This paper was presented at RNDM 2013 - 5th International Workshop on Reliable Networks Design and Modeling, co-located with ICUMT 2013 Congress (Sept. 10-12, 2013, Almaty, KZ)

Robustness of Mobile Ad Hoc Networks Under Centrality-Based Attacks

Dongsheng Zhang*, Egemen K. Çetinkaya*, 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, ekc, 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*—In order to understand the role of critical nodes in mobile ad hoc networks (MANETs), dynamic topologies are modelled as time-varying graphs and network topologies within a certain time window are aggregated as a weighted static graph. Critical node behaviour has been previously studied by evaluating how end-to-end throughput is impacted by the removal of high centrality nodes. However, different routing and transport protocols used between physical and application layers can also affect end-to-end network performance. In this paper, instead of analysing networks that span multiple layers, we focus on the routing-topology level based on synthetic mobility traces. We examine how attacks based on different centrality metrics impact robustness, connectivity, and stability of the mobile networks with different parameters. Our results demonstrate that the betweenness centrality is a relatively accurate centrality metric to indicate node significance in a well-connected multihop ad hoc network.**

***Index Terms*—mobile wireless dynamic topology, challenge modelling, graph theory, centrality, MANET, time-varying weighted graph, resilient survivable disruption-tolerant network**

I. Introduction and Motivation

Mobile ad hoc networks (MANETs) are deployed in the environments where the infrastructure-based Internet is not accessible. Vehicular ad hoc networks, wireless sensor networks, and tactical military networks are the examples of real-world MANET deployments. Ad hoc networks can also be used in personal-area networks and embedded-computing applications. For these applications, a well-connected ad hoc network is critical to the normal functioning of the entire network. However, the challenges caused by malicious attacks or random network element failures are inevitable. Networks should be designed and established to be survivable enough so that network service can remain above a certain level even under the circumstances of network element failures [1], [2]. In order to construct resilient ad hoc networks, we need to understand network behaviour in the presence of various challenges [3], [4]. Previously, we modelled MANETs as the aggregation of dynamic topologies within certain time windows [5]–[7]. A weighted static graph in which the weight represents link availability can be obtained. Simulations have been conducted using ns-3 [8] and we have demonstrated that the removal of nodes that have high centrality values impact overall network performance more than random node failures in term of end-to-end network throughput [5]. Nonetheless, more remains to be understood about the impact of node failures on network topology due to different behaviours of the underlying routing and transport protocols.

In this paper, we analyse and compare the network robustness, connectivity, and stability under random node failures and centrality-based attacks based on synthetically generated mobility traces. In addition to the traditional centrality metrics (degree, betweenness, and closeness), we utilise eigenvector centrality [9] to measure relative node criticality. For MANETs with varying number of nodes, network density, and velocity, different centrality metrics play different roles in the network. For example, degree centrality does not account for the nodes outside of its neighbours. In addition, we improve our previous aggregation approach. Instead of using a uniform time window size for all network scenarios, we provide a more accurate window size to aggregate the mobile networks. Temporal metrics such as link duration are used to examine network stability, and atemporal metrics such as flow robustness [10] are used to examine how well-connected the network is at each snapshot of dynamic topologies. Our results show that betweenness is a relatively precise metric to measure node criticality in a well-connected network compared to other centrality metrics and fails only when the network consists of disconnected graph components of small orders.

The rest of the paper is arranged as follows. In Section II, we introduce a list of graph theory terminology used in this paper and some background information about dynamic network modelling and centrality. In Section III, we evaluate a set of synthetic mobility traces generated using different combinations of network parameters. Network robustness, connectivity, and stability are evaluated for networks with different parameters. Finally, we summarise our work and discuss the steps for future research in Section IV.

978-1-4799-1177-6/13/$31.00

II. Background and Related Work

Dynamic behaviour is an integral part of the nature of MANETs. Mobile networks can be treated as a sequence of static graphs evolving over time [11]. Centrality metrics have been employed as important structural attributes of social networks and recently extended to communication networks [12]. A collection of relevant graph-theoretical terms used in this paper will be introduced as follows.

A. Terminology

- Robustness: The ability of a system to maintain specified features when subject to assemblages of perturbations either internal or external [13].
- Path: Any complete set of nodes and links that form a loop-free connection between a node-pair.
- Flow: A data association between a node-pair that may be distributed over one or more paths.
- Graph components: The components of a graph are its maximal connected subgraphs [14].
- Graph order: Number of nodes in the network.
- Graph size: Number of links in the network.
- Vertex cut: A set of vertices whose removal partitions the graph [14].
- Connectivity: The connectivity of G, written $\kappa(G)$, is the minimum size of a vertex set S such that $G - S$ is disconnected or has only one vertex [14].
- Biconnectivity: A biconnected graph is a connected graph, in which if any vertex were to be removed, the graph still remains connected [14].
- Diameter: The maximum shortest-path between any node-pair [14].
- Stability: The stability of a link is given by its probability to persist for a certain time span [15].
- Degree centrality: The degree of a node is the count of the number of other nodes that are adjacent [16].
- Closeness centrality: The closeness of a node is the inverse of the sum of the shortest paths from the node to all other nodes [16].
- Betweenness centrality: The frequency that a node falls on the shortest paths between pairwise nodes [16].
- Eigenvector centrality: The eigenvector of the largest eigenvalue of an adjacency matrix that represents the topology [9].

B. Dynamic Network Modelling

In delay-tolerant and opportunistic mobile networks, temporal graph metrics based on a time-varying graph model have been used to capture the temporal dynamics of information diffusion [17]. Ideas that are similar to dynamic topology modelling have been pursued in the sociology literature [18], [19]. 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 persons interact with each other, the stronger the ties or the friendship between these persons tends to be. In MANETs, mobility models such as Gauss-Markov or random waypoint statistically describe how overall behaviour of all networked devices move over time [20], however the behaviour of each individual node cannot be accurately captured. Previously, we proposed an aggregation model of time-varying graphs in which weights associated with the edges represent link availability ranging from 0 to 1 [5], [6]. This aggregated network can then be represented by an adjacency matrix. This model is applicable to MANETs with stable end-to-end connectivity. The aggregated weighted graph serves the purpose of detecting nodes of high significance based on centrality measures. A comparison of the impact of the window size confirms that the smaller the window size is, the more accurately centrality metrics indicate relative node significance [5]. The selection of time window size is a tradeoff between aggregation precision and computation overhead, however the window size set as a small value is not always appropriate since it might be the case that dynamic topology changes extremely slowly and the calculation of centrality measures based on small window sizes would be unnecessarily redundant. In this paper, we refine the approach of aggregating topologies. Instead of setting the time window size as a uniform value, we calculate the expected time interval that a topology remains stable for different network scenarios.

C. Centrality Metrics

Centrality metrics (degree, betweenness, closeness) were originally used to identify relative significance of each individual in social network analysis [16]. Centrality-based routing protocols have been proposed in delay-tolerant network scenarios [12]. One of the major disadvantages of centrality-based routing is the potential congestion on highly central nodes. Centrality measures have been extended to weighted networks, which take into account both the link weights and the number of links [21]. The eigenvector centrality of a node not only depends on the number of its neighbours but also the value of the neighbours' centrality [22]. According to the way in which different centrality metrics are calculated, degree and eigenvector account for local graph properties, while betweenness and closeness consider the global properties of the entire network. This distinction makes a difference when using different centrality metrics to determine a node's significance in networks of different orders and sizes. Case studies will be presented in Section III to illustrate different centrality metrics' roles in different set network scenarios.

III. Synthetic Trace Analysis

We generate synthetic mobility traces using the Gauss-Markov mobility model [20], [23] in ns-3. We provide a graph-theoretical analysis of mobile topologies in this paper. A range of number of nodes, velocities, and neighbour counts are set for MANETs so that we can explore a range of scenarios. Neighbour count is the average number of nodes within the transmission range of each node given a finite simulation area. We set neighbour count as a certain percentage of the total number of nodes in the network, ranging from 10% (0.1)

to 50% (0.5). Two nodes are assumed to be adjacent if the distance between them is less than the transmission range. The simulation area can be calculated based on transmission range, number of nodes, and neighbour count. Node velocities are set as a uniform distribution between $[0, 2]$, $[5, 10]$, and $[10, 20]$ m/s, which corresponds to walking speed of pedestrians, the speed of bicycles, and the city speed of automobiles respectively. All the statistics are averaged over 10 runs and 95% confidence intervals are shown as appropriate. We use Python to parse the mobility traces and NetworkX [24] libraries to compute various graph metrics. All simulation parameters are listed in Table I. The performance measures that we use to evaluate MANETs topology quality are as follows:

- *Flow robustness* can be computed as the number of reliable flows divided by total number of flows in the network. Flows are considered reliable if there exists at least one path between node-pairs. It captures the maximum possible paths for a given topology [10].
- *Biconnectedness* captures the survivability of the network under single node failure. It also captures the potential of providing an alternative path for high traffic load. Biconnectedness differentiates graphs of different connectivity levels that cannot be captured by flow robustness.
- *Largest diameter of graph components* is the largest diameter of all connected components in the network. This is relevant to the effectiveness of using local and global centrality metrics as node significance indicators.
- *Minimum node degree* is the smallest value of degree centrality among all the nodes in the network. The relation between the probability of k-connectedness and minimum node degree is [25]:

$$P(G \text{ is } k\text{-connected}) \leq P(d_{\min} \geq k) \qquad (1)$$

- *Average link duration* is the average time that links remain up due to nodes remaining within the range of one another. It captures the stability of a link over time [26]. The longer the links live, the more stable the network is.

TABLE I
SIMULATION PARAMETERS

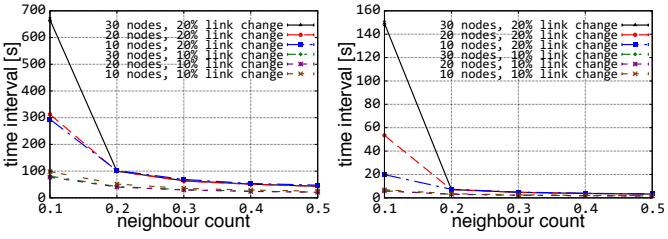
Parameters	Value
number of runs	10
transmit range [m]	100
mobility model	Gauss-Markov
mobility trace generation time [s]	1000
mobility trace time step [s]	0.01
number of nodes	10, 20, 30
node velocity [m/s]	[0, 2], [5, 10], [10, 20]
neighbour count	0.1, 0.2, 0.3, 0.4, 0.5

The simulation scenarios are assumed to be pre-programed networks. Nodes are challenged based on random failures and 4 different centrality metrics (degree, eigenvector, closeness, and betweenness). We assume that attacker has the complete topology information at every time instance. Therefore, the attacker can calculate centrality metrics for the entire topology and determine target nodes continuously. We assume that challenged nodes are completely down and so are the incident links.

A. Determining the Window Size

We previously modelled dynamic topologies of MANETs by aggregating time-varying graphs within certain time windows into a static weighted graph [5]. The aggregation window size is set as the same value for different network parameters. However, based on differing number of nodes, neighbour counts, 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 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. The maximum number of links for a graph of order n is $n(n-1)/2$. We define *global link stability* as the ratio of the number of changed links to the maximum number of links. We consider the link is changed if it only exists in one of the two different topologies. Two levels of stability are measured here: less than 10% or 20% of the maximum number of links in the network changing. Figure 1 shows the average time interval that a topology can stay relatively stable. Generally, the average time that the network stays relatively stable for $[0, 2]$ m/s velocity is much longer than $[10, 20]$ m/s velocity, as shown in Figure 1a and 1b respectively. This is expected since the higher the average velocity, the faster the network topologies change. When neighbour count is only 10%, there is a relatively large variance between 10% and 20% link change. This is because when the network density is relatively low, the number of existing links is small and the time interval that it takes for 20% of total links to change would be much longer.



(a) velocity = $[0, 2]$ m/s (b) velocity = $[10, 20]$ m/s

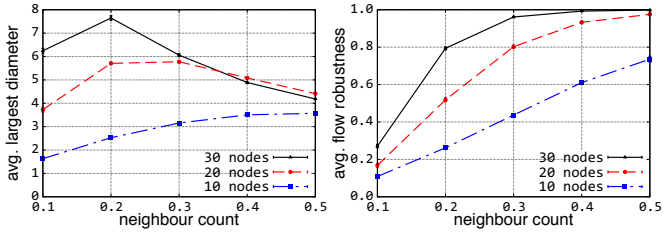
Fig. 1. Window size for different network parameters

Obviously, the smaller the fraction of links changes, the more accurately the centrality metrics could be based on the aggregated graph. We exploit the time intervals of 10% link change as the aggregation window sizes for all different combinations of network parameters for the rest of the paper.

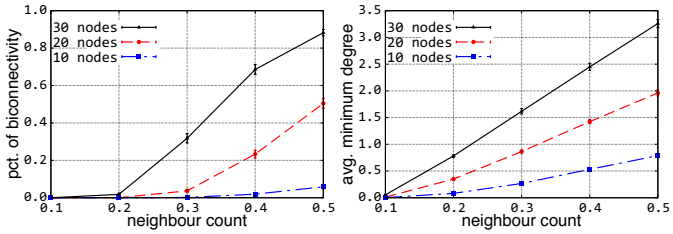
B. Atemporal Properties of the Network

Before we compare how dynamic networks behave under attacks based on different centrality metrics, we first present

characteristics of different networks without node failures, as shown in Figure 2. The x-axis is the fraction of total number of nodes as the average neighbour count.



(a) max. diameter vs.neighbour count (b) flow robustness vs. neighbour count



(c) biconnected vs. neighbour count (d) average $d_{\min}$ vs. neighbour count

Fig. 2. Base scenarios without node failures

For the 30-node network, largest network diameter of graph components peaks when neighbour count is 20%. This is because when the network is about 1-connected, the largest diameter of graph components is at its highest value as shown in Figure 2a. If the network is more connected, nodes can reach each other in fewer hops within a highly-meshed network; if the network is more disconnected, the largest diameter of graph components is constrained by shrinking component size. Flow robustness has a lower requirement on graph connectivity than biconnectedness, as long as the topology is 1-connected, the flow robustness will have a value of 1. As shown in Figure 2b, network flow robustness increases with a larger neighbour count. As suggested in Equation 1, the probability of a topology being 2-connected is less than the probability of minimum node degree being more than 2 as shown in Figures 2c and 2d. When the node count is 10, the average minimum node degrees are all below 1 even with the neighbour count of 5. As expected, the probability of a biconnected graph for 10-node networks is much lower than 20- and 30-node networks in Figure 2c.

As mentioned earlier, for different network order and size, centrality metrics play different roles as the indicators of node significance. Next, we categorise our synthetic mobile networks into 4 types and study how different network performance measures are affected by centrality-based attacks in each individual scenario. The four types are:

1) Dense network with large number of nodes: 30 nodes with 15 neighbour count (0.5)
2) Sparse network with large number of nodes: 30 nodes with 3 neighbour count (0.1)
3) Dense network with small number of nodes: 10 nodes with 5 neighbour count (0.5)
4) Sparse network with small number of nodes: 10 nodes with 1 neighbour count (0.1)

1) Dense network with large number of nodes

In this scenario, we consider 30 nodes with an average of 15 neighbour count as dense network with relatively large number of node as shown in Figure 3. Note that this figure is a single snapshot of mobile networks, whereas the plots are averaged over 1000 s trace time with 10 runs. We also provide the snapshots of topologies for next three scenarios.

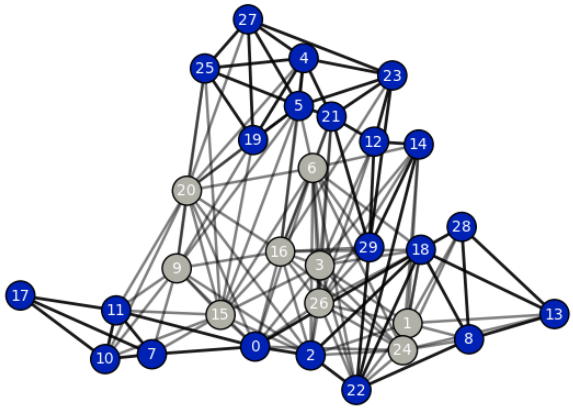
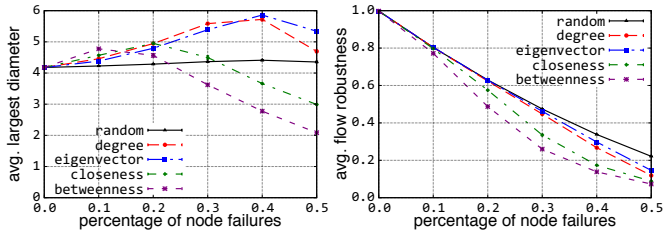
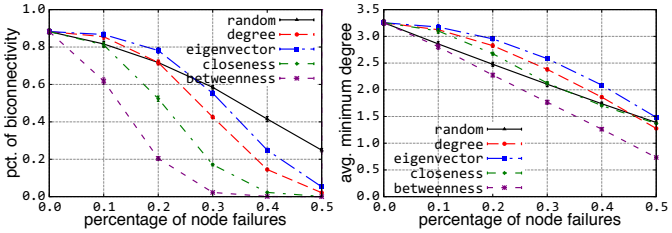


Fig. 3. Topology snapshot of 30 nodes, 50% neighbour count

Network diameter increases with a higher percentage of node failures for attacks based on degree and eigenvector centrality as shown in Figure 4a, since network is still connected after the removal of certain number of nodes and the removal of a non-vertex-cut high degree nodes could increase the length of shortest paths and result in the increase of network diameter.



(a) max. diameter vs. # node failures (b) flow robustness vs. # node failures



(c) biconnectedness vs. # node failures (d) average $d_{\min}$ vs. # node failures

Fig. 4. 30 nodes, 50% neighbour count

In Figure 3, the node set used for degree-based attack is tagged with grey colours. As we can observe, even after removal of 30% of total nodes, the rest of the network is

still connected and network diameter increases from 4 to 8. The flow robustness of betweenness-based attacks stays the lowest of all as shown in Figure 4b. This indicates that the removal of high betweenness nodes partitions the network with a higher probability than other metrics. For node failures less or equal than 30% of all nodes, node attacks based on eigenvector and degree is almost no different from random failures. This can be explained as in a highly-connected network, the removal of any nodes that are not vertex cut would have the same impact on the flow robustness since the network stays connected. In Figure 4c, network biconnectedness is degraded most heavily by the betweenness-based attacks. The removal of high betweenness nodes results in the lowest average minimum node degree of all metrics, which indicates that high betweenness nodes tend to be the neighbours of the lower degree nodes. While being locally high centrality nodes, nodes of high eigenvector values tend to be the neighbours of other high eigenvector centrality nodes. Hence, the removal has less impact on the whole network in terms of minimum node degree as shown in Figure 4d.

2) Sparse network with large number of nodes

In this scenario, nodes are relatively sparsely-connected with an average of 3 neighbour count. An example snapshot of this topology is shown in Figure 5. Results for the average minimum node degree and the percentage of biconnected topologies are not provided here since these two measures are almost equal to 0 for all levels of node failures. As the network is at most 1-connected, the removal of many nodes in the network would increase the number of graph components. Hence, the average largest diameter will decrease as more nodes get removed. Node removal based on betweenness still has the highest impact on the average largest diameter of graph components. Network diameter in each component gets smaller as shown in Figure 6a.

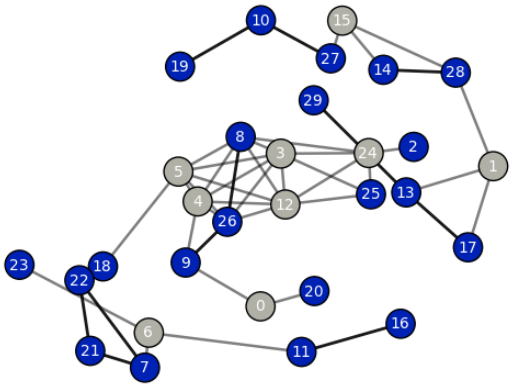
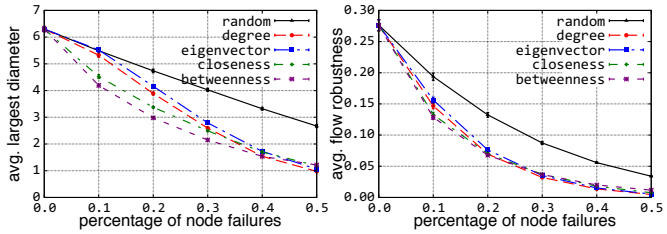


Fig. 5. Topology snapshot of 30 nodes, 10% neighbour count

Grey nodes in Figure 5 are the node list in this example to be removed for 30% node failures based on degree. As we can observe, the topology gets partitioned into multiple components as we remove the links adjacent to the grey nodes. Moreover, the flow robustness degrades heavily as shown in Figure 6b.



(a) max. diameter vs. # node failures (b) flow robustness vs. # node failures

Fig. 6. 30 nodes, 10% neighbour count

3) Dense network with small number of nodes

In this scenario, we consider 10 nodes with 5 neighbour count as the case of a dense network with relatively small network order. A snapshot of this mobile topology is shown in Figure 7.

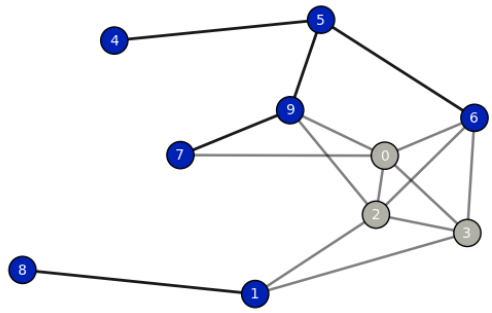
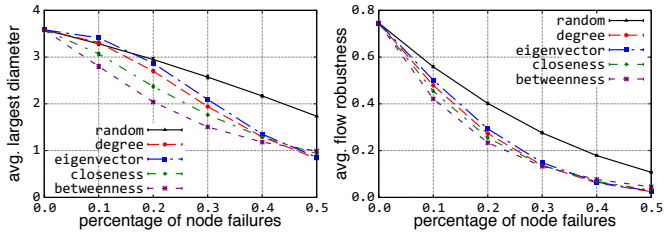
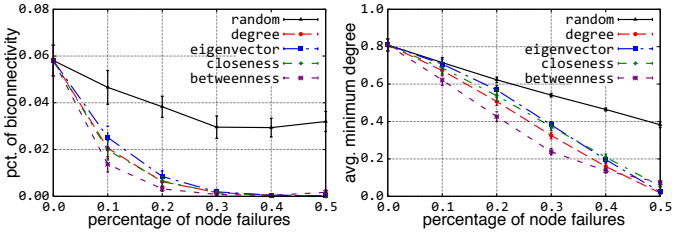


Fig. 7. Topology snapshot of 10 nodes, 50% neighbour count

When only 10% of nodes are removed under degree- and eigenvector-based attacks, the network diameter does not change much since the network is still connected after node removal as shown in Figure 8a.



(a) max. diameter vs. # node failures (b) flow robustness vs. # node failures



(c) biconnectedness vs. # node failures (d) average $d_{\min}$ vs. # node failures

Fig. 8. 10 nodes, 50% neighbour count

By removing some fraction of nodes, networks become partitioned faster in a 10-node network than a 30-node network. Furthermore, with a smaller network order (number of nodes), the graph displays more local properties. Even though the removal of high betweenness nodes still has the greatest impact on the network, the difference between betweenness-based attacks and other centrality-based attacks becomes trivial as can be observed in Figure 8b. The average minimum node degree stays below 0.8 as shown in Figure 8d, which means that there is a high probability of the network being disconnected. Accordingly, the percentage of time that the network stay biconnected is almost zero as shown in Figure 8c. In Figure 7, nodes 0 and 2 will be removed if attacked based on degree while nodes 2 and 3 will be removed if based on betweenness. The removal of node 2 and 3 will partition the network resulting in a lower flow robustness.

4) Sparse network with small number of nodes

Node connectivity is the lowest for this network case. The network is disconnected most of the time. The minimum node degree and percentage of the time network being biconnected are both almost 0. Nodes that are in a connected component can generally reach each other in less than 2 hops as can be seen in Figure 10a. Hence, node attacks based on betweenness have less impact on the network than node attacks based on other metrics as shown in Figure 10b. In a sparsely-connected network with each graph component being a smaller order, there are almost no intermediate nodes between any pair of nodes. In Figure 9, after removing nodes 2 and 4, all nodes within the same components can reach each other in 1 hop and the betweenness for rest of the nodes are equally 0.

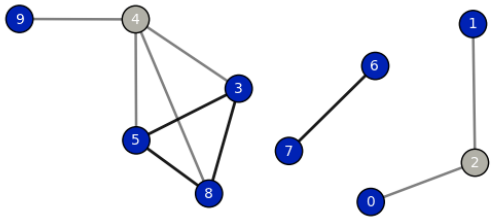
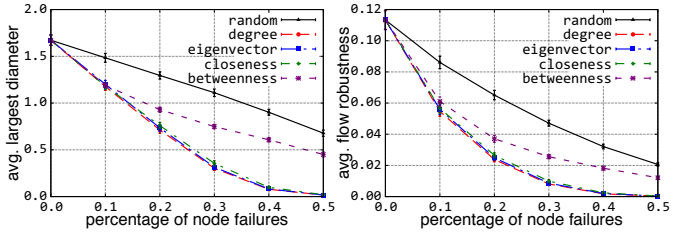


Fig. 9. Topology snapshot of 10 nodes, 10% neighbour count



(a) max. diameter vs. # node failures (b) flow robustness vs. # node failures

Fig. 10. 10 nodes, 10% neighbour count

C. Temporal Properties of the Network

In addition to graph connectivity at each time instance that affects the service level of the network, the global link stability is also critical as frequent routing changes can cause unpredictably long delay and data loss. Figure 11 presents base scenarios of average link durations and shows node velocity plays a dominant role in determining the average link duration. Since the number of nodes has trivial impact on the average link duration, we set the graph order as 30 and neighbour count as 0.5 (15 nodes) and 0.1 (3 nodes) and compare how average link duration is impacted differently for networks under attacks based on different metrics.

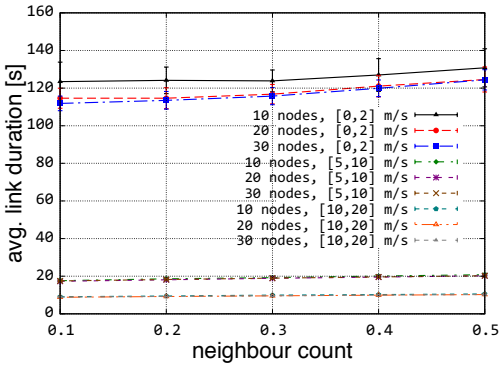
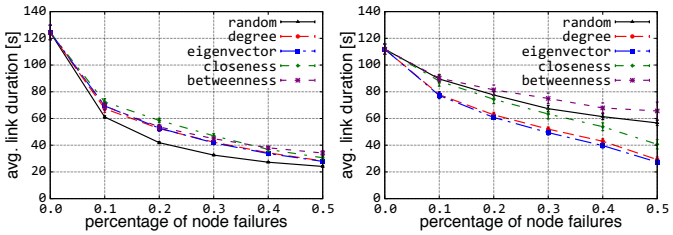
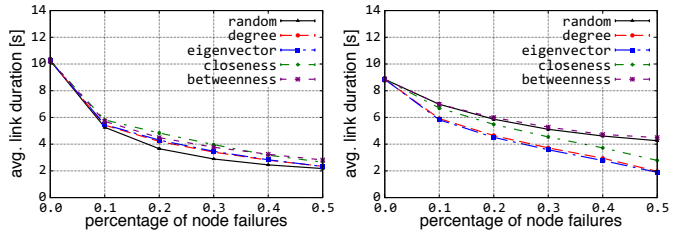


Fig. 11. Average link duration of network without node failures



(a) 15 neighbour count, $[0, 2]$ m/s (b) 3 neighbour count, $[0, 2]$ m/s



(c) 15 neighbour count, $[10, 20]$ m/s (d) 3 neighbour count, $[10, 20]$ m/s

Fig. 12. Average link durations comparison

In Figures 12a and 12c, networks under random node failures have the lowest average link duration; this is because in consecutive time windows, random node failures are independently selected, while for centrality-based attacks, even though topology changes as time evolves there is still a certain level of correlation between high centrality nodes in two consecutive time windows. In addition, relatively high node density makes random node changing a dominant factor that affects average link duration. In contrast, in the network with a 3 neighbour count, since the total number of links is much less than the network of 15 neighbour count, degree-based and eigenvector-based attacks result in shortest average

link duration, since it affects the greatest number of links in each window size around its neighbours. High betweenness and closeness nodes are connected to fewer nodes as compared to high degree and eigenvector centrality nodes. Random node attacks have negligible impact on the average link duration if few links are adjacent to the randomly selected nodes. As illustrated in Figures 12b and 12d, eigenvector- and degree-based attacks impact average link duration most heavily.

IV. Conclusions and Future Work

We analysed robustness, connectivity, and link stabilities of MANETs under various centrality-based attacks. The relation between maximum diameter of the graph component, flow robustness, minimum node degree, and biconnectedness is revealed for different network scenarios. A more precise window size is utilised to aggregate the dynamic networks. We demonstrated that degree and eigenvector centrality represent local properties in term of the impact of removing high degree and eigenvector nodes. In contrast, closeness and betweenness show global characteristics in measuring the significance of a node. In a well-connected network that nodes can communicate with each other in real-time, betweenness is a relatively accurate metric to indicate node significance. Betweenness fails only in poorly-connected networks consisting of sparsely-distributed graph components of small sizes. At the same time, node attacks based on degree and eigenvector centrality affect network stability in sparsely-connected network.

For future work, the theoretical lower bound of flow robustness for different number of node attacks will be calculated to show how accurate centrality-based attack could be compared to the theoretical lower bound. A cross comparison between topological level flow robustness and network throughput in the application layer will also be performed. We will also extend this analysis to disruption-tolerant networks in which network is partitioned for a great fraction of time. Temporal graph metrics will be evaluated to study the robustness of sparsely-connected networks.

Acknowledgment

This research was supported in part by NSF grant CNS-1219028 (Resilient Network Design for Massive Failures and Attacks) and by NSF grant CNS-1050226 (Multilayer Network Resilience Analysis and Experimentation on GENI).

References

[1] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[2] J. P. G. 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 3rd ACM workshop on Wireless Security (WiSE)*, (Atlanta, GA), pp. 31–40, 2002.

[3] E. K. Çetinkaya and J. P. G. Sterbenz, "A Taxonomy of Network Challenges," in *Proceedings of the 9th IEEE/IFIP International Conference on the Design of Reliable Communication Networks (DRCN)*, (Budapest), pp. 322–330, March 2013.

[4] 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.

[5] 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.

[6] 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.

[7] D. Zhang, S. A. Gogi, D. S. Broyles, E. K. Çetinkaya, and J. P. Sterbenz, "Modelling Wireless Challenges," in *Proceedings of the 18th ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, (Istanbul), pp. 423–425, August 2012. Extended Abstract.

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

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

[10] J. P. Rohrer, A. Jabbar, and J. P. Sterbenz, "Path Diversification for Future Internet End-to-End Resilience and Survivability," *Springer Telecommunication Systems*, 2012.

[11] A. Casteigts, P. Flocchini, W. Quattrociocchi, and N. Santoro, "Time-varying graphs and dynamic networks," in *Proceedings of the 10th International Conference on Ad-hoc, mobile, and wireless networks (ADHOC-NOW)*, vol. 6811 of *Lecture Notes in Computer Science*, pp. 346–359, Paderborn: Springer, 2011.

[12] E. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant MANETs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, pp. 606–621, 2009.

[13] E. Jen, *Robust Design: A Repertoire of Biological, Ecological, and Engineering Case Studies*. Oxford University Press, 2005.

[14] D. West, *Introduction to graph theory*. Prentice Hall PTR, 2008.

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

[16] L. C. Freeman, "A set of measures of centrality based upon betweenness," *Sociometry*, vol. 40, pp. 35–41, March 1977.

[17] 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.

[18] G. C. homans, *The human group*. Transaction Publishers, 1951.

[19] M. S. Granovetter, "The strength of weak ties," *American journal of sociology*, pp. 1360–1380, 1973.

[20] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing*, vol. 2, no. 5, pp. 483–502, 2002.

[21] 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.

[22] B. Ruhnau, "Eigenvector-centrality a node-centrality?," *Social networks*, vol. 22, no. 4, pp. 357–365, 2000.

[23] 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.

[24] 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.

[25] C. 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*, (New York, NY, USA), pp. 80–91, ACM, 2002.

[26] J. Boleng, W. Navidi, and T. Camp, "Metrics to enable adaptive protocols for mobile ad hoc networks," in *Proceedings of the International Conference on Wireless Networks (ICWN02)*, pp. 293–298, 2002.