Journal of Engineering and Applied Sciences 13 (24): 10401-10405, 2018
ISSN: 1816-949X

A Secure Data Transmission Mechanism (SDTM) in MANET by Using AODV Routing Protocol with IPsec Protocol and Preemption Control Algorithm

[1]Abdullah A. Alhaj and [2]Nabeel Zanoon
[1]Department of BIT, Faculty of IT and Systems, University of Jordan, Aqaba, Jordan
[2]Department of Applied Science, Al-Balqa Applied University, Aqaba, Jordan

Abstract: The MANET has become a significant topic in computer networks, however, the trend has established a new range of security issues that need to be addressed. One of the main advantages of using the Ad hoc wireless networks is that no infrastructure required creating this network. These nodes are characterized by random motion and dynamic movement in the network with no secure data transmission path. In this study, we analyze the performance of AODV protocol with IPsec and preemption control algorithm to provide secure data transmission mechanism with and without black hole attacks, to study the effect on the quality of service parameters in the network by using NS2 simulation program, through the multi-scenarios and some of metrics to analyze the efficiency of the system.

Key words: SDTM, IPsec, Ad hoc networks, AODV routing protocol C, NS2 simulator, NAM, Xgraph, blackhole

INTRODUCTION

Mobile Ad hoc Network (MANET) consists of two or more connections without the need for an infrastructure to create this technique present in cellular communication devices. This kind of network does not need a central point and each point could operate transceiver and server to pass the signal, this technique is used in emergency and military applications that want quick solutions to wireless network without creating a central data server but because of the nature of the network that enables any node to enter and exit of the network without any restriction, this allows attackers to spy on data and to drop packets sent between network nodes, this study has been reviewed a type of attack called blackhole attack and its impact on the network with the AODV routing protocol, this study has been used simulation program called NS2 to study MANET network (Raju *et al*., 2000) to provide a secure data transmission mechanism for civil and military uses (Fig. 1).

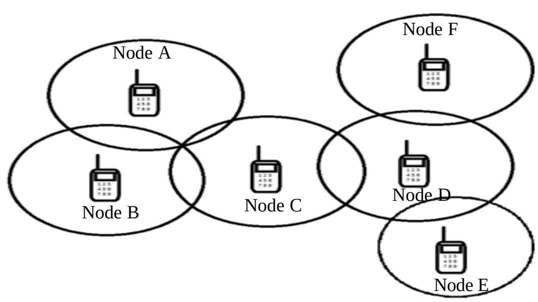

Fig. 1: A group of nodes associated with technical cooperation agents

MATERIALS AND METHODS

AODV routing protocol: The Ad hoc on-Demand Distance Vector (AODV) is a kind of protocols used by cellular node quick movement and permanent adaptation without any restriction for entry and exit nodes from the network and are used in ad hoc networks. This protocol ability from other public sources at lower consumption when used as energy use and the use of resources such as memory and processor for the decade few compared to the other (Perkins *et al.*, 2003). The AODV routing protocol uses a route table that records information on the latest paths used by the node and doing the path discovery function between the source and the destination and the path maintenance function to ensure that the delivered packets are correct for the destination (John and Thomas, 2012).

Blackhole attack: Blackhole attack (Dokurer *et al*., 2007) is one of the attacks doing Denial of Service (DoS) (Shevtekar *et al*., 2005; Al-Shurman *et al*., 2004) with reduce or prevent the completion of the work protocols, especially the AODV protocol. Through the route discovery process, the sender node sends RREQ packets to the nodes of same range of radio to find best path to the destination subject. Attacker nodes respond immediately to the sender node as subject to the routing table. The sender node assumes that the route discovery process is done, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The attacker node does this by assigning a high sequence number to the reply packet.

Corresponding Author: Abdullah A. Alhaj, Department of BIT, Faculty of IT and Systems, University of Jordan, Aqaba, Jordan

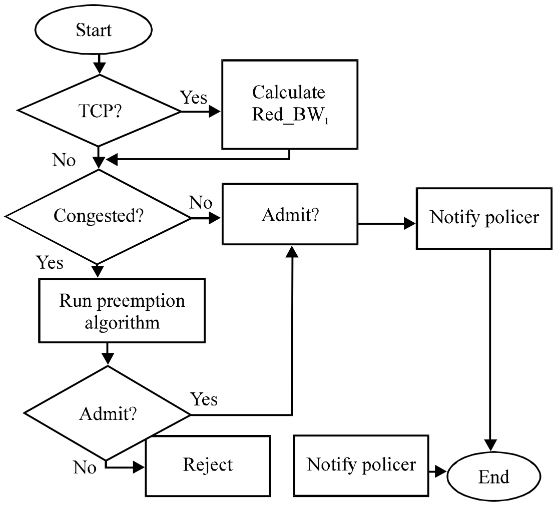

Fig. 2: Secure data transmission mechanism

The malicious node doing drops of packet received from sender node and else (Sanzgiri *et al*., 2002; Yih-Chun and Perrig, 2004).

Secure data transmission mechanism with preemption control algorithm: This data transmission mechanism assumes a distributed bandwidth negotiator (Alhaj, 2014) architecture as depicted in Fig. 2. A Bandwidth Negotiator (BN) is located in each node of the MAN interconnected together: BN is responsible for regulating traffic going into the MAN. Suppose a host in node A has a flow of traffic that needs to be sent to node B, the requesting node A would first make a request to the BN by sending the amount of requested bandwidth to BN. BN would run the SDTM based on real-time measurements made on the existing traffic at the destination side. If an admit decision is made, the requesting host starts sending traffic and the policer is also informed to police the traffic. If a reject decision is made, the requesting host is notified about the decision. In addition, policer is informed to prevent the rejected flow from entering into the public network (Waraich and Singh, 2015). In order for the source to quickly make an admission/preemption decision, we believe the most valuable piece of information is the amount of carried traffic, i.e., the amount of traffic that is successfully sent through the MAN. Therefore, at node B, a measurement device measures the amount carried traffic. Such measurements are done on a per Differentiated Services Code Point (DSCP) basis.

The measurements are periodically sent back to node A which are used for the SDTM and preemption algorithm. Suppose due to congestion in the MAN, the bandwidth of a link along the path in the MAN suddenly decreases to the extent that the link bandwidth is no longer able to support the amount of offered traffic. After a “congested” state is declared by the measurement device in node B and the BN at node A is notified, the preemption algorithm is triggered and a fraction of the ongoing traffic flows are preempted. Then both the affected hosts and Policer are notified by BN. Determination of the traffic flows to be preempted upon congestion or blockage is based on the carried traffic measurements, per-call requested bandwidth and a set of pre-defined policy (e.g., a policy based on MLPP described in Developed draft straw man DSCP mapping for GIG enterprise IP networks nd). Compared to the conventional Bandwidth Broker (BB) such as the one described in, IPsec Developers Forum, nd) in which BB is assumed to have global knowledge about the network, this SDTM utilizes a distributed architecture. Namely, each BN makes admission and preemption decision solely based on the feedback from the destination and there is no other inter BN information exchanged. In addition, BN is consulted only when a call needs to traverse through the public network. If a call originated from node A does not need to go through the MAN, BN will not be consulted. The detailed description of this algorithm is shown in Fig. 2 adopted from (Ipsec Developers Forum).

For UDP flow, the requested bandwidth is assumed to be the encoding rate of the codec. For TCP flows, the requested bandwidth is calculated as file size/speed of service requirement. The result is then sent to PSM where a leaky bucket algorithm is used to regulate the traffic. An alternative way to determine the requested bandwidth for TCP flows would be to deterministically assign a fixed value. We also note that the Preemption algorithm is run as part of the data transmission mechanism. Suppose a high priority flow (e.g., a flash overwrite flow) requests for admission and the congested flag is on, lower priority flows may need to be preempted to accommodate the higher priority call as mandated by the preemption policy. When the “congested” flag is set by the measurement device, the preemption algorithm is triggered to preempt existing flows. Preemption algorithm is shown in Fig. 3 in which two examples of preemption policy are presented? We note that, the preemption policy can be set by the network operator dynamically, according to, the need of the underlying mission. By carefully observing Fig. 2, we note that the data transmission algorithm shows a strong “reactive” nature, i.e., traffic will be admitted until congested state is declared. If the “available bandwidth” can be determined through bandwidth estimation techniques, the data transmission algorithm can be made more “proactive”, namely, traffic flows are rejected before

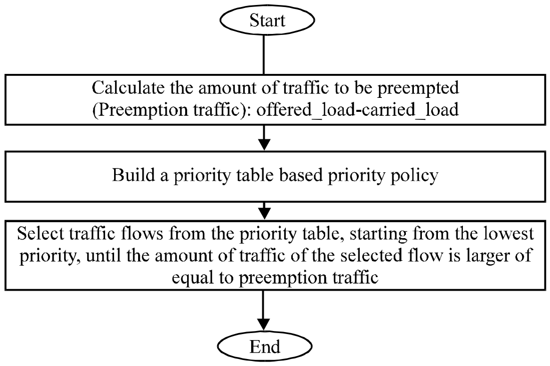

Fig. 3: Preemption algorithm

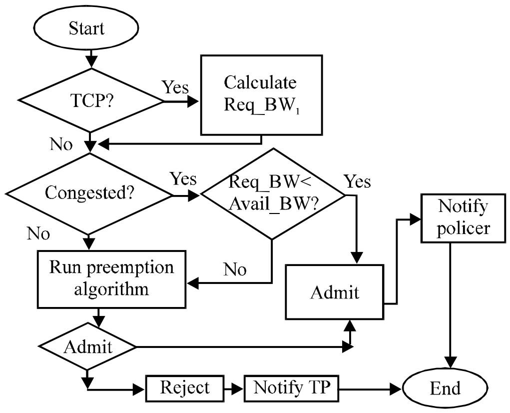

Fig. 4: Data transmission algorithm when available bandwidth can be obtained through bandwidth estimation techniques

congestion is observed. In a companion study (Djenouri *et al*., 2006) powerful bandwidth estimation techniques are presented such that the bottleneck link band-width (defined as the link with the smallest amount of bandwidth along the path) and avail-able bandwidth (defined as how much band-width "headroom" along the path for new traffic) are estimated. They can then be used in the data transmission as shown in Fig. 4. Our analysis showed that using bandwidth estimation, congestion avoidance can be effectively achieved.

RESULTS AND DISCUSSION

NS2 simulation: NS2 is widely used simulator by researchers, it is event driven object oriented simulator, developed in C++ as back end and TCL (Tool Command Language) as front end. If we want to deploy a network then both TCL as scripting language with C++ to be used, we used for simulation NS-2[2.35] Network Simulator (Issariyakul and Hossain, 2011).

Table 1: Simulation parameters

Simulator	NS-2 (Version 2.35)
Simulation time	900 sec Val (stop)
Routing protocol	AODV
Attack type	Blackhole attack with random movement
Area size	750×750
Node placement	Uniform distribution
Simulation traffic	CBR OVER UDP
Number of nodes	20,70,120,170,220
Packet size	512
Mac protocol	IEEE 802.11

Table 2: The average throughput rate in a set of different scenarios

	Average throughput (kbps)		
Number of run	AODV	AODV with black	IPsec with black hole
Simulation 1	30.37	38.28	10.67
Simulation 2	69.75	10.06	16.34
Simulation 3	75.12	24.53	29.56
Simulation 4	80.83	20.50	33.87
Simulation 5	69.13	16.48	25.13
Average (%)	65.04%	21.97%	23.11%

Table 3: The average packet delivery ratio in a set of different scenarios

	Average packet delivery ratio		
Number of run	AODV	AODV with black	IPsec with black hole
Simulation 1	32.46	40.92	11.41
Simulation 2	74.46	8.91	16.99
Simulation 3	80.30	26.22	31.59
Simulation 4	86.40	21.20	36.20
Simulation 5	73.89	16.86	26.86
Average (%)	69.50%	22.82%	24.61%

Simulation parameters: For simulation, we have used Mobility scenarios are generated by varying (20,70,120,170,220) nodes moving in simulation area of 750×750 m and distributed in random way. We have used the following parameters. The simulation parameters observe by using Network Animator (NAM). The below figures are the snapshots of simulation environment (Table 1).

Performance evaluation in average throughput rate: Based on Fig. 5, using AODV protocol in normal profile represented by the blue columns shows that the average throughput is 65.04%, however, about 34.60% of average throughput loss occurred because of congestion, limited energy and dynamic movement of nodes (Table 2).

Furthermore, the study used a black hole attack and recorded readings on different distributions in the network. Table 3 and Fig. 6 showed that the average throughput in the networks represented by the red columns is 21.97% which occurred due to a single node impact from a black hole.

IPsec was also used to reduce the effect of the black hole attack. The program was loaded with each node in the same scenario. It improved the networks and data transfer. The average throughput increased from 21.97-23.11% with an improvement rate of about 1.14%.

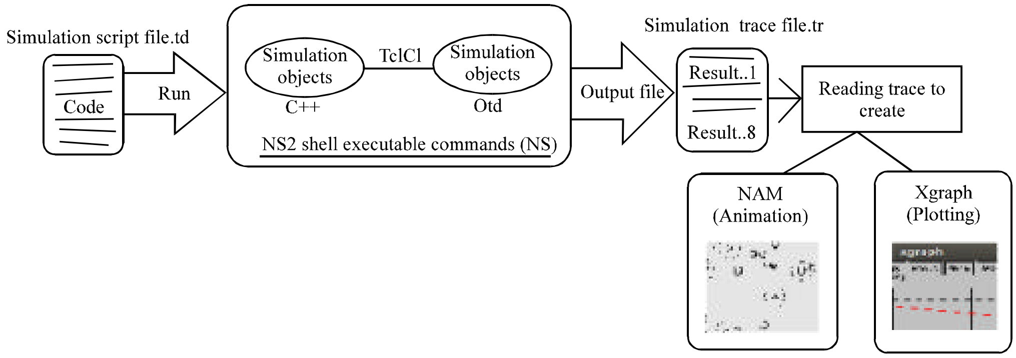

Fig. 5: Basic architecture of NS2 (Issariyakul and Hossain, 2011)

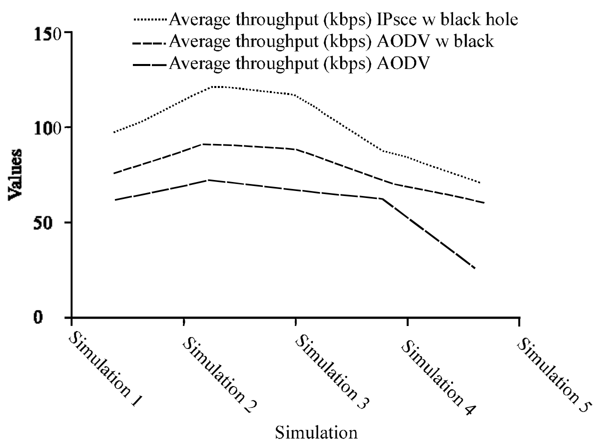

Fig. 6: The average throughput rate in a set of different scenarios

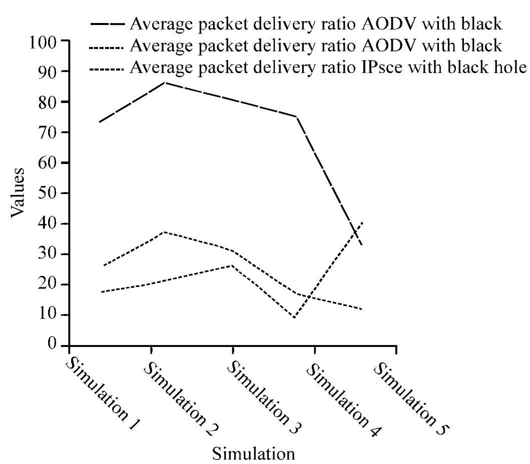

Fig. 7: The average packet delivery ratio in a set of different scenarios

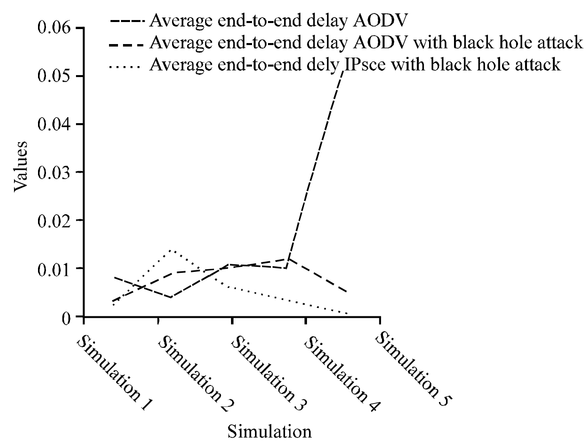

Fig. 8: The average end-to-end delay in a set of different scenarios

Table 4: The average end-to-end delay in a set of different scenarios

Number of run	AODV	AODV with black hole attack	IPsec with black hole attack
Simulation 1	0.0530	0.0051	0.0004
Simulation 2	0.0100	0.0119	0.0030
Simulation 3	0.0105	0.0104	0.0060
Simulation 4	0.0037	0.0087	0.0140
Simulation 5	0.0081	0.0029	0.0016
(Avg.*1000)%	17.06%	7.80%	5.00%

Average end-to-end delay

Performance evaluation in packet delivery ratio: Table 4 and Fig. 7 show the average packet delivery ratio in a set of different scenarios. First the average packet delivery ratio with normal behavior, represented by the blue columns was about 69.50% but with AODV and blackhole attack, the average packet delivery ratio, represented by the red columns was about 22.82% by using the IPsec, the average packet delivery ratio increased by about 1.79% of black hole affect and the IPSEC result of average packet delivery ratio, represented by the green columns was about 24.61% (Fig. 8).

Performance evaluation in average end-to-end delay: Table 4 and Fig. 8 show the average end to end delay in

AODV protocol in normal behavior which is represented by the blue columns at about 17.06% but with AODV and black hole attack the average end to end delay, represented by the red columns, was about 7.80% and with the IPsec with black hole attack, the average end to end delay, represented by the green columns was about 5.00%.

CONCLUSION

Due to various critical situations and perceptive applications, data packet security needs to be achieved in ad-hoc networks but guaranteeing complete security in such a network may be impossible if the nodes are too mobile and suddenly compromised. The proposed secure data transmission mechanism with IPsec implementation attempts to ensure data communication security.

In this study, we chose the AODV routing protocol because it is the best and most convenient among the protocols used in ad hoc networks. We conducted a study of the efficiency of the network without the presence of attacks and the impact of attacks on the network. We conducted the experiment through the NS2 simulation program, using the average Throughput to measure network efficiency. The study showed that, the low rate of average throughput in the network is due to attacks and the problem of congestion and sending and receiving data packets with IPsec needs more time as compared to sending data packets without IPsec.

REFERENCES

Al-Shurman, M., S.M. Yoo and S. Park, 2004. Black hole attack in mobile ad hoc networks. Proceedings of the 42nd International Conference on Annual Southeast Regional, April 02-03, 2004, ACM, New York, USA., ISBN:1-58113-870-9, pp: 96-97.

Alhaj, A.A., 2014. Performance evaluation of Secure Data Transmission Mechanism (SDTM) for cloud outsourced data and Transmission Layer Security (TLS). Intl. J. Cloud Appl. Comput., 4: 45-49.

Djenouri, D., A. Derhab and N. Badache, 2006. Ad hoc networks routing protocols and mobility. Intl. Arab J. Inf. Technol., 3: 126-133.

Dokurer, S., Y.M. Erten and C.E. Acar, 2007. Performance analysis of ad-hoc networks under black hole attacks. Proceedings of the 2007 IEEE International Conference on SoutheastCon, March 22-25, 2007, IEEE, Richmond, Virginia, USA., pp: 148-153.

Issariyakul, T. and E. Hossain, 2011. Introduction to Network Simulator NS2. Springer, Germany.

John, N.P. and A. Thomas, 2012. Prevention and detection of black hole attack in AODV based mobile Ad-hoc networks-a review. Intl. J. Innovative Res. Dev., 1: 232-245.

Perkins, C., E. Royer and S. Das, 2003. RFC 3561 Ad hoc on-demand distance vector (AODV) routing. The Internet Society. http://www.citeulike.org/user/sergiocabrero/article/1840161.

Raju, G.V.S., G. Hernandez and Q. Zou, 2000. Quality of service routing in ad hoc networks. Proceedings of the 2000 IEEE International Conference on Wireless Communications and Networking (WCNC) Vol. 1, September 23-28, 2000, IEEE, Chicago, Illinois, pp: 263-265.

Sanzgiri, K., B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer, 2002. A secure routing protocol for ad hoc networks. Proceedings of the 10th IEEE International Conference on Network Protocols, November 12-15, 2002, IEEE, Paris, France, pp: 78-87.

Shevtekar, A., K. Anantharam and N. Ansari, 2005. Low rate TCP denial-of-service attack detection at edge routers. IEEE Commun. Lett., 9: 363-365.

Waraich, K.K. and B. Singh, 2015. Performance analysis of AODV routing protocol with and without malicious attack in mobile adhoc networks. Intl. J. Adv. Sci. Technol., 82: 63-70.

Yih-Chun, H. and A. Perrig, 2004. A survey of secure wireless ad hoc routing. IEEE Secur. Privacy, 2: 28-39.