A Analysis of Attack and Defense Mobile Ad Hoc Network Based on OPNET

Jiahao Dai* and Xiaofeng Xu

1Science and Technology on Communication Information Security Control Laboratory
2China Electronic Group Corporation No.36 Institute, Zhejiang Jiaxing, China

*Corresponding author

Abstract. Due to the broadcast nature of wireless communications, the damage to mobile ad hoc networks is becoming more and more common. We propose a network stability model that can effectively reflect the network performance when the network is damaged in real time. The Ad Hoc network model is built by using the node model supporting the IEEE802.11 standard provided by OPNET software to simulate the network performance of the network under different degrees of damage. This model provides an effective way for the simulation analysis of network performance under the condition of Ad Hoc network damage.

Keywords: OPNET; Ad Hoc; networks stability; network defense.

1. Introduction

In recent years, the rapid development and application of the Internet in our lives has become an indispensable part of people’s lives. With the development of countries in the political, economic and cultural fields, the Internet plays an important role in these areas, driving political, economic and cultural development. According to the 42nd “China Internet Development Statistics Report” [1], the most authoritative report on domestic network security, mobile device access traffic consumption in the first half of 2018 reached 26.6 billion GB, an increase of 199.6%. However, while people enjoy the convenient communication services brought by the network, cyber attacks also emerge in an endless stream, seriously jeopardizing the interests of users. For example, the famous ransomware incident in 2017, using the local Internet access rights to upload local information and download the encrypted private key and public key, using the private key and public key to encrypt the file, dealing with the virus developer himself, it is almost impossible for others to decrypt. With the maturity of cyber attacks, a variety of new deficiencies are emerging, and the destructive power is getting more and more amazing. Therefore, it is imperative to analyze network destruction behavior.

The mobile ad hoc network [2] is a self-organizing network with a highly dynamic topology, nodes arbitrarily moving, and no control center. It is independent of a fixed infrastructure, and mobile nodes can communicate freely through distributed management. As a distributed network, a mobile ad hoc network can provide mutual communication between terminals without using or facilitating the use of existing network infrastructure (such as base stations, APs). Since the terminal’s transmit power and wireless coverage are limited, if two terminals that are far apart have to communicate, they must use other nodes for packet forwarding, so that a wireless multi-hop network is formed between the nodes. Therefore, for the traditional key-based encryption and decryption technology, due to the broadcast nature of wireless communication, malicious users can conveniently eavesdrop on the transmission of keys, and the destruction against the self-organizing network is more and more common.
Many scholars have carried out research on the damage caused by mobile ad hoc networks. In [3], by analyzing the attack types of mobile ad hoc networks and constructing attack trees initiated from malicious nodes, a FSM-based intrusion detection algorithm is designed by using the idea of finite state machine. The intrusion detection system using this algorithm can pass neighbors. The monitoring of the nodes detects various attacks of the nodes in real time. In [4], the corresponding protection research is proposed for the two attacks faced by the routing protocol AODV, and analyzes the flooded and tamper-attacked of three different network models (chained network, star network, mesh network). Literature [5] analyzes the security problems brought by the exposed topology of mobile ad hoc networks, and proposes a secure multi-path routing protocol with topological concealment. The protocol takes into account the time factor and path length factor to achieve the safest shortest path determination. In [6], a security problem based on the IEEE 802.11 MAC protocol of the mobile ad hoc network is proposed. A DDoS attack method based on attack set is proposed. This method can accurately attack the target node and reduce the detection rate of attack behavior.

Although many literatures have analyzed the vulnerability of mobile ad hoc networks, most of the literature only considers the threats faced by ad hoc networks, and analyzing the performance of ad hoc networks is also an indispensable aspect; in addition, most of the literature The security problem is only considered theoretically, and the reality of the networking situation is more complicated than the theory. Therefore, in this paper, we first propose a network stability model, which can effectively reflect the network performance when the network is damaged in real time. Next, we use OPNET to simulate the network performance of the network under different degrees of damage and give recommendations for maintaining network stability in the event of damage. Finally, we conclude this paper.

2. Networks Stability Model

2.1. Network Security State Model

Remember that the network state in the network at time $t$ is $x(t)$, we can get the Logistic model that $x(t)$ satisfies:

$$\begin{align*}
\dot{x}(t) &= rx(1 - \frac{x}{N}), \\
x(0) &= N_0,
\end{align*}$$

(1)

Where $r$ is the coefficient and $N$ is the optimal state of the network under finite resources. The solution of equation (1) is obtained by the separation variable method.

$$x(t) = \frac{N}{1 + e^{-rt(N - N_0)/N}}$$

(2)

The equation (2) has two equilibrium points, $x_1 = 0, x_2 = N$ where $x_1$ is unstable and $x_2$ is globally stable in the positive half-axis.

2.2. Network Destruction State Model

Establish an equation for network state compliance in the event of network failure and analyze the conditions for stable network conditions. Assume that the number of damaged nodes in the unit time is proportional to the network state $x(t)$. With the proportional coefficient $k$, $k$ can be further decomposed into $k = qE$. $E$ is called the damage strength and is measured by the controllable parameters such as the number of damages, $q$ is called the coefficient of destruction. In order to facilitate us to take $q = 1$, the number of damaged nodes per unit time is $h(x) = Ex(t)$. $h(x)$ is a constant that represents a particular way of breaking. Thus, the network state satisfies the equation

$$\dot{x}(t) = rx \left( 1 - \frac{x}{N} \right) - Ex$$

(3)

This is a first-order Riccati-type nonlinear equation, also known as the Scheafer model.
We want to obtain the steady state of the network and maintain stable conditions, that is, the trend of the network state after time $t$. There is $\frac{dx}{dt} = 0$ at the equilibrium point, and equation (3) has two equilibrium points $x_1 = 0$, $x_2 = N(1 - E/r)$.

- When $E < r$, $x_2$ is a positive equilibrium point. Equation (3) can be expressed as
  $$x(t) = -x(x - x_2)$$  \hfill (4)
  It is easy to know that when $0 < x < x_2$, $x(t) > 0$, when $x > x_2$, $x(t) < 0$, which means the equilibrium solution $x_1$ is unstable, and $x_2$ is a stable equilibrium solution. That is, in the case of the destruction strength $E < r$, the network state will be stabilized at the level of $x_2$, and the destruction ability is stabilized at the extent of $Ex_2$.

- When $E > r$, $x(t) < 0$, the network performance continues to drop, eventually leading to network paralysis. How to maintain the stability of the network. In another words, how to minimize network damage? Mathematically, the expected damage effect is minimized under the condition of $x(t) = 0$ or $rx(t)(1 - x(t)/N) = Ex(t)$, and the damage consumption can be understood. To destroy the number of nodes as $h(x) = Ex(t)$, the problem can be described as the following optimization problem:
  $$H_{\text{max}} = \max Ex(t)$$  \hfill (5)
  The constraint is $rx(t)(1 - x(t)/N) - Ex(t) = 0$. This optimization problem can be attributed to the maximum value of the quadratic function $h(E) = NE(1 - E/r)$ of $E$. By deriving we can get the maximum damage strength $E_{\text{max}} = r/2$, and the number of broken nodes is $h_{\text{max}} = rN/4$. The breaking strength $E_{\text{max}}$ is a strategy to obtain the best network damage effect.

3. Simulation Model

3.1. Network Model
In this paper, we consider the network model of adhoc [7]. As shown in Figure 1, we assume that the simulation area is a plane of 1km*1km, there are four limited moving areas in the plane, and there are 10 mobile nodes in each area. All mobile nodes can move freely in the limited area of 300m*300m. If the distance between two nodes is greater than 100m, the two nodes cannot communicate with each other. The moving speed of each node is any random number in the range of 0-10m/s. During the simulation, the nodes randomly stay, or the nodes move to the edge of the circular area, and the time of each stay is 10s, then the node again Random direction and velocity motion until the end of the simulation, the simulation time is 1h. Nodes located in different areas cannot communicate directly. Data must be exchanged through the corresponding routers in their respective areas. Each router can communicate with each other. That is, if node 1 wants to communicate with node 20, it must first transmit data to node 2 by node 1, then to router 5 by router 2, and finally to node 20 by router 5. The SITL module is implemented by the wireless network card device. The mobile ad hoc network in the OPNET simulation environment is connected to two external computers. The routing protocol uses the AODV routing protocol. The semi-physical simulation environment realizes data communication between different network segments by a semi-physical simulation method.
Figure 1. Network model with lots of mobile nodes and several routers.

3.2. Node Model

The nodes in the network are randomly distributed in a limited area and move randomly, so each mobile node has the same node model, as shown in Figure 2. In order to obtain the network performance parameters in the simulation process in real time, the simulation rewrites the code in the wlan wkstn node model and puts the obtained data into the database. The process module functions in the node model are as follows:

- Wlan port rx (receive) module: adopts a non-directional reception mode to obtain data frames of other nodes and transmit them to the MAC module;
- Wla port tx (send) module: uses a non-directional reception mode to transmit data frames to other mobile nodes;
- Wireless lan mac module: emulation link layer random access channel protocol, channel access protocol is IEEE 802.11 protocol, access mechanism is CSMA/CA, and counts the network performance parameters such as network throughput and delay;
- Tcp/ip module: processing the obtained tcp/ip data packet;
• Application module: set a random destination address for the packet introduced by the upper layer, generate a service request to the routing layer according to the ICI format of the internal communication interface, and the packet is sent to the tcp/ip module together with the ICI.

3.3. Process Model
Each process module in the node model is implemented by a process model, where each process model is a finite state machine implemented by c code. In the mobile ad hoc network, the selection of the MAC protocol needs to consider its service performance for integrated services such as video, voice, and data. The MAC layer emulation protocol of the selected Ad hoc network is IEEE 802.11 MAC with distributed coordination function protocol, the wireless mac module process model for setting the channel access protocol in the node model is shown in Figure 3.

![Figure 3. Process model.](image)

Source process: which is used to forward the obtained packets. When the emulation system starts, the sent information is initialized in the INIT state, and then the GENERATE obtains the data packet according to the given function according to the given function, and sends the data packet out. When the network status triggers the STOP and DISABLED events, the transmission is terminated.

Receive process: which is used to collect data generated in the simulation and analyze the simulation. When the simulation system is started, in the initialization INIT state, the simulation amount is counted through the registration of the corresponding function, and the necessary configuration is performed on the receiving module. After initialization, it directly enters the DISCARD state and waits for the next event to arrive. The DISCARD state is used to split the data packet and count the network simulation amount. After waiting for it, it returns to the DISCARD state and waits for the next trigger.

Routing process: which is used to simulate the packet forwarding, path allocation, and arbitration. When the simulation system starts, the processed information is initialized in the INIT state first, and then enters the state machine IDLE_0. If the PKT_ARR or PK_SEND_INTRPT event is triggered at a certain time, the route v1 function will be executed. If the CHANNEL_STAT_UPDATE or PK_SEND_FLAG event is triggered at a certain time, the PK_RESET event is executed to complete the routing of the packet.

4. Simulation Results
Based on the above model and simulation network, the network model was verified by simulation experiments. Simulation results will be given and the simulation results will be analyzed.

As shown in Figure 4, the relationship between network performance (mainly including network traffic, network data loss, network delay and routing request) under different failure conditions is given. Figure 4 (a) shows that as the number of damaged nodes increases, the network traffic remains unchanged first, followed by a rapid decrease and a slow decrease. This is because the node that was damaged at the beginning is a non-critical node, which has little effect on the network structure. Then, as the important node is destroyed, the network traffic drops drastically; when the damaged node increases to a certain extent, the network becomes simpler and simpler. The flow rate is also slowly reduced. Figure 4 (b) shows the relationship between the number of broken nodes and data loss. The loss of data is related to the stability of the network. The more stable the network, the less data is lost.
We can see that as the number of damaged nodes increases, the lost data first remains stable and then decreases rapidly. This is because at the beginning of the network there are too many nodes, the network structure is too complicated, resulting in serious data loss; and after destroying some nodes, the network structure becomes simple and tends to be stable. Interestingly, when the number of damaged nodes is 21, the data loss suddenly increases. This is due to too many damaged nodes, the basic network structure is destroyed, and the route needs to be searched again.

5. Conclusions

For the destruction of mobile ad hoc networks, this paper uses OPNET to build a network structure to simulate the network performance of the network under different degrees of damage. The simulation results show that the network damage nodes affect network traffic, network data loss, network delay and routing request performance. The network stability model can effectively reflect the network performance under the damaged situation and give suggestions on how to maintain the network stability.

References

[1] C. I. N. I. Center, “The 42nd Statistical Report on Internet Development in China,” Internet World, 2018.7.
[2] W. Daoyuan, T. Hui, and Z. Ping, “Research and application of mobile self-organizing network,” Telecommunications Science, vol. 24, no. 6, pp. 60–64, 2008.
[3] Y. Xia, L. Junshan, and L. Rong, “Research on classification of mobile ad hoc network attack based on fsm detection,” Modern Electronic Technology, vol. 33, no. 21, pp. 89–92, 2010.
[4] Y. Yanfang, “Research on the protection of self-organizing cyber attacks,” University of Electronic Science and Technology.
[5] H. Qi, Z. Jiao, and Z. Yujun, “Topologically Hidden MANET Secure Multipath Routing Protocol,” Journal of Software, vol. 22, no. 5, 2011.
[6] X. Rui, Z. Zemao, and H. Fei, “MAC layer DDoS attack in mobile ad hoc networks based on attack set,” Journal of Computer Applications, vol. 28, no. 3, pp. 1148–1151, 2011.
[7] X. Lei, L. Xiaohui, and F. Hongyu, “Modeling and simulation of adhoc network based on opnet,” Computer Engineering, vol. 35, no. 1, pp. 123–125, 2009.