Impact of IPsec on MANET

Fatin Hamadah M.A Rahman
School of Computing and Informatics
Universiti Teknologi Brunei
Tungku Highway, Gadong, BE1410. Brunei
Darussalam
Fatinh.rahman@gmail.com

Thien Wan Au
School of Computing and Informatics
Universiti Teknologi Brunei
Tungku Highway, Gadong, BE1410. Brunei
Darussalam
Twan.au@utb.edu.bn

Abstract— **Mobile ad hoc networks (MANET) do not have base stations or access points, and due to this nature, the ad hoc networks are susceptible to jamming attack which is the most common attacks. Since many ad hoc networks employed IP-based routing, they should be protected and communication between nodes should be secured. The aim of this study is to investigate the performance of MANET with the application of IPsec protocol and to see the effectiveness of IPsec protocol in providing security when the MANET is under jamming attack. In this study, Riverbed Modeler Academic Edition simulator is used to simulate a comparison of mobile nodes with and without IPsec, using Ad hoc On Demand Distance Vector (AODV), Optimized Link State Routing (OLSR) and Temporarily Ordered Routing Algorithm (TORA). The simulation results indicate that AODV routing protocol gives the largest percentage increase of delay and retransmission attempt in normal operations. However, when it is under attack the AODV with gained the highest throughput. Delay and retransmission attempts are the highest with OLSR.**

Keywords-IPsec, Jammer Attck, AODV,OLSR,TORA

I. INTRODUCTION

Mobile ad hoc network (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. These nodes operate according to the internal architecture of the OSI layer. In order for a node to communicate to the destination, the data has to hop through nearby nodes until it reaches the destination. The nodes in the MANET are not only of high mobility, but they are also self-forming and self-healing.

MANET can be applied in several environments [1] such as in the military battlefield where the modern digital battlefield demands robust and reliable communication in many forms. Similarly, MANET can be used in emergency/rescue operations for disaster area relief efforts. Emergency rescue operations can take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed and information is relayed from one rescue team member to another over a small handheld. Another application of MANET is sensor networks. This technology is a network composed of a very large number of small devices, which can be used to detect any number of properties of an area such as temperature, pressure, pollutions and forecast of earthquakes.

II. BACKGROUND AND LITERATURE REVIEW

A similar study was conducted by [3] where the authors have performed several MANET simulations using Opnet Modeler. They have compared the performance of AODV, OLSR and Geographical Routing Protocol (GRP) under the application of IPsec protocol. The study has concluded that the throughput is degraded and the delay rises in a secured network. With the IPsec integration, the AODV protocol has the worst performance in terms of throughput and delay. The study has also simulated Intelligence Pulse Jamming Attack and Misbehaviour Attack on the network with IPsec that achieved the conclusion that the Misbehaviour Attack gives a better throughput than the Jamming Attack. However, their study did not include the use of TORA routing protocol as part of their research.

In [4] the authors have also simulated MANET using AODV with the addition of IPsec protocol using NS-2 simulator. Their study focuses more on the IPsec components i.e. Authentication Header (AH) and Encapsulation Security Payload (ESP), which have shown that AH-implemented data packets have minimum time overhead. Results also encourage implementing IPsec with ESP for all security services with moderate time overhead. Nonetheless, no attacks were performed in this study to further analyze the network's performance with such circumstances.

Another study [5] on MANET was conducted where the GloMoSim network simulator was used to simulate the effect of using the AODV routing protocol on the network. It is concluded that the AODV did not provide any security mechanisms to defend the network from attackers. Additionally, the authors have proposed Diffie-Hillman Key Algorithm as an alternative to improve the MANET.

The results between the simulated studies have shown that the implementation of different routing protocols varies with many aspects of the MANET itself.

In this project, simulations are divided into two stages. The first stage will show the performance of MANET with and without IPsec using AODV, OLSR and TORA under

978-1-5090-3071-2/16 $31.00 © 2016 IEEE
DOI 10.1109/IS3C.2016.110

normal operations and the second stage will show the exact simulation in Stage 1 but under Jamming attack instead.

A. Ad hoc On-Demand Distance Vector (AODV)

AODV is a reactive routing protocol that creates routes only when they are needed, thus minimizing the number of broadcasts. A sequence number is used to provide loop-free routing and also determine the freshness of the routes. AODV has routing tables, which contains the destination, next hop, number of hops, destination sequence numbers, active neighbours and the expiration time. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighbouring nodes in turn broadcast the packet to their neighbours and the process continues until the packet reaches the destination. Then the destination sends the route reply (RREP) packet to the source as the response.

B. Optimized Link State Routing (OLSR)

OLSR is a proactive routing protocol that stores and updates its routing table information permanently. It keeps track of routing table in order to provide a route if needed or route all time available for communication. OLSR can be implemented in all ad networks. OLSR finds its one-hop neighbours and its two-hop neighbours through their responses. The sender can then select its multipoint relays (MPR) 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 neighbours nodes within range of that node [6].

C. Temporarily Ordered Routing Algorithm (TORA)

TORA is highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. It uses directed acyclic graphs (DAG) to define the routes either as upstream or downstream. This graph enables TORA to provide better route aid for networks with dense, large population of nodes. However to provide this feature TORA needs synchronization of the nodes which limits the application of the protocol. TORA is a fairly complicated protocol but what makes it unique and prominent is its main feature of propagation of control messages only around the point of failure when link failure occurs. In comparison, all the other protocols need to re-initiate a route discovery when a link fails but TORA would be able to patch itself up around the point of failure. This feature allows TORA to scale up to larger networks but has higher overhead for smaller networks [7].

TORA performs four basic functions; route creation, route maintenance, route erasure and route optimization. Generating a directed sequence of links based on the height metric creates the route. The routine maintenance involves adapting the structure in response to topological changes. [8]

III. IPSEC PROTOCOL

As a solution to the security of mobile ad hoc network problems, the IPsec protocol is proposed. 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 [9]. 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 several subsequent components. The Authentication Header (AH) provides data authentication and integrity for IP packets that are passed between two systems, but does not provide data confidentiality (encryption) of packets. Whereas the Encapsulating Security Payload (ESP) is a security protocol that provides encryption of the IP packet where it authenticates the inner IP packet and ESP header [10]. Security Associations (SA) provides the necessary data and algorithm for the AH and ESP operations. Figure 1 below shows the AH and ESP in the Transport mode.

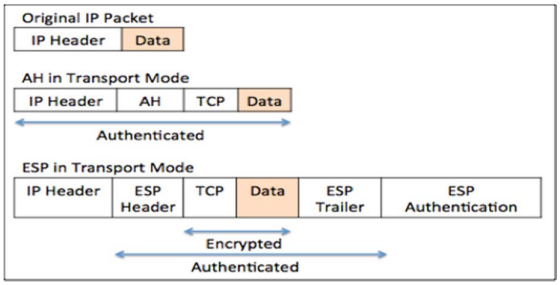

Figure 1. AH and ESP in Transport Mode

What makes IPsec a good solution to minimize the vulnerabilities and thus reducing the effects of attacks in MANET is that the IPsec protocol provides security services that are essential to a network. Unlike the routing protocols stated earlier, IPsec provides all-rounded confidentiality by encryption, data integrity, authentication and also anti-replay protection. Confidentiality ensures that the data cannot be read by anyone other than the person or destination that it was intended for. Meanwhile with integrity, it ensures that the data intended for a destination appears at its destination without being altered. For the destination of the data to verify that the source of the data is legitimate, authentication is needed. Anti-Replay protection detects and rejects the replayed packets and helps prevent spoofing.

IV. SIMULATION DESIGN

In order to simulate a realistic search and rescue operation in a MANET environment, the individuals that partake in the operation are represented as nodes. In this project, the nodes must be able to satisfy the requirements i.e. mobility, supports mobile ad hoc routing protocols, able to run applications, and has IPsec capability.

A. Stage 1 – Without Attack

In stage 1, the simulation is done without any attack. The chosen 'wlan_iphone' nodes are arranged randomly in an area of 500m x 500m where 15 nodes also share the common configuration. To simulate the effect of mobility, the nodes'

trajectory is set to vector. The *Application Configuration, Profile Configuration and Mobility Configuration* models are added to enable better management of application that are needed to be applied to the nodes.

The second scenario of Stage 1 is a duplicate of the first scenario with the addition of the IP Security demand model, which represents the IPsec protocol. This IPsec protocol is applied between all the nodes in a full mesh manner in order to get more accurate results.

B. Stage 2 – Jammer Attack

In the second stage, 3 jam pulsed node model were used to represent the jammer device as shown in Figure 3. These jammer devices are added to the network scenario that is duplicated from Stage 1. Similarly, the scenario with IPsec protocol from the first stage is replicated and the jammer devices are also added in the same way as the scenario without IPsec protocol.

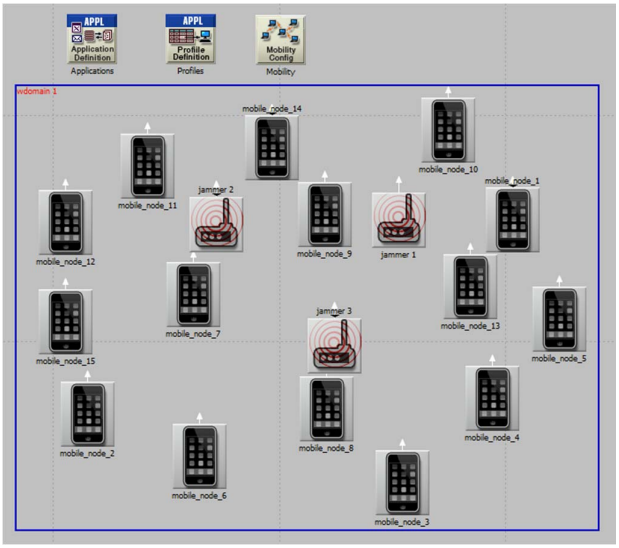

Figure 2. Layout of Jammer in MANET

1) Jammer Configuration

For Stage 2, the attributes to the jammer devices are configured. Since the mobile nodes are using the 802.11a WLAN, their frequency is automatically set to 5GHz and a bandwidth of 20MHz. Using the 802.11a WLAN also means that the nodes are using the Orthogonal Frequency Division Multiplexing (OFDM) multiplexing technique. This also contributes to the success of the attack by eliminating the use of Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS), as their use could prevent the occurrence of the jamming attack. At this point, it is assumed that the initial phase of the jammer trying to locate the actual bandwidth of the target is done. To cause interference to the communication, the jammer base band frequency is set to the same frequency as the mobile nodes i.e. 5,000MHz. The jammer is configured to run with 1,000,000kHz bandwidth value to give a worst-case scenario of the jamming attack. There are two ways to perform this attack successfully. Firstly is by increasing the jammer's pulse width from the default 1 second to a maximum of 10 seconds, yet still maintaining other attributes of the jammer parameter. But the drawback of this method is that it causes the simulator to crash. Secondly, is simply by increasing the number of jammer devices in the network to achieve a wider target range. The second method is used for this project as it produces more consistent result.

V. RESULTS

There are six scenarios in stage 1 of the simulation and all were simulated within the duration of 5 minutes; two scenarios for each of the routing protocols AODV, OLSR and TORA. The six scenarios demonstrate AODV without IPsec, AODV with IPsec, OLSR without IPsec, OLSR with IPsec, TORA without IPsec and TORA with IPsec. The simulation within the first 100 seconds shows a constant for all the scenarios to allow appropriate network convergence activity. The throughput, delay and number of hopes were compared for the different protocols. In stage 2 Jammer attack was included and the same set of simulation were carried out.

In stage 1, the results indicated that the throughput of OLSR routing protocol gives the highest value compared to AODV and TORA. With the implementation of IPsec protocol on all the three routing protocols, the simulations have shown a decrease in throughput. The AODV with the use of IPsec has the lowest value among the three as displayed in Figure 4.

During Stage 2 when under Jammer attack, the throughput shows that the scenario of AODV with IPsec protocol has a better performance compared to the scenario without IPsec protocol. The same result is also achieved with OLSR protocol. But, the IPsec protocol has no effect on the throughput on the TORA routing protocol when it is under attack shown in Figure 5.

We have used the arithmetic mean of value of the results in calculating the percentage difference of the performance metrics between the routing protocols as shown in Table 1 below. With the implementation of IPsec, it has shown deterioration of MANET's performance in all three routing protocols based on the decreased value in throughput, increase of delay, number of hops and also the retransmission attempts. The high retransmission attempts may indicate that the packet transmission has failed or it is discarded along the way. Although OLSR with IPsec has the highest percentage decrease in throughput, figuratively, OLSR still gives the highest throughput value shown in Figure 4. This could be due to the fact that OLSR is a proactive routing protocol whereby the route information is available immediately. AODV routing protocol is most affected by the IPsec protocol as it gives the largest percentage rise of delay of 119.0% and retransmission attempts of 26.43%.

Table 2 shows the different performance of MANET with the jamming attack. When the MANET is under attack, the IPsec still adds delay to the network as expected, but the delay improves significantly in all routing protocols in

contrast with the scenarios in Stage 1 without attack. The delay in AODV drops to only 5.787% from the previous result of 119.0% in stage 1. The throughput is also enhanced in this stage, except with TORA protocol that did not have any changes with the implementation of IPsec.

Based on the statistics above, it has shown that the IPsec protocol has achieved its purpose in providing its security services and managed to ensure the security of the network from a more damaging physical layer attack. The simulation has nonetheless supported the initial prediction whereby with the addition of the IPsec protocol, throughput of the network will decrease and the delay will increase as a result of the overhead.

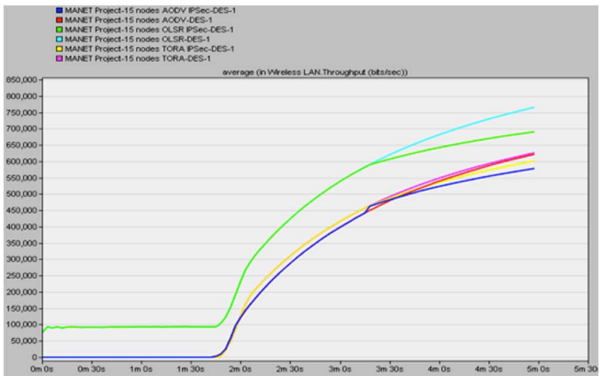

Figure 3. Stage 1 Throughput values with IPsec

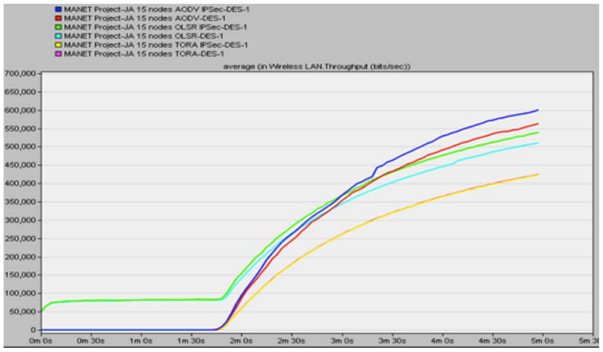

Figure 4. Stage 2 Throughput values with IPsec under attack

TABLE I. MANET STAGE 1 PERFORMANCE COMPARISON

	Routing Protocols		
	AODV	***OLSR***	***TORA***
Throughput (%)	-3.373	-7.688	-2.346
Delay (%)	+119.0	+49.75	+12.04
Retransmission Attempts (%)	+26.43	+22.73	+11.04

TABLE II. MANET STAGE 2 UNDER ATTACK PERFORMANCE COMPARISON

	Routing Protocols		
	AODV	***OLSR***	***TORA***
Throughput (%)	+9.898	+6.536	0
Delay (%)	+5.787	+8.889	+7.330
Retransmission Attempts (%)	-5.660	-1.747	+1.587

VI. CONCLUSION

Based on the MANET simulations using three different protocols, implementing the IPsec protocol introduces an overhead to the packets during transmission thus reducing the throughput on the network as well as increasing the delay and retransmission attempts. Although there is still a slight delay, it is proven that the IPsec protocol indeed serves its primary purpose to provide security services as shown in the simulation where the MANET under attack performs better with the implementation of IPsec protocol. In normal operation, the OLSR routing protocol with IPsec still gives the highest throughput value although it has the highest percentage decrease in throughput. In terms of delay and retransmission attempts, OLSR has achieved the lowest in normal operation. On the other hand, when the MANET is under attack, the AODV with IPsec gained the highest throughput. Delay and retransmission attempts are the highest with OLSR when it is under attack. Therefore, using the OLSR protocol is recommended in preventing Jamming attack and it is crucial for a MANET when a high throughput is desired.

REFERENCES

[1] Bakshi, A., Sharma, A., & Mishra, A. (2013). Significance of Mobile AD-HOC Networks (MANETS) . *International Journal of Innovative Technology and Exploring Engineering (IJITEE) , 2* (4), 1-5.

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

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

[4] Adas, A. A., & Shawly, T. A. (2010). Simulation of IPsec Protocol in Ad-Hoc Networks. *JKAU: Eng. Sci , 21* (2), 3-14.

[5] Jaiswal, K., & Prakash, O. (2014). Simulation of MANET using GloMoSim Network Simulator. *International Journal of Computer Science and Information Technologies , 5* (4), 4975-4980.

[6] 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.

[7] 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.

[8] Ilyas, M., & Mahgoub, I. (2004). *Mobile Computing Handbook.* New York: CRC Press.

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

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