Poster: Attack Survivability Prediction

Jaime C. Acosta (Project Lead)
U.S. Army Research Laboratory
White Sands Missile Range, NM 88002–5513
http://www.jaimeacosta.info/

Brenda G. Medina (Project Member)
U.S. Army Research Laboratory
White Sands Missile Range, NM 88002–5513

I. Introduction

Survivability analysis focuses on the ability of network entities to function during incidents such as attacks. Currently, testing survivability of mobile ad hoc networks consists of running scenarios with several configurations, often thousands, to obtain an understanding of the impacts of an attack. This process is very latent, choice of configurations are subjective or random, and results do not generalize to different scenarios.

Focusing on these problems, our work-in-progress is towards a previously unexplored field of research: efficient attack survivability analysis via machine learning and an attacker-centric network representation. Using a collected dataset, we provide some evidence showing that the network representation is suitable for creating an attack survivability predictor.

II. Mobile Ad Hoc Network Evaluation

As the capabilities of wireless technologies increase, so do the capabilities of mobile devices, and as a result, the development of more advanced mobile systems is made possible. Mobile ad hoc networks (MANETs) are systems that enable wireless entities to communicate over long distances without the need for centralized management. MANETs are designed to adapt to environmental changes and require low maintenance. MANETs have numerous applications spanning many diverse fields; these applications include military field exercises, intelligent transportation, environmental monitoring, and others [1]. As a trade-off to flexibility and self-management, these systems are vulnerable to a wide range of network attacks. Therefore, security evaluation is a critical step in the design of these networks.

Field testing is not conducted until a system has undergone extensive laboratory evaluation. For very small systems with limited capabilities, visual inspection may satisfy limited analysis requirements. Some research has attempted to use formal methods to prove a syste of very small and limited-capability systems.

In most cases, the evaluation methods of choice are simulation or emulation. These methods involve developing scenarios that represent the environment where the mobile systems will be used. This includes instituting security measures such as secure routing protocols, trust management, encryption at multiple network layers, and others. Threat is then introduced into the scenario and general measures of performance (throughput, goodput, delay) are produced, e.g., [2], [3]. Simulation and emulation are not perfect. These methods produce results that are specific to a given scenario and do not generalize. For this reason, analysts run thousands of scenarios and vary parameters associated with threat (attack node, duration, attack types, etc.). These parameters are mostly chosen at random; therefore, there is a lack of scientific backing for the process and results. In addition, while emulation is more accurate than simulation, emulation takes much longer.

We hypothesize that by representing a network from an attacker's perspective, it is possible to create a predictor to determine communication survivability from attacks. In this paper, we describe our methodology, some preliminary results, and we conclude with future directions.

III. Methodology

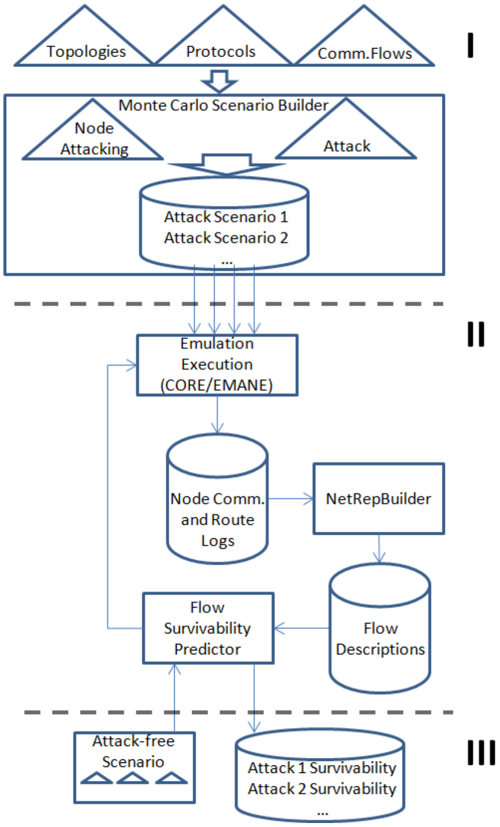

Fig. 1. Survivability Prediction Workflow

Figure 1 shows our envisioned workflow. The monte carlo method is used with various parameters (triangles) to generate scenarios. During scenario execution, for each node, communication and route information is stored and later converted to flow descriptions. These flow descriptions (training set) are then used to build the Flow Survivability Predictor (I and II in Figure 1). A new scenario is then executed once to produce its flow descriptions. The predictor can then answer what will happen if any node issues any attack in the training set for the new scenario (II and III in Figure 1).

IV. Network Representation

Previous representation models are only capable of describing very limited systems. Part of the reason is that their representation of large systems leads to state-space explosion.

To avoid this, instead of representing the network as a collection of source and destination IP addresses, the distances (hops) from the attacker's location are used along with a few other flow description parameters. Figure 2 shows an example of this. In the sample, there are two flows: a flow from node n1 to n3 and from n3 to n4 (denoted by dashed lines). From the attacker's view, the n1 to n3 flow is seen as hop (1) to hop (1). This flow passes through the attacker. The n3 to n4 flow is seen as hop (1) to hop (2) with no passthrough.

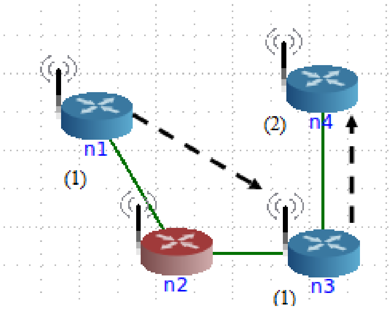

Fig. 2. Representation by hops. Hop counts are labeled in parentheses and dashed lines show traffic flows.

A preliminary list of the flow description parameters used for a preliminary analysis are shown in Table I.

TABLE I
Preliminary Flow Description Parameters

No.	Attribute	Description
1	fromHop	Hops from attacker node to source.
2	toHop	Hops from attacker node to destination.
3	dataType	Packet type (TCP, UDP)
4	distanceTraveled	Hops from source to destination.
5	passthrough	Flow passes through the attacker.
6	srcIsSpoofed	Source address spoofed by attacker.
7	destIsSpoofed	Destination is spoofed by attacker.
8	attackName	Spoofing or forwarding.
9	duringFlowLost	Flow is lost during an attack.

V. Preliminary Analysis

We defined a process to determine the feasibility of using a predictor, trained using the network representation described above, for evaluation. Specifically, we wanted to determine if the network representation is capable of reliably and consistently capturing effects of attacks. In our testing environment we used Unix and Python scripts for the majority of processing.

A. Dataset

We used CORE [4] to execute scenarios. Parameters for the monte carlo method included three 10-node topologies (cycle, connected grid, and two-centroid). Routing protocols used were Quagga's OSPFv3MDR and NRL's OLSR. Two attacks were implemented, namely spoofing and data forwarding, which are well-known in the security community [5]. We used round-robin to select attacking nodes.

B. Observations

Using parameters 1–8 from Table I, we stored the duplicate flow descriptions that resuled from the emulation executions. Next, we took the duplicates and counted how many had conflicting values for the *duringFlowLost* parameter. In all cases, there were less than 10% conflicting (see Table II).

TABLE II
Flow Description Counts

Protocol	Attack	Total	Unique	Conflicts
OLSR	Data Forwarding	448	443	0
	Spoofing	4407	119	11
OSPF	Data Forwarding	443	42	0
	Spoofing	4384	126	4

Overall, these results provide some evidence that the network representation is adequate and can be used to build a system for predicting effects of attacks on traffic flows.

VI. Future Work

As future work, we will look into generating a richer set of flow-parameters that will decrease conflicts and then we plan to build and evaluate a predictor. We will also test with a more comprehensive dataset consisting of mobile nodes and more traffic types (TCP, ICMP, VPN, etc.) and routing protocols.

References

[1] J. Yi, "A survey on the applications of manet," *Architecture*, 2008.

[2] K. Kim, B. Roh, Y. Ko, W. Choi, and E. Son, "Survivability measure for multichannel manet-based tactical networks," in *Advanced Communication Technology (ICACT), 2011 13th International Conference on*. IEEE, 2011, pp. 1049–1053.

[3] J. Wang and Z. Yu, "Research on quantitative analysis model of manet survivability," in *Electrical and Control Engineering (ICECE), 2011 International Conference on*. IEEE, 2011, pp. 2506–2510.

[4] J. Ahrenholz, C. Danilov, T. Henderson, and J. Kim, "Core: A real-time network emulator," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*. IEEE, 2008, pp. 1–7.

[5] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," *Wireless Network Security*, pp. 103–135, 2007.