A MANET Simulator (M-SIM) with an Extended Worm Propagation Epidemic Model

Fredric M. Ham[1], Matthew Reedy[1], Attila Ondi[2], Richard Ford[2], William Allen[2] and Eyosias Imana[1]
[1]Florida Institute of Technology, Electrical and Computer Engineering Department
[2]Florida Institute of Technology, Computer Science Department

***Abstract* - An approach for the simulation of a mobile *ad hoc* network (MANET), as a TCP worm infiltrates the network, has been developed. The network simulator mimics the actual performance and protocols of a MANET while taking into account the payload size, channel bandwidth, initial infection probabilities, collisions, radio range, and routing protocols, as well as various other conditions. The simulator demonstrates the propagation of a TCP worm through the network using an extended epidemic model that allows the TCP worm to grow based on network conditions—topology, performance, protocols, etc.**

I. INTRODUCTION

A mobile *ad hoc* network (MANET) is a self-configuring network of mobile nodes connected over a wireless channel with an arbitrary dynamic topology. The MANET technology concept is an ideal network scenario for military applications in enemy territory or simply for relief efforts after disasters such as hurricane Katrina where an infrastructure is nonexistent, unavailable, or damaged. The dynamic network topology can be unpredictable and prone to change rapidly as the conditions in the wireless channel change. The MANET Simulator (M-SIM) which is developed in the Information Processing Laboratory (IPL) at Florida Institute of Technology mimics the physics of radio wave propagation and protocols of an actual mobile *ad hoc* network using the IEEE 802.11g protocols [1]. This simulator incorporates components from a freeware wireless network simulator available at [2].

The simulator is advantageous because it requires relatively less time to learn as compared to the other simulation packages such as OPNET and NS-2. Since it is an open source, modifying parameters, debugging processes and verifying results is straightforward. Most importantly, the versatile environment of MATLAB allows comfortable integration of computationally heavy algorithms such as Kalman Predictors and neural networks in order to study their application in ad hoc networks. In this paper, the simulator is integrated with a second order non-linear differential equation that describes the worm infection propagation in MANET. This equation is called the extended epidemic model [3].

This paper is organized as follows. Section II details the features included in M-SIM to model MANETs. This is followed by a brief description of the theoretical backgrounds of the Extended Epidemic Model. Section IV discusses the procedures followed to integrate the extended epidemic model with the M-SIM and Section V presents the results obtained from the research. Finally, Section VI concludes the paper by outlining the contributions of the research.

II. FEATURES OF M-SIM

The simulator runs in the MATLAB (including SIMULINK) environment and has the flexibility of using either of the two main MAC protocols of IEEE 802.11: Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA); or Request to Send / Clear to Send (RTS/CTS).

The simulator also employs free space radio propagation, two-ray radio propagation, and log-normal shadowing radio propagation based on the distance between receiving and transmitting nodes, as well as the network topology. The motion of nodes in the network is modeled by the random waypoint mobility model.

III. THE EXTENDED EPIDEMIC MODEL

The extended epidemic model [3] is developed to model the propagation of TCP worms with a low flow state in a MANET. It is incorporated into the MANET simulator to determine the probability of infection at a specific network node at a given time. The epidemic model is based on a differential equation that mathematically describes how the probability of infections increases as the network environment changes. The following is the differential equation that

978-1-4244-5827-1/09/$26.00 ©2009 IEEE

describes the growth of $i_n(t)$, the probability of infection for node *n*:

$$\frac{di_n(t)}{dt} = \beta(t)i_n(t)[N - i_n(t)] \qquad (1)$$

$$\beta(t) = \frac{\alpha b}{P_w(1+\pi d(r(1+c))^2 i(t)} \qquad (2)$$

where

$i_n(t)$ = probability of infection

$\beta(t)$ = growth rate

α = TCP throughput ratio

b = bandwidth of the radio channel (Bps)

P_w = payload size of the worm

d_n = nodal density (nodes/meter^2)

c = radio interference range factor

MATLAB® SIMULINK is used to integrate the second-order differential equation into the M-SIM. The integration of the two shows the movement of a worm between the nodes in the network with respect to time. The SIMULINK model for (1) is shown in Figure 1.

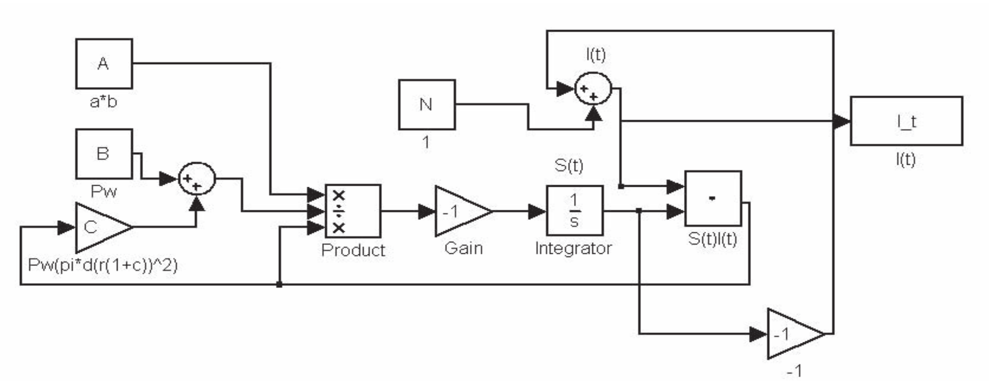

Figure 1 The SIMULINK model of the extended Epidemic Model given in Equation 1.

III. INTEGRATION OF THE EXTENDED EPIDEMIC MODEL INTO M-SIM

Integrating M-SIM with the extended epidemic model supports the stimulation of a TCP worm intrusion through the network. In this simulation, the probability of infection is related by success or failure of transmission. Hence, has a probability of infection greater than or equal to 0.5, it is assumed to be unresponsive to a transmission and the transmission attempt fails. Hence, for successful transmission, the receiver node should have probability of infection which is less than 0.5 in addition to being in the radio range of the transmitter node. If a node has reached the destination node, then the process is complete. If the message did not reach the destination node, then the process is repeated until the message reaches the destination node or is prevented from reaching the destination node by infected nodes. The flow chart in Figure 2 depicts the integration of the epidemic model into M-SIM.

VI. SIMULATION

The M-SIM yields a network topology and randomly disperses the *n* nodes throughout the topology and defines one node to be the initially infected node. The nodes in the network move within the square boundaries of the topology based on a *waypoint* movement or a random walk. Figure 3 shows a 20-node configuration with the initially infected node highlighted with a red cross.

Figure 3 describes the initial topology which ensures that all nodes are in radio range of each other. The number of nodes which desire to transmit is limited to five to stay consistent with the low-flow requirement.

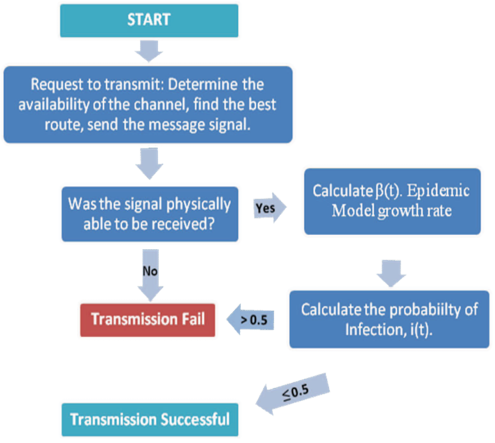
START
Request to transmit: Determine the availability of the channel, find the best route, send the message signal.
Was the signal physically able to be received?
Yes
Calculate β(t). Epidemic Model growth rate
No
Transmission Fail
> 0.5
Calculate the probabilty of Infection, i(t).
≤0.5
Transmission Successful

Fig. 2. Flow chart of the integration of M-SIM and the Epidemic Model

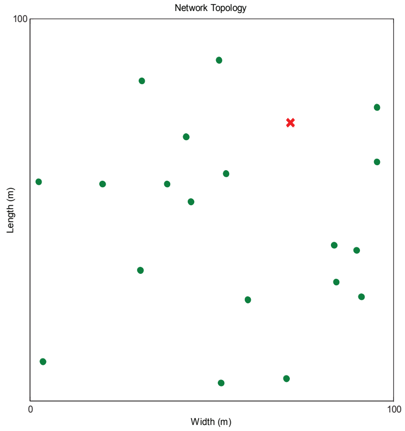

Fig. 3. MANET topology for 20 nodes with one node infected (shown in red)

The MANET simulator generates two important attributes for each node, the probability of infection, i(t), and the growth rate, β(t), that vary over the simulation time. Recalling (2), β(t), is defined by the prior probability of infection, network environment and the proximity to infected nodes. Figure 4 shows the growth rate, β(t), for Node 6 which illustrates how the probability of infection, i(t), grows.

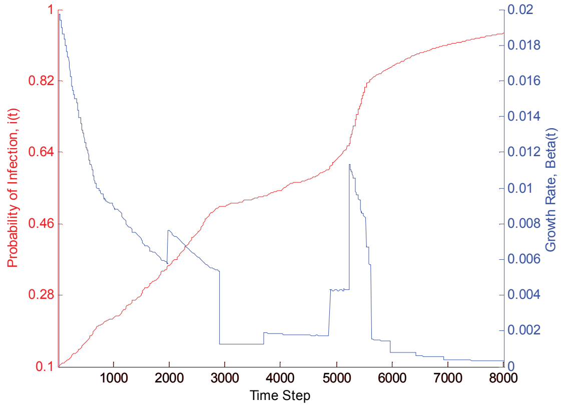

Fig. 4. Growth rate, β(t), in blue and the probability of infection, i(t), in red for Node 6.

V. RESULTS

The simulation took 2 hours and 16 minutes to run on a 2.2 GHz Intel Pentium (M) processor and 512MB of RAM. It also measures a simulation time of 2280.150 seconds. Sixteen of the 19 uninfected nodes attained a probability of infection which is greater than 0.5 during the simulation run. Table 1 shows the increase in probability of infection of the first 10 nodes at different stages of the simulation.

Table 1. The increase in probability of infection of nodes 1 to 10 at different stages of the simulation

Simulation Completion Percentage	Initial Conditions	15% Completion	30% Completion	45% Completion	60% Completion	75% Completion	90% Completion	100% Completion
Network Average	**0.0000**	**0.1824**	**0.2808**	**0.3632**	**0.4250**	**0.4809**	**0.5123**	**0.5279**
Node 1	0.0000	0.1417	0.1745	0.2034	0.2306	0.2672	0.3092	0.3342
Node 2	0.0000	0.1816	0.2772	0.4080	0.5063	0.5371	0.5440	0.5452
Node 3	0.0000	0.2128	0.3328	0.4729	0.5241	0.5619	0.5894	0.6045
Node 4	0.0000	0.2131	0.3353	0.4313	0.5101	0.5168	0.5683	0.5919
Node 5	0.0000	0.2155	0.3456	0.5034	0.5602	0.5986	0.6213	0.6342
Node 6	0.0000	0.2423	0.4193	0.5258	0.5916	0.5889	0.9170	0.9400
Node 7	0.0000	0.2331	0.3551	0.4821	0.5301	0.5671	0.5960	0.6116
Node 8	0.0000	0.1857	0.2516	0.2933	0.3465	0.3712	0.4045	0.4202
Node 9	0.0000	0.1335	0.1908	0.2531	0.3420	0.5139	0.5376	0.5494
Node 10	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

VI.CONCLUSIONS

The MANET simulator with worm intrusion was created by modifying an existing wireless simulator to MANET specifications with an incorporated mathematical equation to describe the worm propagation. The underlying growth of the worm through the network is dictated by β(t) in a second-order differential equation described in (1). The purpose of this MANET simulator is to produce data that can be dissected to explore how the worm propagates through the network and what makes a node more vulnerable to infection. Future work will involve these investigations and possibly others as well; for example, focusing on intrusion mitigation for real-world applications by employing mathematical tools such as neural networks, and Kalman filtering. These methods could be used to predict possible levels of node intrusion by extrapolating ahead in time the "state of the node." These advances in the simulator's capabilities will make it even more attractive to organizations such as the United States Army who are interested in the idea that MANETs can be safely deployed in a hostile environment. Specifically, the Army requires safe and secure implementation of wireless networks in a dynamic environment where data is crucial and the network requires an extremely robust architecture. A mobile *ad hoc* wireless network is ideal for this application. The MANET simulator presented here can yield insight into how the required level of security can be achieved, and thus, expands the technological tools that can be used to advance the development of MANETs.

Moreover, future work also includes the extending the simulator to include the features of the transport and network layer of ad hoc networks. This enables us to study the performance of different routing and security protocols relative to the defense algorithms being proposed in our research. In addition, to facilitate code reuse, code maintenance and future developments, we are planning to introduce modularity in the simulator by using the object oriented programming capabilities of MATLAB®.

ACKNOWLEDGMENT

This work was sponsored in part by the U.S. Army Research Laboratory under Cooperative Agreement W911NF-080200023.

REFERENCES

[1] IEEE Standards for Information Technology—802.11g, June 2003. LAN/MAN Standards Committee of the IEEE Computer Science Society.

[2] "Wireless Network Simulator in Matlab" 2006. University of Pennsylvania. 30 Aug 2008. http://wireless-matlab.sourceforge.net.

[3] Abdelhafez, Mohamed; Riley, George; Cole, Robert G.; Phamdo, Nam. "Modeling and simulations of TCP MANET worms." 2*007* Proceedings of the Workshop on Principles of Advanced and Distributed Simulation, PADS.