ATLANTIS PRESS

Advances in Computer Science Research, volume 62

2nd Joint International Information Technology, Mechanical and Electronic Engineering Conference (JIMEC 2017)

Performance Of MANET With IPSec Under Jelly Fish Attack

Fatin Hamadah Rahman[1], Thien-Wan Au[2] , Wida Susanty Suhaili[3], Yan Liu[4]

[1, 2, 3]School of Computing and Informatics, Universiti Teknologi Brunei
Jalan Tungku Link, Gadong, BE 1410, Brunei Darussalam

[4]Harbin University of Science and Technology, Heilongjiang Sheng, China

[1]fatinh.rahman@gmail.com, [2]twan.au@utb.edu.bn, [3]*wida.suhaili@utb.edu.bn*, [4]*liuyan@hust.edu.cn*

Keywords: MANET, Jellyfish attack, IPSec, OLSR, TORA.

Abstract

MANET is a self-organizing network that uses multi-hop routing for data communication. Without any centralization, network monitoring is problematic thus making it vulnerable to attacks such as Jellyfish attack. Hence IPSec protocol can be used as one of its security means. The aims of this paper is to study the performance of MANET using OLSR and TORA routing protocols alongside with the application of IPSec when the MANET is under Jellyfish attack, to see which routing protocol is least affected by the attack and to see which routing protocol benefitted the most with the application of IPSec using Riverbed Modeler Academic Edition. Based on the simulations, it shows that OLSR performs better under Jellyfish attack, and TORA benefits the most with the use of IPSec.

1 Introduction

MANET is a type of wireless ad-hoc network that allows communication without the need of a fixed infrastructure in the network. It consists of nodes, which represent each individual user that is using mobile devices. In order for a node to communicate to the destination, the data has to hop through nearby nodes until it reaches the destination. It is very scalable as it can be deployed to hundreds or thousands of nodes at a time, depending on the needs of the network. MANET is applied in emergency/rescue operations for disaster area relief efforts. These emergency rescue operations can take place where non-existing or damaged communications infrastructure and swift distribution of a communication network is required and information is relayed from one rescue team member to another over a small handheld device. However, MANET also possesses some challenges and vulnerabilities that should be considered beforehand should it be deployed. The challenges include limited resource availability, scalability, limited power supply, and bandwidth constraint. Lacking centralized management also means that monitoring the network traffic can be rather difficult. Without having a centralized server, it makes attack or anomaly detection within the network unfeasible. Moreover, the absence of specific defense line in this dynamic topology would introduce more security issues [5]. Only a handful of studies have been simulated to see the effects of Jellyfish attack in MANET with the IPSec protocol. These studies have only performed the attack on the AODV routing protocol. Moreover, most of the researches done on Jellyfish attack using simulation also did not focus on the application of IPSec protocol on MANET. Therefore, it is a good opportunity to explore the attack to further study its impact on a secured network using other MANET routing protocols such as OLSR and TORA. The best approach to understand the underlying flow architecture of MANET can simply be accomplished through simulations. In fact, on average, the simulation-based results account for 70% of the papers published in conference proceedings [11]. The upcoming Section 2 describes the routing protocols, transport layer protocols, IPSec protocol as well as the background study on Jellyfish attack. The experiment of the study will be presented in Section 3, followed by the results and findings in Section 4 and 5 respectively. Finally, Section 6 concludes the whole study.

2 Background study

The routing protocols for MANET can be categorized into proactive and reactive. Proactive protocols continuously learn the topology of the network by exchanging topological information among the network nodes. Meanwhile reactive routing protocol creates routes only when they are needed, thus minimizing the number of broadcasts.

2.1 Optimized Link State Routing (OLSR)

OLSR is a proactive routing protocol that stores and updates its routing table information permanently. The routing table is monitored in order to provide a route if needed or route all time available for communication. Using "Hello" messages, OLSR finds its one-hop neighbours and its two hop neighbours through their responses. The multipoint relays (MPR) can then be selected by the sender based on the one hop node that offers the best routes to the two hop nodes. Each node has also an MPR selector set, which is obtained from HELLO packets sent between in neighbours nodes within range of that node only neighbours [9].

2.2 Temporarily Ordered Routing Algorithm (TORA)

TORA is reactive routing protocol that is highly adaptive and can provide loop-free routing algorithm based on the concept of link reversal. It is unique and prominent in a way that its main feature of propagation of control messages revolves only around the point of failure when link failure occurs. It would be able to mend itself up around the point of failure unlike all the other protocols that need to re-initiate a route discovery when a link fails [6].

2.3 Transport Layer Protocols

The function of this layer is generally to ensure a complete end-to-end data transfer. It also provides error detection and recovery of packets that is received from the routing of the network layer. These packets are further assembled into segments before they are forwarded to the upper layers. Two of the most common transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

2.4 Jellyfish Attack

Jellyfish attack is a type of DoS attack that occurs on the transport layer. This attack disrupts the operations of the TCP and UDP protocols in the transport layer, producing delays before the transmission and reception of data packets in the network, especially targeting closed loop network flows. TCP is vulnerable to delay, drop and misorder of the packets; hence nodes can change the sequence of the packets and drop some of the data packets. However, the Jellyfish attacker nodes still fully obey protocol rules and thus this attack is considered as a passive attack that makes it harder to detect [10]. There are three possible ways that this attack can occur, namely the Jellyfish Reorder Attack, Jellyfish Periodic Dropping Attack and Jellyfish Delay Variance Attack [12]. In this study, the latter attack type is performed. The packets delayed by the malicious Jellyfish nodes have the capability to significantly reduce throughput of network by postponing a certain amount of time before attending to the packets. Although the order of packets is maintained, they significantly increase the delay variance. In other words, the TCP sends traffic in bursts due to "self-clocking" from the high delay variation that leads to increased collisions and loss. It also causes false estimation of available bandwidth and high delay variation [1].

2.5 IPSec Protocol

IPSec is a protocol suite that works on the Internet layer of the TCP/IP stack. Not only does it encrypt the packet data, it can also encrypt the header information [3]. It has two modes of operation, namely the transport mode and tunnel mode. In transport mode, authentication and encryption only occurs at the payload of the IP packet. Meanwhile, the tunnel mode provides authentication and encryption of the entire IP packet. It is an open standard protocol that contains other subsequent components. IPSec contains several components that serve their respective functions such as Authentication Header (AH) and Encapsulating Security Payload (ESP). The AH provides data authentication and integrity for IP packets that are passed between two systems, but it does not provide data confidentiality of packets. Whereas the ESP is a security protocol that provides encryption of the IP packet where it authenticates the inner IP packet and ESP header [4].

3 Experiment

The Riverbed Modeler Academic Edition best suits this study as it provides the supporting MANET protocol and IPSec capability along with GUI. There are two scenarios carried out in this study; the first scenario shows the performance of MANET without IPSec under Jellyfish attack and the second scenario shows MANET with IPSec under the same attack. The network layout is shown in Figure 1 below.

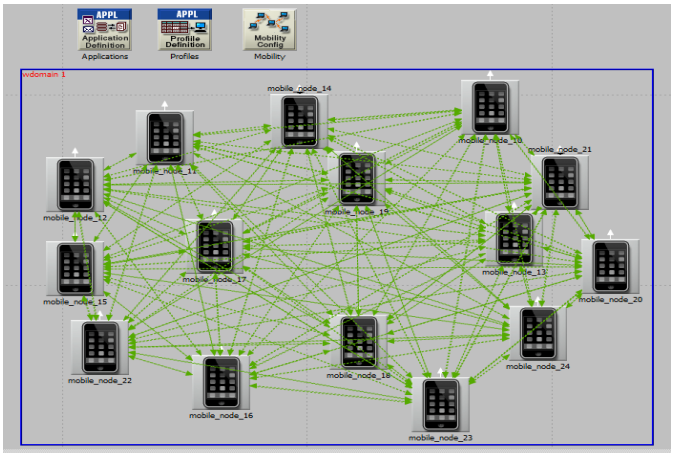

Fig. 1 MANET design

3.1 IPSec Configuration

Since the MANET communication is peer-to-peer, the IPSec transport mode should be used. Hence, the 'IP Security demand' feature is selected. Unfortunately, this feature lacks of configuration options such as choosing the authentication and encryption type. The IP Security demand for a MANET has also been used previously on a study [7]. The rest of the IPSec configurations can be found in Table 1.

Attribute	Value
No of Nodes	15
IP Addressing	IPv4
Model	WLAN IPhone
Standard	IEEE 802.11a
Data Rate	54Mbps
Trajectory	Vector
Simulation Area	500m x 500m
IPSec Configuration:	
• Destination and Source Port	Voice
• Type of Service	Best Effort (8)

Table 1: Nodes attributes and values

Since the Jellyfish attack is an outsider attack, it is assumed that the malicious node does not use IPSec protocol. Therefore,

there are no outgoing IPSec configurations set on the malicious node. However, the malicious node can still accept IPSec-encrypted packets from its surrounding nodes, as it is possible for IPSec communication to occur between IPSec and non-IPSec devices.

3.2 Jellyfish Attack Configuration

Since the Jellyfish delay variance attack focuses on causing high delay in transmitting traffic from the malicious node, the forwarding rate of the malicious node is decreased from the default value of infinity to just 1000 packets per second to introduce the high delay as shown in Figure 2.

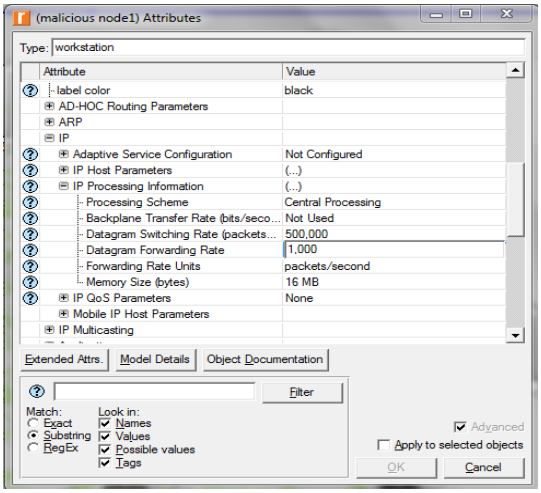

Fig 2 Malicious node Attributes

3.3 Node, Profile, Application and Mobility Configurations

In order to simulate a realistic MANET environment, fifteen nodes are used throughout the simulations as shown in Figure 1. One of the nodes is set to be the malicious Jellyfish attacker. The Profile Configuration, Application Configuration and Mobility Configuration models are added to enable better management of application. For ease and consistency of study, all of the nodes thus have the same settings in these aspects. To generate data traffic between them, the VoIP application is used whereas the rest of the applications such as database, email, FTP and HTTP are set to 'Off' as they are not used in this project. One important aspect in MANET is in its mobility. There are many mobility models that are used in MANET simulations such as Random Waypoint Model (RWM), Random Direction Model, Gauss-Markov Model, and Pathway Mobility Model. But the most common model used for MANET simulations is the RWM. In this model, each node begins the simulation by remaining stationary for a predetermined time in seconds. It then selects a random destination in the 500m by 500m space and moves to that destination at a speed distributed uniformly between 0 and some maximum speed. Upon reaching the destination, the node pauses again for a set duration of seconds, selects another destination, and proceeds there as previously described, repeating this behavior for the duration of the simulation [2]. Each different routing protocol scenario ran for 300 seconds of simulated time.

4 Results

The x-axis of graphs shown in Figures 3, 4 and 5 represents the routing protocol being used, and whether or not the routing protocol is using IPSec. The y-axis of Figure 3 represents the throughput measured throughout the simulation in Mbps. Meanwhile the y-axis in Figures 4 and 5 represents the delay in millisecond (ms) and retransmission attempt in number of packets respectively. There is no significant difference in OLSR routing protocol with or without IPSec for the delay and retransmission attempts shown in Figures 4 and 5. But for TORA routing protocol, the application of IPSec has shown better performance with the reduction of delay of 1.4ms compared to the scenario without the use of IPSec with delay of 1.6ms. Furthermore, the use of IPSec has nonetheless increased the throughput and decreased the retransmission attempt of TORA to only 0.23 packets.

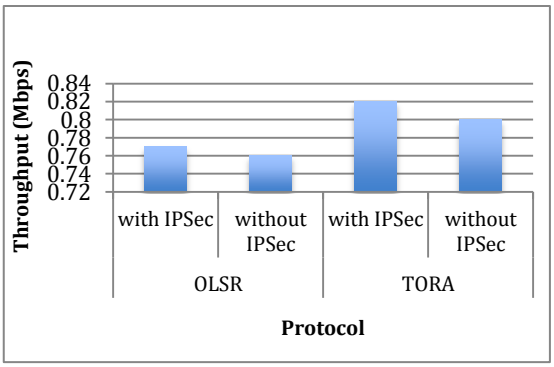

Fig 3 Throughput results

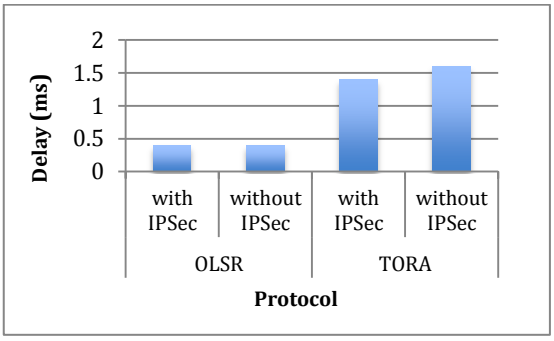

Fig 4 Delay results

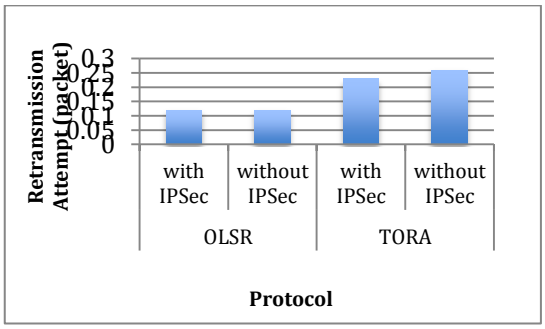

Fig 5 Retransmission attempt results

5 Findings

Table 2 shows the performance comparison. Both routing protocols have their strengths and weaknesses with simultaneous use of IPSec protocol on the network layer. Out of the two routing protocols, the table shows that IPSec has proven most beneficial for TORA routing protocol as it improves the throughput and reduced the delay and retransmission attempts. The more the nodes try to retransmit packets until they are received successfully, the higher the delay and the lower the throughput will be. The varying obtained results of between both routing protocols could also stem from their routing mechanisms such that TORA, a reactive routing protocol, is able to provide better route aid for dense networks by having synchronization of the nodes. Although the attack did not decrease the performance of MANET, it did not give any noteworthy change with the use of IPSec as well. The attack does not disrupt the mechanisms of the routing protocols in the first place, hence the use of IPSec is not significant with regards to protecting MANET against this attack. It might bypass that routing aspect as the attack targets the transport layer protocols. Since there is only one malicious node to begin with, the effect of the attack is very subtle and can be deemed insignificant if performance of the MANET is viewed as a whole, unless there are numerous attackers that wished to cause high delay in the data transmission. Although the attack did not give such an impact to MANET, it is always recommended to secure the network as much as possible on all levels. There are countermeasures to avoid the Jellyfish attack. On the transport layer, instead of using the usual TCP and/or UDP protocols, Stream Control Transmission Protocol (SCTP) can be used. SCTP is a transport layer protocol that serves in a related role to the TCP and UDP. It provides some of the same service features of both: it is message-oriented similar to UDP and ensures consistent, organized transport of messages with congestion control similar to TCP [8]. In addition to that, more advanced routing protocols that have security features embedded to deter the attack from occurring such as Authenticated Routing for Ad hoc Networks (ARAN) and Cooperation of Nodes: Fairness In Dynamic Ad-hoc Networks (CONFIDANT) can be used to give more protection for the network.

Routing Protocol	Throughput (%)	Delay (%)	Retransmission Attempt (%)
OLSR	+0.29	+1.44	0.00
TORA	+0.84	-2.90	-3.52

Note:
1. A –ve sign means a decrease in value with the implementation IPSec,
2. A +ve sign means an increase in value with the implementation IPSec

Table 2: Performance comparison

6 Conclusions and Future Work

MANET can be secured with IPSec, where the right combination of routing protocol and IPSec can give a good performance and can be effective in providing sufficient amount of protection and defending it from certain types of attack. But there is a give-and-take mechanism to consider if one is to employ IPSec - communication can be secured but the performance will most likely be compromised either in terms of throughput, delay, retransmission attempts or other performance metrics. Based on the simulations, the scenario with IPSec has better performance compared to the one without IPSec in terms of throughput, delay and retransmission attempts. The study has demonstrated that without IPSec, OLSR performs better and is least affected under Jellyfish attack compared to TORA routing protocol. However, the study also has shown that the use of IPSec is most beneficial to TORA routing protocol, as it has reduced the delay and retransmission attempt of the network in contrast to the performance of TORA not using the IPSec protocol. The IPSec's architecture alone is not enough to provide thorough network security, but it is a good approach to strengthen the network if combined with other protection tools. As MANET's focus is towards mobility and this paper only uses the RWM model, future studies on MANET with different mobility types can be carried out to investigate the impacts of doing so. More studies can be conducted to explore alternative transport layer protocols such as SCTP and TCP Vegas to see whether they can help prevent the occurrence of Jellyfish attack in a network.

References

[1] Begum, S. A., Mohan, L., & Ranjitha, B. (2012). Techniques for Resilience of Denial of Service Attacks in Mobile Ad Hoc Networks. International Journal of Electronics Communication and Computer Engineering, 3.

[2] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y. C., & Jetcheva, J. (1998). A performance comparison of multi-hop wireless ad hoc network routing protocols. Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking - MobiCom '98, (p. 85).

[3] Eastom, C. (2012). Computer Security Fundamentals (2nd Edition ed.). indiana: Pearson.

[4] Forouzan, B. A. (2007). Data Communications and Networking (4th Edition ed.). New York: McGraw-Hill.

[5] Goyal, P., Parmar, V., & Rishi, R. (2011). MANET: Vulnerabilities, Challenges, Attacks, Applications. International Journal of Computational Engineering and Management , 11, 32-37.

[6] Gupta, A. K., Sadawarti, H., & Verma, A. K. (2011). A Review of Routing Protocols for Mobile Ad Hoc Networks. WSEAS Transactions on Communications , 10 (11), 331-340.

[7] Ibrahem, M., & Aboud, A. (2014). A Secure Routing Protocol for MANET. International Journal of Computer Science Engineering and Technology (IJCSET), 4 (7), 223-230.

[8] Kaur, A., & Rani P. (2015). A Review On Comparative Analysis Of Different Transport Layer Protocols In MANETs. International Journal Of Engineering And Computer Science, 4(6)

[9] Kumar, J. (2013). Performance Analysis and Simulation of OLSR Routing Protocol in MANET. International journal of Computer Networking and Communication (IJCNAC), 1 (1), 45-55.

[10] Patel, H., & Chaudhari, M. (2010). Survey: Impact of Jellyfish On Wireless Ad-Hoc Network. INJCR, 10, pp. 5-9.

[11] Pawlikowski, K., Hae-Duck, J. J., & Jong-Suk, R. L. (2002). On credibility of simulation studies of telecommunication networks. IEEE Communications Magazine.

[12] Purohit, N., Sinha, R., & Diwanji, H. (2012). Simulation Study of Black Hole and Jellyfish attack on MANET Using NS3. Special Issue of International Journal of Computer Applications, 42-46.