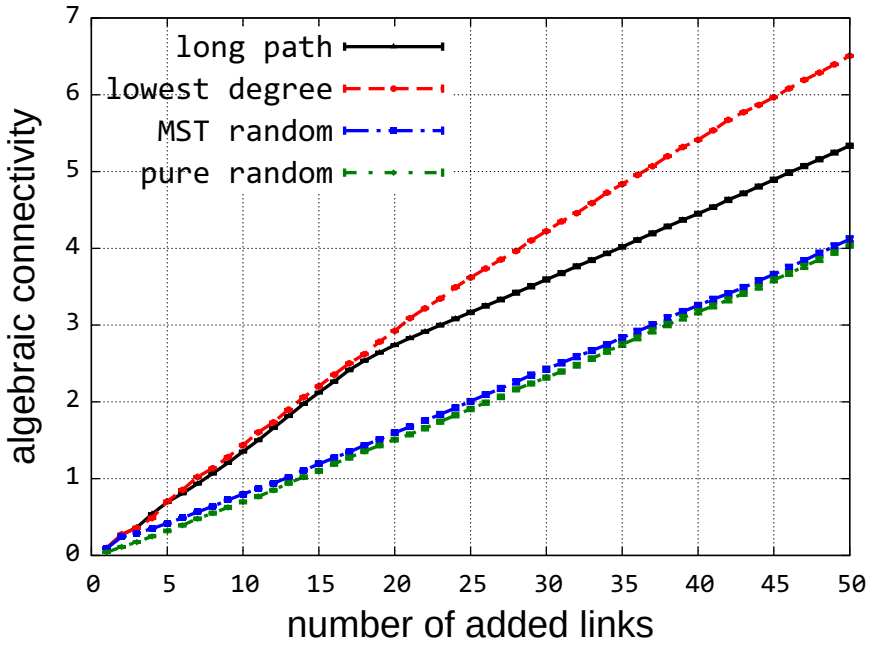


Figure 5.13: Algebraic connectivity of NCSU with an increased number of added links

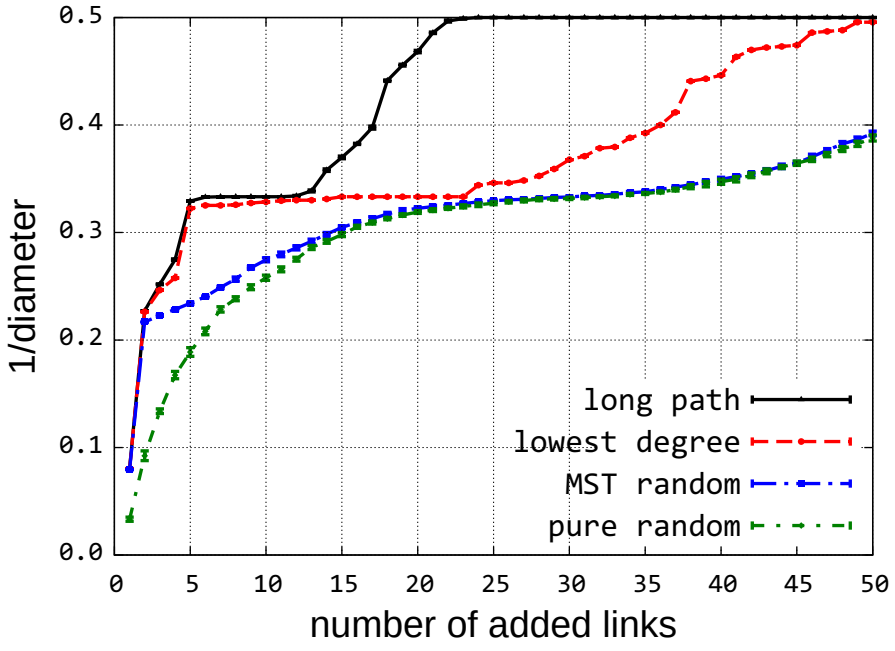


Figure 5.14: Inverse of diameter of NCSU with an increased number of added links

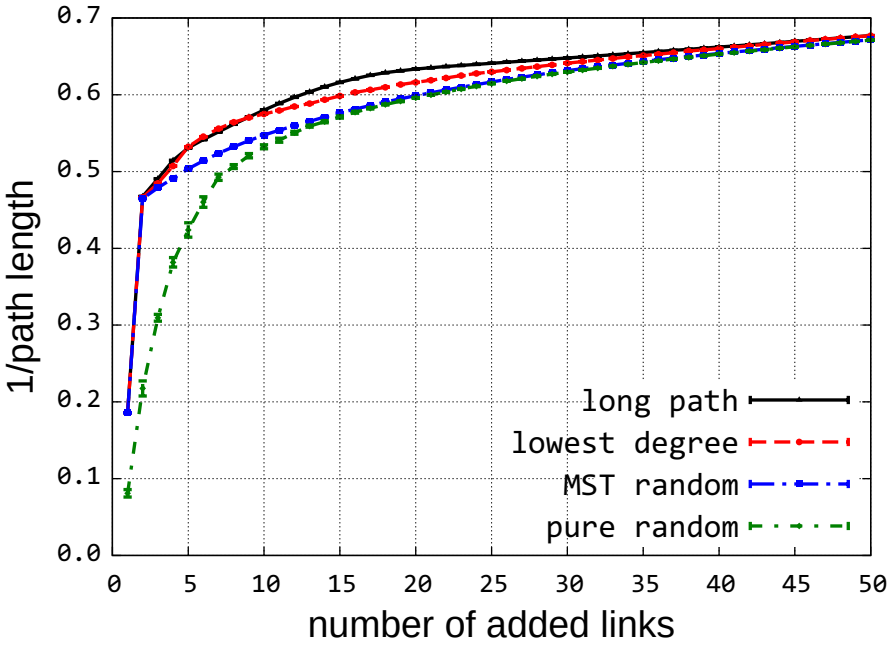


Figure 5.15: Inverse of path length of NCSU with an increased number of added links

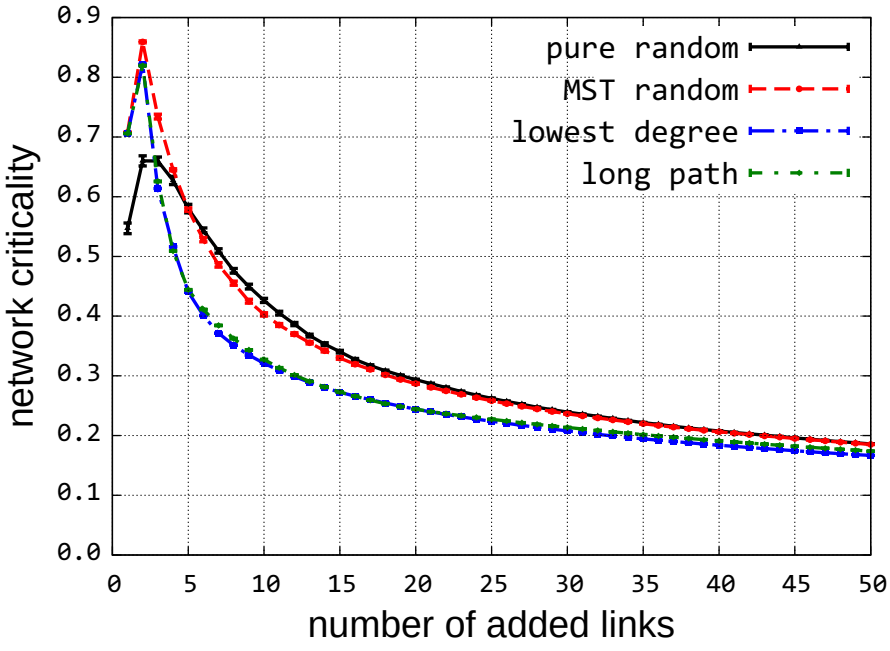


Figure 5.16: Network criticality of NCSU with an increased number of added links

The network criticality curves in the NCSU site reach the peaks when the network just becomes 1-connected by adding the bridging links. This has been explained in the previous section that the articulation points arising from adding bridge links are regarded as the weakness by the network critical metric because of the nodes' high betweenness. Once passing the 1-connectedness boundary, the network criticality of both LP- and LD-based strategies decreases faster than the random addition strategies. The average clustering coefficient in the NCSU site under different enhancement strategies follows a similar pattern as in the StateFair site.

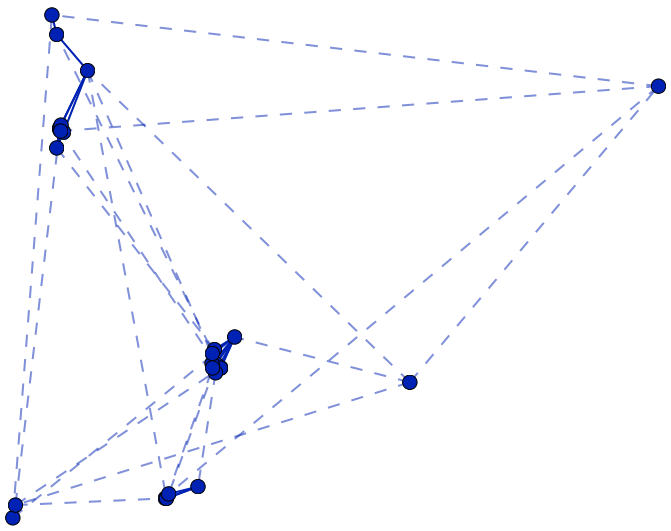


Figure 5.17: A snapshot of Orlando trace with 20 added links based on long-path strategy

Figure 5.17 presents a snapshot of the Orlando site enhanced with 20 links using LP-based strategy. Compared to the StateFair and NSCU sites, the connectivity in the Orlando

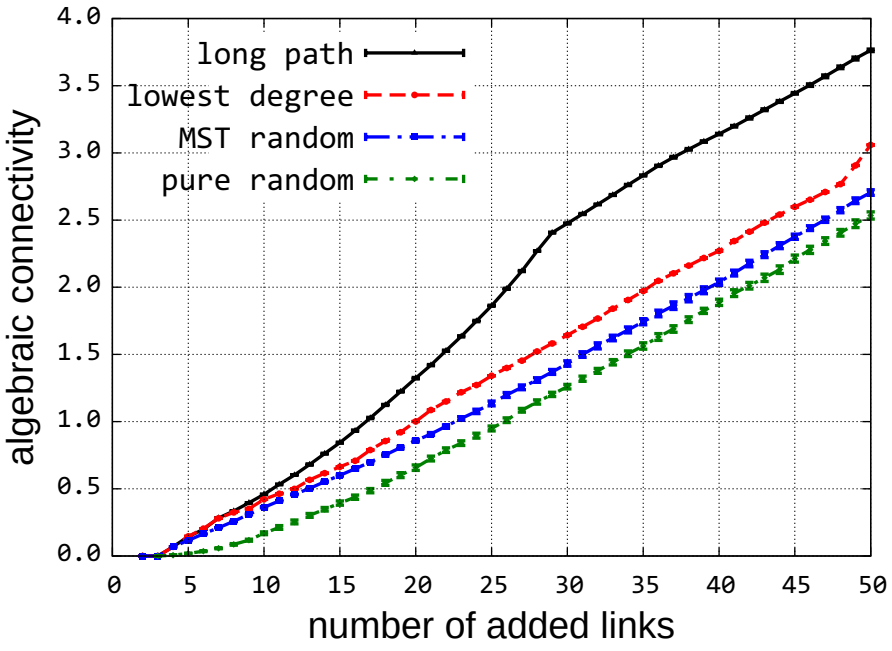


Figure 5.18: Algebraic connectivity of Orlando with an increased number of added links

site is much poorer. The Orlando site consists of several disconnected graph components, and the distances between component-pairs are considerably longer than the transmission range. This means that a modest increase of uniform transmission ranges for all node can hardly improve the global connectivity; as shown in Table 4.6, the giant component size and average flow robustness climbs slightly with the increase of transmission range from 250 m to 1000 m.

With the addition of 50 long links, the LP-based enhancement strategy performs the best of all strategies in terms of algebraic connectivity as shown in Figure 5.18. The LD-based strategy improves algebraic connectivity only moderately better than the two random strategies. The increasing rate of all curves becomes nearly identical after adding 29 links. For the LP-based strategy, there exists a change in the growing rate of the algebraic connectivity curve when the inverse of network diameter reach 0.4, which means the network diameter is within the range of 2 and 3. In Figure 5.19, the inverse of network

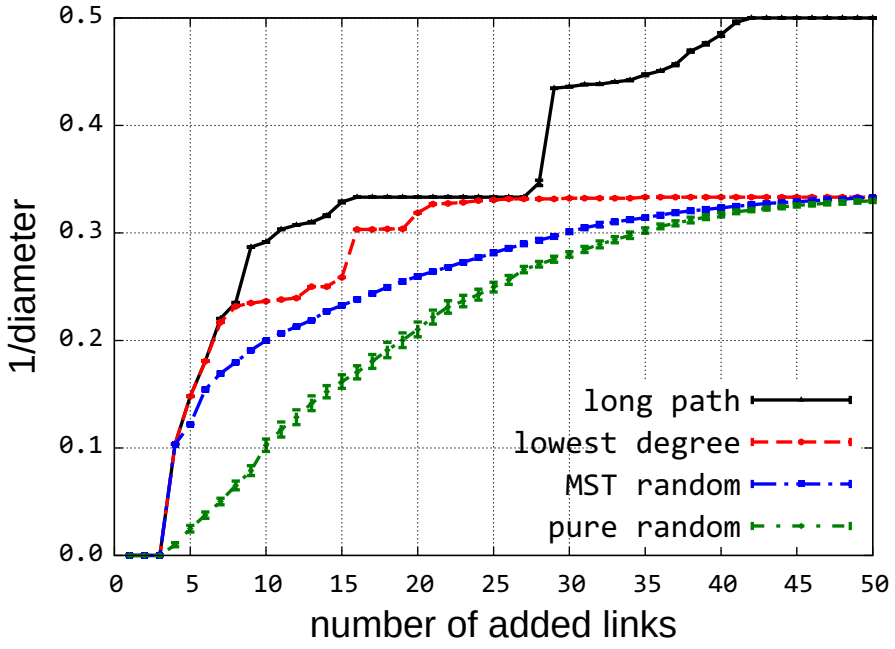


Figure 5.19: Inverse of diameter of Orlando with an increased number of added links

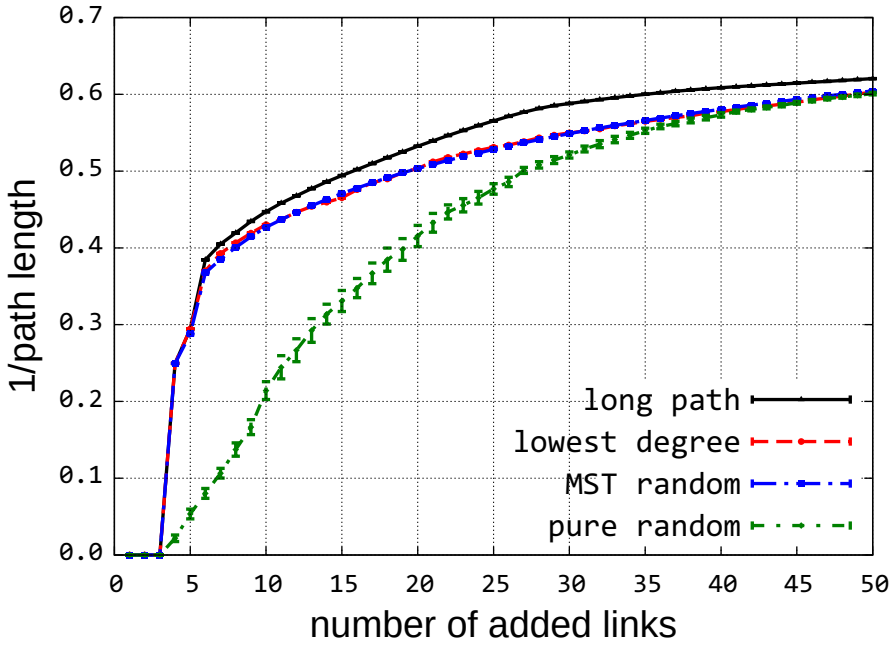


Figure 5.20: Inverse of path length of Orlando with an increased number of added links

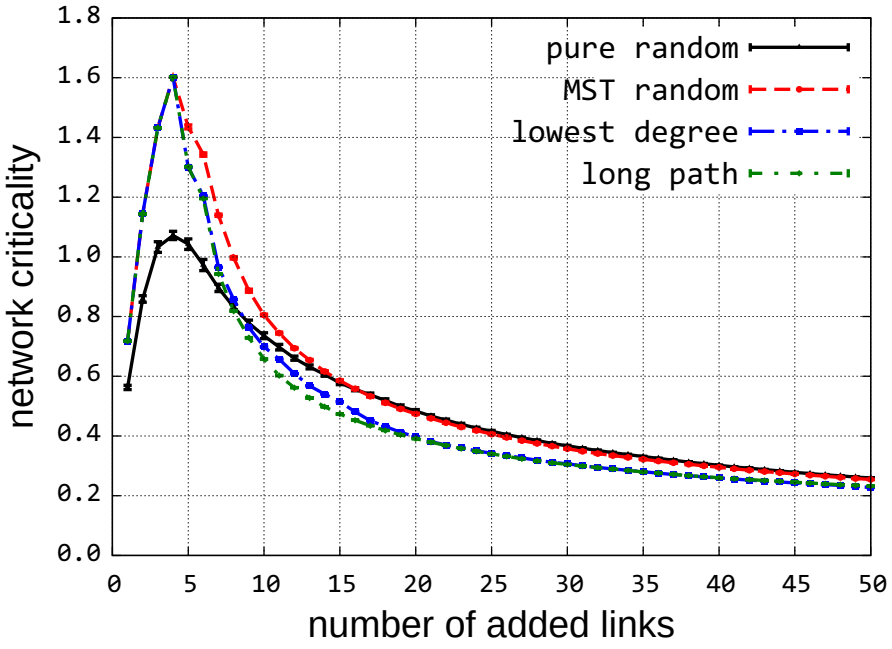


Figure 5.21: Network criticality of Orlando with an increased number of added links

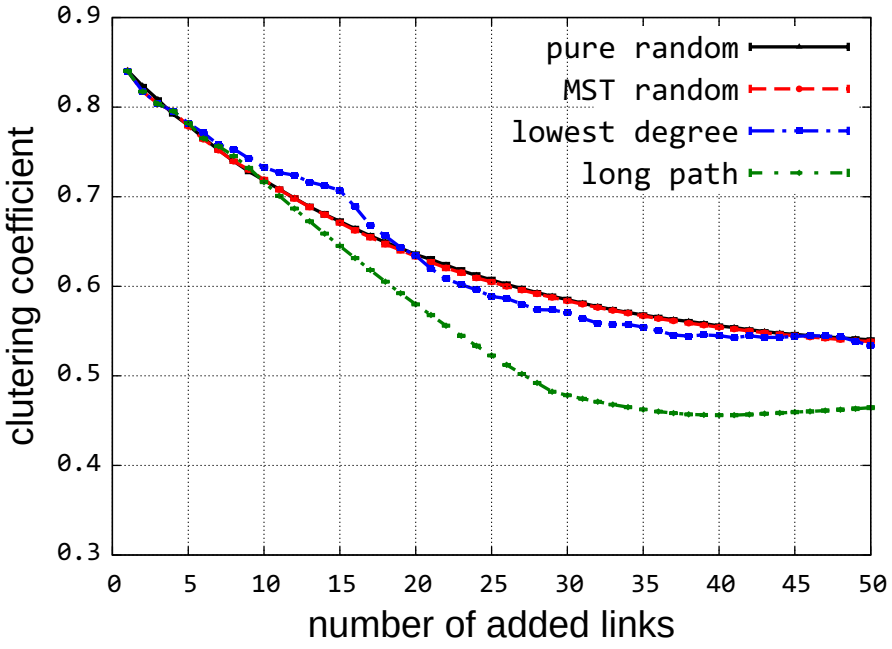


Figure 5.22: Clustering coefficient of Orlando with an increased number of added links

diameter of LP-based strategy quickly jumps to 1/3 after adding 15 links, and continues moving up to 1/2 after adding another 12 links. The change of diameter in LD-based strategy is slightly faster than in the random strategy, and after adding 50 links, all of them has an average of diameter of 3 (1/0.33). The LP-based strategy also results in a shorter average path length than other strategies as shown in Figure 5.20. The average path lengths in LD- and MR-based strategy are close to each other. The small value of the inverse of path length in PR-based strategy is due to the network partition even after adding some links randomly. We can infer from the diameter plots that the network becomes saturated much slower in Orlando site than in the Statefair and NCSU sites. In a less-connected network, the improvement based on the longest paths is more effective than other strategies as shown in the algebraic connectivity plot.

Except for the peak of network criticality after adding 4 links as also observed in the Statefair and NCSU sites, there is almost no difference between the network criticality between LP- and LD-based strategies after adding more than 20 links. However, there still exists a large variance between algebraic connectivity of two strategy. From this way, we can see that the algebraic connectivity and network criticality captures the network robustness from different perspectives. The algebraic connectivity can capture the minor difference of network robustness in a small-world network better than network criticality. The clustering coefficient of LP-based strategy is the lowest of all, and there is almost no change from adding 35 to 50 links. The clustering coefficient change of LD-based strategy fluctuates since the link addition between two lowest degree nodes might contribute to the formation of a local clique if they are in the same neighborhood. It might also bring a new node to the neighborhood with no links connected to other neighborhood nodes.

Figure 5.24 provides a snapshot of the NewYork site improved by 20 links using LP-based strategy, from which we can observe that the NewYork site has the worst connectivity of all five sites. The LP- and LD-based enhancement strategies have similar effects on the

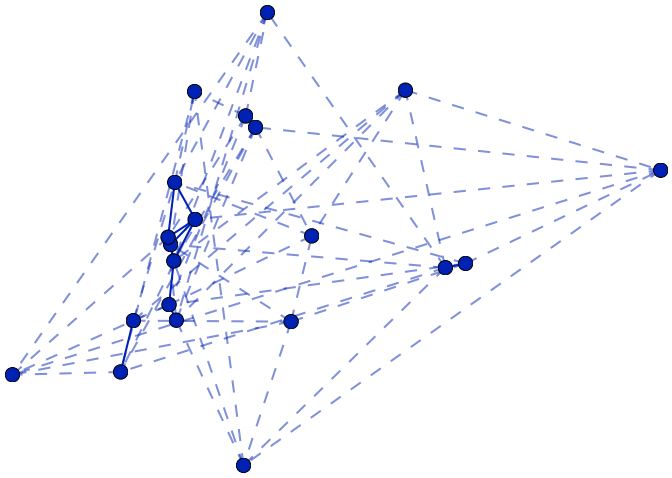


Figure 5.23: A snapshot of NewYork trace with 20 added links based on long-path strategy

improvement of algebraic connectivity and network criticality as shown in 5.24 and 5.25. The number of added links that corresponds to the peak in network criticality curves is approximately 9 to 10, which means that the NewYork site consists of an average of 9 to 10 disconnected components. The inverse of network diameters for all strategies are around 0.33 after adding 50 links. Network diameter decreases quickly after adding a small number of links even to an extremely poorly-connected network. Both LP- and LD-based strategies reduce the network diameter faster than the random strategies as shown in Figure 5.26. Due to the initial poor connectivity, the clustering coefficient starts as 0.25. Hence, after adding 10 links, the clustering coefficients of random enhancement strategies reach the lowest values and begin to increase. The lowest point of pure random

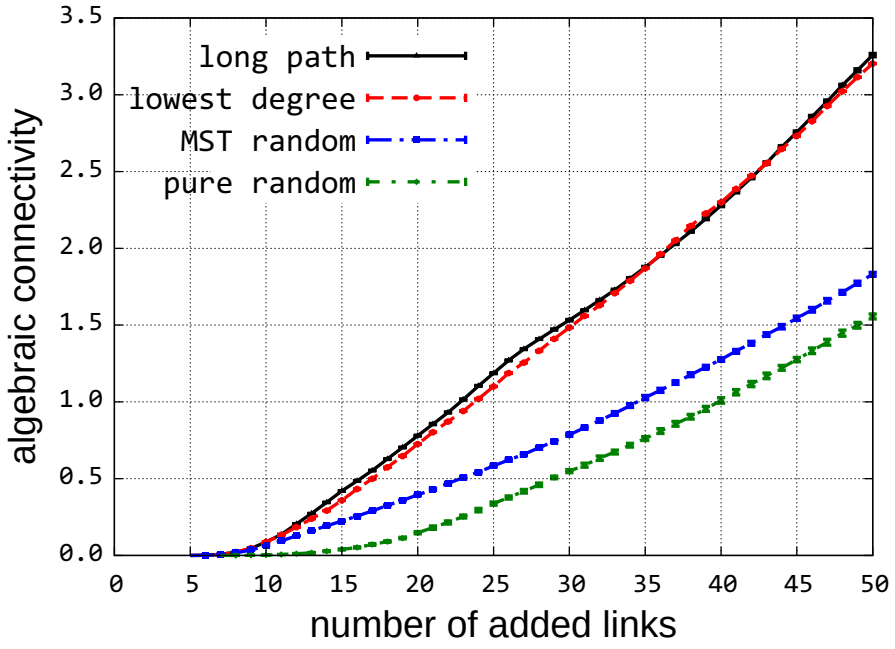


Figure 5.24: Algebraic connectivity of NewYork with an increased number of added links

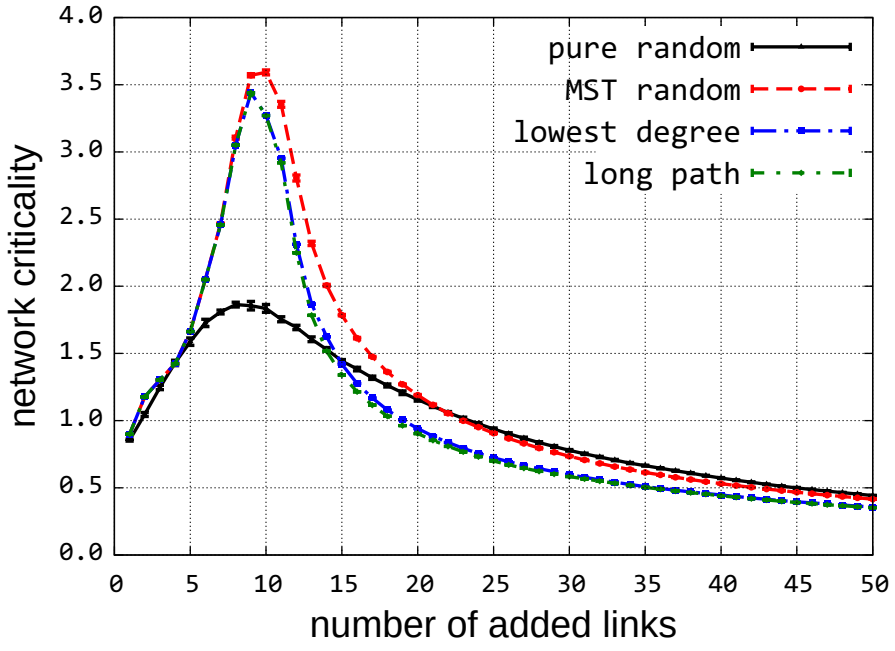


Figure 5.25: Network criticality of NewYork with an increased number of added links

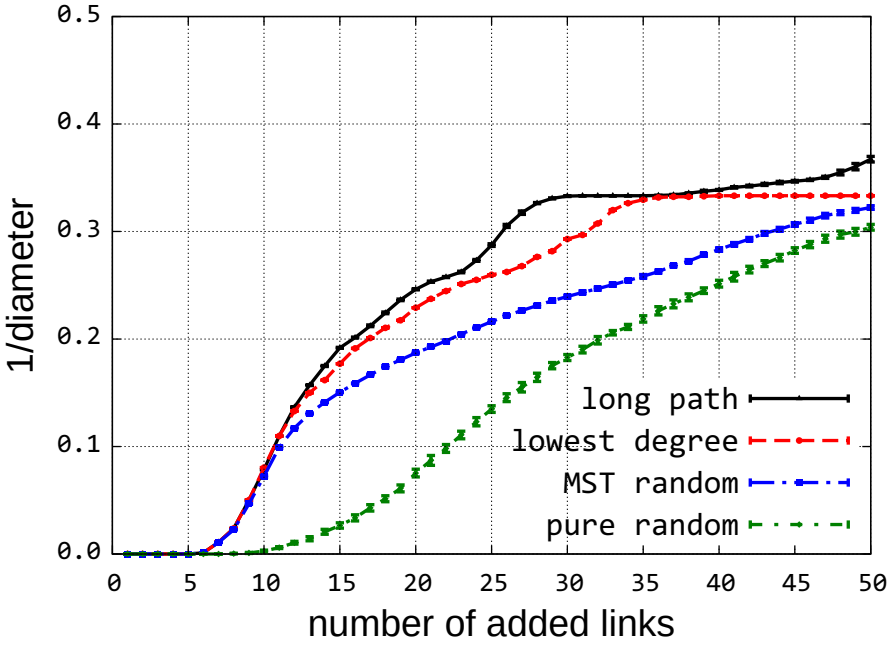


Figure 5.26: Inverse of diameter of NewYork with an increased number of added links

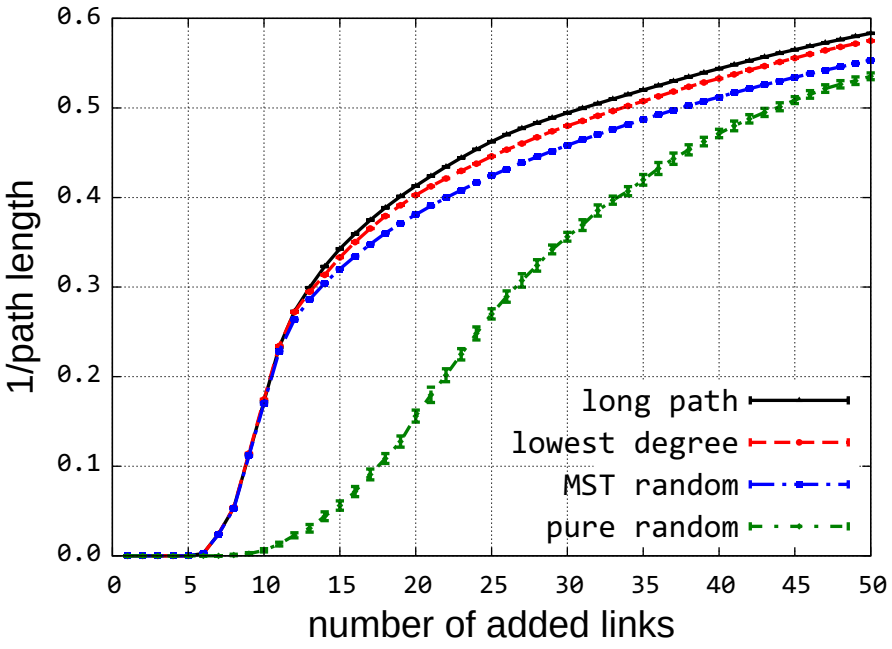


Figure 5.27: Inverse of path length of NewYork with an increased number of added links

strategy is slightly higher than the other three enhancement approaches that use MST to bridge the disconnected components. This is because bridging two disconnected reduces

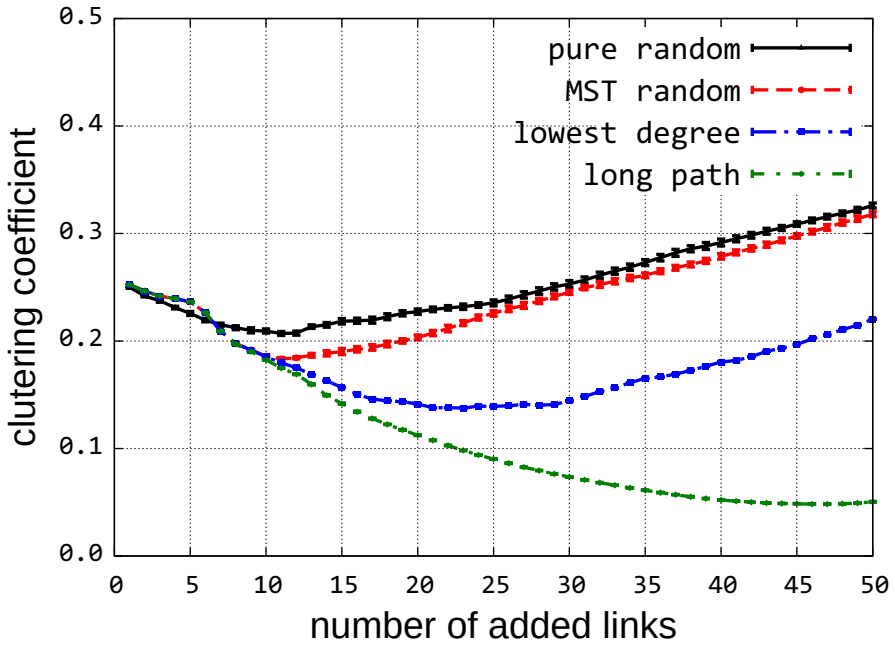


Figure 5.28: Clustering coefficient of NewYork with an increased number of added links

the average clustering coefficient in that the two end-points of the bridging link do not contribute to any triangles. The bridging links improve the global connectivity however contribute less to the local connectivity. The clustering coefficient of LP-based strategy keeps decreasing down to 0.05 with up to 50 links additions. At the same time, the average diameter, that is the longest path length, is less than 3 after adding 50 links using the LP-based strategy. A path length of 1 would directly contribute to a high value of clustering coefficient, which means that the majority of path length in the LP-enhanced NewYork site are higher than 1 but less than or equal to 3.

Figure 5.29 presents a snapshot of KAIST site improved by 20 links using LP-based strategy. The majority of nodes in the KAIST site form a dense cluster with a small number of other nodes spread out in the site. The algebraic connectivity of LP-, LD-, and MR-based strategies are close to each other with up to 30 link additions. However, after adding more than 30 links, LP-based strategy improves the algebraic connectivity

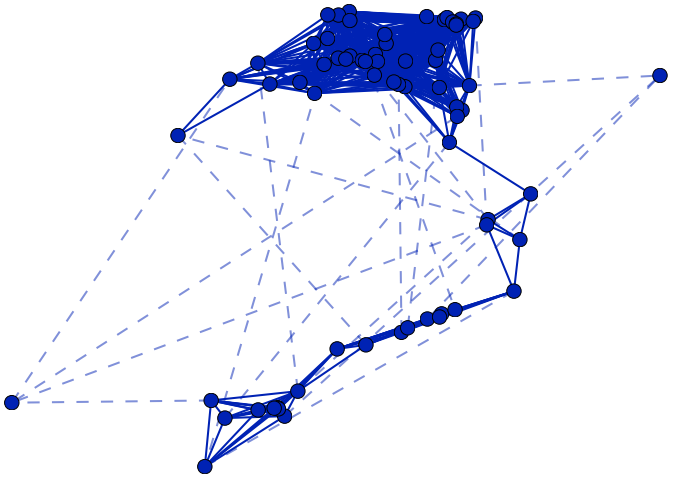


Figure 5.29: A snapshot of KAIST trace with 20 added links based on long-path strategy

far greater than other strategies. The point where LP-based strategy diverges from LD- and MR-based strategies is almost the same place where the inverse of network diameter reaches 0.33. The LD-based enhancement strategy improves algebraic connectivity better than the LD-based heuristic, which only has a slightly better performance than MR-based strategy. Even though the LD-based approach guarantee the highest algebraic connectivity improvement for a single addition, the heuristic is far from optimal overall after iteratively adding a number of enhancing links. We do not provide the results for network criticality for the KAIST site due to the convergence failure when computing the Moore-Penrose inverse of the graph Laplacian matrix.

Due to the large number of nodes in the KAIST site, the addition of initial 10 links using

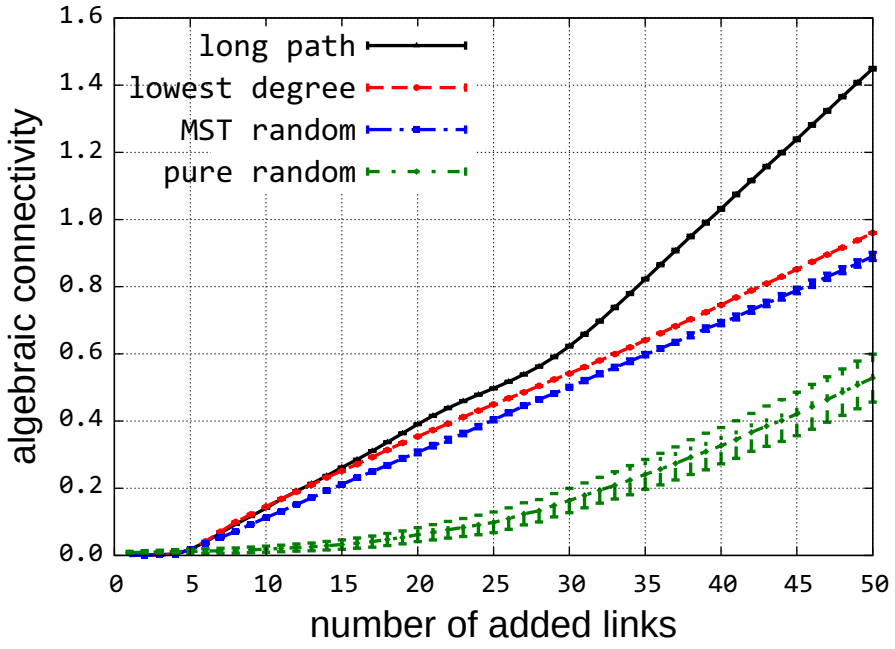


Figure 5.30: Algebraic connectivity of KAIST with an increased number of added links

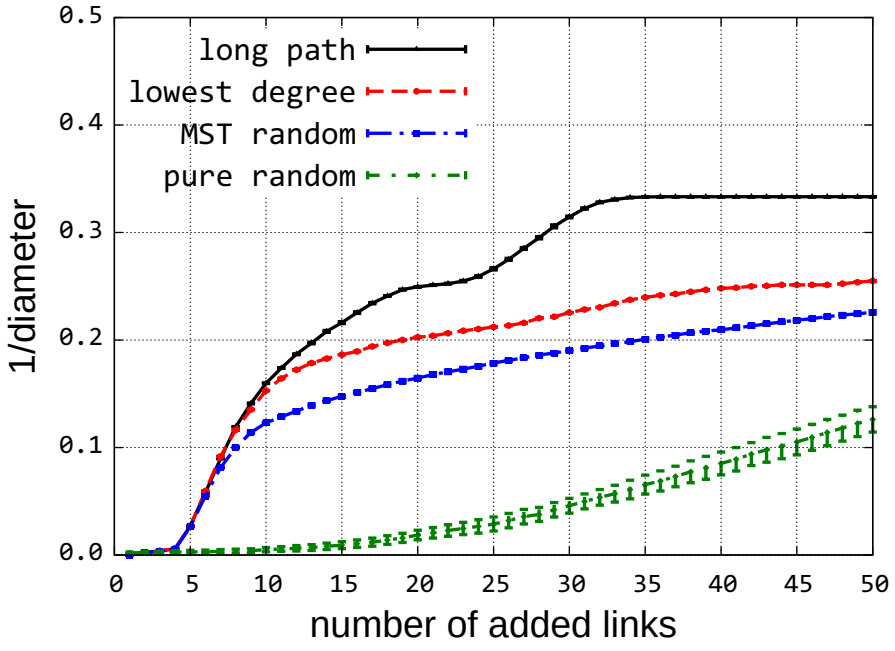


Figure 5.31: Inverse of diameter of KAIST with an increased number of added links

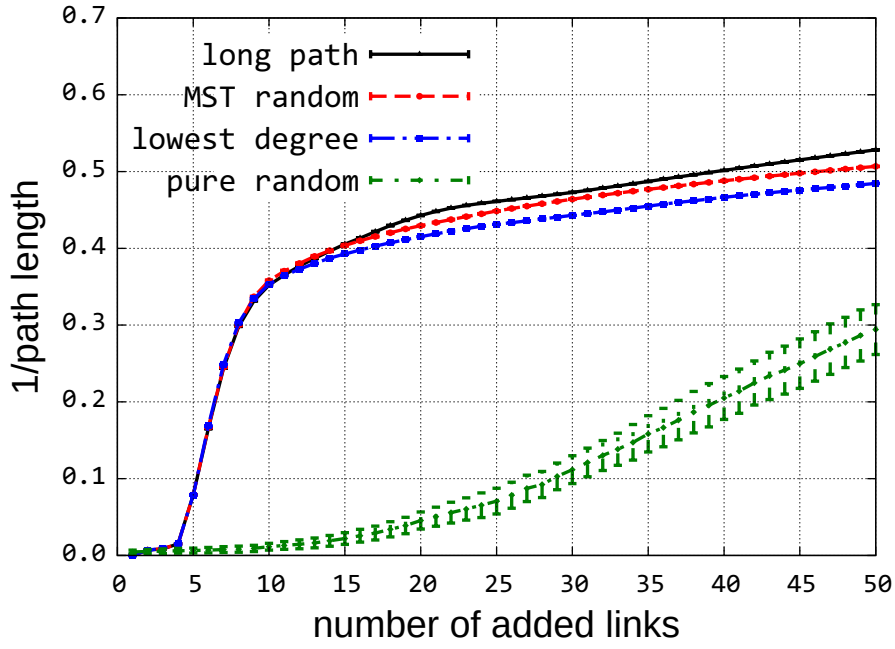


Figure 5.32: Inverse of path length of KAIST with an increased number of added links

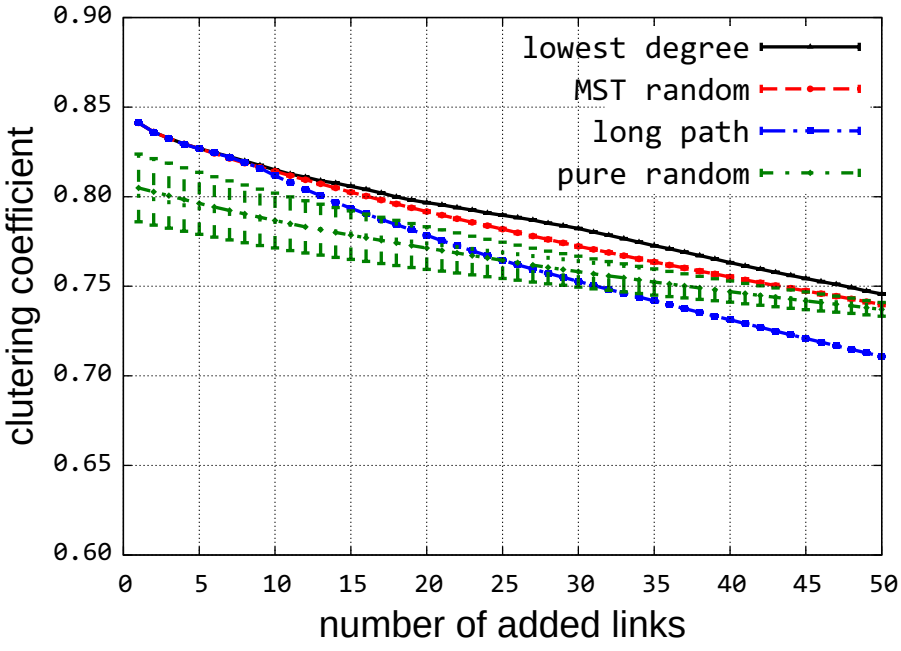


Figure 5.33: Clustering coefficient of KAIST with an increased number of added links

PR-based strategy produces a high variation of clustering coefficient. The LP-based strategy has the lowest clustering coefficient after adding 35 links. However, the average clustering coefficients arising from the large cluster are far higher than the other four sites for all strategies .

Of all the five sites, the LD-based heuristics strategy results in the highest algebraic connectivity in the StateFair and NCSU sites after the inverse of network diameter reaches 0.5, while the LP-based enhancement results in the highest algebraic connectivity in the Orlando and KAIST sites. The network criticality for LD- and LP-based strategy are very close to each other in all five sites. Noting that the LD-based heuristic is optimized in each step for a high algebraic connectivity, our proposed LP-based strategy with a much less computational complexity provides a comparative performance in terms of both algebraic connectivity and network criticality. The clustering coefficients of LP-based strategy in all fives begin with a decrease to a lowest value, and depending on the network connectivity, the cluster coefficients start increasing quickly after reaching the lowest value. The low clustering coefficient and small network diameter have been observed at the same time for a certain range of link additions in the NewYork site using the LP-based strategy.

5.2.2 Sum of Flow Robustness Evaluation

We have evaluated the five different sites using the algebraic connectivity, network criticality, network diameter, path lengths, and cluster coefficient. Next, we evaluate the sum of flow robustness $\sum \mathcal{F}$ of the real-world traces by adaptively applying malicious attacks until all the links are removed in each network. We select the degree, closeness, betweenness, and flexible centrality as the attack strategies to study network robustness. The $\sum \mathcal{F}$ for unimproved sites is provided as the comparison for $\sum \mathcal{F}$ of the different enhancement strategies. The $\sum \mathcal{F}$ of all the sites under attacks present a straightforward

Table 5.2: $\sum \mathcal{F}$ of the enhanced real-world traces under attacks

	Unimproved	Pure random	MST random	Lowest degree	Longest path
$\sum \mathcal{F}^d_{\text{StateFair}}$	3.867	5.924	6.025	**6.339**	6.116
$\sum \mathcal{F}^c_{\text{StateFair}}$	3.434	5.798	5.865	**6.239**	6.055
$\sum \mathcal{F}^b_{\text{StateFair}}$	3.328	5.508	5.594	**6.006**	5.828
$\sum \mathcal{F}^f_{\text{StateFair}}$	3.202	5.503	5.593	**6.001**	5.819
$\sum \mathcal{F}^d_{\text{NCSU}}$	3.441	7.501	7.523	**7.942**	7.864
$\sum \mathcal{F}^c_{\text{NCSU}}$	3.474	7.278	7.317	7.367	**7.685**
$\sum \mathcal{F}^b_{\text{NCSU}}$	3.339	6.531	6.579	7.161	**7.383**
$\sum \mathcal{F}^f_{\text{NCSU}}$	3.187	6.496	6.536	7.125	**7.369**
$\sum \mathcal{F}^d_{\text{Orlando}}$	1.727	6.459	6.680	**7.893**	7.333
$\sum \mathcal{F}^c_{\text{Orlando}}$	1.723	6.114	6.290	6.293	**6.794**
$\sum \mathcal{F}^b_{\text{Orlando}}$	2.096	5.653	5.805	6.250	**6.526**
$\sum \mathcal{F}^f_{\text{Orlando}}$	1.709	5.549	5.708	6.129	**6.445**
$\sum \mathcal{F}^d_{\text{NewYork}}$	0.371	3.479	4.150	4.552	**4.886**
$\sum \mathcal{F}^c_{\text{NewYork}}$	0.353	3.435	3.979	4.493	**4.797**
$\sum \mathcal{F}^b_{\text{NewYork}}$	0.451	3.148	3.652	4.220	**4.509**
$\sum \mathcal{F}^f_{\text{NewYork}}$	0.344	3.111	3.620	4.190	**4.482**
$\sum \mathcal{F}^d_{\text{KAIST}}$	10.020	17.221	19.455	19.978	**20.621**
$\sum \mathcal{F}^c_{\text{KAIST}}$	7.318	13.346	14.215	14.526	**15.077**
$\sum \mathcal{F}^b_{\text{KAIST}}$	7.342	11.856	12.195	12.267	**12.874**
$\sum \mathcal{F}^f_{\text{KAIST}}$	6.425	11.360	11.660	11.663	**12.247**

perspective to understand how the networks survive malicious attacks by measuring the number of node pairs can communicate with each other under node attacks. For the same types of attacks, values in each row compare how each enhancement strategy performs for this particular type of attacks.

In the StateFair site, the LD-based strategy generates the highest $\sum \mathcal{F}$ for all attack strategies with the LP-based strategy comes as the second. For the other four sites, it follows that LP > LD > MR > PR for all types of attacks except for the degree-based attacks in NCSU and Orlando. Even for the cases that LP-based strategy presents worse performance than LD-based strategy, the difference between them is smaller than other cases. By considering the overall scenarios, our LP-based strategy predominantly

provides the best enhancement performance for MANETs in face of malicious centrality-based attacks.

Small-world networks have been known for the characteristic short average path length as in random graphs and the high clustering coefficient as in regular graphs. Our results show that the degree of separation will decease drastically by adding a small number of nodes. The LP-based link addition strategy in all sites has a smaller clustering coefficient than random link addition when the network has a relatively low connectivity (the initial additions in the Statefair site, the entire range of 50 link additions in Orlando, NCSU, and NewYork sites); however, the average path length of LP-based strategy is also the lowest of all. All the sites except for the NewYork site enhanced by different strategies still have a relatively high clustering coefficient but also have reduced path lengths, which fall into the category of small-world networks. The NewYork site improved by LP-based strategy has an extremely low clustering coefficient with a small path length at the same time. These properties are more similar to that of random networks.

Page left intentionally blank.

Chapter 6

Conclusions and Future Work

This dissertation presents a comprehensive model to investigate the topological robustness of MANETs and enhancement strategies to improve network resilience under malicious attacks. We model the dynamic topologies of MANETs as the aggregation of snapshots into a weighted graph and evaluate network robustness under centrality-based attacks from various perspectives. We compare the effectiveness of centrality metrics for different network scenarios and proposed a *flexible* centrality metric. We propose a MST and longest-path-based network enhancement scheme to improve the resilience of intermittent MANETs. The relationship among small-world networks and random geometric graphs is investigated by examining the changes of network structural properties after link additions. We evaluate our attack model and enhancement scheme by using traces generated by a synthetic mobility model and real-world mobility traces. Simulations are run in ns-3 by applying different MANET routing protocols to verify the PDR and network delay performance. Furthermore, we employ the resilience quantification approach to evaluate network resilience with a range of network operational states.

We define *mobility coefficient* to determine the window size by incorporating the impact of the transmission range and average moving velocity on the global topological structure change. We compare the effectiveness of centrality-based attacks using aggregated

topologies and current time instant topology. Our results reveal that the high degree nodes have less impact on the global topological structure than high closeness and betweenness nodes in dynamic networks. Our proposed flexible centrality metric overcomes the deficiency of betweenness metric in networks consisting of multiple well-connected components. Our results pinpoint the vulnerability of dynamic topologies in MANETs by attacking high betweenness nodes, particularly in a large network. The $\sum \mathcal{F}$ of networks enhanced by longest-path-based strategy demonstrates that our small-world-network-motivated remedy could alleviate the vulnerability caused by high betweenness nodes.

6.1 Conclusions

In Chapter 3, we introduce a model to represent dynamic topologies as a weighted static graph, in which the weight represents the link availability between node pairs. We define a metric *mobility coefficient* to represent the ratio of the average node distance traveled within a given window size to the transmission range. This metric is calculated independent of the number of nodes. We select a transmission range that can ensure a decent connectivity for synthetic trace analysis. By modifying the value of mobility coefficient, we have a corresponding window size for the computation of aggregated graphs. Weighted centrality metrics can be applied to the aggregated graph within a certain window as node significance indicators. We iteratively remove all the links that are incident to the highest centrality node and compute the flow robustness after each node attack. The high centrality nodes based on the real-time topology are also employed as the node significance indicators. We propose a flexible metric that combine the advantages of both betweenness and degree centrality.

Due to the dynamic and intermittent connectivity of MANETs, it is challenging to always

maintain a connected network with a high level of network performance. We propose a two-step network enhancement strategy that first addresses of issue of network partition and then further improves network resilience by adding long-range links. The first step is a MST-based algorithm by considering each disconnected graph component as a node and the square of distance between any two disconnected components as the link weights. We represent the distance between two components by using the distance between the closest node pair in two components. Motivated by the characteristic path in small-world network, we add long-range links to MANETs to mitigate the reliance on the bridging nodes that have a high betweenness. We employ four enhancement strategies that add long-range links to achieve different goals of network properties. Random addition strategy simply chooses links that do not exist in the original graphs in random. The other strategies begin with adding bridging links. The lowest-degree-based heuristic adds each link to optimize algebraic connectivity. Our proposed enhancement strategy add links between node pairs with largest number of hops.

In Chapter 4, we apply the attack model to synthetic and real-world mobility traces. We generate synthetic mobility traces with three different number of nodes (20, 50, and 100) to evaluate how network orders can affect the accuracy of using centrality metrics as node significance indicators. We first analyze the network connectivity with a range of wireless radio transmission ranges. We investigate the giant component size, flow robustness, and the probability of being 1-connected. Each of them provides different levels of granularities for network connectivity. We also confirm that networks of larger number of nodes have a short transition from 0 to 1 for connectivity. We select a transmission range that is way less than the critical transmission range however can provide higher than 90% flow robustness.

For the synthetic trace analysis, the betweenness-based attacks cause the highest degradation of flow robustness among all attack strategies. The degree and eigenvector-based

attacks cause no more damage than the random node failures with less than 20% nodes being attacked. The effectiveness of betweenness and the ineffectiveness of degree and eigenvector centrality become more apparent in a well-connected network with a larger number of nodes. However, the accuracy of betweenness-based attacks is more sensitive to the increase of window sizes. In contrast, the degree-based attacks are less affected by the aggregation window sizes. The difference between attacks based on topology of current time instant and based on aggregation is provided. The betweenness-based attacks using real-time topology information with a small time window has comparable performance with the betweenness-based attack calculated using aggregated graphs. The larger the window size is, the less accurate the betweenness calculated according to current time instant. With the change of global topological structure, the high degree and eigenvector centrality nodes stay relatively stable than the high closeness and betweenness nodes. Our results show that betweenness-based attack can cause the most damage to the network robustness, and the phenomena becomes more apparent in a network with a larger number of nodes.

For the real-world trace analysis, we select three different transmission ranges for each site. Each of the five sites including two campus sites, one theme park, one local fair, and one metro area presents a different distribution of the mobile nodes. We evaluate the auto-correlation of the time-varying flow robustness of mobility traces in selective sites with different transmission ranges. We use the resilience quantification approach to evaluate how network resilience under different centrality-based attacks in comparison to random failures. Our results show that flexible attacks can cause the greatest decrease of resilience in all sites. The second level of resilience analysis is conducted by using topological flow robustness as the operational states and the PDR and delay by running different MANET routing protocols as the service states. Our resilience analysis shows that OLSR provides the best application layer services.

In Chapter 5, we apply four enhancement strategies to the same data set as in Chapter 4. The four strategies are PR (pure random), MR (MST random), LD (lowest degree heuristic), and LP (longest path). We evaluate five graph robustness metrics for each scenario: algebraic connectivity, network criticality, inverse of diameter, inverse of average path length, and clustering coefficient. We add up to 50 links to each network scenarios. The algebraic connectivity of LP-based strategy has comparable performance as LD-based strategy when the inverse of diameter is less than 0.5. After the inverse of diameter reaches 0.5 meaning that all nodes can reach each other with less than or equal to 2 hops, the LP-based strategy becomes less effective and behaves more like random link additions. In the 50 nodes networks that span a larger diameter than 20 nodes networks, the algebraic connectivity enhanced using LP is always the highest of all with up to 50 link additions. The inverse of diameter in LP-based strategy increases faster than others. The inverse of path length using LD-based strategy is closer to MR-based strategy in 50 nodes networks; however, it is closer to LP-based strategy in 20 nodes networks. The link additions to the lowest degree nodes affect the average path length almost in the same way as random additions. The relative value of network criticality for different enhancement strategies is almost the same as that of algebraic connectivity. The higher network criticality indicates a lower robustness. The clustering coefficient of LP-based strategy is the lowest with initial link additions. In 20 nodes networks, the clustering coefficient hits the lowest point and then reverts to the highest with 50 link additions. For the sum of flow robustness, we apply degree, closeness, betweenness, and flexible centrality-based attacks to 20, 50, and 100 nodes networks enhanced by 20 link addition using all strategies. In 20 nodes networks, the LD-based enhancement strategy produces the highest $\sum \mathcal{F}$ with LP-based strategy next to it; whereas, in the 50 and 100 nodes networks, the LD-based enhancement strategy provides the highest $\sum \mathcal{F}$ of all.

For the real-world trace enhancement, the LD-based heuristic strategy results in the high-

est algebraic connectivity in the StateFair and NCSU sites when the inverse of network diameter reaches 0.5, and the LP-based enhancement results in the highest algebraic connectivity in the Orlando and KAIST sites. The network criticality for LD- and LP-based strategy are very close to each other in all five sites. Due to original poor connectivity of the real-world sites, the network criticality peaks when the network just becomes connected with all the articulation points exposed as the weak points of the network. The clustering coefficient of LP-based strategy stays the lowest of all when the average network diameter is less than 2. Considering the high computational cost incurred by LD-based heuristic, our proposed LP-based enhancement strategy can improve network resilience with less computational cost.

6.2 Future Work

This dissertation presents a preliminary study of link additions to random geometric graphs and examines how it relates to the small-world networks. The relationship among various types of small-world networks, random graphs, and random geometric graphs can be further studied. With the increasing advancement of commercial UAV technologies, a number of UAVs could establish a three dimensional ad hoc network for various purposes. It would be interesting to investigate the modeling and enhancement of network resilience and survivability in three dimensional ad hoc networks. The attack strategies used in this work assume the knowledge of global node positions, and a distributed attack and enhancement mechanism might be able to applied to a wider range of real-world MANET scenarios. Node positions generated by the Gauss-Markov mobility model follows a Poisson distribution. Different mobility patterns such as parent-child, Lévy-walk, and Manhattan mobility model can be used to model specific real-world scenarios. Centrality metrics are recalculated after the attack of each node in this work, while a fast

algorithm might exist that can compute current high centrality nodes based on the previous calculation. This work determines the existence of a link purely based on the Euclidean distance between the node pair. More realistic radio model such as log-normal shadowing [65, 73] can be applied. It has been shown in this work that attacks against the highest degree nodes are no more effective than random node failure in particular in a large network and the high betweenness nodes are usually those bridging node with a lower degree. It would be interesting to explore the impact of attacks against the lower degree nodes.

In terms of network enhancement schemes, we did not consider the cost of extra radios for each device in this dissertation. Further work on this part could include a cost-constrained enhancement approach with limited number of directional radios and compare the energy cost for each enhancement scheme. MANET resilience enhancement approach other than using directional antennas could be done by using extra mobile nodes such as programmed UAVs, which could reduce the energy cost while maintaining a high connectivity. One of the issues with the directional antennas that needs to addressed is how to consistently adjust beamforming directions in an accurate manner. We use a static method to calculate the MST for each snapshot of the dynamic topologies. The computation of MST for dynamic networks is worth exploring.

Topological analysis in this work assumes the use of MANET routing protocols. The application of DTN (delay-tolerant network) routing protocols to dynamic wireless network presents a new problem to be solved. Some work has been done to model and evaluate the robustness of dynamic temporal graphs in both social network and wireless networks [27, 88, 147]. The mappings of mobility contacts to an aggregated social graph can be utilized to optimize forwarding decisions of DTN [148]. It would be worthy to examine how to exploit the critical roles in a temporal network to improve the resilience and survivability of DTNs.

Page left intentionally blank.

Bibliography

[1] Ram Ramanathan and J. Redi. A brief overview of ad hoc networks: challenges and directions. *Communications Magazine, IEEE*, 40(5):20–22, 2002.

[2] Imrich Chlamtac, Marco Conti, and Jennifer J.-N. Liu. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, 1(1):13–64, 2003.

[3] Hannes Hartenstein and Kenneth P Laberteaux. A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE*, 46(6):164–171, 2008.

[4] Ian F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38(4):393–422, 2002.

[5] Thoams Guthrie Zimmerman. Personal area networks: near-field intrabody communication. *IBM systems Journal*, 35(3.4):609–617, 1996.

[6] Magnus Frodigh, Per Johansson, and Peter Larsson. Wireless ad hoc networking: the art of networking without a network. *Ericsson Review*, 4(4):249, 2000.

[7] Chyi-Ren Dow, Pei-Jung Lin, Sheng-Chang Chen, Jyh-Horng Lin, and Shiow-Fen Hwang. A study of recent research trends and experimental guidelines in mobile ad-hoc network. In *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*, volume 1, pages 72–77. IEEE, 2005.

[8] Open garden. http://opengarden.com.

[9] Textme. http://http://go-text.me/.

[10] Firechat. https://opengarden.com/firechat.

[11] Noam Cohen. Hong kong protests propel firechat phone-to-phone app. *The New York Times*, 2014.

[12] Twimight. https://code.google.com/p/twimight.

[13] Theus Hossmann, Paolo Carta, Dominik Schatzmann, Franck Legendre, Per Gunningberg, and Christian Rohner. Twitter in disaster mode: security architecture. In *Proceedings of the Special Workshop on Internet and Disasters*, page 7. ACM, 2011.

[14] James P.G. Sterbenz, Rajesh Krishnan, Regina Rosales Hain, Alden W. Jackson, David Levin, Ram Ramanathan, and John Zao. Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions. In *Proceedings of the 1st ACM Workshop on Wireless Security (WiSe)*, pages 31–40, Atlanta, GA, September 2002.

[15] 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.

[16] Bing Wu, Jianmin Chen, Jie Wu, and Mihaela Cardei. A survey of attacks and countermeasures in mobile ad hoc networks. In Yang Xiao, XueminSherman Shen, and Ding-Zhu Du, editors, *Wireless Network Security*, Signals and Communication Technology, pages 103–135. Springer US, 2007.

[17] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications*, 11(1):38–47, 2004.

[18] Elizabeth M Daly and Mads Haahr. The challenges of disconnected delay-tolerant manets. *Ad Hoc Networks*, 8(2):241–250, 2010.

[19] Ashwin Arulselvan, Clayton W. Commander, Lily Elefteriadou, and Panos M. Pardalos. Detecting critical nodes in sparse graphs. *Computers and Operations Research*, 36(7):2193–2200, 2009.

[20] Arnaud Casteigts, Paola Flocchini, Walter Quattrociocchi, and Nicola Santoro. Time-varying graphs and dynamic networks. *International Journal of Parallel, Emergent and Distributed Systems*, 27(5):387–408, 2012.

[21] Mathew Penrose. *Random Geometric Graphs*. Oxford Studies in Probability 5, 2003.

[22] Duncan J Watts and Steven H Strogatz. Collective dynamics of small-worldnetworks. *nature*, 393(6684):440–442, 1998.

[23] Linton C. Freeman. A Set of Measures of Centrality Based on Betweenness. *Sociometry*, 40(1):35–41, 1977.

[24] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. Çetinkaya, and James P.G. Sterbenz. Modelling Attacks and Challenges to Wireless Networks. In *Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 806–812, St. Petersburg, October 2012.

[25] John Whitbeck, Marcelo Dias de Amorim, Vania Conan, and Jean-Loup Guillaume. Temporal reachability graphs. In *Proceedings of the 18th annual international con-*

ference on Mobile computing and networking, Mobicom '12, pages 377–388, New York, NY, USA, 2012. ACM.

[26] A. Ferreira. Building a reference combinatorial model for MANETs. *IEEE Network*, 18(5):24–29, 2004.

[27] John Tang, Mirco Musolesi, Cecilia Mascolo, and Vito Latora. Temporal distance metrics for social network analysis. In *Proceedings of the 2nd ACM workshop on Online social networks*, pages 31–36, 2009.

[28] E.M. Daly and M. Haahr. Social network analysis for information flow in disconnected delay-tolerant MANETs. *IEEE Transactions on Mobile Computing*, 8(5):606–621, 2009.

[29] Jesper Dall and Michael Christensen. Random geometric graphs. *Physical Review E*, 66(1):016121, 2002.

[30] Dietrich Stauffer and Ammon Aharony. *Introduction to percolation theory*. CRC press, 1994.

[31] Josep Díaz, Dieter Mitsche, and Xavier Pérez-Giménez. Large connectivity for dynamic random geometric graphs. *Mobile Computing, IEEE Transactions on*, 8(6):821–835, 2009.

[32] Olivier Dousse, Petteri Mannersalo, and Patrick Thiran. Latency of wireless sensor networks with uncoordinated power saving mechanisms. In *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*, pages 109–120. ACM, 2004.

[33] Piyush Gupta and Panganamala R Kumar. Critical power for asymptotic connectivity in wireless networks. In *Stochastic analysis, control, optimization and applications*, pages 547–566. Springer, 1999.

[34] Bhaskar Krishnamachari, Stephen B Wicker, Ramon Bejar, and Marc Pearlman. Critical density thresholds in distributed wireless networks. *Communications, information and network security*, 1:15, 2002.

[35] Miguel Sanchez, Pietro Manzoni, and Zygmunt J Haas. Determination of critical transmission range in ad-hoc networks. In *Multiaccess, Mobility and Teletraffic in Wireless Communications: Volume 4*, pages 293–304. Springer, 1999.

[36] Olivier Dousse, Patrick Thiran, and Martin Hasler. Connectivity in ad-hoc and hybrid networks. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 1079–1088. IEEE, 2002.

[37] Peng-Jun Wan and Chih-Wei Yi. Asymptotic critical transmission radius and critical neighbor number for k-connectivity in wireless ad hoc networks. In *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*, pages 1–8. ACM, 2004.

[38] Mark EJ Newman and Duncan J Watts. Renormalization group analysis of the small-world network model. *Physics Letters A*, 263(4):341–346, 1999.

[39] Jon Kleinberg. The small-world phenomenon: An algorithmic perspective. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 163–170. ACM, 2000.

[40] Chaug-Ing Hsu and Hsien-Hung Shih. Small-world network theory in the study of network connectivity and efficiency of complementary international airline alliances. *Journal of Air Transport Management*, 14(3):123–129, 2008.

[41] Dave Cavalcanti, Dharma Agrawal, Judith Kelner, and Djamel Sadok. Exploiting the small-world effect to increase connectivity in wireless ad hoc networks. In *Telecommunications and Networking-ICT 2004*, pages 388–393. Springer, 2004.

[42] A. Bavelas. A mathematical model for group structures. *Human organization*, 7(3):16–30, 1948.

[43] Linton C. Freeman. Centrality in Social Networks Conceptual Clarification. *Social Networks*, 1(3):215–239, 1978–1979.

[44] P. Nikolopoulos, T. Papadimitriou, P. Pantazopoulos, M. Karaliopoulos, and I. Stavrakakis. How much off-center are centrality metrics for routing in opportunistic networks. In *Proceedings of the 6th ACM workshop on Challenged networks*, pages 9–14, September 2011.

[45] T. Opsahl, F. Agneessens, and J. Skvoretz. Node centrality in weighted networks: Generalizing degree and shortest paths. *Social Networks*, 32(3):245–251, 2010.

[46] M. E. J. Newman. Scientific collaboration networks. ii. shortest paths, weighted networks, and centrality. *Phys. Rev. E*, 64(1):16132, 2001.

[47] Ulrik Brandes. A faster algorithm for betweenness centrality*. *Journal of Mathematical Sociology*, 25(2):163–177, 2001.

[48] Phillip Bonacich. Factoring and Weighting Approaches to Status Scores and Clique Identification. *Journal of Mathematical Sociology*, 2(1):113–120, 1972.

[49] Britta Ruhnau. Eigenvector-centrality–a node-centrality? *Social networks*, 22(4):357–365, 2000.

[50] RV Mises and Hilda Pollaczek-Geiringer. Praktische verfahren der gleichungsauflösung. *ZAMM-Journal of Applied Mathematics and Mechanics/Zeitschrift für Angewandte Mathematik und Mechanik*, 9(1):58–77, 1929.

[51] Lawrence Page, Sergey Brin, Rajeev Motwani, and Terry Winograd. The pagerank citation ranking: bringing order to the web. 1999.

[52] Stephen P. Borgatti. Identifying sets of key players in a social network. *Comput. Math. Organ. Theory*, 12(1):21–34, April 2006.

[53] Miroslav Fiedler. Algebraic connectivity of graphs. *Czechoslovak Mathematical Journal*, 23(2):298–305, 1973.

[54] Huijuan Wang and Piet Van Mieghem. Algebraic connectivity optimization via link addition. In *Proceedings of the 3rd ICST International Conference on Bio-Inspired Models of Network, Information and Computing Sytems (BIONETICS)*, pages 22:1–22:8, Hyogo, Japan, November 2008.

[55] William Liu, Harsha Sirisena, Krzysztof Pawlikowski, and Allan McInnes. Utility of algebraic connectivity metric in topology design of survivable networks. In *Proceedings of the 7th IEEE International Workshop on Design of Reliable Communication Networks (DRCN)*, pages 131–138, Washington, DC, October 2009.

[56] Ali Sydney, Caterina Scoglio, and Don Gruenbacher. Optimizing algebraic connectivity by edge rewiring. *Applied Mathematics and Computation*, 219(10):5465–5479, 2013.

[57] Ali Tizghadam and Alberto Leon-Garcia. Autonomic traffic engineering for network robustness. *Selected Areas in Communications, IEEE Journal on*, 28(1):39–50, 2010.

[58] Ali Tizghadam and Alberto Leon-Garcia. Betweenness centrality and resistance distance in communication networks. *Network, IEEE*, 24(6):10–16, 2010.

[59] Justin P. Rohrer, Abdul Jabbar, and James P.G. Sterbenz. Path Diversification for Future Internet End-to-End Resilience and Survivability. *Springer Telecommunication Systems*, 56(1):49–67, May 2014.

[60] Orhan Dengiz, Abdullah Konak, and Alice E Smith. Connectivity management in mobile ad hoc networks using particle swarm optimization. *Ad Hoc Networks*, 9(7):1312–1326, 2011.

[61] Mark EJ Newman, Steven H Strogatz, and Duncan J Watts. Random graphs with arbitrary degree distributions and their applications. *Physical review E*, 64(2):026118, 2001.

[62] Agata Fronczak, Piotr Fronczak, and Janusz A Hołyst. Average path length in random networks. *Physical Review E*, 70(5):056110, 2004.

[63] Réka Albert and Albert-László Barabási. Statistical mechanics of complex networks. *Reviews of modern physics*, 74(1):47, 2002.

[64] Egemen K. Çetinkaya, Dan Broyles, Amit Dandekar, Sripriya Srinivasan, and James P. G. Sterbenz. A Comprehensive Framework to Simulate Network Attacks and Challenges. In *Proceedings of the 2nd IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 538–544, Moscow, October 2010.

[65] R. Hekmat and P. Van Mieghem. Degree distribution and hopcount in wireless ad-hoc networks. In *Proceeding of the 11th IEEE International Conference on Networks (ICON)*, pages 603–609, September 2003.

[66] C. Bettstetter. On the connectivity of ad hoc networks. *The Computer Journal*, 47(4):432–447, 2004.

[67] T.N. Dinh, Y. Xuan, M.T. Thai, EK Park, and T. Znati. On approximation of new optimization methods for assessing network vulnerability. In *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, pages 1–9, 2010.

[68] George Caspar homans. *The human group*. Transaction Publishers, 1951.

[69] Mark S Granovetter. The strength of weak ties. *American journal of sociology*, pages 1360–1380, 1973.

[70] Egemen K. Çetinkaya, Dan Broyles, Amit Dandekar, Sripriya Srinivasan, and James P. G. Sterbenz. Modelling Communication Network Challenges for Future Internet Resilience, Survivability, and Disruption Tolerance: A Simulation-Based Approach. *Telecommunication Systems*, 52(2):751–766, 2013.

[71] Ioannis Chatzigiannakis, Athanasios Kinalis, Georgios Mylonas, Sotiris Nikoletseas, Grigorios Prasinos, and Christos Zaroliagis. Trails, a toolkit for efficient, realistic and evolving models of mobility, faults and obstacles in wireless networks. In *ANSS '08: Proceedings of the 41st Annual Simulation Symposium*, pages 23–32, April 2008.

[72] Ioannis Chatzigiannakis, Georgios Mylonas, and Sotiris Nikoletseas. Modeling and evaluation of the effect of obstacles on the performance of wireless sensor networks. In *ANSS '06: Proceedings of the 39th Annual Simulation Symposium*, April 2006.

[73] R. Hekmat and P. Van Mieghem. Connectivity in wireless ad-hoc networks with a log-normal radio model. *Mobile Networks and Applications*, 11(3):351–360, 2006.

[74] Bhaskar Krishnamachari, Deborah Estrin, and Stephen Wicker. Modelling data-centric routing in wireless sensor networks. In *IEEE infocom*, volume 2, pages 39–44, 2002.

[75] Benjie Chen, Kyle Jamieson, Hari Balakrishnan, and Robert Morris. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. *Wireless Networks*, 8(5):481–494, 2002.

[76] Jeffrey G Andrews, Radha Krishna Ganti, Martin Haenggi, Nihar Jindal, and Steven Weber. A primer on spatial modeling and analysis in wireless networks. *Communications Magazine, IEEE*, 48(11):156–163, 2010.

[77] Arunabha Sen, Sudheendra Murthy, and Sujogya Banerjee. Region-based connectivity-a new paradigm for design of fault-tolerant networks. In *High Performance Switching and Routing, 2009. HPSR 2009. International Conference on*, pages 1–7. IEEE, 2009.

[78] Arunabha Sen, Sujogya Banerjee, Pavel Ghosh, and Shahrzad Shirazipourazad. Impact of region-based faults on the connectivity of wireless networks. In *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*, pages 1430–1437. IEEE, 2009.

[79] Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama, and Nei Kato. Reliability assessment for wireless mesh networks under probabilistic region failure model. *Vehicular Technology, IEEE Transactions on*, 60(5):2253–2264, 2011.

[80] Siqian Shen and J. Cole Smith. Polynomial-time algorithms for solving a class of critical node problems on trees and series-parallel graphs. *Networks*, 60(2):103–119, 2012.

[81] M. Di Summa, A. Grosso, and M. Locatelli. Branch and cut algorithms for detecting critical nodes in undirected graphs. *Computational Optimization and Applications*, pages 1–32, 2012.

[82] Devendra Goyal and James Caffery Jr. Partitioning avoidance in mobile ad hoc networks using network survivability concepts. In *Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh International Symposium on*, pages 553–558. IEEE, 2002.

[83] Michaël Hauspie, Jean Carle, and David Simplot. Partition detection in mobile ad-hoc networks using multiple disjoint paths set. In *International Workshop on Objects models and Multimedia technologies*, page 15, 2003.

[84] Milenko Jorgic, Michaël Hauspie, David Simplot-Ryl, and Ivan Stojmenovic. Localized algorithms for detection of critical nodes and links for connectivity in ad hoc networks. In *Mediterranean Ad Hoc Networking Workshop*, page 12, 2004.

[85] M.T. Gardner and C. Beard. Evaluating Geographic Vulnerabilities in Networks. In *IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, pages 1–6, May 2011.

[86] T.H. Kim, D. Tipper, and P. Krishnamurthy. Connectivity and critical point behavior in mobile ad hoc and sensor networks. In *IEEE Symposium onComputers and Communications ISCC*, pages 153–158. IEEE, 2009.

[87] Tae-Hoon Kim, D. Tipper, P. Krishnamurthy, and A.L. Swindlehurst. Improving the topological resilience of mobile ad hoc networks. In *7th International Workshop*

on Design of Reliable Communication Networks (DRCN), pages 191–197, October 2009.

[88] S. Scellato, I. Leontiadis, C. Mascolo, P. Basu, and M. Zafer. Evaluating temporal robustness of mobile networks. *IEEE Transactions on Mobile Computing*, 12(1):105–117, January 2013.

[89] Goutham Karumanchi, Srinivasan Muralidharan, and Ravi Prakash. Information dissemination in partitionable mobile ad hoc networks. In *Reliable Distributed Systems, 1999. Proceedings of the 18th IEEE Symposium on*, pages 4–13. IEEE, 1999.

[90] James Davis, Andrew H Fagg, Brian N Levine, et al. Wearable computers as packet transport mechanisms in highly-partitioned ad-hoc networks. In *Wearable Computers, 2001. Proceedings. Fifth International Symposium on*, pages 141–148. IEEE, 2001.

[91] Karen H Wang and Baochun Li. Efficient and guaranteed service coverage in partitionable mobile ad-hoc networks. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 1089–1098. IEEE, 2002.

[92] Wenrui Zhao, Mostafa Ammar, and Ellen Zegura. A message ferrying approach for data delivery in sparse mobile ad hoc networks. In *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*, pages 187–198. ACM, 2004.

[93] Qun Li and Daniela Rus. Communication in disconnected ad hoc networks using message relay. *Journal of Parallel and Distributed Computing*, 63(1):75–86, 2003.

[94] Chia-Ho Ou, Kuo-Feng Ssu, and Hewijin Christine Jiau. Connecting network partitions with location-assisted forwarding nodes in mobile ad hoc environments. In *Dependable Computing, 2004. Proceedings. 10th IEEE Pacific Rim International Symposium on*, pages 239–247. IEEE, 2004.

[95] Karthikeyan Chandrashekar, Majid Raissi Dekhordi, and John S Baras. Providing full connectivity in large ad-hoc networks by dynamic placement of aerial platforms. In *Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE*, volume 3, pages 1429–1436. IEEE, 2004.

[96] Zhu Han, KJ Liu, et al. Smart deployment/movement of unmanned air vehicle to improve connectivity in manet. In *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, volume 1, pages 252–257. IEEE, 2006.

[97] Abdullah Konak, George E Buchert, and James Juro. A flocking-based approach to maintain connectivity in mobile wireless ad hoc networks. *Applied Soft Computing*, 13(2):1284–1291, 2013.

[98] Paolo Santi. Topology control in wireless ad hoc and sensor networks. *ACM computing surveys (CSUR)*, 37(2):164–194, 2005.

[99] Volkan Rodoplu and Teresa H Meng. Minimum energy mobile wireless networks. *Selected Areas in Communications, IEEE Journal on*, 17(8):1333–1344, 1999.

[100] Ram Ramanathan and Regina Rosales-Hain. Topology control of multihop wireless networks using transmit power adjustment. In *IEEE 19th Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 2, pages 404–413. IEEE, 2000.

[101] Lefteris M Kirousis, Evangelos Kranakis, Danny Krizanc, and Andrzej Pelc. Power consumption in packet radio networks. In *STACS 97*, pages 363–374. Springer, 1997.

[102] Abhik Banerjee, Rachit Agarwal, Vincent Gauthier, Chai Kiat Yeo, Hossam Afifi, and Francis Bu-Sung Lee. A self-organization framework for wireless ad hoc networks as small worlds. *Vehicular Technology, IEEE Transactions on*, 61(6):2659–2673, 2012.

[103] Ahmed Helmy. Small worlds in wireless networks. *Communications Letters, IEEE*, 7(10):490–492, 2003.

[104] Nabil Afifi and Kah-Seng Chung. Small world wireless mesh networks. In *Innovations in Information Technology, 2008. IIT 2008. International Conference on*, pages 500–504. IEEE, 2008.

[105] Lichun Bao and Jose Joaquin Garcia-Luna-Aceves. Channel access scheduling in ad hoc networks with unidirectional links. In *Proceedings of the 5th international workshop on Discrete algorithms and methods for mobile computing and communications*, pages 9–18. ACM, 2001.

[106] Dongkyun Kim, Chai-Keong Toh, and Yanghee Choi. On supporting link asymmetry in mobile ad hoc networks. In *Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE*, volume 5, pages 2798–2803. IEEE, 2001.

[107] Marc R Pearlman, Zygmunt J Haas, and Benjamin P Manvel. Using multi-hop acknowledgements to discover and reliably communicate over unidirectional links in ad hoc networks. In *Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE*, volume 2, pages 532–537. IEEE, 2000.

[108] Venugopalan Ramasubramanian, Ranveer Chandra, and Daniel Mosse. Providing a bidirectional abstraction for unidirectional ad hoc networks. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1258–1267. IEEE, 2002.

[109] 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). *Telecommunication Systems*, 52(2):705–736, 2013.

[110] Abdul Jabbar, Hemanth Narra, and James P. G. Sterbenz. An approach to quantifying resilience in mobile ad hoc networks. In *Proceedings of the 8th IEEE International Workshop on the Design of Reliable Communication Networks (DRCN)*, pages 140–147, Krakow, Poland, October 2011.

[111] Hyoungshick Kim, John Tang, Ross Anderson, and Cecilia Mascolo. Centrality prediction in dynamic human contact networks. *Computer Networks*, 56(3):983–996, 2012.

[112] Hongmei Deng, W. Li, and D.P. Agrawal. Routing security in wireless ad hoc networks. *Communications Magazine, IEEE*, 40(10):70–75, Oct 2002.

[113] Romit RoyChoudhuri, Somprakash Bandyopadhyay, and Krishna Paul. Topology discovery in ad hoc wireless networks using mobile agents. In *Mobile Agents for Telecommunication Applications*, pages 1–15. Springer, 2000.

[114] Theus Hossmann. Mobility prediction in manets. 2006.

[115] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack Vulnerability of Complex Networks. *Phys. Rev. E*, 65:056109, May 2002.

[116] Ram Ramanathan. On the performance of ad hoc networks with beamforming antennas. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 95–105. ACM, 2001.

[117] Su Yi, Yong Pei, and Shivkumar Kalyanaraman. On the capacity improvement of ad hoc wireless networks using directional antennas. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 108–116. ACM, 2003.

[118] Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 114–128. ACM, 2004.

[119] Mahesh K Marina, Samir R Das, and Anand Prabhu Subramanian. A topology control approach for utilizing multiple channels in multi-radio wireless mesh networks. *Computer networks*, 54(2):241–256, 2010.

[120] Julien Cartigny, David Simplot, and Ivan Stojmenovic. Localized minimum-energy broadcasting in ad-hoc networks. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pages 2210–2217. IEEE, 2003.

[121] P-J Wan, G Călinescu, X-Y Li, and Ophir Frieder. Minimum-energy broadcasting in static ad hoc wireless networks. *Wireless Networks*, 8(6):607–617, 2002.

[122] Robert J Marks, Arindam K Das, Mohamed El-Sharkawi, Payman Arabshahi, Andrew Gray, et al. Minimum power broadcast trees for wireless networks: optimizing using the viability lemma. In *Circuits and Systems, 2002. ISCAS 2002. IEEE International Symposium on*, volume 1, pages I–273. IEEE, 2002.

[123] Stephanie Lindsey and Cauligi S Raghavendra. Energy efficient broadcasting for situation awareness in ad hoc networks. In *Parallel Processing, 2001. International Conference on*, pages 149–155. IEEE, 2001.

[124] Suman Banerjee and Archan Misra. Minimum energy paths for reliable communication in multi-hop wireless networks. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, pages 146–156. ACM, 2002.

[125] Omer Egecioglu and T Gonzalez. Minimum-energy broadcast in simple graphs with limited node power. In *Proceedings of IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS 2001)*, volume 338. Anaheim, CA, 2001.

[126] Jeffrey E Wieselthier, Gam D Nguyen, and Anthony Ephremides. On the construction of energy-efficient broadcast and multicast trees in wireless networks. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 585–594. IEEE, 2000.

[127] Errol L Lloyd, Rui Liu, Madhav V Marathe, Ram Ramanathan, and SS Ravi. Algorithmic aspects of topology control problems for ad hoc networks. *Mobile Networks and applications*, 10(1-2):19–34, 2005.

[128] François Ingelrest, David Simplot-Ryl, and Ivan Stojmenović. Energy-efficient broadcasting in wireless mobile ad hoc networks. In *Resource Management in Wireless Networking*, pages 543–582. Springer, 2005.

[129] Laura Marie Feeney. An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks. *Mobile Networks and Applications*, 6(3):239–249, 2001.

[130] Joseph B Kruskal. On the shortest spanning subtree of a graph and the traveling salesman problem. *Proceedings of the American Mathematical society*, 7(1):48–50, 1956.

[131] Thomas H Cormen. *Introduction to algorithms*. MIT press, 2009.

[132] Robert Clay Prim. Shortest connection networks and some generalizations. *Bell system technical journal*, 36(6):1389–1401, 1957.

[133] Mohammed J.F. Alenazi, Egemen K. Çetinkaya, and James P. G. Sterbenz. Cost-Efficient network improvement to achieve maximum path diversity. In *RNDM'14 - 6th International Workshop on Reliable Networks Design and Modeling (RNDM 2014)*, pages 202 – 208, Barcelona, Spain, November 2014.

[134] Christian Bettstetter. On the minimum node degree and connectivity of a wireless multihop network. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 80–91, New York, NY, USA, 2002. ACM.

[135] The ns-3 Network Simulator. `http://www.nsnam.org`, July 2009.

[136] B. Liang and Z.J. Haas. Predictive distance-based mobility management for PCS networks. In *The Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, volume 3, pages 1377–1384, March 1999.

[137] Dan Broyles, Abdul Jabbar, and James P. G. Sterbenz. Design and analysis of a 3–D gauss-markov mobility model for highly-dynamic airborne networks. In *Proceedings of the International Telemetering Conference (ITC)*, San Diego, CA, October 2010.

[138] Injong Rhee, Minsu Shin, Seongik Hong, Kyunghan Lee, Seongjoon Kim, and Song Chong. CRAWDAD data set ncsu/mobilitymodels (v. 2009-07-23). Downloaded from http://crawdad.org/ncsu/mobilitymodels/, July 2009.

[139] Injong Rhee, Minsu Shin, Seongik Hong, Kyunghan Lee, Seong Joon Kim, and Song Chong. On the levy-walk nature of human mobility. *IEEE/ACM Transactions on Networking (TON)*, 19(3):630–643, 2011.

[140] Dongsheng Zhang and James P. G. Sterbenz. Robustness analysis of mobile ad hoc networks using human mobility traces. In *Proceedings of the 11th International Conference on Design of Reliable Communication Networks (DRCN)*, Kansas City, USA, March 2015.

[141] Charles E. Perkins and Pravin Bhagwat. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In *ACM SIGCOMM*, pages 234–244, London, 1994.

[142] Hemanth Narra, Yufei Cheng, Egemen K. Çetinkaya, Justin P. Rohrer, and James P.G. Sterbenz. Destination-sequenced distance vector (DSDV) routing protocol implementation in ns-3. In *Proceedings of the ICST SIMUTools Workshop on ns-3 (WNS3)*, pages 439–446, Barcelona, Spain, March 2011.

[143] David B. Johnson, David A. Maltz, and Josh Broch. DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. In Charles E. Perkins, editor, *Ad Hoc Networking*, chapter 5, pages 139–172. Addison-Wesley, Boston, MA, 2001.

[144] Yufei Cheng, Egemen K. Çetinkaya, and James P.G. Sterbenz. Dynamic source routing (DSR) protocol implementation in ns-3. In *Proceedings of the ICST SIMUTools Workshop on ns-3 (WNS3)*, pages 367–374, Sirmione, March 2012.

[145] C.E. Perkins and E.M. Royer. Ad-hoc On-demand Distance Vector Routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pages 90–100, February 1999.

[146] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626 (Experimental), October 2003.

[147] Vincenzo Nicosia, John Tang, Cecilia Mascolo, Mirco Musolesi, Giovanni Russo, and Vito Latora. Graph metrics for temporal networks. In *Temporal Networks*, pages 15–40. Springer, 2013.

[148] Theus Hossmann, Thrasyvoulos Spyropoulos, and Franck Legendre. Know thy neighbor: Towards optimal mapping of contacts to social graphs for dtn routing. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9. IEEE, 2010.

Appendix A

Plots for Additional Scenarios

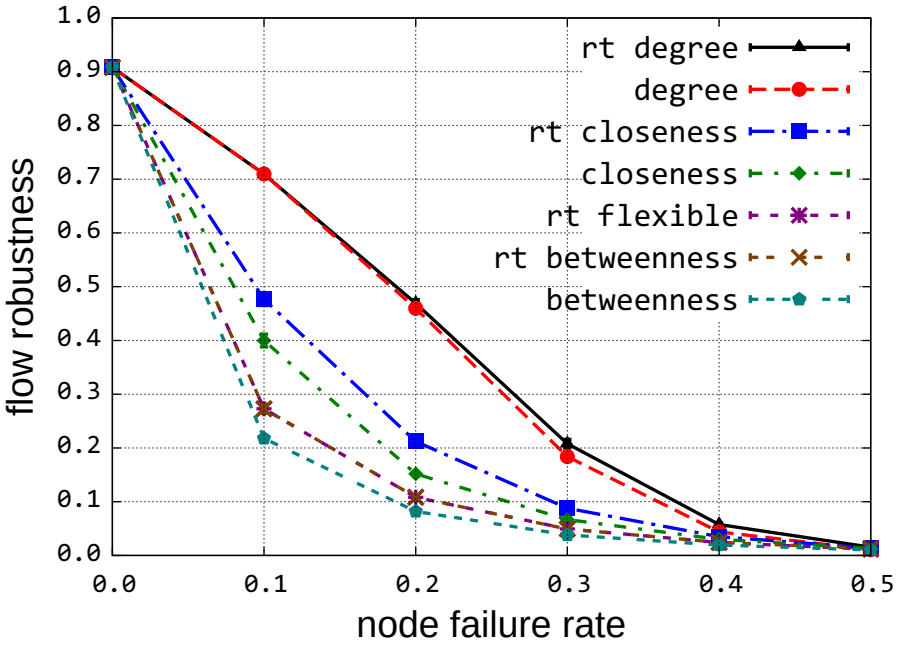


Figure A.1: 100 nodes MANETs under real-time simultaneous node attacks

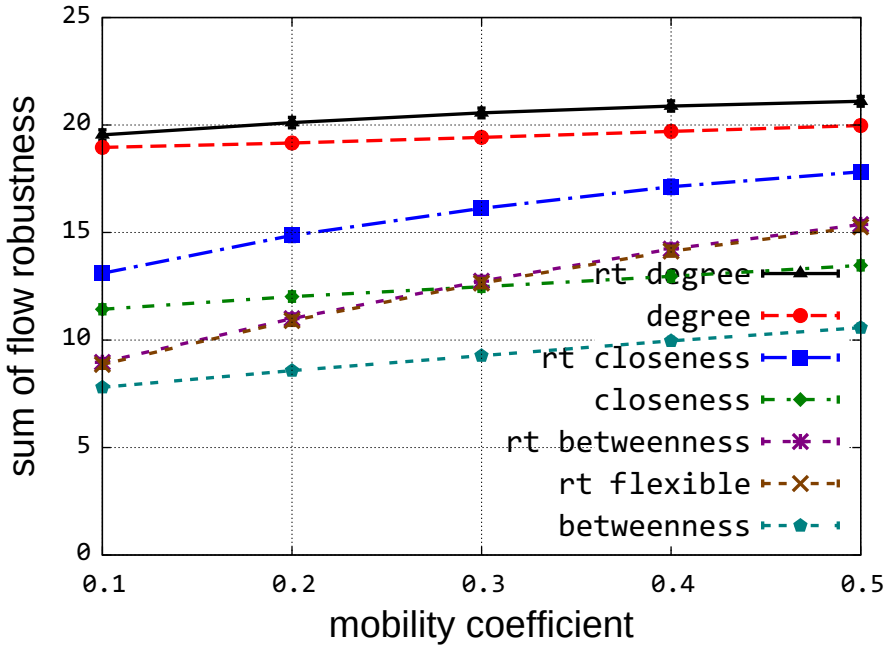


Figure A.2: 100 nodes MANETs under real-time simultaneous node attacks

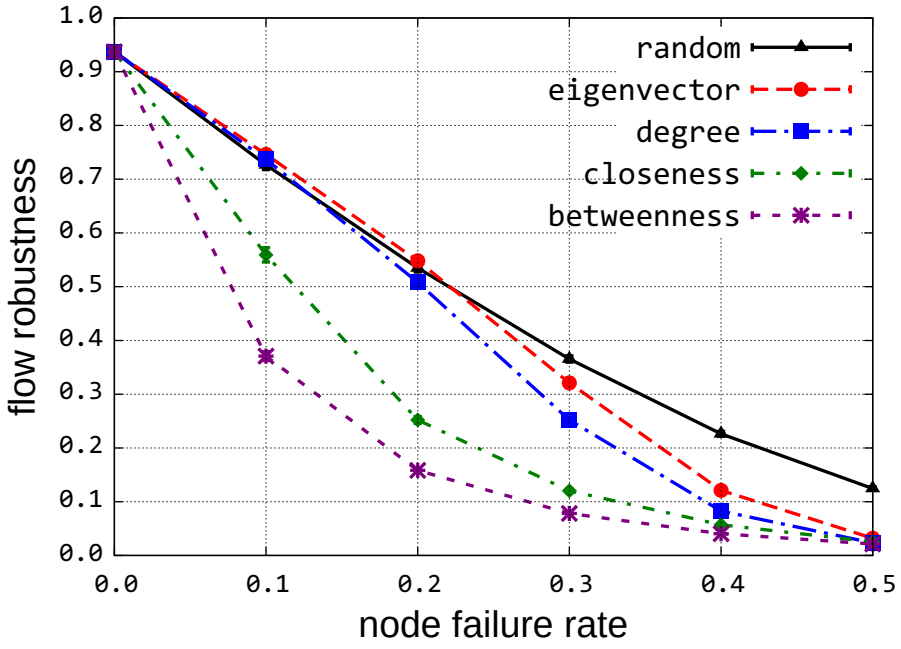


Figure A.3: 50 nodes MANETs under simultaneous node attacks

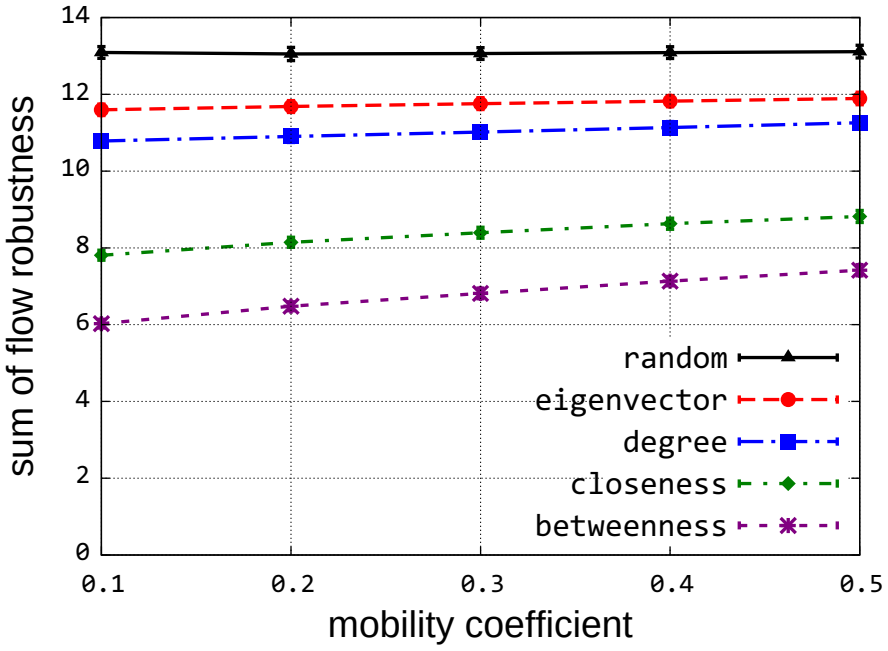


Figure A.4: Sum of flow robustness in 50 nodes MANETs

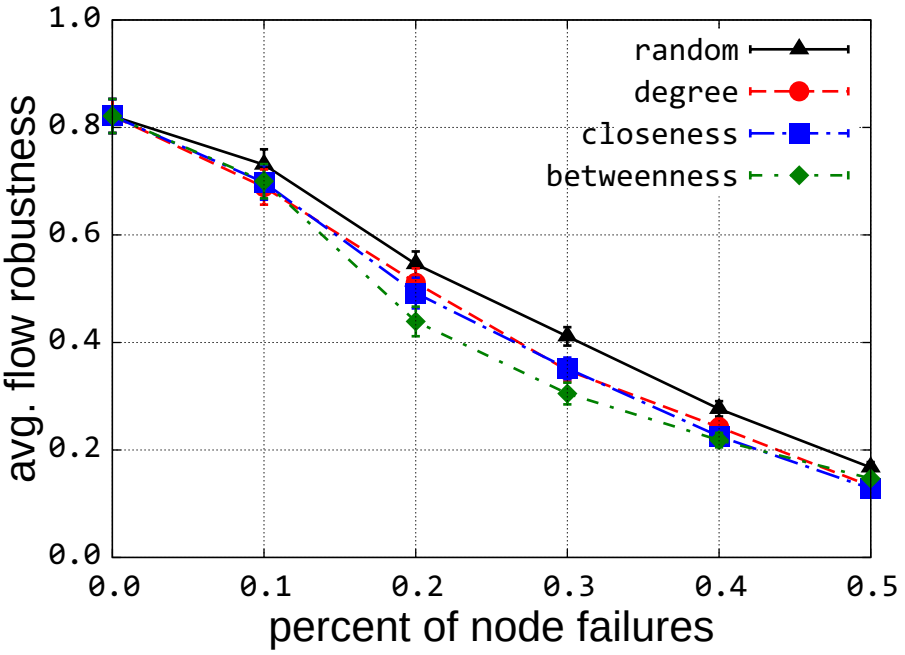


Figure A.5: Centrality-based attacks in StateFair with window size of 900 s

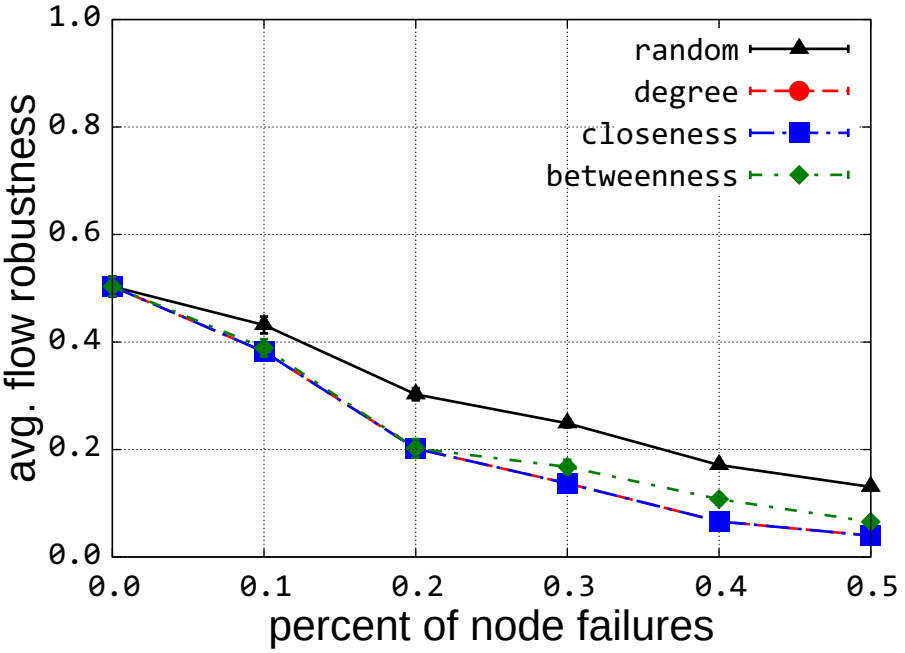


Figure A.6: Centrality-based attacks in NCSU with window size of 900 s

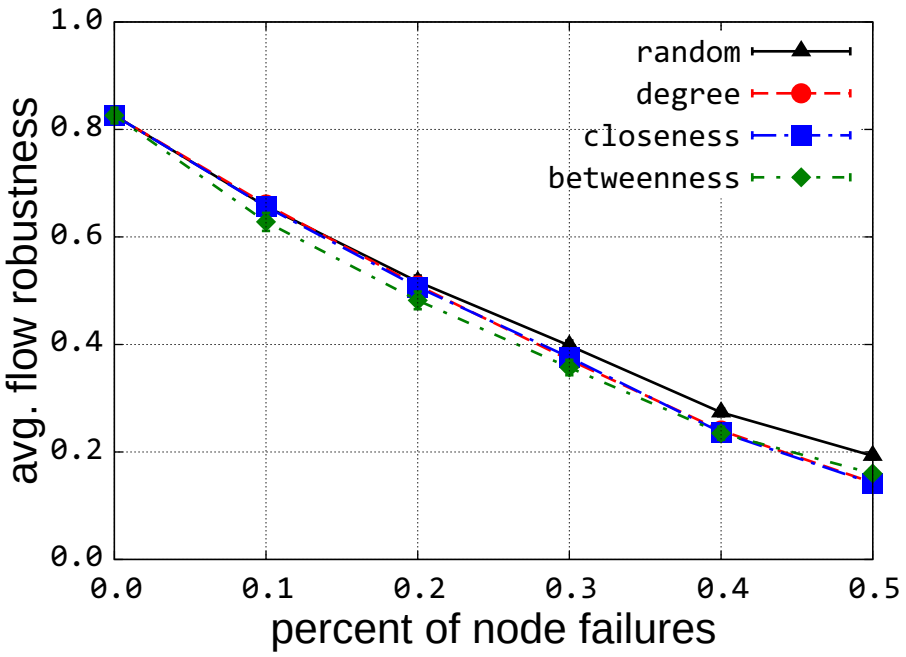


Figure A.7: Centrality-based attacks in KAIST with window size of 900 s

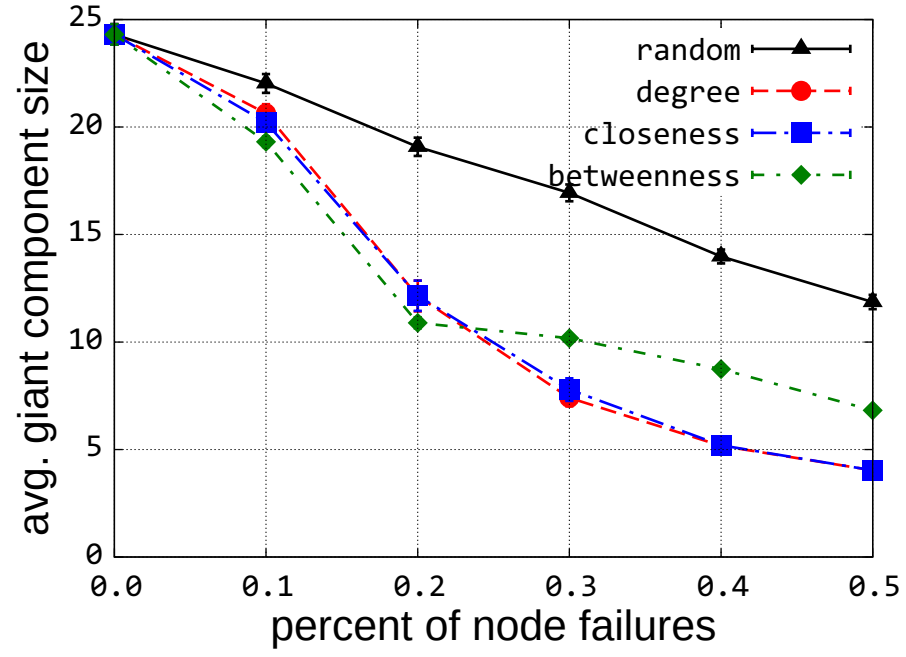


Figure A.8: Giant component size under centrality-based attacks in NCSU

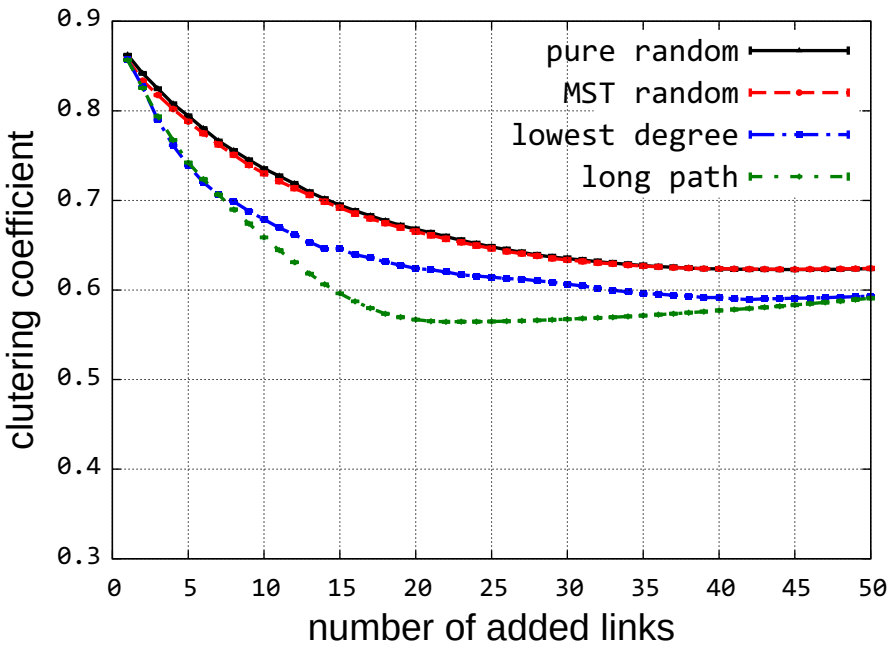


Figure A.9: Clustering coefficient of NCSU with an increased number of added links