This peer-reviewed full text paper was presented at RNDM 2012 - 4th International Workshop on Reliable Networks Design and Modeling, co-located with ICUMT 2012 Conference

Modelling Attacks and Challenges to Wireless Networks

Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. Çetinkaya, James P.G. Sterbenz
Information and Telecommunication Technology Center
Department of Electrical Engineering and Computer Science
The University of Kansas, Lawrence, Kansas, 66045, USA
{dzhang, santoshag, dbroyl01, ekc, jpgs}@ittc.ku.edu
www.ittc.ku.edu/resilinets

***Abstract*—Due to the tremendous potential of MANETs (mobile ad hoc networks) for deployment in commercial and military services, a thorough understanding of network behaviour when exposed to challenges is essential for constructing a resilient and survivable MANET. Therefore, it is vital to have a comprehensive framework that can model it under various network attacks and challenges. The MANET environment has a dynamic and intermittent connectivity resulting from channel fading and mobility of the nodes, which makes it difficult to model the network as well as its challenges. We provide a model to simulate malicious and area-based challenges to wireless networks. In the modelling of malicious attacks, we treat MANETs as time-varying graphs (TVGs) represented as a weighted adjacency matrix, in which the weights refer to the link availability. We evaluate the relations between node significance and weighted centrality metrics. Area-based challenges representative of real-world scenarios are also modelled. Our ultimate goal is to provide a comprehensive network challenge model of MANETs and also heterogeneous networks.**

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

I. 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 decentralised and self-organised manner. Because of its independence and flexibility, MANETs have been applied in various scenarios, such as wireless sensor networks, military networks, vehicular ad hoc networks, and integrated cellular and ad hoc networks. With the ever-increasing deployment of MANETs, stable and resilient network performance is essential to satisfy the requirements of the various applications. In order to construct a resilient wireless network, we need to understand network behaviour in the face of various challenges [1].

In addition to the challenges that exist in traditional wired networks, the MANET environment has dynamic and intermittent connectivity resulting from channel fading and mobility of the nodes. Furthermore, some MANET environments suffer from the constraint of limited energy and unpredictable propagation delays due to distance or episodic connectivity [2]. Hence, it is complex to model these networks as well as the challenges against them. In this paper, we assume each node has sufficient energy during the experiment and focus on the challenges caused by dynamic network connectivity with mobile nodes. Based on our previous work KU-CSM [3], [4], we model attacks and challenges against MANETs in two aspects, malicious and area-based. In the malicious attack model, the challenges are exerted on a few specific nodes based on their importance. In this paper, we model MANETs as TVGs (time-varying graphs) and pairwise node interactions are aggregated within a certain time window [5], [6]. The network can be represented as a weighted adjacency matrix, in which the weights refer to link availability. We utilise centrality metrics of weighted graphs to measure the significance of a node. Attacks targeted toward nodes with high significance could degrade network performance severely. Previous work has exploited centrality metrics from social network analysis as indicators for routing mechanisms of DTNs (delay tolerant networks) [7], but our approach for malicious attacks is the first to make use of TVGs and weighted graph centrality to study network challenges from a topological perspective.

As opposed to node and link failures that affect single or multiple elements, area-based challenges could affect numerous network components. Natural phenomena that are geographically correlated might impact quite large areas. Hurricanes, earthquakes, and solar storms are examples of natural disasters that can impact the network at large scale [4]. While previous studies mostly consider circular area-based challenges in wireless networks, to best of our knowledge, we are the first to model n-sided polygons for propagation loss models, which are more realistic; this follows our work in wired networks [3], [4].

The rest of the paper is arranged as follows. In Section II, we introduce background and related work about wireless networks and challenge modelling. In Section III, we provide graph-theoretical metrics that are fundamental to our model. By utilising these metrics, we illustrate how to model malicious attacks and then describe how we simulate area-based challenges in Section IV. In Section V, we analyse our models by giving several examples with plots showing network performance under challenges. Finally, we summarise our work and mention the next steps for future research in Section VI.

978-1-4673-2017-7/12/$31.00 ©2012 IEEE

II. Background and Related Work

Graph theory has been applied in various areas of the computing, networking, social, and natural sciences. Using node centrality metrics for DTN routing criteria in opportunistic scenarios has been proposed [7]. However, because routing algorithms are greedy and node centrality values are averaged among all node pairs globally, centrality-based routing is ineffective [8]. Due to the topological multi-hop diversity and rerouting in MANETs, the attack of a random node might have only a trivial impact on the overall network performance. The novel aspect of our work is to model malicious network attacks based on node significance associated with centrality metrics. We consider local graph metrics that describe individual node properties more accurately than global metrics.

A number of approaches have been taken to study topological properties of MANETs. An algorithm for finding critical points in MANETs and improving the network resilience has been proposed [9]. Geographic vulnerabilities in networks are evaluated by using 2-terminal and all-terminal methods [10]. However, all these approaches do not take node mobility into account. A combinatorial model has been developed to capture characteristics of TVGs [11]. A comprehensive analytical framework for the calculation of several stochastic topology properties has been proposed [12]. A MANET has been modelled as an undirected geometric random graph and network connectivity has been studied using realistic radio channel models [13].

A comprehensive framework to simulate network attacks and challenges was developed in our previous work [3], [4], in which we mainly simulate challenges against wired networks. For wireless networks, a toolkit to represent obstacle presence and disaster scenarios has been introduced in the ns-2 simulator [14], [15]. When modelling a wireless network environment, the understanding of various propagation models aids in channel modelling and characterisation [16]. Natural phenomena such as weather disruptions due to rainstorms have been taken into consideration when analysing routing protocols in wireless-mesh networks [17]. This work is distinct in that we provide an integrated model of attacks and challenges against MANETs from graph-theoretical and topological perspectives.

III. Graph-Theoretic Metrics

Certain models are required to address the dynamics of MANETs. Malicious attacks targeting the most influential nodes in the network could severely impact a network. In this section, we review two key graph-theoretic concepts that can address these two issues: TVGs and centrality for weighted graphs.

A. Time-varying Graphs

A TVG is defined as $\mathcal{G} = (V, E, \mathcal{T}, \rho, \zeta)$, where the definitions of V and E is the same as in static graphs except that $V(G)$ and $E(G)$ vary over time [18]. Since it is used to describe dynamic systems, the relation between nodes change with time; $\mathcal{T} \subseteq \mathbb{T}$ is called the *lifetime* of the system; $\rho \colon E \times \mathcal{T} \rightarrow \{0, 1\}$, is the presence function that indicates the availability of a specified edge at a given time; $\zeta \colon E \times \mathcal{T} \rightarrow \mathbb{T}$, is the latency function that indicates the time needed to traverse a certain edge E. We add an additional parameter $\nu \colon V \times \mathcal{T} \rightarrow \{0, 1\}$ used to denote the availability of a specified node; our new TVG model is $\mathcal{G} = (V, E, \mathcal{T}, \rho, \zeta, \nu)$. Since information propagates at a speed that is close to velocity of light and is far higher than the speed of mobile nodes, latency function ζ is negligible in our cases. The *footprint* of a TVG $\mathcal{G}$ from t_1 to t_2 can be represented as a static graph $G^{[t_1, t_2)} = \left(V, E^{[t_1, t_2)}\right)$ such that $\forall e \in E, e \in E^{[t_1, t_2)} \Leftrightarrow \exists t \in [t_1, t_2), \rho(e, t) = 1$ [18]. Fundamentally, the footprint denotes an aggregation of node interactions within a certain time window $[t_1, t_2)$. Thus, we can have a static graph for each time interval. 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 $\tau_{\text{up}} \subseteq \tau_{i,j}$ to the time window length $\tau_{i,j}$, where τ_{up} is the time two nodes are within the transmission range of each other and able to communicate. Then we can have availability matrices of all time windows, in which each element denotes the link availability of certain pair of nodes with a value ranging from 0 to 1. Based on different ranges of time windows, we can obtain the availability matrix of different granularities. Atemporal metrics of the static graph are applied on the availability matrix. Since the matrix is aggregated over time, the atemporal metrics become less accurate as the time window increases. Next, we introduce several atemporal indicators built on the footprint, which are degree centrality, betweenness centrality, and closeness centrality.

B. Weighted Centrality Metrics

Centrality metrics have been used for network analysis [19]. Each of these three metrics plays a different role in the network. Degree centrality is a measure of communication ability of a node in the network. Both betweenness and closeness centrality are related to the shortest path between a pair of nodes. Betweenness is defined as the frequency that a node falls on the shortest paths between pairwise nodes [19]. A node's betweenness is a measure of the degree to which it enables communication between other 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 [19].

The unweighted centrality metrics represent the relationship between nodes as a binary measure. Recently, generalised centrality definitions for weighted graphs have been proposed to describe node relationship in a more general way [20]. In these definitions, a tuning factor α is introduced to express the relative significance of link weights as compared to link number. Degree centrality for weighted graphs is formally defined as $C_{\mathrm{D}}^{w\alpha}(i) = k_i^{(1-\alpha)} \times \left(\sum_k^N w_{ik}\right)^{\alpha}$, where α is a non-negative tuning factor that can be set based on network scenarios, k_i is the number of neighbours and w_{ik} represents the weight of link between n_i and n_k [20].

The calculation of betweenness and closeness is relevant to the identification and the 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 [21]. Hence, the shortest paths between two nodes is defined as $d^{w\alpha}(n_i, n_k) = \min\left(\frac{1}{(w_{ih})^{\alpha}} + \cdots + \frac{1}{(w_{hk})^{\alpha}}\right)$, where h represents the internal nodes between n_i and n_k and α is the tuning factor that controls the tendency towards link weights or the number of internal nodes [20]. A weighted version of closeness is defined as $C_{\text{C}}^{w\alpha}(n_k) = \left[\sum_{i=1}^{n} d^{w\alpha}(n_i, n_k)\right]^{-1}$. Similarly, by applying adapted shortest path algorithm, the measure of weighted betweenness can be obtained as: $C_{\text{B}}^{w\alpha}(n_k) = \sum_i \sum_j \frac{g_{ij}^{w\alpha}(n_k)}{g_{ij}^{w\alpha}}$, where $i < j$ and $i \neq j \neq k$, and $g_{ij}^{w\alpha}(n_k)$ is the number of shortest paths that include n_k [20].

IV. Modelling Attacks and Challenges

We model three types of network challenges: non-malicious random, malicious, and area-based. Non-malicious challenges can simply be modelled as failures of randomly selected nodes. For malicious attacks, the purpose is to model attacking specific nodes with certain characteristics to maximise overall network performance degradation. For area-based challenges, we exploit moving impairments of varying size to model certain large-scale disasters that impact a wide area. We use ns-3 version 3.13 as our simulation tool [22]. `MovingPropagationLossModel` is utilised to shut down nodes under malicious attack and simulate moving and scaling challenges in area-based attacks.

A. Moving Propagation Loss Model

We have developed a new propagation loss model, `MovingPropagationLossModel` in ns-3, which includes a mobility model parameter and range of influence [3], [4]. Using these two parameters, we can specify where the loss takes place and how it moves over time. A realistic challenge can be modelled based upon a specific set of channel impairments that have locality rather than relying solely upon statistical methods.

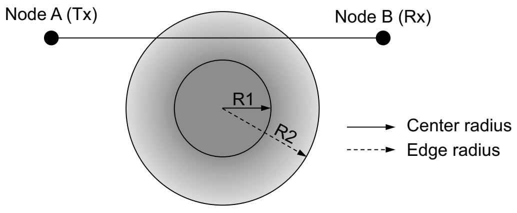


Fig. 1. Moving propagation loss model

Channel loss occurs based upon the closest distance from the center of the impairment to the line segment between two wireless nodes as illustrated in Figure 1. The path loss incurred is based upon two radii, the center and the edge radius. Any path within the center radius suffers the full path loss value of the impairment. Any path outside the edge radius suffers no path loss. A path that falls between the center radius and the edge radius suffers a signal loss between zero and the full impairment loss value as the loss tapers linearly from the center radius to the edge radius. The center radius may be set to zero to model any situation where the path loss should be directly proportional to the path distance affected by the impairment.

B. Malicious Attacks

In real-time MANET communications, it is critical that nodes are available as transceivers or relay nodes for others. A set of fixed nodes can be modelled 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 multi-hop links. We assume node pair communication is symmetric to simplify the graph model for malicious attacks, and therefore undirected graphs are sufficient to model our network.

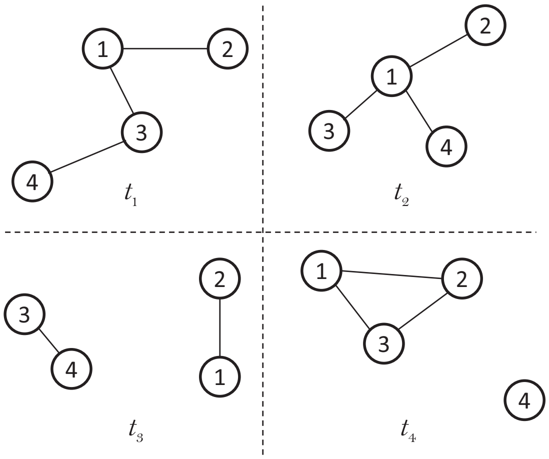
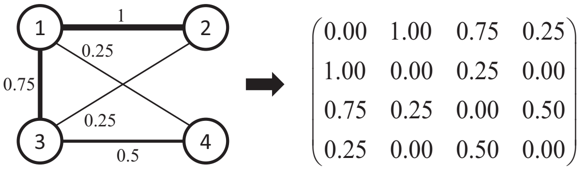


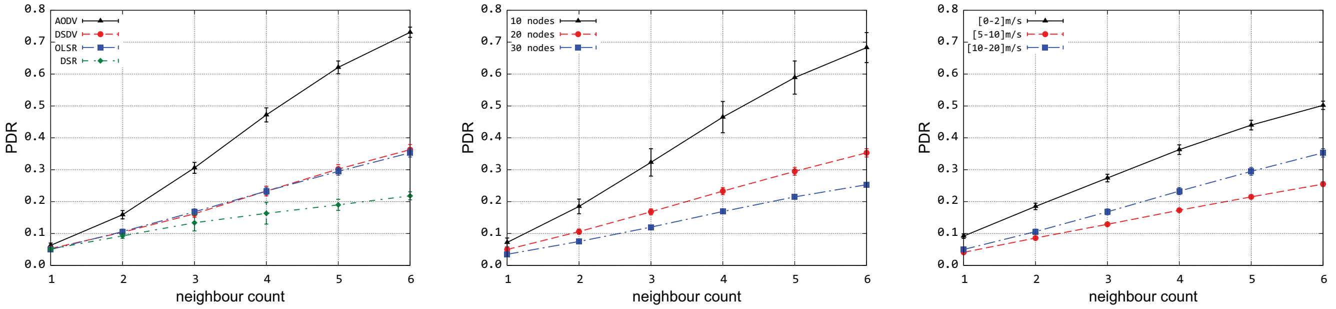
Fig. 2. Topology of a MANET at four consecutive time steps



$$\begin{pmatrix} 0.00 & 1.00 & 0.75 & 0.25 \\ 1.00 & 0.00 & 0.25 & 0.00 \\ 0.75 & 0.25 & 0.00 & 0.50 \\ 0.25 & 0.00 & 0.50 & 0.00 \end{pmatrix}$$

Fig. 3. Pairwise link availability in a matrix

In a MANET environment, all the nodes are mobile and the pairwise node connectivity is dynamic. The evolution of the network 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. Next, we calculate three atemporal metrics of the weighted graphs:



(a) 20 nodes, 5-10 m/s

(b) OLSR, 5-10 m/s

(c) 20 nodes, OLSR

Fig. 4. Selective baseline scenarios

degree, betweenness, and closeness centrality. We employ them as the node significance indicators and model attacks adaptively toward the most critical nodes. Aggregation of node activities of different time window sizes impact the accuracy of using centrality metrics as significance indicators, since time range affects granularities of the aggregation.

We use the mobility trace file output from the ns-3 simulation. A Python script is used to parse the mobility trace and extract node position information at each time step. For each time step, an adjacency matrix representing the transient topology can then be obtained. We sum up the matrices for each time step within the time window and the link availability of any pair of nodes can be calculated as the number of 1s divided by the total number of time steps during that time window. Therefore, node interactions for each time window are aggregated into a static graph, based on which centrality metrics can be calculated. Figure 2 presents MANET topologies at four consecutive time steps and Figure 3 shows the aggregation of MANETs over time and its representation as an adjacency matrix. By feeding centrality information into ns-3, we can obtain simulation results of attacks according to different metrics.

C. Area-based Challenges

The challenge specification for area-based challenges is a polygon with user-specified behaviour and a circle centered at a user-specified coördinates with radius r as in [3]. The former uses the Computational Geometry Algorithms Library (CGAL) [23], which is an open source library with efficient geometric algorithms implemented in C++. Both of these propagation loss models determine the wireless channels that are encompassed by the defined shape and do not allow transmission over that channel during the challenge interval. These models can behave dynamically by moving or scaling (expanding or contracting) over time.

V. Simulation Analysis

The simulation consists of two major parts. In the malicious attack model, we assume the channel depends only on distance so as to better concentrate on pure topological properties. In the area-based challenge scenario, a couple of realistic models are introduced to simulate large-area radio channel failures. PDR (packet delivery ratio) is used to measure the network performance under attacks and challenges.

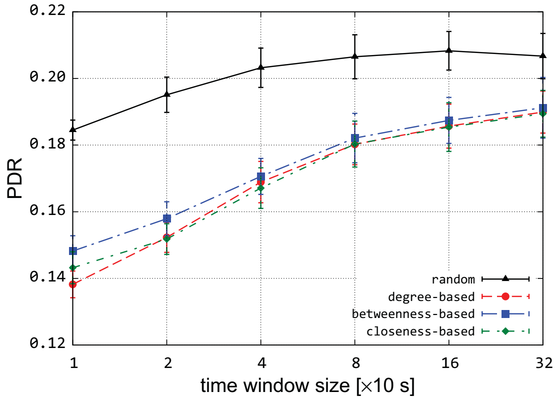


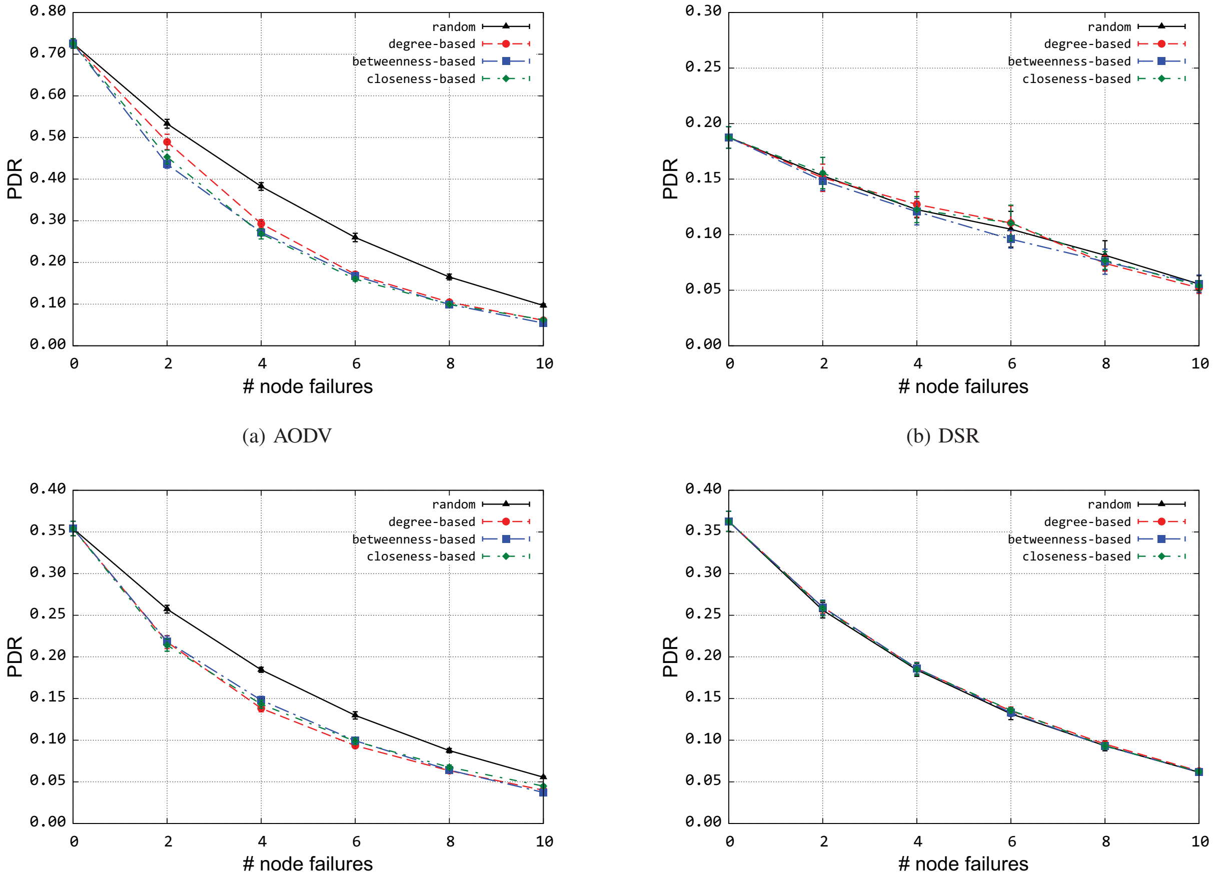
Fig. 5. Impact of time windows size on accuracy of node centrality indicators

TABLE I
Simulation Parameters

number of iterations	20
simulation time	1200 s
routing warm-up time	100 s
traffic generation time	1000 s
transmission range	100 m
mobility model	Gauss-Markov
number of nodes	10, 20, 30
neighbour count	1, 2, 3, 4, 5, 6
physical channel	802.11g (54 Mb/s)
routing protocol	AODV, DSDV, DSR, OLSR
node velocity	[0, 2], [5, 10], [10, 20] m/s
traffic model	CBR (constant bit rate)
time window size	10, 20, 40, 80, 160, 320 s

A. Malicious Attacks

We set up simulation parameters as follows. Data traffic is generated during the steady-state and different seeds are set for each iteration of the simulation. Every node sends traffic to every other node to ensure the fairness between all the nodes. Node velocities are given in three different ranges of uniform distribution, [0, 2], [5, 10], and [10, 20] m/s, and they



(a) AODV

(b) DSR

(c) OLSR

(d) DSDV

Fig. 6. Random and malicious attacks on MANETs using different routing protocols

correspond to walking speed, cycling speed, and downtown vehicle speed respectively. We use the Gauss-Markov mobility model to describe node mobility [24]. Neighbour count is the average number of neighbour nodes and the simulation area can be calculated according to the number of nodes, transmission range, and neighbour count [25]. The main simulation parameters for malicious attack models are displayed in Table I.

Due to space constraints, we only provide a selective set of base scenario results for functional verification. We model malicious attacks based on centrality metrics representative of scenarios in which attackers understand network topologies. High centrality nodes are attacked prior to others. Figure 4 shows the PDR results for three sets of variables, routing protocols, node numbers, and node velocities. Figure 4a shows that the AODV (ad hoc on-demand distance vector) routing protocol achieves PDR higher than the other three with 20 nodes at the same speed range. Figure 4b gives PDRs for different number of nodes at the same speed range using the OLSR (optimised link state routing) protocol. Figure 4c presents PDRs using the OLSR routing protocol with 20 nodes at three different speed ranges. Generally, PDR increases with the growing number of average number of neighbour count. With a fixed neighbour count, the increased node number or node speed will result in PDR degradation.

As mentioned earlier, centrality-based attacks are effective within relatively short time windows in that the link availabilities between pairwise nodes become increasingly homogeneous to each other as the time window increases, resulting in a small standard deviation between the values of centrality metrics for each node. Figure 5 shows the impact of the time window on the PDR difference between random and centrality-based attacks with simulation parameters set as OLSR routing protocol, 20 nodes, [5, 10] m/s, 4 simultaneous node failures, and 6 neighbour count. When the window size is 10 s, the PDR difference between random and centrality-based attacks is approximately 0.04. When the window size increases to 320 s, the PDR difference is only about 0.02.

Placement of network resources must be balanced to the optimised resilience and cost in real-world deployment [1]. We select a scenario with a node number of 20 and node speeds given by a uniform random variable in the interval of [5, 10] m/s for our studies of network behaviour under malicious attacks.

The difference between random attacks and centrality-based attacks with window sizes of 10 s are presented in Figure 6.

The overall PDR degrades with the increased number of simultaneous node attacks. The maximum difference between random and centrality-based attacks are approximately 0.1 for the AODV routing protocol and 0.05 for the OLSR routing protocol, which account for about 14% of the baseline PDR without node failures. DSR (dynamic source routing) and DSDV (destination sequenced distance-vector) routing protocols exhibit a completely different behaviour from AODV and OLSR. Almost no difference can be observed between random and centrality-based attacks. Although both AODV and DSR are on-demand routing protocols and have similar route discovery mechanisms, DSR exploits route caching more aggressively than AODV. For each source–destination pair, DSR maintains multiple routes while AODV occupies only one entry. Therefore, when a node with high centrality value fails, DSR can discover an alternative path and perform re-routing more quickly than AODV that makes attacks toward high-centrality and random node almost indistinguishable. Futhermore, AODV uses a timer in its routing table maintenance which might make it slow to update a number of broken links caused by high-centrality node teardown. The OLSR routing protocol starts route rediscovery from the neighbouring nodes. Due to its optimised forwarding mechanism using MPR (multipoint relays), it takes a long time to fix the broken paths caused by high-centrality nodes. In the DSDV routing protocol, since up-to-date routes between all source-destination pairs are available at all times, the routing algorithm is greedy enough to overwhelm the impact of the attacks on a high-centrality node. Another explanation is that since both DSDV and DSR routing buffer the packets when no route to destination is available, less packet drop occurs due to broken links [26].

Network performance is about the same when perturbed as a result of attacks based on three centrality metrics, even though these metrics indicate different measures in the network. The minor differences between attacks based on different centrality metrics can be examined by studying special cases in the future. One point to note is that in a highly-connected network environment, when each node has numerous neighbours as relay nodes to the destinations, the difference between network behaviour under random attack and centrality-based attacks is negligible due to the greedy routing algorithm. However, high network connectivity usually comes with high cost and might not be a representative of most network deployments.

B. Area-based Challenges

To model area-based challenges, we use polygons and circles representative of large-scale disasters as discussed previously. Instantaneous PDR is used to measure the steady state performance of wireless networks under challenges.

1) Moving Polygon: We simulate the attenuation effect of a rainstorm in a fixed wireless backbone network. The topology consists of 16 stationary nodes in a square mesh structure with link distance between each pair of nodes being 1000 m. Each node is both the CBR traffic source and sink. We measure the network performance during a simulated rainstorm [17], which is modelled as an 8-sided polygon shown in Figure 7. At 60 s, the challenge starts moving across the topology at 100 m/s horizontally.

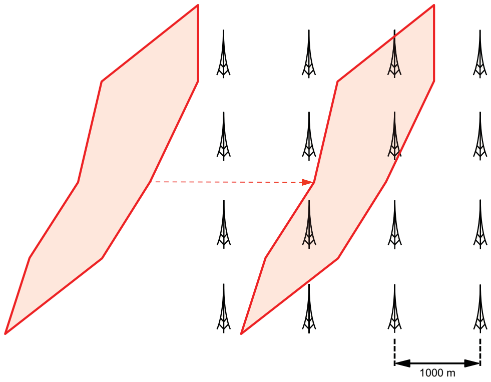


Fig. 7. Moving polygon with simulation topology

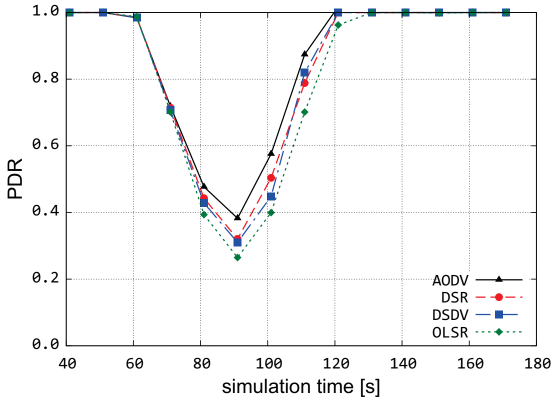


Fig. 8. PDR for moving polygon

As the challenge moves across the network, it experiences loss due to the effect of the storm as shown in Figure 8. During the challenge scenario, well-known MANET routing protocols behave similarly, with the AODV routing protocol performing slightly better. The severe degradation due to the large-scale effect of weather disruption can be observed from 82 to 86 s as the network is partitioned. The mesh network experiences maximum degradation of service by approximately 75% during this period. As the rainstorm moves away from the topology, routing reconverges back to normal operation.

2) Scaling Circle: We place an impairment at the center of the simulation area to model a scaling circle form of area-based challenge. The scenario is illustrative of an electromagnetic pulse (EMP) attack [27]. The challenge is applied starting at 110 sec, with initial radius of the circle being 10 m. The circle is scaling linearly by 10 m every 5 seconds. The topology consists of 20 mobile nodes with a 5 neighbour count moving according to the Gauss-Markov mobility model with each node's speed given by a uniform random variable range [10, 20] m/s. All the nodes are sources of CBR traffic as well as sinks. As expected, the PDR decreases as the area covered by the impairment increases. The AODV routing protocol achieves significantly higher PDR since it has a higher baseline

PDR. As the challenge itself grows, so does its impact on the performance of the network.

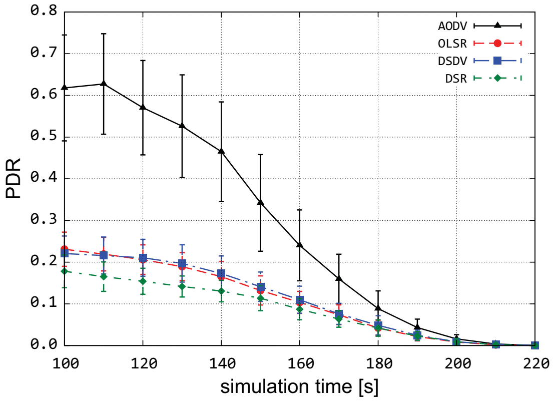


Fig. 9. PDR for scaling circle challenge

VI. Conclusions and Future Work

In this paper, we presented comprehensive modelling of attacks and challenges on MANETs. We modelled time-varying MANETs as a link availability matrix by aggregating evolving graphs into a static graph. We demonstrated that routing protocols behave differently under malicious attacks and DSR and DSDV routing protocols in the ns-3 implementation are more resilient under centrality-based attacks. Three centrality metrics exploited as node significance indicators are more accurate within a relatively short time window. For large-scale challenges, we simulated a rainstorm using moving polygon and network performance severely degrades due to multiple channel failures. Future work includes a detailed analysis of cached and uncached routing protocols' behaviour under malicious attacks and determining MANET scenarios for which malicious attacks are significantly more disruptive than random failures. Directed graphs could be used to model asymmetric networks. Energy constraints for each mobile node and other mobility models will be considered when modelling the network. Combined centrality metrics might provide a more precise indication of node significance than single metric. Other graph metrics might be used to measure and study MANETs properties. Furthermore, we intend to provide a comprehensive model of challenges and attacks in heterogeneous (wired and mobile ad hoc) networks.

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 *ACM WiSE*, (Atlanta, GA), pp. 31–40, 2002.

[3] E. K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. P. G. Sterbenz, "A comprehensive framework to simulate network attacks and challenges," in *IEEE/IFIP RNDM*, (Moscow), pp. 538–544, October 2010.

[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," *Springer Telecommunication Systems*, pp. 1–16, 2011. Published online: 21 September 2011.

[5] D. Zhang, S. A. Gogi, D. S. Broyles, E. K. Çetinkaya, and J. P. Sterbenz, "Modelling malicious attack in MANETs," in *Great Plains Graduate Student Network Research Summit*, (Kansas City, MO), May 2012. Extended Abstract.

[6] D. Zhang, S. A. Gogi, D. S. Broyles, E. K. Çetinkaya, and J. P. Sterbenz, "Modelling Wireless Challenges," in *ACM MobiCom*, (Istanbul), August 2012. Extended Abstract.

[7] 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.

[8] 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*, pp. 9–14, September 2011.

[9] T.-H. Kim, D. Tipper, P. Krishnamurthy, and A. Swindlehurst, "Improving the topological resilience of mobile ad hoc networks," in *IEEE DRCN*, pp. 191–197, October 2009.

[10] M. Gardner and C. Beard, "Evaluating geographic vulnerabilities in networks," in *IEEE International Workshop on Communications Quality and Reliability (CQR)*, pp. 1–6, May 2011.

[11] A. Ferreira, "Building a reference combinatorial model for MANETs," *IEEE Network*, vol. 18, no. 5, pp. 24–29, 2004.

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

[13] 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.

[14] I. Chatzigiannakis, A. Kinalis, G. Mylonas, S. Nikoletseas, G. Prasinos, and C. Zaroliagis, "Trails, a toolkit for efficient, realistic and evolving models of mobility, faults and obstacles in wireless networks," in *ANSS '08*, pp. 23–32, April 2008.

[15] I. Chatzigiannakis, G. Mylonas, and S. Nikoletseas, "Modeling and evaluation of the effect of obstacles on the performance of wireless sensor networks," in *ANSS '06*, April 2006.

[16] T. K. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A Survey of Various Propagation Models for Mobile Communication," *IEEE Antennas and Propagation Magazine*, vol. 45, no. 3, pp. 51–82, 2003.

[17] A. Jabbar, J. P. Rohrer, A. Oberthaler, E. K. Çetinkaya, V. Frost, and J. P. G. Sterbenz, "Performance comparison of weather disruption-tolerant cross-layer routing algorithms," in *IEEE INFOCOM*, (Rio de Janeiro), pp. 1143–1151, April 2009.

[18] A. Casteigts, P. Flocchini, W. Quattrociocchi, and N. Santoro, "Time-varying graphs and dynamic networks," in *ADHOC-NOW*, vol. 6811 of *LNCS*, pp. 346–359, Paderborn: Springer, 2011.

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

[20] 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.

[21] M. E. J. Newman, "Scientific collaboration networks. ii. shortest paths, weighted networks, and centrality," *Phys. Rev. E*, vol. 64, no. 1, p. 16132, 2001.

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

[23] "CGAL, Computational Geometry Algorithms Library." http://www.cgal.org.

[24] B. Liang and Z. Haas, "Predictive distance-based mobility management for PCS networks," in *IEEE INFOCOM*, vol. 3, pp. 1377–1384, Mar. 1999.

[25] S. Kurkowski, T. Camp, and M. Colagrosso, "MANET simulation studies: the incredibles," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 9, no. 4, pp. 50–61, 2005.

[26] J. Broch, D. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," *ACM/IEEE MobiCom*, pp. 85–97, Oct 1998.

[27] "Report of the commission to assess the threat to the United States from electromagnetic pulse (EMP) attack," report, Critical National Infrastructures, 2004.