An Approach to Understand Secure MANET Routing Using OPNET

Virendra Singh Kushwah[1], and Gaurav Sharma[2]

[1] Department of Computer Science
Hindustan Institute of Management and Computer Studies, Farah, Mathura, India
[2] Department of Computer Science
GLA University, Mathura, India
{kushwah.virendra248,gauravsharma53}@gmail.com

Abstract. Mobile Ad-Hoc Network (MANET) is a wireless network without infrastructure. Self-configurability and easy deployment feature of the MANET resulted in numerous applications in this modern era. Efficient routing protocols will make MANETs reliable. The open and dynamic operational environment of MANET makes it vulnerable to various network attacks. A common type of attacks targets at the underlying routing protocols. Malicious nodes have opportunities to modify or discard routing information or advertise fake routes to attract user data to go through themselves. The aim of the research is to prevent network using secure routing protocols and to study the performance of the secure network.

Keywords: Secure, OPNET, ad hoc, routing.

1 Introduction

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbour closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still [1] [4]. Therefore the network topology changes from time to time. MANET has various potential applications. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers.

2 Literature Review

It is understandable that most security threats target routing protocols – the weakest point of the mobile ad-hoc network. There are various studies and many researches in this field in an attempt to propose more secure protocols [1] [2]. However, there is not a complete routing protocol that can secure the operation of an entire network in

V.V. Das, E. Ariwa, and S.B. Rahayu (Eds.): SPIT 2011, LNICST 62, pp. 198–200, 2012.

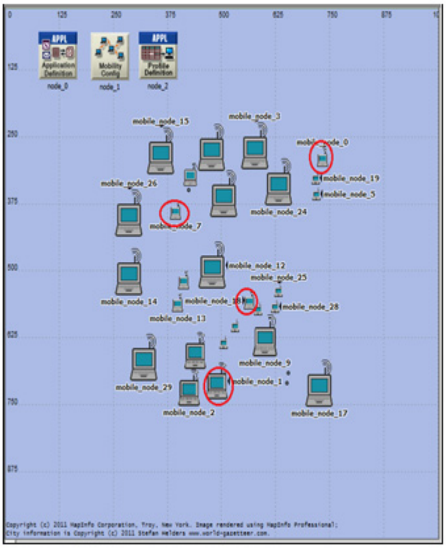
every situation. Typically a “secure” protocol is only good at protecting the network against one specific type of attacks [3].Many researchers have been done to evaluate the performance of secure routing protocols in comparison with normal routing protocols [3] [4]. One of the objectives of this research is to examine the additional cost of adding a security feature into non-secure routing protocols in various scenarios. The additional cost includes delay in packet transmission, the low rate of data packets over the total packets sent, etc.It is well known that the real-world network does not operate in an ideal working environment, meaning that there are always threats and malicious actions affecting the performance of the network. Thus, studying the performance of secure routing protocols in malicious environments is needed in order to effectively evaluate the performance of those routing protocols [5] [6].

3 Simulation Setup

In this paper, simulation set up of a network with 30 wireless nodes moving at random, each with various speed between 1 and 10 meters per second. Each of the objects can move at a random direction, stop for some time (per the *pause time*), and then change its direction at random and move again. The *traffic pattern* models the voice data transferred from one node to the other [1] [4]. The data is sent at a rate of 2 kbps to represent compressed voice data. The number of data source nodes is chosen based on the assumption that a half of the nodes send the data and a half of the nodes receive the data. The destination of data is determined at random to mimic the real situations. The simulation scenario is summarized below:

Table 1. SimulationSetup Parameters

Sr. No.	Parameters	Value
1	Simulation Area	1000 M x 1000 M
2	Mobility Model	Random Waypoint
3	Simulation Time	10 Min
4	Number of Nodes	30
5	Node speed	1-10 m/second
6	Type of traffic	Constant Bit Rate (voice)
7	Packet size	512 bytes (or ~ 4096 bits)
8	Sending frequency	4 packets/second
9	Traffic destination	Random



Copyright (c) 2011 MapInfo Corporation, Troy, New York. Image rendered using MapInfo Professional;
City information is Copyright (c) 2011 Stefan Helders www.world-gazetteer.com.

Fig. 1. Simulation Environment with 30 nodes

4 Result and Analysis

The simulation is done using AODV protocol into OPNET[4] Simulator. The 30 nodes in which 26 are free nodes and 4 are attackers. A scenario is set up for data collection. This scenario is run 10 times with 10 different values of the mobility *pause time* ranging from 1 to 10 seconds. The data is collected according to two metrics – *Packet Delivery Fraction* and *Normalized Routing Load* [1] [3]. In general, the actual values of the performance metrics in a given scenario are affected by many factors, such as node speed, moving direction of the nodes, the destination of the traffic, data flow, congestion at a specific node, etc. It is therefore difficult to evaluate the performance of a protocol by directly comparing the acquired metrics from individual scenarios. In order to obtain representative values for the performance metrics, we decided to take the average values of multiple simulation runs [1] [4] [5].

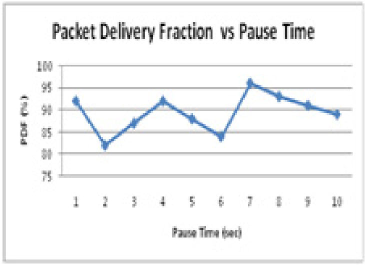


Fig. 2. PDF vs. pause time values in benign environment

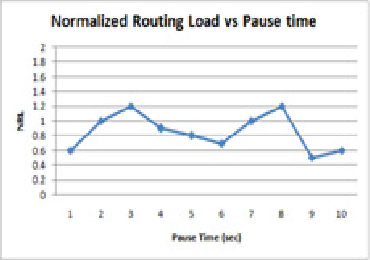


Fig. 3. NRL vs. pause time values in benign environment

References

1. Juwad, M.F., Al-Raweshidy, H.S.: Experimental Performance Comparisons between SAODV & AODV. In: IEEE Second Asia International Conference on Modelling & Simulation (2008)
2. Cerri, D., Ghioni, A.: Securing AODV: The A-SAODV Secure Routing Prototype. IEEE Communications Magazine (February 2008) 0163-6804/08 © 2008 IEEE
3. Tsaur, W.-J., Pai, H.-T.: A New Security Scheme for On-Demand Source Routing in Mobile Ad Hoc Networks. In: IWCMC 2007, Honolulu, Hawaii, USA, August 12-16 (2007) Copyright 2007 ACM 978-1-59593-695-0/07/0008
4. Ali, M.H., Odah, M.K.: Simulation Study of 802.11b DCF using OPNET Simulator. Eng. & Tech. Journal 27(6), 1108–1117 (2009)
5. Lu, S., Li, L., Lam, K.Y., Jia, L.: SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack. In: International Conference on Computational Intelligence and Security (2009)
6. Kushwah, V.S., Tapaswi, S.: Securing Nodes in MANETs Using Node Based Key Management Scheme. In: Proceeding of the IEEE Xplore 2010 International Conference on Advances in Computer Engineering– ACE 2010, Bangalore, India, June 21-22, pp. 228–231 (2010)