International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2016 IJSRCSEIT | Volume 1 | Issue 1 | ISSN : 2456-3307

A Case Study on Mobile Adhoc Network Security for Hostile Environment

Dr. D. Devi Aruna, Dr. D.Vimal Kumar

Department of Computer Science, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India

ABSTRACT

A mobile adhoc network (MANET) is a peer to peer wireless network where nodes can communicate with each other without infrastructure. Due to this nature of MANET; it is possible that there could be some malicious and selfish nodes that try to compromise the routing protocol functionality and makes MANET vulnerable to Denial of Service attack in military communication environments. Hence security is an important challenge while deploying MANET. This research effort examines the case study for a Layerwise Security (LaySec) framework that provides security for an ad-hoc network operating in a military environment. LaySec incorporates three security features (Secure neighbor authentication and Layerwise Security techniques and multipath routing) into its framework while maintaining network performance sufficient to operate in hostile environment. layerwise security protocol has been implemented and simulated on Qualnet 5.0. Based on the simulation result, it is observed that the proposed approach has shown better results in terms of Quality of Service parameters like Average packet delivery ratio, Average throughput, Average end to end delay and Routing Overhead.

Keywords : Mobile Adhoc Network, Layer Wise Security Protocols, Denial of Service Attack.

I. INTRODUCTION

Recent years Mobile ad hoc Networks start gaining attention from the industrial and academic research community due to their wide deployment and inherent nature of solving practical real world applications[1][4].The ease of deployment without the existing infrastructure makes ad hoc networks an attractive choice for dynamic situations such as military operations, disaster recovery, and so forth. Especially, military communication environments have been considered as one of the original motivations for MANET, due to the need for battlefield survivability and rapid deployment of self-organizing mobile infrastructure. This research work evaluates the case study for mobile adhoc network with concentration to defend against Denial of Service attack in MANET layers. A military case study scenarios is introduced: the scenario modifies its channel and physical layer settings for army military devices in an unknown and unstable MANET military environment system with concentration to defend against Denial of Service attack[2].

The paper is organized in such a way that Chapter 2 discusses Review of Literature, Chapter 3 discusses problem statement,, Chapter4 discusses proposed method, Chapter5 discusses Experimental evaluation and Chapter6gives the conclusion.

II. METHODS AND MATERIAL

2. Review of Literature

2.1 Denial of Service attack

This chapter briefly describes the Denial of Service Attacks for MANET.

An attacker attempts to avoid authorized and legitimate users from the services offered by the network. The typical way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operate in the manner in which it is designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. DoS attacks can be launched against any layer in the network protocol stack. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the ongoing transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session but simply drop a certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bringdown critical services such as the key management service. For example, consider the following: In figure1 assume a shortest path that exists from S to X and C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial of service attack. Suppose S wishes to communicate with X and that S has an unexpired route to X in its route cache. S transmits a data packet towards Xwith the source route S --> A --> B--> M --> C --> D--> X contained in the packet's header. When M receives the packet, it can alter the source route in the packet's header, such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to forward the packet toX. Since X cannot hear C,the transmission is unsuccessful [2][3].

$$S \leftrightarrow A \leftrightarrow B \leftrightarrow M \leftrightarrow C \leftrightarrow D \leftrightarrow X$$

Equation 1 : Denial of Service attack

3. Problem Statement

This research investigates how to integrate security policies of a MANET with secure neighbor authentication that will allow the MANET to function securely in a military environment without degrading network performance. The specific problem to be addressed is how to use secure neighbor authentication of nodes in a multipath routing algorithm in MANET protected from Denial of service attack in military environment. Most of such performance analysis are normally done on commercial settings. For instance, wireless LAN technologies in the 2.4 GHz ISM frequency band are generally assumed, offering data rates up to 2 Mbps within the range of 250 m. This paper is motivated by the observation that such propagation and network models assumed by the current ad hoc networking simulations are quite different from real world military environments. In fact, a few hundred MHz frequency band (i.e., VHF or even HF) is used with very low data transmission rates (e.g., 384 Kbps) for the military scenarios

4. Proposed Methodology

This approach aims in improving the performance in terms of QoS characteristics as metrics. The methodology is proposed in order to assure Layerwise security for Mobile Ad hoc Networks. The specific contributions are structured in six phases.

Phase I. Integration of SNAuth with SPMAODV
Phase II. SNAuth-SPMAODV with SIP for Application and Network layer Security
Phase III. SNAuth-SPMAODV with WTLS for Transport and Network Layer Security
Phase IV. SNAuth-SPMAODV with IPSec for Network Layer Security
Phase V. SNAuth-SPMAODV with CCMP-AES for Link and Network Layer Security
Phase VI. SNAuth-SPMAODV with DSSS for Physical and Network Layer Security

Integration of SNAuth with SPMAODV SPMAODV provides multiple paths between sender and receiver nodes that can be used to offset the dynamic and unpredictable configuration of ad-hoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth. The proper selection of routes using a strict-priority multipath protocol can increase further the network throughput. The main idea of this phase to integrate strict priority multipath AODV with secure neighbor authentication that facilitate neighboring nodes exchange messages to discover and authenticate each other. Thus this phase provides security mechanism like message integrity, mutual authentication, and non-repudiation; defend against Denial of Service attacks and increase network throughput.

SNAuth-SPMAODV with SIP for Application and Network layer Security Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing) with Session Initiation Protocol (SIP) provides application layer and network layer security and it is robust against Denial of Service attack. It reduces dependency on single nodes and routes; it discovers multiple paths between sender and receiver nodes and it has the advantages of a multipath protocol without introducing extra packets into the network offering robustness in a secured MANET. It can be used to offset the dynamic and unpredictable configuration of adhoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth in hostile environment [15].

SNAuth-SPMAODV with WTLS for Transport and Network Layer Security The primary focus of this phase is to provide transport layer security for authentication, securing end-to-end communications through data encryption and to provide security services for both routing information and data message at network layer. It also handles delay and packet loss. The proposed model combines SNAuth-SPMAODV Routing with Wireless Transport Layer Security (WTLS) to defend against Denial of Service (DoS) attack and it also provides authentication, privacy and integrity of packets in routing, end-to-end communications through data encryption, packet loss and transport and network layers of MANET [14]. SNAuth-SPMAODV with WTLS is found to be a good security solution even with its known security problems[9].

SNAuth-SPMAODV with IPSec for Network Layer Security Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing) with IPSec is robust against Denial of Service attack and it also provides security services for both routing information and data message at network layer in MANET.The proposed method uses a hybrid version of the IPSec protocol, which includes both AH and ESP modes. IPSec is a protocol suit for securing IP based communication focusing on authentication, integrity, confidentiality and support perfect security forward. The significant importance of the aforementioned protocol is that it offers flexibility, which cannot be achieved at higher or lower layer abstractions in addition to the symmetric cryptographic schemes [11]. These are 1000 times faster than asymmetric cryptographic schemes, a fact that makes IPSec appropriate to be used in handheld resources constrained devices such as PDAs. SNAuth-SPMAODV with CCMP-AES for Link and Network Layer Security.

SNAuth-SPMAODV combines with CCMP-AES model to defend against Denial of Service attack and it provide confidentiality and authentication of packets in both network and data link layers of MANETs[2]. The primary focus of this phase is to provide security mechanisms applied in transmitting data frames in a node-to node manner through the security protocol CCMP-AES working in data link layer. It keeps data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination.

SNAuth-SPMAODV with DSSS for Physical and Network Layer Security SNAuth-SPMAODV combines with DSSS to defend against Denial of Service attack. The physical layer protocol in MANETs is reliable for bit-level transmission between network nodes and network layer is responsible to provide security services for both routing information and data message [10]. The proposed model combines SNAuth-SPMAODV routing protocol and spread spectrum technology Direct Sequence Spread Spectrum (DSSS) to defend against signal jamming denial-of-service attacks in physical layer and network layer for MANET.

III. RESULTS AND DISCUSSION

A. Experimentation and Evaluation

Using the QualNet network simulator [7], comprehensive simulations are made to evaluate the protocol. Qualnet provides a scalable simulation environment for multi-hop wireless ad hoc networks, with various medium access control protocols such as CSMA and IEEE 802.11. channel and physical layer settings are modified to apply more realistic military scenarios. Note that PRC 999K device is used as a reference model. 802.11 DCF and UDP protocols are used for MAC and a transport protocols, respectively. Also, CBR traffic is utilized in the study. As the TCP based application protocols such as telnet or FTP show unstable performance in mobile wireless communication, it cannot evaluate precise performance of routing protocol itself. CBR application model sends one packet per second, which represents relatively low traffic patterns in military environments. Each packet size is 512 Bytes. In military environments, operational network size is very large as compare to conventional case. Nodes in the simulation are assumed to move according to the "random way point" mobility model. Pause time is fixed to 20 seconds. The attackers are positioned around the center of the routing mesh in all experiments. To evaluate the performance of proposed method by 4 measurements: Packet delivery radio, average end-to-end delay, routing overhead and Throughput.This simulated environment is defined by the following parameters as shown in Table 1 and Table 2.

Table 1: Simulation Metrics of Laysec Framework for Military Scenario

Parameter	Value
Simulator	Qualnet 5.0
Transmitter range	300 meters
Bandwidth	2 Mbps
Interface queue length	100 packets
Traffic type	VBR
Packet size	512 bytes
Simulation time	10000 sec
Number of trials	30
Topology size	1500m x 1500m
Number of nodes	100 to 600
Maximum speed	3m/sec 5m/s, 10m/sec, 15m/sec

Table 2: Physical Layer Model for Hostile Environments

Parameters	Military devices
Frequency	30-300 *MHz*
Propagation limits	-120 *dBm*
Radio propagation model	Two-Ray
Data rates	*200 Kbps*
Transmit power	45 *dBm*
Receive sensitivity	-150 *dBm*
Reference model	PRC-999K device

B. Performance Evaluation

The performance analysis of Layerwise security framework with SNAuth-SPMAODV has been conducted using the simulation setup for Hostile Environment as outlined in Table 2 and 3. The simulation scenarios consist of different network density or size is assessed by deploying a different number of mobile nodes over a space of 1500m x 1500m.

Average Packet Delivery Ratio (PDR)

In Figure 1, the Average Packet Delivery Ratio of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV for different network sizes of 100 to 600 nodes are placed in a topology area of 1500m x 1500m. Packet delivery ratio shows how successfully a protocol performs delivering packets from source to destination.

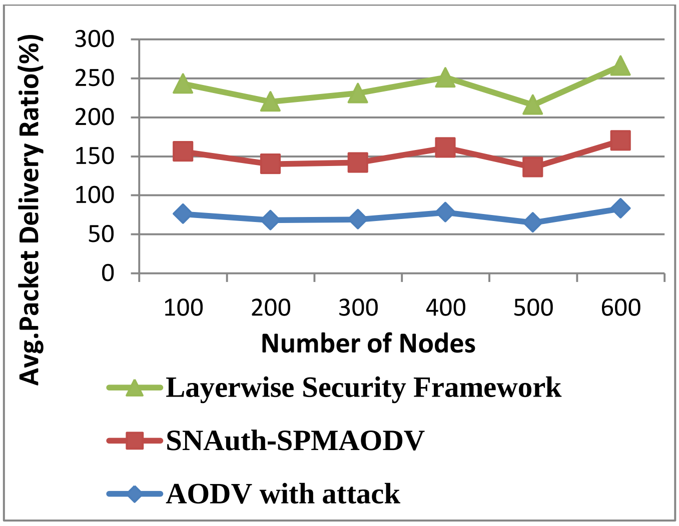

Figure 1 : Average Packet Delivery Ratio

Average Throughput

Figure 2 shows the network throughput is the average rate of successful message delivery over a communication channel.

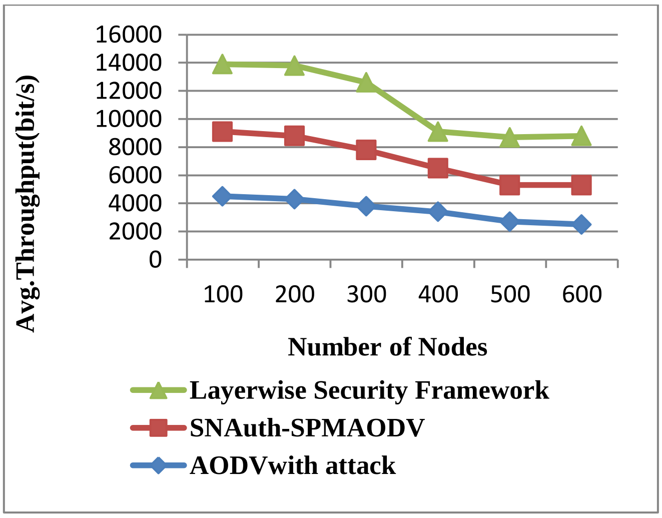

Figure 2 : Average Throughput Ratio

Average End-to-End Delay

Figure 3 shows an average end-to-end delay of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV according to the increase of network density. Layerwise Security Framework with SNAuth-SPMAODV exhibits the lowest end-to-end delay most of the time. AODV has much higher end-to-end delay than proposed method. Layerwise Security Framework with SNAuth-SPMAODV keeps up good performance in delay as the network density becomes high. Layerwise Security Framework with SNAuth-SPMAODV performs poorly in sparse networks. (eg 200 to 300 nodes)

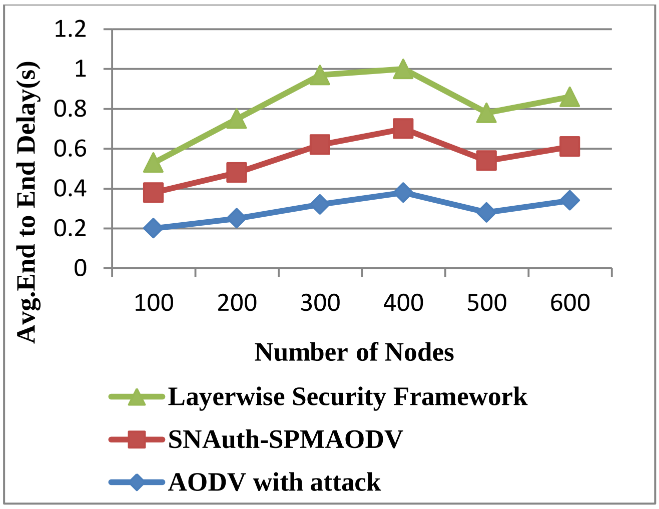

Figure 3 : Average End to End Delay

Routing Overhead

Figure 5 illustrates the routing overhead generated by the proposed framework when the number of nodes is varied. The figure shows that the generated routing overhead in AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased number of nodes. Layerwise Security Framework with SNAuth-SPMAODV performs well compared to AODV and SNAuth-SPMAODV

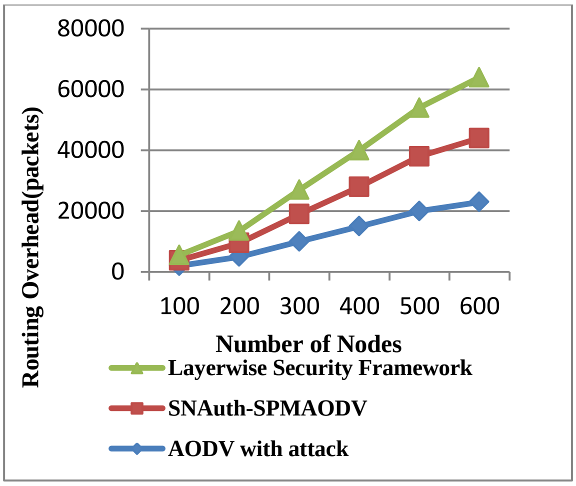

Figure 5 : Routing Overhead

IV.CONCLUSION

Mobile ad hoc networks (MANETs) can be applied to many situations without the use of any existing network infrastructure or centralized administration. In hostile environment, there is a need for the network to route packets through dynamically mobile nodes. MANETs can be considered as the solution for this highly mobile and dynamic military network. However it is not appropriate to directly apply conventional mobile ad hoc networks scheme to military network, since military communication system is different from conventional counter parts both in device's physical layer specification and networking environment. Therefore consider these particularities of military communication system through simulation, and evaluate the performance of Layerwise security framework on the assumed military environment. In simulation results, the proposed methods provide good performance with every measurement metric in high network density environment

V. REFERENCES

[1] Arunkumar B. R., Reddy L.C., and Hiremath P.S., 2008, "A Survey of Mobile Ad Hoc Network Routing Protocols" Journal of Intelligent System Research, 8(6), 49-64.

[2] Bajaj. L., Takai.M., Ruja.R., Tang.K., Bagrodia.R., and Gerla.M.,1999,"GlomoSim: A Scalable Networks Simulation Environments", UCLA Computer Science Departments Technical Report 900027.

[3] Biswas K., Ali L., 2001, "Security Threats in Mobile Ad Hoc Network" Department of Interaction and System Design School of Engineering, 1-39.

[4] Boomaranimalany.A., Dhulipala.S., and Chandrasekaran R.M, 2009, "Throughput and Delay Comparison of MANET Routing Protocols"International Journal Open Problems Computational Mathematics, ICSRS Publications, 2(3), 461-468.

[5] Chenna. P and Dr. ChandraSekhar.P., 2007, "Performance Analysis of Adhoc Network Routing Protocols", International Symposium on Ad Hoc and Ubiquitous Computing, ISAUHC'06, 17, 186 – 187.

[6] Dwivedi.A.K., kushwaha.S., and Vyas O.P., 2009,"Performance of Routing Protocols for Mobile Ad hoc and wireless sensor networks: A Comparative study", International Journal of Recent Trends in Engineering, 2(4) ,101-105.

[7] Garg.N. and Mahapatra.R.P, 2009, "MANET Security Issues". International Journal of Computer Science and Network Security, 9(8), 241-246.

[8] Islam.S, 2006, "Implementation & Comparison of IPSec Protocols for Secure Datab Communication in Ad-Hoc Networks", Royal Institute of Technology.

[9] Jang H.C., Lien Y.N., and Tsai T.C., 2009 ,"Rescue Information System for Earth-quake Disasters Based on MANET Emergency Communication Platform" Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World wirelessly, 623–627.

[10] Junaid.M., Dr Muid Mufti and Ilyas M.U., 2006, "Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol", In the Proceedings Of World Academy Of Science, Engineering And Technology, 11, 228-233.

[11] Pravin P.G., and Katkar G.G., 2010,"Mobile Ad Hoc Networking: Imperatives and Challenges", IJCA Special Issue on MANETs, 153–158.

[12] Reidt S., and Wolthusen S.D, 2008, "Exploiting UAVs Capabilities in Tactical MANETS". Proceedings of the 2nd Annual Conference of ITA ,322–323.

[13] Salsano,, Veltri S., and Papalilo D., 2002,"SIP Security Issues: The SIP authentication procedure and its processing load" IEEE Network,38-44.

[14] Taneja K., and Patel R.B., 2007, "Mobile Ad hoc Networks: Challenges and Future" Proceedings of National Conference on Challenges & Opportunities in Information Technology pp. 133-135.

[15] Vaidya.B. and Lim H., 2009 "Secure Framework for Multipath Multimedia Streaming Over Wireless Ad Hoc Network". Proceedings of the 2009 IEEE Conference on Wireless Communications & Networking Conference,2678–2683.

[16] D.Devi Aruna and Dr.P.Subashini.,2014," Layerwise Security Framework with Snauth-SPMAODV to Defend Denial of Service Attack in Mobile Adhoc Networks for Hostile Environment" International Journal of Innovative Research in Science & Engineering.

[17] Qualnet Documentation, "Qualnet 5.0 Model Library, Network Security", Available: Http:// Www.Scalablenetworks.Com/Products/Qualnet/ Downlaod