This paper was presented at RNDM 2014 - 6^{th} International Workshop on Reliable Networks Design and Modeling (Nov. 17-19, 2014, Barcelona, Spain)

Analysis of Critical Node Attacks in Mobile Ad Hoc Networks

Dongsheng Zhang* and James P.G. Sterbenz*†
*Information and Telecommunication Technology Center
Department of Electrical Engineering and Computer Science
The University of Kansas, Lawrence, KS, 66045, USA
{dzhang, jpgs}@ittc.ku.edu
†School of Computing and Communications (SCC) and InfoLab21
Lancaster LA1 4WA, UK
jpgs@comp.lancs.ac.uk
www.ittc.ku.edu/resilinets

***Abstract*—Understanding network behavior under 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 MANETs (mobile ad hoc networks) under various challenges. Previously, we have modeled network attacks based on a priori complete knowledge of network structure and mobility. In this paper, we present the analysis of MANET behavior under random node failures and centrality-based attacks based on real-time topological information, and provide a comparison of network performance under complete information and real-time attacks. In addition, we adapt betweenness and closeness centrality to measure node significance in asymmetric source/sink network scenarios. The ns-3 simulator is used to examine network throughput under various intelligent attacks. By analyzing network topological properties, we provide a theoretical verification of the simulation results.**

***Index Terms*—mobile wireless topology challenge modeling, MANET, time-varying weighted graph, resilient survivable disruption-tolerant network, ns-3 simulation**

I. Introduction

MANETs (mobile ad hoc networks) have been widely utilized in many real-world scenarios, such as VANETs (vehicular ad hoc networks), WSNs (wireless sensor networks), and PANs (personal area networks) [1]. With the emergence of driverless cars, using ad hoc networking for communications between auto-piloted vehicles could be an emerging application. 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. However, due to the properties of wireless channels, the potential attacks and challenges are also tremendously high [2]. 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.

Previously, we built a model to simulate malicious attacks against MANETs with complete knowledge of the entire network topology [3]–[5]. Malicious attackers can camouflage as normal nodes within MANETs and obtain complete network topology information by exploiting routing messages [6], [7]. In addition, topology inference algorithms have been proposed for wireless sensor networks [8]. Physical or DDoS attacks can be conducted against nodes of highest importance [6]. Dynamic topologies within certain time windows are aggregated into a weighted graph, so that centrality metrics can be calculated based on the aggregated graph to identify the most significant nodes in the network. However, in most real-world scenarios, it is difficult for the attackers to accurately predict the network topology in the future. In this paper, we model network attacks based on the real-time topological information.

In our previous work, all the nodes within MANETs have been considered as both traffic sources and sinks [3]–[5]. However, in many real-world applications, MANETs are established such that only some nodes in the network function as the receivers of information. For example, two companies (Open Garden [9] and TextMe [10]) 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. Such a scenario differs from traditional MANETs in which each device is symmetric to every other device in terms of the role of data sending and receiving. In certain WSN scenarios, not all nodes in the network perform the function of data collection. Hence, in addition to the traditional MANET scenarios, it is also important to understand the impact of attacks against asymmetric source/sink networks, in which some nodes may be more critical than others due to their special role in providing connectivity to other nodes.

Traditional centrality metrics have been used to measure relative node significance in various network scenarios in which network activities could occur among all node pairs [11], [12]. When calculating closeness and betweenness centrality, asymmetric sink/source networks require a different approach of considering node pairs, since the traffic flow is exchanged only between specific sink and source nodes. By understanding how nodes of varying significance impact the network performance, we can design networks with enhanced resilience and survivability. In this paper, our major contributions are as follows:

978-1-4799-7040-7

1) proposing adjusted betweenness and closeness
2) simulating real-time centrality-based attacks
3) modeling asymmetric application scenarios
4) verifying simulation results with theoretical values

The rest of the paper is arranged as follows. In Section II, we introduce background about dynamic network modeling and graph centrality. In Section III, we introduce the approach to model the malicious attacks in MANETs. In Section IV, we use the ns-3 simulator to simulate complete information and real-time attacks based on centrality metrics. Cross-comparison analysis between topological structures and application performance is provided in Section V. Finally, we summarize our work and discuss future steps in Section VI.

II. Background and Related Work

Fundamental mathematical properties of MANETs have been studied with networks being modeled using the log-normal shadowing radio model [13], [14]. The graph connectivity of wireless multihop networks has been investigated, and a mathematical derivation between node density and desired k-connectedness has been shown [15]. A simulation framework that models simple jamming effect in wireless mesh networks has been developed [16]. The impact of the number of placement sources and node density on the performance of WSNs using data-centric routing has been examined [17]. The aggregation of consecutive network topologies into an unweighted static graph fails to capture the time information of the entire network. The overestimation of the number of links in the aggregated graph results in an inaccurate estimation of many graph properties [5].

In social networks or delay-tolerant networks, temporal centrality metrics have been proposed to overcome the shortage of static aggregation by taking into account time-varying information [18]. Temporal network robustness has been adopted to evaluate network performance in the face of random node failures and it does provide better estimation of the resilience of real-world temporal networks [19]. However, this approach is not appropriate for non-delay-tolerant MANETs because real-time routing protocols must be used if we want packets to be delivered without store-and-forward delay. Therefore, we have proposed another approach to model the dynamics of MANETs by aggregating time-varying topologies into a weighted graph, in which the weights represent link availability during a specific time window [3], [4].

Centrality metrics have been used as structural attributes in social networks [11]. Generalized centrality metrics have also been proposed, in which a tuning factor is introduced to control the tendency toward link weights or the number of links (the length of weighted paths) [12]. Traditionally, individual betweenness and closeness centrality of each node in a network are calculated based on all pairs of nodes. However, for networks with asymmetric source/sink pairs, betweenness and closeness metrics need to be adjusted so that they can reflect the actual application traffic flow model. Centrality metrics can in some way indicate relative node significance in the network; however, it has been shown in social networks that they are not optimal in terms of how the removal of high centrality nodes impact overall network connectivity [20]. An approximation algorithm has been proposed to assess the vulnerability by investigating how many nodes/links need to be torn down such that the pairwise connectivity can be degraded to a certain low level [21]. A general mathematical formulation of this problem is how to select a subset of nodes in a graph so that after the removal of selected nodes, the connectivity of the rest of the graph is minimized, which is known as NP-hard [22]. Heuristics and algorithms have been to proposed to solve this problem by putting certain constraints on the types of graph structure [22]–[24]. However, these solutions cannot be applied to general weighted graphs. As there are no efficient algorithms to compute optimally-critical nodes in a general graph, we use centrality metrics to measure relative node significance in this work.

III. Modeling Approach

We model network attacks for two types of scenarios: attacks based on real-time topology information and complete-chronological topology information. We previously assumed that we have complete information of network topologies during the entire simulation time [3], [4]. In order to identify the most significant nodes, the dynamic topologies within a certain time window are aggregated into a static weighted graph, and weighted centrality metrics are calculated based on the aggregated graph. For real-time attacks, due to correlation of network topologies within a short time period, we identify node significance based on centrality metrics calculated using the topology of current time instance.

The significance of each node is judged by how the entire network is impacted if that node fails. It has been shown that the higher the average node velocity, the faster network topologies change as expected [5]. This might result in rapid replacement of the most significant nodes. Centrality metrics can be calculated based on each snapshot of dynamic topologies, which could cause an overwhelmingly high computation complexity hinging on the time step used for sampling. The aggregation approach is a balance between accuracy of identification of critical nodes and computational efficiency [5]. With a higher number of nodes in the network, MANET routing protocols need more time to update their routing tables globally. The aggregation window size cannot be arbitrarily small, since the failures or attacks against certain nodes in the network rarely occur from the perspectives of cost and practicality. Dynamic topologies that change at a high rate are relatively resilient in that high velocity obscures the relative criticality of each individual node; each node plays an approximately equivalent role in the network over time. The failure of any node during a certain period would result in the same impact on the network.

A. Modeling dynamic networks

We introduced an approach to model the dynamics of MANETs in our previous work [3]–[5]. The network topology of each time step can be represented as a binary adjacency

matrix in which a link is either up or down between any node pair. The purpose of aggregation is to detect the most critical nodes within a certain time window. However, depending on the duration of the time step, the computation of centrality metrics for each time step could be extremely expensive and redundant. The size of the aggregated time window hinges on how fast the topology changes. We consider the network topology *changed* if the state of link existence between any node pair changes. The selection of an appropriate window size is the tradeoff between computation overhead and the precision of measuring node significance as shown in our previous work [3]. To achieve similar precision for different network scenarios, the faster the entire network topologies change, the smaller the aggregation window size needs to be.

In order to model real-time attacks, we assume attackers only have the network topology information prior to the current time instance. We use current network topology to approximately predict significant nodes depending on the duration of time after current time instance. Without perfect topology information of the entire simulation, the identification of significant nodes are less precise. Simulation results in Section IV will show that network attacks based on current topology have slightly lower impact on the network than based on complete information of the next time window if the window size is selected properly.

B. Identifying critical nodes

Centrality metrics have been used to identify significant nodes in the network [25]. Degree centrality presents local properties of network in that it is calculated completely based on the relation between the node and its neighbors. In contrast, betweenness and closeness centrality [25] of each individual node are calculated based on the global topology information. Eigenvector centrality is computed as the largest eigenvalue of an adjacency matrix that represents the topology [26]. Centrality metrics for weighted graph have been proposed, which take into account both the number of links and link weights [12]. The weighted version of closeness centrality metric for node n_k is defined as:

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

where $d^{w\alpha}\left(n_i, n_k\right)$ is the weighted version of the shortest paths between two nodes and α is the tuning parameter to favor link weight or the number of intermediate nodes. The weighted betweenness for node n_k is defined as:

$$C_{\mathrm{B}}^{w\alpha}\left(n_k\right) = \sum_{i}\sum_{j} \frac{g_{ij}^{w\alpha}\left(n_k\right)}{g_{ij}^{w\alpha}} \tag{2}$$

where $i < j$ and $i \neq j \neq k$, $g_{ij}^{w\alpha}$ is the total number of paths between node i and j, and $g_{ij}^{w\alpha}\left(n_k\right)$ is the number of shortest paths that pass via n_k [12].

The above mentioned centrality metrics can be applied to MANET scenarios in which each node functions as transceiver; whereas, for some network scenarios such as PANs, WSNs, and hybrid ad hoc networks, only a subset of nodes in the network are traffic sinks. Hence, we propose the corresponding betweenness and closeness for asymmetric network scenarios based on the algorithms used for the computation of betweenness and closeness in NetworkX [27]. We modify them based on the actual source/sink traffic flow pairs. The adjusted closeness of a node n_k can be formulated as:

$$C_{\mathrm{C}}^{w\alpha}\left(n_k^a\right) = \left[\sum_{i\in T} d^{w\alpha}\left(n_i, n_k\right)\right]^{-1} \tag{3}$$

and the adjusted betweenness for node n_k can be formulated as:

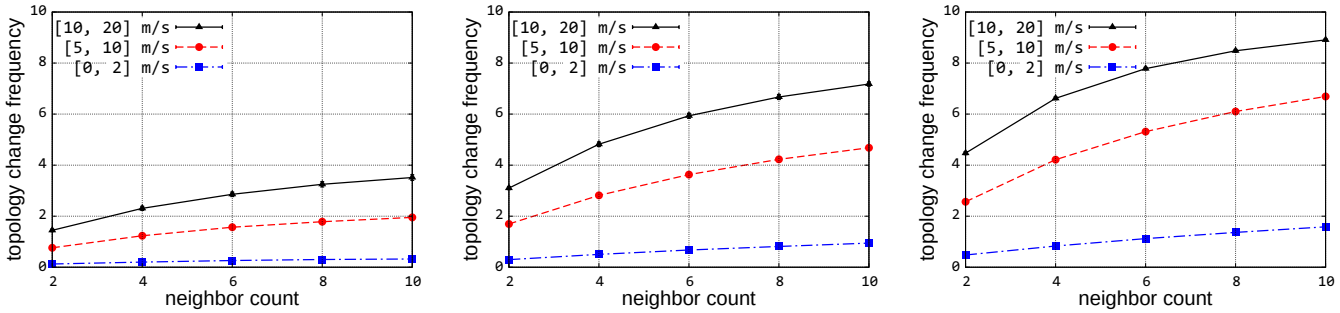
$$C_{\mathrm{B}}^{w\alpha}\left(n_k^a\right) = \sum_{i\in T}\sum_{j\in S} \frac{g_{ij}^{w\alpha}\left(n_k\right)}{g_{ij}^{w\alpha}} \tag{4}$$

where T is the subset of nodes that function as the traffic sinks, S is the subset of nodes that function as the traffic sources, and $g_{ij}^{w\alpha}\left(n_k\right)$ is the number of shortest paths between source and sink nodes that pass via n_k. We calculate centrality metrics adaptively after the removal of the previous highest centrality node, since node centrality would change whenever some nodes are removed from the network. It has been shown that attacks based on recalculated centrality could degrade network more than based on initial centrally metrics [28].

IV. Simulation

In this section, we use the network simulator ns-3.17 [29] to model and analyze dynamic network attacks. We have studied the impact of window sizes and MANET routing protocols in our previous work [4]. We have shown that a smaller window size results in a more precise indication of node significance based on centrality metrics. The relative impact of different types of attacks on the network performance is similar in both a reactive routing protocol ADOV [30] and a proactive routing protocol DSDV [31]. We use AODV as the routing protocol in the paper as it provides higher baseline network throughput without node failures [4]. It has also been shown that Gauss-Markov and Random Waypoint mobility model present similar characteristics [32], and we select Gauss-Markov mobility model for this paper as it provides more realistic node movements in many scenarios [33]. All simulation results are averaged over 10 runs with 95% confidence interval shown in the plots.

In order to maintain a desired level of communication quality, the network density cannot be too low, while a high node density would cause interference and high use of network resources. Different density levels of the dynamic networks can be selected by changing the neighbor count parameter. This is equivalent to varying node transmission range while fixing the number of nodes in the network and simulation area. Nodes send CBR (constant bit rate) traffic to other nodes. Each node is assumed to have a unique transmission power with a fixed transmission range is 100 m. Two nodes are considered adjacent if the distance between them is less than transmission range (without interference). We assume



(a) 10 nodes (b) 20 nodes (c) 30 nodes

Fig. 1. Average times of topology change per second

there is no obstruction in the simulation area. The rest of the parameters for this paper is shown in Table I.

TABLE I
SIMULATION PARAMETERS

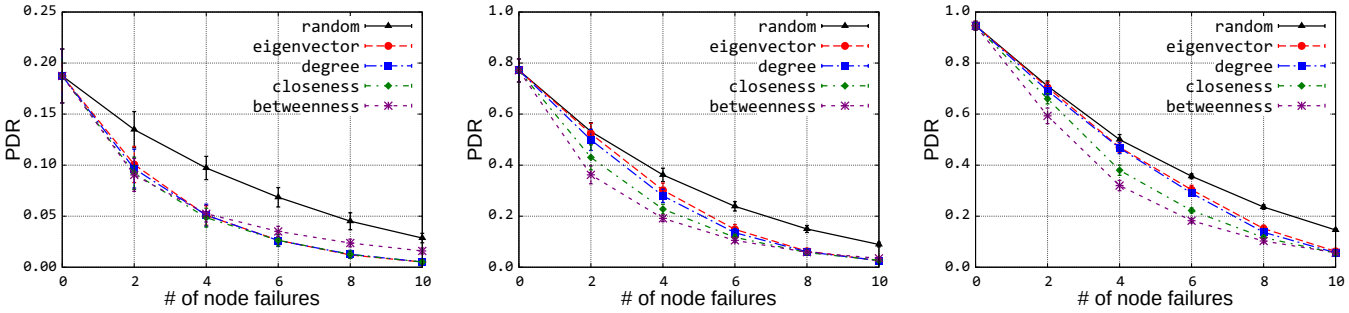
number of iterations	10
traffic generation time	1000 s
transmission range	100 m
mobility model	Gauss-Markov
number of nodes	20
neighbor count	2, 4, 6, 8, 10
physical channel	802.11g (54 Mb/s)
routing protocol	AODV
node velocity	[0, 2], [5, 10], [10, 20] m/s
traffic model	CBR (constant bit rate)
sink-source type	symmetric, asymmetric
attack scenarios	complete information, real-time

We use PDR (packet delivery ratio) to measure network performance. Other performance measure such as energy constraint and delay are also important, but in this work we focus on the evaluation of network resilience under challenges from a topological perspective. With uniform transmission range, the energy cost to send packets for each node would be the same. High centrality nodes could cost more energy as more data traffic is forwarded via them. Figure 1 describes the number of times that dynamic topologies change per second for a set of parameters. For 10, 20, and 30-node networks, the topology change frequency increases with greater node velocities as expected. With increased neighbor count, topology changing frequency also increases due to the fact that nodes with random mobility associate/dissociate with others more frequently in a denser network. With the same velocity and neighbor count, the network with a higher number of nodes has more links, resulting in a higher probability of topology change. The window size is determined according to the topology change frequency of the network. We have used the uniform distribution between [0, 2], [5, 10], and [10, 20] m/s to simulate the speed of pedestrian, bicycle, and automobile [5]. For the following simulation, we use the average velocity of pedestrians, with 3 different node density levels (2, 6, 10 neighbor count). The window size for each neighbor count is calculated as the average time for network topology changing 10 times based on the results in Figure 1. Hence, for the 20-node network scenario, 31, 14, and 10 s are set as the window sizes for 2, 6, and 10 neighbor count respectively. The steps of modeling real-time centrality-based attacks is as follows:

1) selecting a proper window size to apply attacks according to average node velocity
2) calculating node centrality based on network topology at current time instance
3) attacking nodes of high centrality values for the next time window iteratively
4) measuring network PDR under malicious attacks

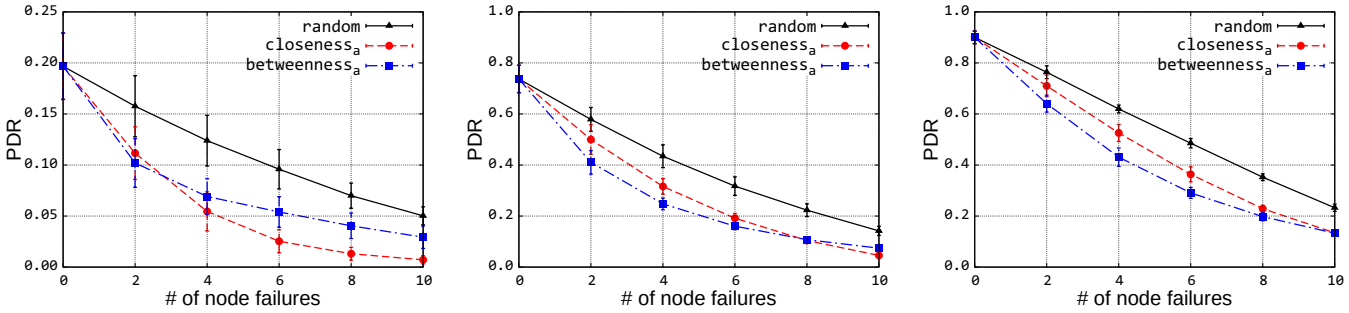
For asymmetric scenarios, we use the adjusted closeness and betweenness to measure node significance. The failure of a sink node in an asymmetric scenario could degrade network performance more than a non-sink node, because all the traffic directed to the sink node will be dropped if a sink nodes fails and less traffic flows would be affected if a non-sink node fails. Hence, we only rank the centrality values of non-sink nodes to have a fair comparison. Simulation results of symmetric source/sink network scenarios with complete chronological topology information under centrality-based attacks have been presented in our previous works [3], [4]. In this paper, we concentrate on real-time network attack scenarios.

Two factors could result in network partition: i) high number of node failures, ii) nodes sparsely-distributed in the network (small neighbor count). Figure 2 presents PDRs under real-time centrality-based attacks of symmetric source/sink scenarios. For the network with 2-neighbor count, the PDR without attacks is less than 20%. PDRs under different centrality-based attacks are close to each other except that betweenness-based attacks have less impact on the network than other centrality-based attacks with a high number of node failures as shown in Figure 2a. This is because there are almost no intermediate nodes between node pairs due to the small order of each connected component. In a well-connected network with 6- or 10-neighbor count, betweenness-based attacks degrade PDR the most of all centrality metrics. With 10 nodes



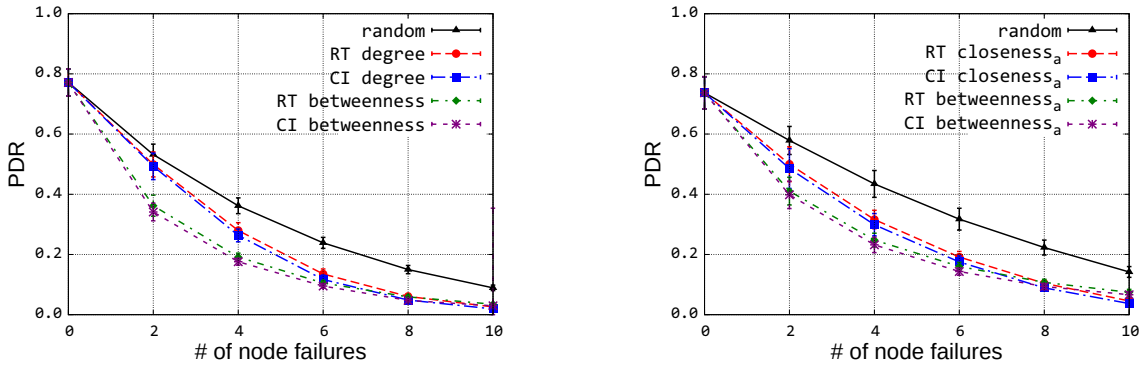
(a) 2 neighbor count (b) 6 neighbor count (c) 10 neighbor count

Fig. 2. Symmetric network with real-time information



(a) 2 neighbor count (b) 6 neighbor count (c) 10 neighbor count

Fig. 3. Asymmetric network with real-time information

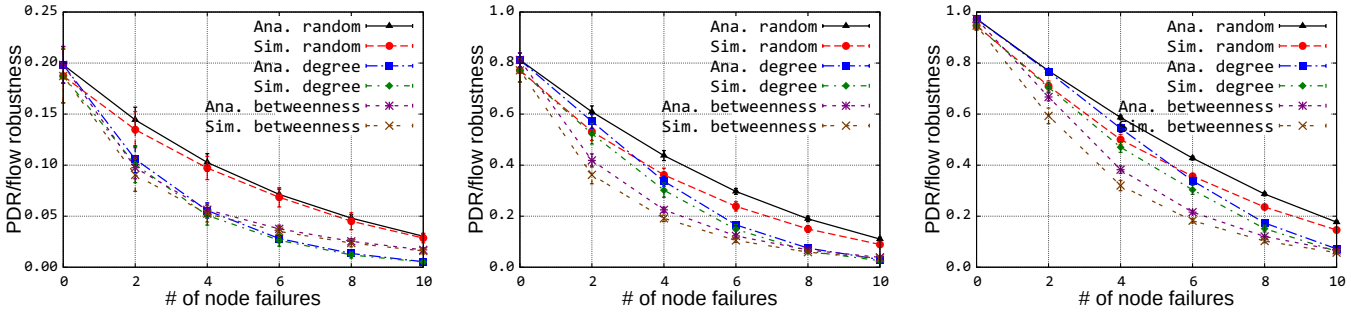


(a) 6 neighbor count, symmetric (b) 6 neighbor count, asymmetric

Fig. 4. Real-time vs. complete information

being attacked, network becomes so disconnected that there is almost no difference among network performance under different attacks. Generally, the relationship of the impact of different attack types on the PDR is: random $<$ eigenvector $<$ degree $<$ closeness $<$ betweenness, as shown in Figures 2b and 2c. Betweenness and closeness indicate node significance better in that they can identify the key mediators of traffic flows across the entire network. Figure 3 presents PDRs of asymmetric source/sink scenarios under real-time centrality-based attacks with 4 nodes being traffic sinks and the rest being traffic sources. Both asymmetric closeness- and betweenness-based attacks degrade PDRs more than random node failures. Similar to the symmetric scenarios, adjusted betweenness-based attacks have less impact on the network than asymmetric closeness when the network is poorly connected. With decent network connectivity, PDRs under adjusted betweenness-based attacks stay the lowest of all.

Figure 4 presents the comparison of PDRs between real-time (RT) attacks and complete information (CI) attacks. For real-time attacks, the priority of nodes to be attacked is determined according to the centrality metrics of the initial



(a) 2 neighbor count (b) 6 neighbor count (c) 10 neighbor count

Fig. 5. Simulation PDR vs. analytical flow robustness for symmetric source/sink scenarios

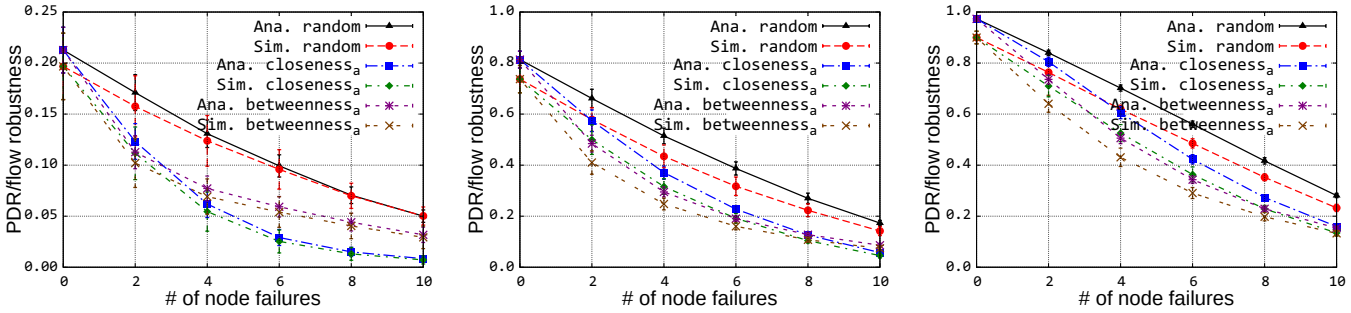
topology of each time window, and for attacks with complete information, the attack priority is based on the aggregated weighted graph of the entire time window. We select degree and betweenness centrality metrics for the cross comparison of symmetric scenarios to display each curve clearly in one plot. As shown in Figure 4a, PDRs under complete information centrality-based attacks are slightly lower than real-time attacks 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 the same for asymmetric scenarios using adjusted closeness and betweenness, and networks under attacks based on complete information asymmetric betweenness have lowest PDRs of all as shown in Figure 4b.

V. Analytical Verification and Discussion

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. In this section, we examine the network topological properties that provide the underlying theoretically highest network performance under attacks. The mobility traces generated from simulations are parsed to obtain dynamic topologies in each time step. *Flow robustness* is used to measure topological connectivity of each snapshot of topology, which is computed as the number of reliable flows divided by total number of flows in the network [34]. Flows are considered reliable if there exists at least one path between source/sink pairs. For asymmetric scenarios, only flows that are directed to sink nodes are counted. We present the comparison between simulation PDRs and analytical flow robustness for real-time symmetric and asymmetric scenarios.

In order to display each curve in the plots clearly, we only select random, degree, and betweenness centrality out of five metrics for symmetric scenarios. As shown in Figure 5, for all different neighbor counts, 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. For networks with high density, the difference between application PDRs and topological flow robustness increases as shown in Figure 6b and 6c. This is because in a relatively dense network, the probability of wireless interference and network collision is higher than in a relatively sparse network, which results in a higher degradation of network performance. Figure 6 presents the relationship between PDR and flow robustness for asymmetric scenarios. For a given network under the same type of attacks, analytical flow robustness remains higher than PDR.

We present the comparison between real-time and complete information centrality-based attacks with average velocity in [0, 2] m/s and the window size being the average time for topology varying 10 times. We do not provide the simulation results for the networks with higher average velocities. On the one hand, dynamic networks with extremely high velocity are resilient enough since relative node significance is obscured by the fast changing topology; on the other hand, the relative impact of different centrality-based attacks on the PDR would be the same for network scenarios with slightly higher average velocity if appropriate window sizes are used. It is apparent that centrality metrics based on either aggregated graph or instant topology become less precise if we increase the window size. The difference of PDRs under real-time and complete information attacks is slight, 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. Even though nodes are moving constantly within the certain simulation area, the global structure of the entire network remains relatively stable in that nodes with the highest centrality do not vary much within each time window. 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 attacks should be almost equal to flow robustness. In theory, flow robustness provides the best network performance under certain types



(a) 2 neighbor count (b) 6 neighbor count (c) 10 neighbor count

Fig. 6. Simulation PDR vs. analytical flow robustness for asymmetric source/sink scenarios

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.

For asymmetric scenarios, the adjusted closeness and betweenness centrality fit the scenarios by considering the actual sink/source traffic models. This adjustment makes the computation of these two metrics less complex since only some of the node-pairs needs to be accounted for. The proposal of the adjusted metrics solve the problem of identifying important nodes in the networks consisting of nodes of different roles. Node attacks according to the adjusted closeness and betweenness metrics degrade overall network throughput faster than random nodes failures.

VI. Conclusions and Future Work

In this paper, we modeled real-time network attacks based on different centrality metrics. Our simulation results showed that PDR under real-time betweenness-based attacks stays the lowest of all metrics in a well connected network. We proposed adjusted closeness and betweenness metrics to identify nodes in networks with asymmetric sink/source models. The adjusted betweenness identifies the significant node more precisely than adjusted closeness. We compute the flow robustness of underlying network topologies as the theoretical bound for the actual simulation results. Our method identifies the critical network elements within dynamic network and network resilience could be improved by strengthening critical node. An ideal situation is all the nodes within the network are of equal significance. For the future work, we will model network challenges in DTNs (delay-tolerant networks) by employing temporal centrality metrics. Real-world mobility traces will be used to verify our attack model.

Acknowledgments

The authors would like to thank Mohammed J.F. Alenazi, Egemen K. Çetinkaya, and Siddharth Gangadhar for the review of the paper and other members of ResiliNets group for the discussions. This research was supported in part by NSF FIND (Future Internet Design) Program under grant CNS-0626918 (Postmodern Internet Architecture), by NSF grant CNS-1050226 (Multilayer Network Resilience Analysis and Experimentation on GENI), and by the EU FP7 FIRE Programme ResumeNet project (grant agreement no. 224619).

References

[1] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, 2003.

[2] J. P. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao, "Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions," in *Proceedings of the 1st ACM Workshop on Wireless Security (WiSe)*, (Atlanta, GA), pp. 31–40, September 2002.

[3] D. Zhang, S. A. Gogi, D. S. Broyles, E. K. Çetinkaya, and J. P. 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), pp. 806–812, October 2012.

[4] D. Zhang and J. P. G. Sterbenz, "Modelling critical node attacks in manets," in *Proceedings of IWSOS: Third International IFIP/IEEE Workshop on Self-Organizing Systems*, Lecture Notes in Computer Science, Springer, 2013.

[5] D. Zhang, E. K. Çetinkaya, and J. P. G. Sterbenz, "Robustness of Mobile Ad Hoc Networks Under Centrality-Based Attacks," in *Proceedings of the 5th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, (Almaty), pp. 229–235, September 2013.

[6] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, 2004.

[7] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," *Communications Magazine, IEEE*, vol. 40, pp. 70–75, Oct 2002.

[8] T. Kontos, G. Alyfantis, Y. Angelopoulos, and S. Hadjiefthymiades, "A topology inference algorithm for wireless sensor networks," in *IEEE Symposium on Computers and Communications (ISCC)*, pp. 479–484, July 2012.

[9] "Open garden." http://opengarden.com.

[10] "Textme." http://http://go-text.me/.

[11] L. C. Freeman, "A Set of Measures of Centrality Based on Betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, 1977.

[12] T. Opsahl, F. Agneessens, and J. Skvoretz, "Node centrality in weighted networks: Generalizing degree and shortest paths," *Social Networks*, vol. 32, no. 3, pp. 245–251, 2010.

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

[14] R. Hekmat and P. V. Mieghem, "Connectivity in wireless ad-hoc networks with a log-normal radio model," *Mobile Networks and Applications*, vol. 11, no. 3, pp. 351–360, 2006.

[15] C. Bettstetter, "On the connectivity of ad hoc networks," *The Computer Journal*, vol. 47, no. 4, pp. 432–447, 2004.

[16] E. K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. P. G. Sterbenz, "Modelling Communication Network Challenges for Future Internet Resilience, Survivability, and Disruption Tolerance: A Simulation-Based Approach," *Telecommunication Systems*, vol. 52, no. 2, pp. 751–766, 2013.

[17] B. Krishnamachari, D. Estrin, and S. Wicker, "Modelling data-centric routing in wireless sensor networks," in *IEEE infocom*, vol. 2, pp. 39–44, 2002.

[18] J. Tang, M. Musolesi, C. Mascolo, and V. Latora, "Temporal distance metrics for social network analysis," in *Proceedings of the 2nd ACM workshop on Online social networks*, pp. 31–36, 2009.

[19] S. Scellato, I. Leontiadis, C. Mascolo, P. Basu, and M. Zafer, "Evaluating temporal robustness of mobile networks," *IEEE Transactions on Mobile Computing*, vol. 12, pp. 105–117, January 2013.

[20] S. P. Borgatti, "Identifying sets of key players in a social network," *Comput. Math. Organ. Theory*, vol. 12, pp. 21–34, April 2006.

[21] T. Dinh, Y. Xuan, M. Thai, E. Park, and T. Znati, "On approximation of new optimization methods for assessing network vulnerability," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, pp. 1–9, 2010.

[22] A. Arulselvan, C. W. Commander, L. Elefteriadou, and P. M. Pardalos, "Detecting critical nodes in sparse graphs," *Computers and Operations Research*, vol. 36, no. 7, pp. 2193–2200, 2009.

[23] S. Shen and J. C. Smith, "Polynomial-time algorithms for solving a class of critical node problems on trees and series-parallel graphs," *Networks*, vol. 60, no. 2, pp. 103–119, 2012.

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

[25] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, vol. 1, no. 3, pp. 215–239, 1978–1979.

[26] P. Bonacich, "Factoring and weighting approaches to status scores and clique identification," *Journal of Mathematical Sociology*, vol. 2, no. 1, pp. 113–120, 1972.

[27] A. A. Hagberg, D. A. Schult, and P. J. Swart, "Exploring Network Structure, Dynamics, and Function using NetworkX," in *7th Python in Science Conference (SciPy)*, (Pasadena, CA), pp. 11–15, August 2008.

[28] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E*, vol. 65, p. 056109, May 2002.

[29] "The ns-3 network simulator." http://www.nsnam.org, July 2009.

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

[31] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," in *ACM SIGCOMM*, (London), pp. 234–244, 1994.

[32] M. Gerharz, C. De Waal, M. Frank, and P. Martini, "Link stability in mobile wireless ad hoc networks," in *Proceedings of the 27th Annual IEEE Conference on Local Computer Networks*, pp. 30–39, IEEE, 2002.

[33] J. P. Rohrer, E. K. Çetinkaya, H. Narra, D. Broyles, K. Peters, and J. P. G. Sterbenz, "AeroRP Performance in Highly-Dynamic Airborne Networks using 3D Gauss-Markov Mobility Model," in *Proceedings of the IEEE Military Communications Conference (MILCOM)*, (Baltimore, MD), pp. 834–841, November 2011.

[34] J. P. Rohrer, A. Jabbar, and J. P. Sterbenz, "Path Diversification for Future Internet End-to-End Resilience and Survivability," *Springer Telecommunication Systems*, vol. 56, pp. 49–67, May 2014.