Simulation and Analysis of Layerwise Security in Mobile Adhoc Network for Military Scenario

Dr.D.Devi Aruna
Assistant Professor
Department of Computer Applications
Dr.N.G.P Arts & Science College
Coimbatore

Abstract

Mobile Ad-hoc Networks (MANETs) have received significant research interest in recent years. It has the ability to setup networks on the fly in a military environment where it may not be possible to deploy a traditional network infrastructure. Their characteristics make them vulnerable to passive and active attacks. Particularly, Denial of Service attack is one such severe attack against MANET Layers which is a challenging one to defend against. Hence security is an important challenge while deploying MANET. So security issues are analyzed for individual layers namely application layer, transport layer, network layer, link layer and physical layer. There is no solution that provides layer wise security which is a major challenge for Mobile Adhoc networks. 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. From the simulated results, 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, Average jitter and Routing Overhead.

Keywords- Mobile adhoc network, Layer wise security protocols, secure neighbor authentication, Adhoc On demand Distance Vector (AODV) routing.

I. Introduction

Mobile ad hoc networks are considered to be the future of wireless networks owing to their specific characteristic features namely practical, simple, self-organization, selfconfiguration, ease to use and inexpensive when operating in a licence-free frequency band. There are many applications to ad hoc networks, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, having highly dynamic mobility. This research work evaluates Layerwise Security Framework with SNAuth-SPMAODV with concentration to defend against Denial of Service attack in MANET layers. A military 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 proposed method, Chapter4 discusses Experimental evaluation and Chapter 5 gives the conclusion.

II. REVIEW OF LITERATURE

This chapter briefly describes the different existing security framework for MANET.

Table1: Comparison of proposed with existing security framework

Framework	**Layerwise Security framework(LaySec) [Proposed]**	**Security Aware Ad-hoc Routing [2001]**	**Self-Organized Network-Layer Security [2002]**	**On-demand Secure Routing Protocol [2002]**	**MObile Certification Authority [2003]**	**Secure Efficient Adhoc Distance Vector [2003]**	**Alliance of Remote Instructional Authoring and Distributed Networks for Europe [2005]**
Features							
Encryption	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**
Multipath	**Yes**	No	No	No	No	No	No
Based on Reactive protocol	**Yes**	**Yes**	**Yes**	**Yes**	No	No	**Yes**
Neighbor Authentication	**Yes**	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**
Certification Service	**Yes**	**Yes**	No	No	**Yes**	No	**Yes**
Attack Defense							
Denial of Service attacks	**Yes**	No	No	No	No	**Yes**	No
Wormhole attack	**No**	No	**Yes**	No	No	No	No
Spoofing	**No**	**Yes**	No	**Yes**	**Yes**	No	**Yes**
Eavesdropping	**No**	**Yes**	No	**Yes**	**Yes**	Yes	**Yes**

III. 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.

IV EXPERIMENTATION AND EVALUATION

The LaySec framework is simulated using Qualnet5.0[17].This simulated environment is defined by the following parameters as shown in Table 2 and Table 3.

TABLE2: 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 3: 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

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

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.

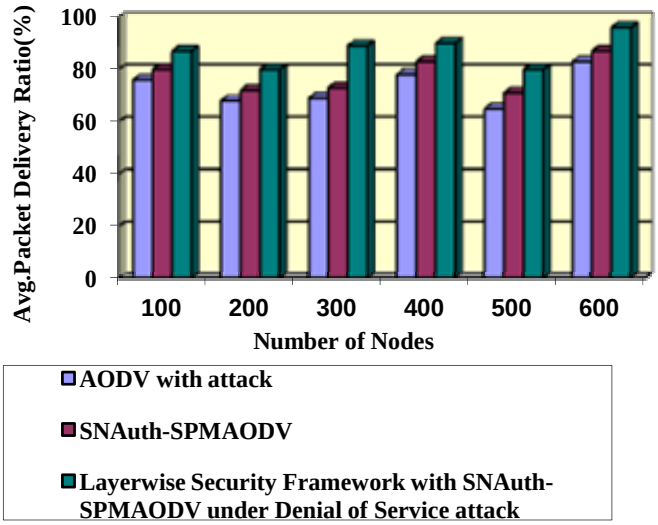

Figure1:Average Packet Delivery Ratio

Average Throughput

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

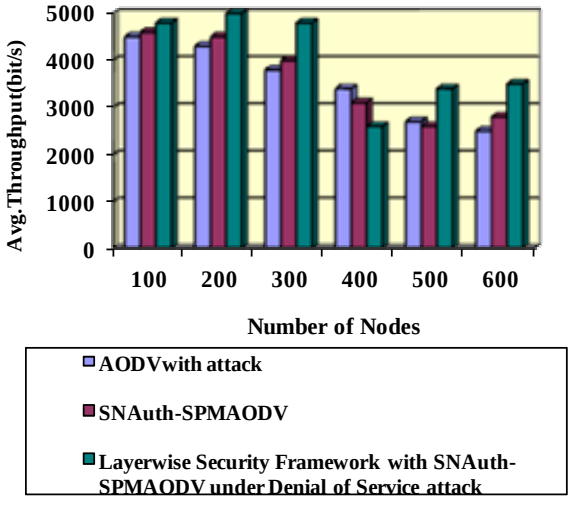

Figure 2: Average Throughput Ratio

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)

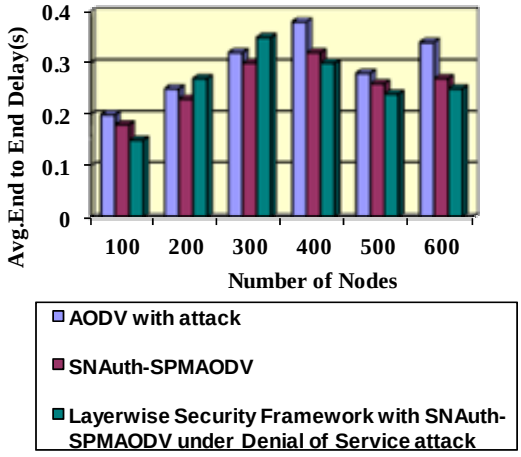

Figure 3:Average End to End Delay

Average Jitter

Figure 4 depicts the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of Average Jitter over varying network density. Layerwise Security Framework with SNAuth-SPMAODV performs poorly in sparse networks (eg 100 to 200 nodes). However, in a relatively dense network, Layerwise Security Framework with SNAuth-SPMAODV outperforms compared to SNAuth-SPMAODV and AODV.

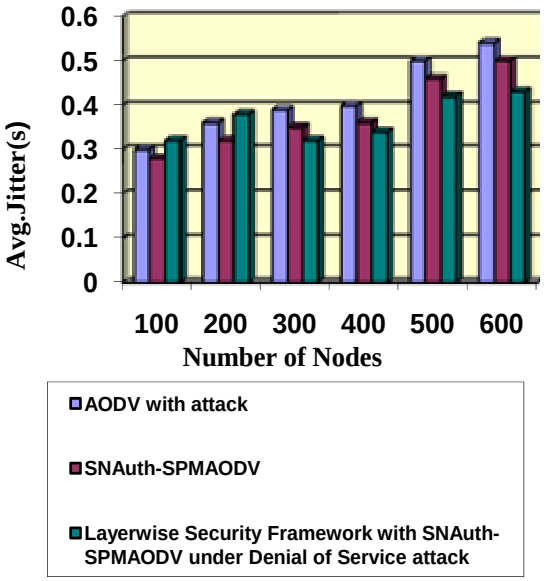

Figure 4:Average Jitter

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

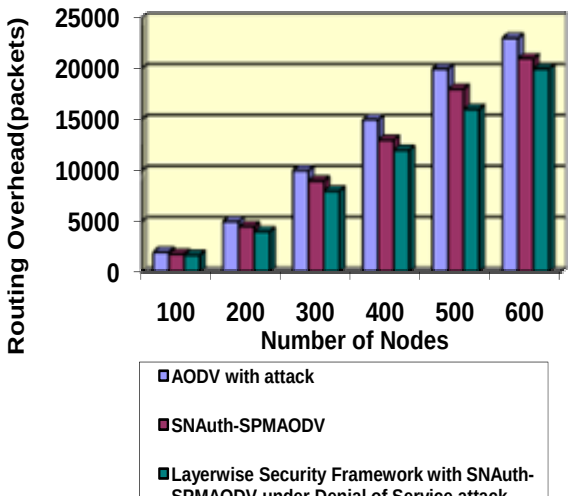

Figure 5:Routing Overhead

CONCLUSION

This research effort examines the case study have been provided with specific concentration on a military case study in an unknown and an unsecure territory with different channel and physical layer settings for military scenario. Scenario defines three Army countries in a battlefield and this scenario shows the implementation and evaluation of Layerwise Security Framework with SNAuth-SPMAODV to defend against Denial of Service attack.

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....

Dr.D.Devi Aruna is the Assistant Professor in Department of Computer Applications, Dr.N.G.P Arts & Science College, Coimbatore. She has 4 years of teaching experience. Her areas of interest include cryptography and Network Security. She has 20 publications at national and International level**.**