Modelling Wireless Challenges

Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles,
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, santoshag, dbroyl01, ekc, jpgs}@ittc.ku.edu

ABSTRACT

A thorough understanding of the network behaviour when exposed to challenges is of paramount importance to construct a resilient MANET (mobile ad hoc network). However, modelling mobile and wireless networks as well as challenges against them is non-trivial due to dynamic and intermittent connectivity caused by channel fading and mobility of the nodes. We treat MANETs as time-varying graphs (TVGs) represented as a weighted adjacency matrix, in which the weights denote the link availability. We present how centrality-based attacks could affect network performance for different routing protocols. Furthermore, we model propagation loss models that represent realistic area-based challenges in wireless networks.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Network topology, Wireless communication*; G.2.2 [**Discrete Mathematics**]: Graph Theory—*Graph labeling*; I.6.5 [**Simulation and Modeling**]: Model Development—*Modeling methodologies*

General Terms

Algorithms, Performance, Reliability, Security

Keywords

MANET routing, ns-3 simulation, time varying graphs, mobile wireless network challenges, resilience, survivability

1. INTRODUCTION

The performance of mobile and wireless networks suffer due to dynamic and intermittent connectivity resulting from channel fading and mobility of the nodes. Furthermore, some MANET (mobile ad hoc network) environments suffer from the constraint of limited energy and unpredictable propagation delays due to distance or episodic connectivity [8]. Hence, it is complex to model these networks as well as the challenges against them. In order to construct a resilient wireless network, we need to understand network behaviour in the face of various challenges [7]. Furthermore, understanding the network behaviour under perturbation can help devise Future Internet architectures [4].

MobiCom'12, August 22–26, 2012, Istanbul, Turkey.
ACM 978-1-4503-1159-5/12/08.

We model MANETs as TVGs (time-varying graphs) and pairwise node interactions are aggregated within a certain time window. The network can be represented as a weighted adjacency matrix, in which the weights refer to the 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. 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 [4]. In this extended abstract, we present our ongoing efforts to model attack- and area-based challenges that disrupts communication in mobile and wireless networks.

2. 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 [2]. 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 called 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 called the latency function that indicates the time needed to traverse a certain edge E. 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 for the cases investigated here.

The *footprint* of a TVG $\mathcal{G}$ from t_1 to t_2 can be represented as a static graph $G^{[t_1,t_2)} = (V, E^{[t_1,t_2)})$ such that $\forall e \in E, e \in E^{[t_1,t_2)} \Leftrightarrow \exists t \in [t_1, t_2), \rho(e, t) = 1$ [2]. 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. 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.

3. MODELLING CHALLENGES

We model three types of network challenges: non-malicious, 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 degradation. For area-based challenges, we exploit moving impairments of varying size and shapes to model certain large-scale disasters that impact a wide area. We use the ns-3 version 3.13 as our simulation tool [1]. We have developed a new propagation loss model, `MovingPropagationLossModel` in ns-3, which includes a mobility model parameter and range of influence to manipulate the communication in a wireless network [4, 3].

3.1 Malicious Attacks

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, where the link weights represent link availability between node pairs. Next, we calculate three atemporal metrics (degree, betweenness, and closeness centrality) of the weighted graphs [6]. We employ them as the node significance indicators and model attacks 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.

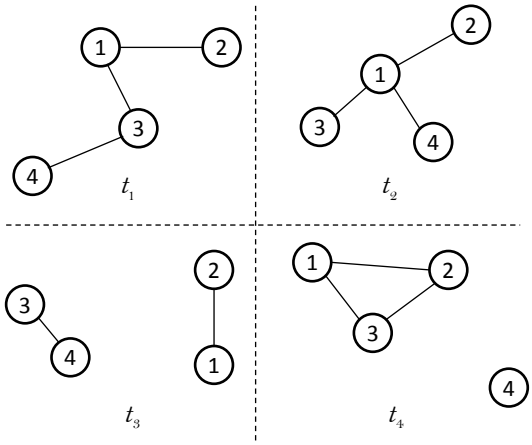

Figure 1: MANET topology at four time steps

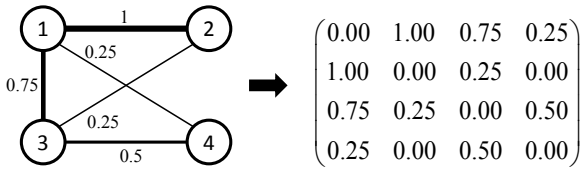

Figure 2: Pairwise link availability in a matrix

An adjacency matrix representing the instantaneous topology can be obtained in each time step. 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 1 presents MANET topologies at four consecutive time steps and Figure 2 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.

3.2 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]. 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.

4. SIMULATION ANALYSIS

The simulation consists of two major parts. In the malicious attack model, we assume the channel strength 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 challenges.

4.1 Malicious Attacks

We select a scenario with node number of 20 and node speeds given by uniform random variable in the interval of [5, 10] m/s for our studies of network behaviour under malicious attacks using the Gauss-Markov mobility model.

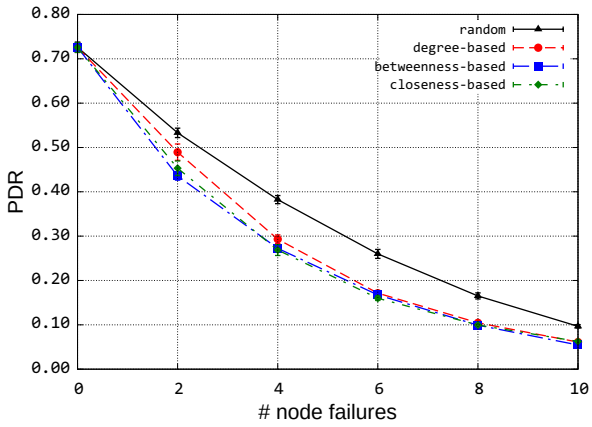

Figure 3: Random and malicious attacks

The difference between random attacks and centrality-based attacks for the AODV routing protocol with window sizes of 10 s are presented in Figure 3. The overall PDR degrades with an increased number of simultaneous node attacks. The maximum difference between random and centrality-based attacks are approximately 0.1 for AODV. PDR decreases resulting from the attacks based on three centrality metrics are close to each other generally, even

though they play different roles in the network. The minor differences between attacks based on different centrality metrics can be examined by studying special cases in the future. In a *highly-connected* network environment, 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.

4.2 Area-based Challenges

We measure the network performance during a simulated rainstorm [5], which is modelled as an 8-sided polygon shown in Figure 4. 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.

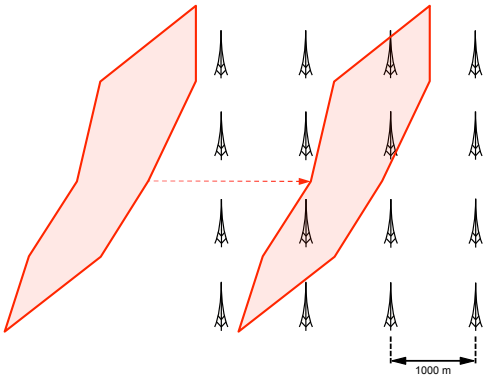

Figure 4: Moving polygon challenge scenario

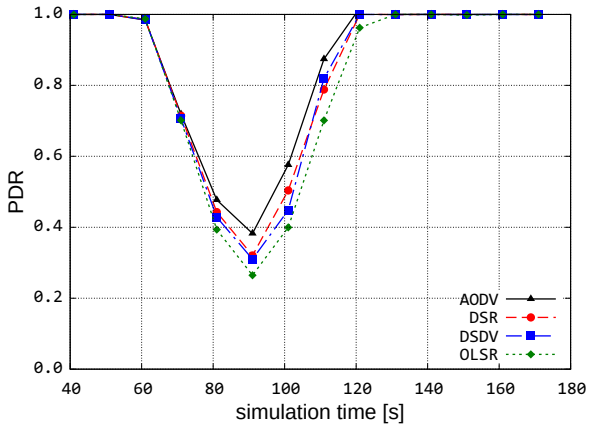

Figure 5: PDR for moving polygon

As the challenge moves across the network, it experiences loss due to the effect of the storm as shown in Figure 5. 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 backbone network experiences maximum degradation of service by approximately 75% during this period. As the rainstorm moves away, the routing reconverges to provide full services.

5. CONCLUSIONS AND FUTURE WORK

We modelled time-varying MANETs as a link availability matrix by aggregating evolving graphs into a static graph. 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 a moving polygon and network performance severely degrades due to multiple channel failures. We will investigate combined centrality metrics that might provide a more precise indication of node significance than single metric as part of our future work, and examine the impact of mobility and node density.

Acknowledgments

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).

6. REFERENCES

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

[2] A. Casteigts, P. Flocchini, W. Quattrociocchi, and N. Santoro. Time-varying graphs and dynamic networks. In *ADHOC-NOW*, volume 6811 of *LNCS*, pages 346–359. Springer, Paderborn, 2011.

[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 *Proceedings of the 2nd IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 538–544, Moscow, 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*, pages 1–16, 2011. Published online: 21 September 2011.

[5] 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*, pages 1143–1151, Rio de Janeiro, April 2009.

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

[7] 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*, 54(8):1245–1265, 2010.

[8] 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)*, pages 31–40, Atlanta, GA, 2002.