ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

A Novel Approach for Multiple Layer Attack Detection in MANET

Vaishnavi.S[1], Divya Prasannan[2]

MTech Student[1], Assistant Professor[2]

Department of Electronics and Communication Engineering

APJ Abdul Kalam Technological University

vaishnavi21294@gmail.com[1], divyaprasannan93@gmail.com[2]

***Abstract*— Mobile ad hoc networks can be used in many applications ranging from sensors for environment, rescue operations, defense, weapons etc due to its flexibility and mobility. To protect mobile ad hoc networks, security protocols have been developed to protect routing and data. These protocols only protect routes or communication (data), not both. To provide full protection, both secure routing and communication security protocols must be implemented. So that a novel secure framework is designed to provide node authentication, access control and communication security without modifying routing protocol in the network layer and also detect jamming attacks in the physical layer. Finally, simulation results are realized in NS2.**

Key words: Mobile ad hoc networks, communication system security, Diffie-Hellman key-exchange algorithm, jamming, posterior probability method.

I. INTRODUCTION

MANETs can be used in many applications such as rescue operations, defense etc due to its flexibility and mobility. MANETs are self-configuring, dynamic and infrastructure-less groups of mobile stations connected by wireless links. In a MANET, network topology changes dynamically in an unpredicted manner and each node has limited transmitting power.MANETs are created for specific purposes. Each device in a MANET is known as node. Communication can be achieved by sending packets between source node and destination node.

MANETs are basically peer-to-peer, multihop wireless networks. Communications in MANETs are commonly wireless. Wireless communication can be intercepted by any node in range of transmitter. This will leads MANETs to a range of attacks, such as Sybil attack, route manipulation attacks, manipulating routing tables and modifying routes. Man in the middle attacks can be introduced by manipulating routing information to pass traffic trough malicious nodes [1]. Secure routing protocols have been proposed to prevent attacks against MANETs, but they do not protect data.

Jamming in wireless networks is defined as the disruption of wireless communications at the receiver sides through the transmission of interfering wireless signals. Jamming in wireless networks are becoming a major issue due to ease in blocking communication in wireless network. Jamming attacks are a subset of Denial of Service attack in which unauthorized nodes block legitimate communication causing intentional interference in network.

II. LITERATURE SURVEY

MANETs are infrastructure-less groups of mobile devices. So they depend on intermediate nodes to route messages between source node and destination node. Ad hoc on demand distance vector (AODV) is a reactive protocol, establishes routes to destinations on demand and supports both unicast and multicast routing [3]. The optimized link state routing (OLSR) is a proactive protocol which periodically flooding the network to generate entries for routing table that persist until the next update[2]. Both approaches have motion-tolerance and co-operative communication characteristics make ideal for UAV MANETs [7]. AODV and OLSR lack security mechanisms, as they are unable to distinguish legitimate nodes from malicious nodes [4],[5],[6].

The ITU-T Rec., through X.805, defines seven classifications of wireless end- to- end security, which are called dimensions[8]. The seven dimensions are:

- **Access control** ensures that malicious nodes are kept out of the network.
- **Authentication** confirms the identity of nodes which are communicating.
- **Non-repudiation** prevents nodes from sending false information about previous transmissions.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

- **Confidentiality** allows only the authorized nodes to access information in the network.
- **Communication security** ensures that data only flows between source and destination nodes.
- **Availability** ensures that network resources should be available only to authorized nodes.
- **Integrity checking** allows authorized nodes to ensure packets received are in the same manner they were sent.

Secure ad hoc on demand distance vector(SAODV) secures routing mechanism by adding ransom numbers in Route Request packets(RREQs)[9]. This protocol requires at least two Secure RREQs(SRREQs) reached at the destination node by different routes with same random numbers to identify the source node. Secure Optimized Link State Routing(SOLSR) prevents wormhole attacks during its neighbor detection phase [11]. Nodes should be authenticated before establishing neighbor status to prevent malicious nodes. SOLSR sent each packet which is digitally signed using a shared secret. If the signature of incoming packet is not readable, then the packet is discarded. SOLSR uses time stamped- packets to prevent replay attacks[11], [12]. The main objective of SAODV and SOLSR is to prevent unauthorized nodes from gaining control of topology generation mechanisms of routing protocol and to protect against wormhole attacks and black hole attacks.The Diffie-Hellman key generation algorithm is a means of generating symmetric keys[13]. Nodes exchange generated data using globally known primes and secret data. The resulting secret key is then communicated by both nodes.

SUPERMAN (Security Using Pre-Existing Routing for Mobile Ad hoc Networks) [10] is a security protocol in the network layer combines routing and communication security. This protocol provides security only at the layer 3 of OSI model.

III. PROPOSED SYSTEM

The proposed framework operates at network layer and physical layer.

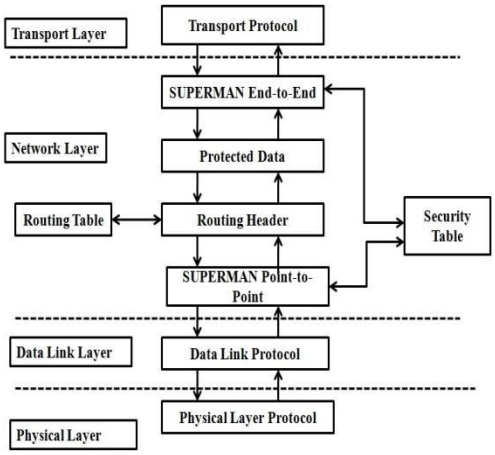

Fig. 1. Proposed system framework

This framework is designed to provide fully secured communication for MANETs, without modifying existing routing protocol. Fig. 1 shows data flow from transport, through the network layer and data link layer to the physical layer. The elements of SUPERMAN process the packets, provide confidentiality, integrity and node authentication.

SUPERMAN operates at the network layer. It depends on dynamic key generation to provide communication security. The Diffie-Hellman key exchange algorithm is used to generate symmetric keys dynamically. Each node in the network has a security table. SUPERMAN stores keys in the security table of each node. A certificate based method is used to control the access to the network. Every authorized node in the network is provided with a certificate by the associated Trusted Authority.

SUPERMAN provides two types of security: end-to-end security and point-to-point security. End-to-end security provides secure services between source node and destination node by using their shared key. Payload data is encrypted using an appropriate cryptographic algorithm such as Authenticated Encryption with Associated Data (AEAD) which provides confidentiality and integrity services. The purpose of SUPERMAN end-to-end element is to provide confidentiality and source authentication services.

At point-to-point security, data is transmitted over multiple hops. So that it is authenticated at each hop. This can be achieved by using a hash algorithm, such as HMAC which provides integrity and authenticity services to the packet. HMAC is then applied to the entire packet. A digest of the packet is created, encrypted using appropriate key and appended to the packet. This tag is removed at each intermediate hop, until the destination node is reached. This tag can be used for integrity checking.

At initialization of the network, the first node about to join the network will generate a symmetric network

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

key. This key is then sent to all authorized nodes in the network. This key provides a basis for all broadcast communication security in the network. A node will use these keys to encrypt and sign the packets, which is sent to the broadcast address of the network. This key is used for broadcast and multicast communication, such as route updates but not used for communication between individual end-points.

Jamming can be referred as intentional interference attacks on wireless networks at the physical layer. Jamming attacks are severe Denial of Service attack. These attacks usually introduced by emitting radio frequency signals. The aim of jammer is to interfere with legitimate wireless traffic. The jamming attack in the physical layer can be overcome by posterior distance method. The posterior probability method is the probability of an event (attack) will happen after all background information has been taken into account.

IV. SIMULATION PARAMETERS

All simulation is performed using NS2. TABLE 1 shows the parameters for the stimulation environment. It is assumed that all nodes in the network are stationary during initialization and association phases.

TABLE 1
SIMULATION PARAMETERS

Number of Nodes	10 - 100
Routing Algorithm	Dijkstra Algorithm
Number of Iterations	100
Stimulation Area	100m x 100m
Communication Range	100m
Max Hop Count	5
Random Seed	11
Key Share Size	128 and 256 bytes
Certificate Size	1013 and 1275 bytes

V. SIMULATION RESULTS

In this section, we evaluate Packet Delivery Ratio (PDR), average delay and packet loss of our proposed system compared to the existing system.

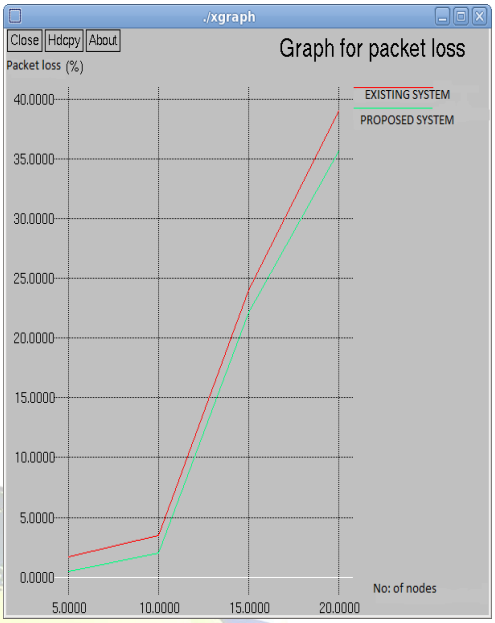

Fig. 2. Graph comparing packet loss in proposed system and existing system

The above figure (Fig.2) shows the comparison of packet loss in the proposed system and the existing system. In proposed system, multiple layer security is provided. So that packet loss can be reduced in this system.

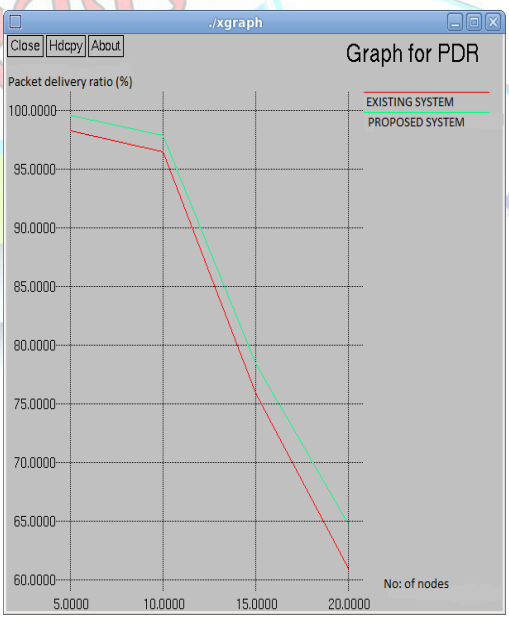

Fig. 3. Graph comparing packet delivery ratio in proposed system and existing system

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

The above figure (Fig.3) shows the comparison of packet delivery ratio in the proposed and the existing system. In proposed system, multiple layer security is provided. So that packet loss is reduced in this system. As packet loss reduces maximum packets will reach at the destination.

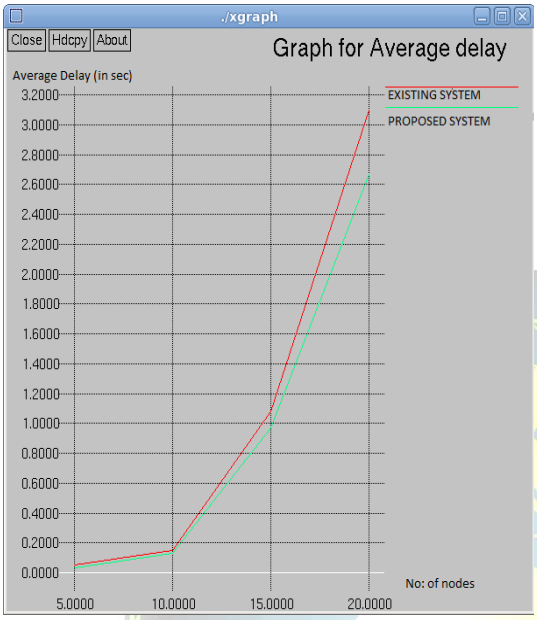

Fig. 4. Graph comparing average delay in proposed system and existing system

The above figure (Fig.4) shows the comparison of average delay in proposed system and existing system. In the proposed system, multiple layer security is provided. So that average delay can be reduced in proposed system than in existing system.

VI. CONCLUSION

The proposed framework provides security for multiple layers as it identifies multiple layer based attackers. At network layer SUPERMAN provides node authentication, access control, communication security without modifying existing routing protocol. At physical layer, jamming attacks can be overcome by posterior probability method.

The simulation resultsshow that proposed system reduces packet loss and average delay when compared to the existing system. Also it provides a better packet delivery ratio. Thus the proposed system is more efficient than existing system.

ACKNOWLEDGMENT

The authors would like to thank all the support of all the authors and reviewers of reference papers.

REFERENCES

[1] A. K. Rai, R. R. Tewari and S. K. Upadhyay, "Different types of attacks on integrated manet-internet communication," *International Journal of Computer Science and Security, vol. 4, no. 3, 2010.*

[2] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot et al., "Optimized link state routing protocol (olsr)," *2003.*

[3] I. D. Chakeres and E. M. Belding-Royer, "Aodv routing protocol implementation design," *in Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. IEEE, 2004.*

[4] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *Wireless Communications, IEEE, vol. 11, no. 1, 2004.*

[5] N. Garg and R. Mahapatra, "Manet security issues," *IJCSNS, vol. 9, no. 8, 2009.*

[6] W. Ivancic, D. Stewart, D. Sullivan, and P. Finch, "An evaluation of protocols for uav science applications," *2011.*

[7] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, "Performance analysis of mesh routing protocols for uav swarming applications," *in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011.*

[8] A. R. McGee, U. Chandrashekhar, and S. H. Richman, "Using itu-t x. 805 for comprehensive network security assessment and planning," *in Telecommunications Network Strategy and Planning Symposium. NETWORKS 2004, 11th International. IEEE, 2004.*

[9] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "Saodv: a manet routing protocol that can withstand black hole attack," *in Computational Intelligence and Security, 2009. CIS'09. International Conference on, vol. 2. IEEE, 2009.*

[10] Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle," SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

hoc Networks"*IEEE Transactions on Mobile Computing,Vol 16,2017.*

[11] F. Hong, L. Hong, and C. Fu, "Secure olsr," *in Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on, vol. 1. IEEE, 2005.*

[12] A. Hafslund, A. Tønnesen, R. B. Rotvik, J. Andersson, and Ø. Kure, "Secure extension to the olsr protocol," *in Proceedings of the OLSR Interop and Workshop, San Diego, 2004.*

[13] E. Rescorla, "Diffie-hellman key agreement method," *1999.*