MOBILE AD HOC NETWORKS UNDER WORMHOLE ATTACK: A SIMULATION STUDY

Nadher M. A. Al_Safwani, Suhaidi Hassan, and Mohammed M. Kadhum

Universiti Utara Malaysia, Malaysia, {suhaidi, khadum}@uum.edu.my, nadher@internetworks.com

ABSTRACT. Security has become the main concern to grant protected communication between mobile nodes in an unfriendly environment. Wireless Ad Hoc network might be unprotected against attacks by malicious nodes. This paper evaluates the impact of some adversary attack on mobile Ad Hoc Network (MANET) system which has been tested using QualNet simulator. Moreover, it investigates the active and passive attack on MANET. At the same time, it measures the performance of MANET with and without these attacks. The simulation is done on data link layer and network layer of mobile nodes in wireless Ad Hoc network. The results of this evaluation are very important to estimate the deployment of the MANET nodes for security. Furthermore, this study analyzes the performance of MANET and performs "what-if" analyses to optimize them.

Keywords: MANET, Networks Security, Wormhole Attack.

INTRODUCTION

The wireless arena has been growing exponentially in past few decades. We have seen great advances in network infrastructures as growing availability of wireless applications and the emergence of universal wireless devices like laptops, PDA, and cell phone [7]. Nowadays, mobile users can rely on cellular phone to check emails and browse the Internet. For example, travelers with laptop can use the Internet anytime and anywhere [11]. In the next generation of wireless communication systems, there will be a need for the fast deployment of independent mobile users. Important examples include establishing survivable, efficient, dynamic communication for emergency operations, disaster recovery, and military networks. Such network scenarios cannot rely on centralized and organized connectivity. There are currently two kinds of mobile wireless networks. The first type is known as infrastructure networks with fixed and wired gateways. Typical applications of this type of "one-hop" wireless network include wireless local area networks (WLANs). The second type of mobile wireless network is infrastructureless mobile network commonly known as the Ad Hoc network or wireless Ad Hoc network [5].

Ad Hoc network systems are independent systems which consist of a collection of mobile nodes that use wireless transmission for communication. They are self–organized, self-configured, and self–controlled infrastructureless networks [3]. In Ad Hoc network, the devices themselves are the network, and this allows seamless communication at low cost, self organizing and free deployment as shown in Figure 1.

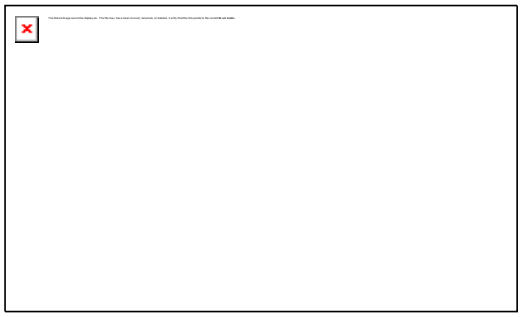

Figure 29. Ad Hoc Network [3].

Hence, mobile Ad Hoc (MANET) is different from other network solutions. Users can create their own network which can be deployed and configured easily and cheaply. On the other hand, the radio transmission range is small, therefore, communication partners are not often within direct radio range; so connections should be setup over multiple nodes and these nodes might change their location depending on node mobility. These changes cause frequent route break and force source to maintain connections to their distant communication partner. For all of these reasons, MANET is one of the more modern and challenging area of network security [11]. The nodes in MANET consider as routers. The routers are free to move randomly, and organize themselves at random; so the network wireless topology may change rapidly. Mobility and large network size combined with devices heterogeneity, security, bandwidth, and battery power constraints make the design of sufficient routing protocols as a major challenge.

MANET Security Issues

Security in MANET system is one of the main concerns to provide protected communication between mobile nodes in strange environment. Unlike the wired line networks, the unique characteristics MANET create a number of nontrivial challenges to security design like open peer-to-peer network architecture, shared wireless medium, inflexible resources constraints and highly dynamic network topology [3].

A security attack is an attempt to compromise the security of information owned by others. Any protected system might have weaknesses or vulnerabilities that can be considered as a target for attacker. Hence, one approach to design security mechanisms for any system is to look at the threats and attacks to the system through possible vulnerabilities. This approach should ensure that the system is secured under these threats, attacks, and vulnerabilities. Due to its nature, MANETs are vulnerable to several types of attacks. Even within the current available mechanisms, such as encryption and authentication, it still cannot perfectly prevent the attacks on the air-link [7].

In order to implement security in MANET, environment needs to be secured against attacks. Security services in MANET's are needed to protect from attacks and to ensure the security of the information. These services can be categorized into tow type, namely *communications security* and *computer security* as shown in Figure 2. Communication security protects against passive and active attacks through communication links or accidental emanations. This ensures that communication services continue with the required level of quality, and their information cannot be captured or derived by unauthorized node [1].

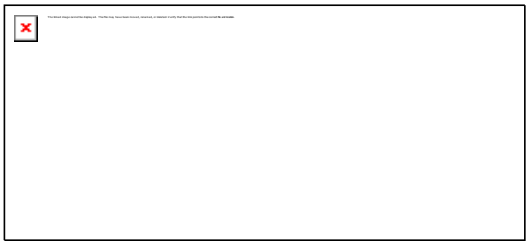

Figure 30. Information Security [1]

The Current Status of Security in MANET

The nature of mobile compute environment makes it very vulnerable to an adversary's malicious attacks. The use of wireless links renders the network susceptible to attacks range from passive eavesdropping to active nosy attacks such as wormhole attack, rushing attack, black hole attack, neighbor attack, and jellyfish attack. Unlike wired networks where an adversary must gain physical access to the network wires, or pass through several lines of defense gateways such as firewall, attacks on a wireless network can come from all directions and target at any node. Damages can include exploring secret information and node impersonation. It means that a wireless network does not have a clear line of defense and every node must be prepared for encounters with an adversary directly or indirectly [7]. There is no well defined place where we deploy to protect a single security solution. Moreover, laptops and mobiles are vulnerable to attack. Attackers may creep into the network through these subverted nodes which pose the weakest link and incur a domino effect of security breaches in the system.

The deployment of mobile Ad Hoc network is growing in the world. This leads to new challenges as large amount of data which may hold malicious content such as Worms, Viruses, or Trojans to move over these networks. There is a need to detect active and passive attacks. The network service providers (NSPs) are supposed to offer improved security features to customers as a value adding feature into the frame work of the network. In addition, network security administrators need to understand the vulnerabilities and the attacks in their environments with their effect on MANET before applying their deployment in the real environment to detect the threats and find efficient solutions for the MANET framework. Also, there are plenty of features existing in real life networks, but new standards and attack signatures are changing continuously at a rapid rate. Therefore, MANET should be upgraded with up-to-date security services.

This paper examines the performance of some of the aforementioned challenges features on MANET. The goals of this study are to determine the likelihood of an attack such as wormhole attacks in MANET; and to evaluate the performance of MANET, in terms of throughput, average jitter, and average end-to-end delay, with and without wormhole attack. In this study, the experiments are conducted using QualNet QualNet 4.5.1 GUI simulator running on Windows XP sp 2 operating.

WORMHOLE EXPERIMENT

Testing Scenario

We conducted our scenario using different combination of nodes for each experiment to evaluate the performance of MANET under wormhole attach. We configure some of the node as wormhole subnet and we have connected them to a wireless subnet. One CBR application is configured for all nodes. More than 100 packets are sent from a source node to the destination node. We enabled wormhole by making all parameter as *pass* in the wireless subnet.

Results

In the end of the test, many frames were intercepted by the wormhole node. In addition, a huge amount of frames were tunneled by the wormhole nodes. We noticed the number of frames replayed by the wormhole node is increased. We have noticed that many signals have transmitted by wormhole nodes are more than signals transmitted by others. Moreover, the broadcast packets received clearly from normal nodes are more than those received from wormhole nodes. Changing the wormhole parameter to *drop* in the experiment showed that many packets in wormhole nodes were dropped.

We have gathered all the results from the simulation and compared them to obtain the differences and the similarities between both situations, with and without wormhole, and how the attack affects the MANET network.

In the following, we show the effect of wormhole attack on MANET under this experiment in terms o, Total packet received, Throughput (bit/s), Average end to end delivery, and Average jitter.

Total Packets Received

The total packets received without wormhole gained comparing to those experiments with wormhole are shown in Figure 4.

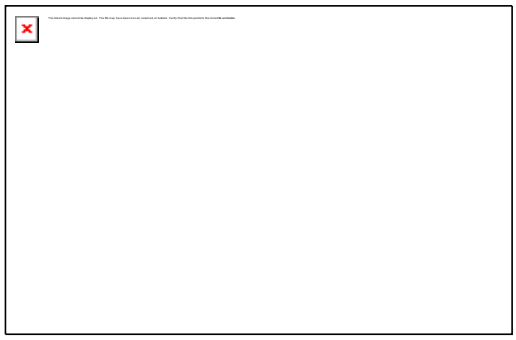

Figure 31: Total Packets Received with and without Wormhole

Throughput (bit/s)

The effect of wormhole on MANET regarding the throughput is shown in Figure 5. The results show that 80% of packets are received successfully when no wormhole attack is attempted. While, under the wormhole attack, the number of packets received is decreased to 10%.

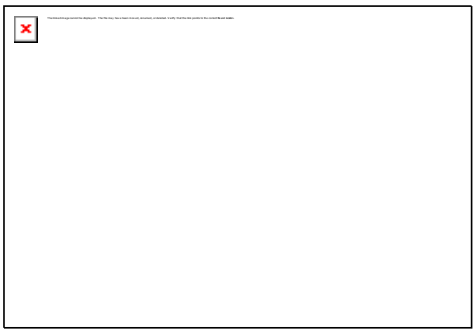

Figure 5: Throughput (bits/sec) with and without Wormhole

Average End-to-End Delay

It can be observed from Figure 6 that, under the condition where no wormhole attack is existed, there is an increase in the average end-to-end delay, compared to the effect of wormhole attack on the network. This is due to the immediate reply from the malicious node which does not need to check its routing table.

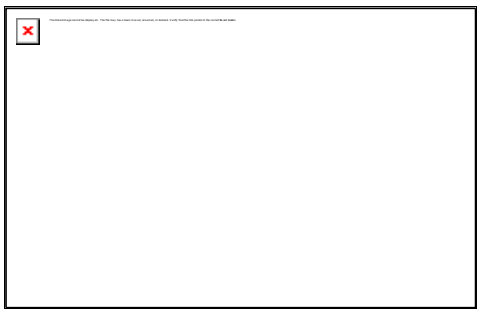

Figure 6: Average End-to-End Delay with and without Wormhole

Average Jitter

As shown in Figure 7, the average jitter between the nodes is more without the wormhole attack as compared to the case of wormhole attack. This is due to that malicious nodes provide the path to their destinations with a few number of nodes, or short path. Thus, average jitter between the nodes is reduced.

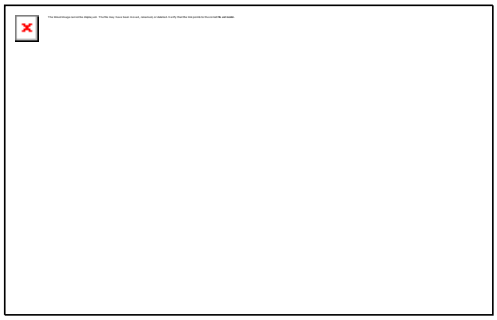

Figure 7: Average Jitter with and without Wormhole Attack

Comparing all the results obtained from Figures 5, 6, and 7, we can notice that the affect of wormhole on throughput values more than the affect on average end-to-end delay and average jitter values. That illustrated the main affect of wormhole attack on the value of throughput successful messages in MANET.

CONCLUSIONS

Attacks in wireless Ad Hoc are one of the mandatory issues and challenges in the network. There are a wide variety of attacks that target the weakness of MANET. The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks. This paper assesses the MANET under wormhole attack. Determining wormhole attack and evaluating the performance of the MANET are the main objectives in this paper. To achieve these objectives, QualNet 4.5 simulator was used. The work done in this paper consists of two scenarios. The scenario presented in this paper was meant to detect

the active wormhole attack and evaluate the performance of MANET under different conditions.

REFERENCES

[1] E. Çayırcı and C. Rong, Security in Wireless Ad Hoc and Sensor Networks, 1 ed.: John Wiley & Sons, feb 2009.

[2] S. Sharma and R. Gupta, "Simulation Study of Blackhole Attack in the Mobile Ad Hoc Networks," Engineering Science and Technology, vol. 4, pp. 243-245, 2009.

[3] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, ad hoc mobile wireless networks : principles, protocols, and applications, 1st ed.: Auerbach Publications, 2007.

[4] P. P. Garrido, M. P. Malumbres, and C. T. Calafate, "ns-2 vs. OPNET: a comparative study of the IEEE 802.11e technology on MANET environments," in the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops, Marseille, France, 2008.

[5] C. Jin and S.-W. Jin, "Invulnerability Assessment for Mobile Ad Hoc Networks," 2008.

[6] E. Schoch, M. Feiri, F. Kargl, and M. Weber, "Simulation of Ad Hoc Networks: ns-2 compared to JiST/SWANS," in International Conference on Simulation Tools and Techniques for Commuications, Networks and Systems & Workshops, Marseille, France, 2008.

[7] F. Anjum and P. Mouchtaris, Security for Wireless Ad Hoc Networks, 1st ed.: Wiley-Interscience, 2007.

[8] C. Calafate, P. Manzoni, and M. P. Malumbres, "On the interaction between IEEE 802.11e and routing protocols in mobile ad-hoc network," in Parallel, Distributed and Network-Based Processing, 2005. PDP 2005. 13th Euromicro Conference, 2005, pp. 110- 117.

[9] H. Otrok, J. Paquet, M. Debbabi, and P. Bhattacharya, "Testing Intrusion Detection Systems in MANET: A Comprehensive Study," in Communication Networks and Services Research, 2007. CNSR '07. Fifth Annual Conference Frederlcton, NB, 2007, pp. 364-371.

[10] K. Erciyes, O. Dagdeviren, and D. Cokuslu, "Modeling and Simulation of Wireles sensor and Mobike Ad Hoc Networks " in Proceedings of the International Conference on Modeling and Simulation 2006, Konya, TURKEY, 2006.

[11] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Mobile Ad Hoc Networking, 1st ed.: Wiley-IEEE Press, 2004

[12] E. a. A. Turban, J.E decision support systems and intelligent systems, 5th ed.: Upper Saddle River, N.J, 1998.