A SIMULATOR OF A MOBILE AD-HOC NETWORK IN A HOSTILE ENVIRONMENT

Davide Cannone[1], Maurizio Naldi[1], Giuseppe F. Italiano[1] and Andrea Brancaleoni[2]
[1]*Dipartimento di Informatica Sistemi Produzione, Università di Roma Tor Vergata, Via del Politecnico 1, 00133 Rome, Italy*
[2]*Elettronica SpA, Via Tiburtina Valeria Km 13,700, 00131 Rome, Italy*

Keywords: Mobile ad-hoc networks, Cyber-warfare.

Abstract: Mobile Ad-Hoc Networks (MANETs) allow to connect mobile devices in the absence of any fixed communications infrastructure. The routing function may be disrupted under cyber-attacks. We have developed a network simulator, based on the publicly available platform Ns2, to evaluate the performance of a number of routing protocols in MANETs under cyber attacks. For two simulation scenarios, considering respectively Denial of Service and Fabrication attacks, and Impersonation and Interception attacks, the Fisheye State Routing protocol and the Zone Routing Protocol exhibit the best performance.

1 INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are wireless networks where the nodes are mobile and play both the role of endnodes and routers, and no fixed infrastructure exists. The topology is continually changing because of the movements of nodes, which create new radio links and break existing ones. Each node relies on the cooperation of other nodes to have its packets delivered to destination. Such networks have their main application domain in harsh environments, such as rescue operations or military battlefields.

MANETs are however prone to a number of problems: radio links may break, so that connectivity is not guaranteed, and are anyway prone to eavesdropping and jamming/spoofing attacks. A relevant field of analysis, especially for military applications, is the robustness of MANETs to cyber-attacks. However, so far only a few researchers have analysed the performance of MANETs in a hostile environment (Cole et al., 2005; Abdelhafez et al., 2007).

Our aim is to analyse the operations of a MANET in a tactical context, where the mobile nodes are exposed to cyber-attacks on the battlefield. We have chosen a simulation approach, which allows us to model a wide variety of scenarios. Our simulator is based on the open NS2 platform (Issariyakul and Hossain, 2009), relying in turn on C++ and OTcl (Object-oriented Tool Command Language). The main feature of our simulator are its focus on cyber-attacks (an issue so far neglected in most analyses) and its capability to simulate the full protocol stack. In this paper we provide an overview of the first version of the simulator, and report early results on use of the simulator to analyse the resilience of a MANET to cyber-attacks in the battlefield.

The paper is organized as follows. In Section 2 we provide a macro view of the simulator's structure, and then we devote Sections 3-4 to the most relevant modules of the simulator. In Section 5 we describe the different kinds of cyber-attacks. In Sections 6 and 7, where we describe respectively the simulation scenario and the simulation results.

2 THE STRUCTURE OF THE SIMULATOR

Our analysis relies on the use of a simulator, for whose development we have used the NS2 platform. We have used a modular architecture, where every module incorporates models for a different aspect of MANET operations, to achieve customizability, reusability (every module is written in C++, to port functions to other applications with little or no changes), maintainability (problems due to new modules are easier to isolate and fix when the core is stable), and extensibility (we can add new features just by adding new modules).

A major feature of our simulator is the capability to simulate all the layers of the Internet Protocol

Cannone D., Naldi M., F. Italiano G. and Brancaleoni A..
A SIMULATOR OF A MOBILE AD-HOC NETWORK IN A HOSTILE ENVIRONMENT.
DOI: 10.5220/0003600304130417
In *Proceedings of 1st International Conference on Simulation and Modeling Methodologies, Technologies and Applications* (SIMULTECH-2011), pages 413-417
ISBN: 978-989-8425-78-2

Suite. Namely, we start from the physical layer (by simulating the radio link) and go all the way up to the Application Layer. The network layer uses IPv4, while both TCP and UDP can be used for the Transport Layer. The modules that have been developed specifically for this simulator currently cover the following aspects: mobility, physical layer, routing, and threats.

In addition, special care has been taken to allow a vivid representation of the simulator's output, a lacking feature in NS2 (Kurkowski et al., 2005b). For that purpose, in addition to using the Tcl/TK-based built-in animation tool Nam, we have resorted to iNSpect, a C++ OpenGLbased visualization tool that allows animation of wireless networks (Kurkowski et al., 2005a).

3 MOBILITY MODELS AND CONNECTIVITY

A key characteristic of a MANET is the mobility of its nodes. A number of models have been proposed in the literature, which suit different situations (Camp et al., 2002). In the military context the nodes are physically located aboard tanks or other military vehicles, and we expect them to move quite orderly, with all the vehicles following a group leader.

For that purpose we use a hierarchical mobility model, where we first describe the model of the set of vehicles (hence of nodes) as a group, and then the movement of individual nodes with respect to the group. We have adopted the Reference Point Group Mobility Model (RPGM) for the relationship between the group movement and the individual movements (Hong et al., 1999), the Random Waypoint model for the group as a whole (Broch et al., 1998), and a random walk for the movement of each individual node with respect to its reference position.

The connectivity between any two nodes keeps changing because they move and the radio link between them may break. The network is fully connected if any pair of nodes is connected through at least one chain of wireless links. In the current version of the simulator we consider a wireless link to exist if the two following conditions are satisfied:

1. Positive power budget on the link connecting the transmitter and the receiver;
2. Distance between transmitter and receiver lower than the radio horizon.

In order to assess the first condition, we have employed the Egli propagation model, a refinement of the inverse fourth-power model through a multiplicative term that reduces the received power proportionally to the square of the operating frequency (Parsons, 2000).

4 MAC AND ROUTING PROTOCOLS

After having defined both the kinetic characteristics of mobile nodes and the conditions for the existence of radio links among them in Section 3, we now consider the functions pertaining to Layers 2 and 3 of the ISO/OSI protocol stack, namely the MAC (Medium Access Control) and routing protocols.

For the MAC protocol we have chosen the IEEE 802.11 protocol (Crow et al., 1997), since it is the most widely used for MANETs and has been fully standardized.

As to the routing protocol, we have considered the following selection of routing protocols:

- Destination-Sequenced Distance-Vector (DSDV);
- Ad-Hoc On-Demand Distance Vector (AODV);
- Dynamic Source Routing (DSR);
- Zone Routing Protocol (ZRP);
- Fisheye State Routing (FSR).

Two of them are proactive protocols (DSDV and FSR), two are reactive (AODV and DSR), and one is hybrid (ZRP).

5 THREAT MODELS

We wish to study the performance of a MANET in a hostile enviroment, where adversaries aim at downgrading the performance of the network. A taxonomy of cyber attacks in MANETs has been consolidated in (Djenouri et al., 2005). In this section we describe our threat models.

In the current version of our simulator we assume that an adversary can take control of one or more friendly nodes, replacing them with a malicious node. Malicious nodes are at least as computationally strong as the friendly ones; they are able both to send packets (*fake* packets) and to receive them (*intercepted* packets), and may cooperate to attack the system, by communicating on a reserved wireless channel. On the other hand, friendly nodes cannot detect malicious nodes and organize a defense.

We grouped cyber attacks in four main categories (see Figure 1, where nodes marked with a X represent

malicious nodes, and dotted lines represent communication channels with a malicious node):

- *Denial of Service.* The adversary overloads the network, so that it begins to misbehave. In our simulator this attack is simulated by replacing a friendly node with a malicious one, with the malicious node sending a costant flow of messages towards a target friendly node.
- *Fabrication.* The attacker fabricates and sends spurious messages. In our simulator this attack is simulated by inserting a malicious node near a friendly one and tagging as *fake* all the packets sent by that node.
- *Interception.* The attacker does not interfere with the network operations, but eavesdrops packets. In our simulator this attack is simulated by tagging a friendly node and all the incoming packets as *intercepted*.
- *Impersonation.* The attacker mimics a target node, intercepting its messages and sending packets signed by it (a.k.a. Man in the Middle). In our simulator this attack is simulated by replacing a friendly node with a malicious one, and tagging all the packets sent as *fake*, and all the incoming packets as *intercepted*.

In order to evaluate the impact of a cyber attack against the system under investigation, we compute the percentage of the overall *fake* packets received by any friendly node, and the percentage of the overall packets *intercepted* by the adversary. Both are measured at the routing layer.

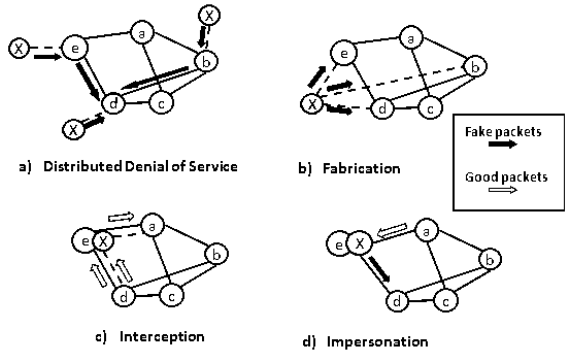

Figure 1: Threats models.

By varying properties of these four attacks and combining them, we can represent a number of different attacks. For example, in the *Impersonation* attack, when the malicious node does not fabricate any fake packet, this can represent a sinkhole attack (Karlof and Wagner, 2003).

Table 1: Number of malicious nodes in the two scenarios.

	Creation Scenario	**Listening Scenario**
DoS Fixed/Mobile	1/2	1/0
Fabric. Fixed/Mobile	0/2	1/0
Impers. Fixed/Mobile	1/0	2/0
Interc. Fixed	0/1	1/2

6 THE SIMULATION SCENARIOS

In order to test our simulator we have defined a realistic simulation scenario. We assume that the geographical enviroment is nearly flat (there are no relevant obstacles either for movements or signal propagation) and the nodes move within a square region with sides of 10 kilometers. There are 15 nodes, either fixed or mobile. The fixed nodes represent base station, located at 2.5 meters above the ground and with random position. The mobile nodes represent slow vehicles at ground height, with speeds uniformly distributed between 20 km/h and 40 km/h; they move in groups of two, starting from a random position, and following the RPGM mobility model with a random pause ranging between 4 and 10 seconds.

Every node communicates through bidirectional wireless channels. The transmitter has a power of 30 W, at the frequency of 900 MHz, and uses an omnidirectional antenna. The receiving threshold has been set so that any two nodes are connected if their distance is lower than 2 km.

Any node can generate traffic network towards any other node: the network traffic matrix has random entries, with every flow having a probability of 50% to exist. Every node spawns packets with an average size of 1000 bytes according to an On/Off process with exponential distributions for both On and Off times, and an average rate of 1 Mbit/s.

We have defined two scenarios of cyber attacks (see Table 1), named *Creation Scenario* and *Listening Scenario*. The former is an aggressive attack against the network, composed mostly of malicious nodes performing Denial of Service and Fabrication attacks. The latter is instead composed mostly of malicious nodes performing Impersonation and Interception attacks.

7 SIMULATION RESULTS

Both attack scenarios were simulated as ten replicas of 1000 seconds each. In Figure 2 we report the re-

Table 2: Simulation results in the Creation/Listening Scenario.

Parameter	AODV	DSR	DSDV	FSR	ZRP
Avg. connectivity (%)	79.97/83.27	91.40/89.83	83.84/90.90	94.17/88.01	81.37/94.18
Avg. goodput (kbps)	250.64/315.42	240.26/275.73	206.99/359.25	220.21/361.98	263.05/299.72
Pkt delivery ratio (%)	95.14/94.02	94.13/87.63	96.07/96.63	96.32/96.67	95.22/95.27
Avg delay (ms)	231.2/190.3	350/271	162.7/162.1	169.7/166.8	165.2/161.7
Interc. packets (%)	2.95/12.83	1.12/11.24	7.05/17.01	5.72/13.23	4.57/13.64
Fake packets (%)	37.54/0.94	15.09/0.82	43.25/0.67	22.69/0.43	14.85/1.29

sults. Next we comment the results separately for each metric.

The goodput (expressed in kbps) is the amount of useful data received in the time unit, excluding routing information and duplicates. As we can expect, the goodput is worse in the Creation Scenario than in the Listening Scenario (even with a 42% reduction in goodput for DSDV), while DSR e ZRP have similar performance under the two attack scenarios, with a goodput reduced by about 12.5%. Reactive protocols have better goodput values than proactive protocols in the Creation Scenario: the routing information in reactive protocols becomes quickly obsolete, and nodes get new information as soon as they issue new requests, while in proactive protocols nodes trust their routing tables until the next information exchange. The performance of the ZRP protocol is not bad, probably thanks to its hybrid nature.

The delay (expressed in milliseconds) is the time between the sending of a message and its complete reception by its recipient. We see that the average delay is generally larger in the Creation Scenario than in the Listening case. However, the growth is appreciable in AODV and DSR (nearly 30%), but negligible for the other three protocols. It addition, we note that proactive protocols have an average delay lower than reactive protocols (penalized by the Route Discovery mechanism), with performances of DSDV a little better than FSR and ZRP.

The percentage of intercepted packets is the ratio of all intercepted packets received by malicious nodes, and the number of packets not tagged as fake. This metric represents the probability that the attacker gets routing information. It is strongly influenced by the routing protocol, in particular by the mechanism used by a node to share its own routing tables. Proactive protocols send their routing tables at regular intervals, and continuosly provide the attacker with up-to-date infos on the network status. That's the reason for the bad performance of DSDV. FSR and ZRP seem have a similar behavior in the number of packets sent to the attacker, with FSR slightly better than ZRP, probably because the amount of shared data in FSR is inversely proportional to the distance of the recipient.

The percentage of fake packets is the ratio of all *fake* packets received by friendly nodes, and the number of packets received by friendly nodes (excluding packets received by malicious nodes). This metric represent the probability that a friendly node receives spoofed or corrupted packets. ZRP seems to have the best perfomances: a malicious node, that does not want to be detected and decides to show a routing behavior like a friendly node, will be limited in sending fake packets by the hop radius of ZRP.

8 CONCLUSIONS

We have developed a simulator for MANETs, based on NS2, and have evaluated its performances in a hostile enviroment through two scenarios that included attackers with different capabilities.

The results show that DSR performs badly in scenarios with large traffic, with DSDV being the second worst. DSDV exhibits a large percentage of *fake* and *intercepted*) packets, while FSR and ZRP have the best security performance. For the reference scenarios considered here, the hybrid protocol ZRP seems to be a good choice, though different values of the radius can led to very different results.

REFERENCES

Abdelhafez, M., Riley, G., Cole, R. G., and Phamdo, N. (2007). Modeling and Simulations of TCP MANET Worms. In *Proceedings of the 21st International Workshop on Principles of Advanced and Distributed Simulation*, PADS '07, pages 123–130.

Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y.-C., and Jetcheva, J. G. (1998). A performance comparison of multi-hop wireless ad hoc network routing protocols. In *MOBICOM*, pages 85–97.

Camp, T., Boleng, J., and Davies, V. (2002). A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502.

Cole, R., Phamdo, N., Rajab, M., and Terzis, A. (2005). Requirements on worm mitigation technologies in

MANETS. In *Principles of Advanced and Distributed Simulation, 2005. PADS 2005. Workshop on*, pages 207 – 214.

Crow, B., Widjaja, I., Kim, L., and Sakai, P. (1997). Ieee 802.11 wireless local area networks. *Communications Magazine, IEEE*, 35(9):116 –126.

Djenouri, D., Khelladi, L., and Badache, A. (2005). A survey of security issues in mobile ad hoc and sensor networks. *Communications Surveys & Tutorials, IEEE*, 7(4):2–28.

Hong, X., Gerla, M., Pei, G., and Chiang, C.-C. (1999). A group mobility model for ad hoc wireless networks. In *Proceedings of the 2nd ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, MSWiM '99, pages 53–60.

Issariyakul, T. and Hossain, E. (2009). *Introduction to Network Simulator NS2*. Springer.

Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, 1(2-3):293–315.

Kurkowski, S., Camp, T., and Colagrosso, M. (2005a). A visualization and animation tool for NS-2 wireless simulations: iNSpect. In *Proceedings of the 13th Annual Meeting of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, pages 503–506.

Kurkowski, S., Camp, T., and Colagrosso, M. (2005b). MANET simulation studies: the incredibles. *Mobile Computing and Communications Review*, 9(4):50–61.

Parsons, J. (2000). *The Mobile Radio Propagation Channel*. J. Wiley.