ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Security in Wireless Adhoc Networks based on Trust and Encryption

Sumimol L.[1], Janisha A.[2]

PG Scholar, Dept. of CSE, LBSITW, Thiruvananthapuram, India [1]

Assistant Professor, Dept. of CSE, LBSITW, Thiruvananthapuram, India [2]

Abstract: Ad hoc network is a group of wireless mobile computers for temporary communication. Here autonomous and self-interested nodes in the network and the broadcast nature of radio transmission make the network highly vulnerable to serious security attacks. In a multi-hop wireless ad hoc network, packet losses are attributed to harsh channel conditions and intentional packet discard by malicious nodes. Packet losses may due to link errors or the combined effect of link errors and malicious drop. It becomes more difficult to detect internal attacks, whereby a malicious node that is part of the route exploits communication information to selectively drop a small number of packets which may critically affect network performance. Secure and efficient communication is one of the most important aspects in ad-hoc wireless networks, so it needs to a develop protocol strategy which take less computational power, better performance and efficiently utilizes the bandwidth. Here I reviewed various security aspects in adhoc networks, and proposed the countermeasures to prevent them. Performance comparison between two network scenarios has also been studied, a standard network scenario and packet dropping attack scenario.

Keywords: Security, AODV, Trust, Encryption, Integrity.

I. INTRODUCTION

Wireless ad hoc networks have attracted significant attentions recently due to its wide applications in different areas. In a wireless ad hoc network, there exists no fixed infrastructure such as switching centres or base stations. Mobile nodes that are within the communication range of each other can communicate directly whereas; the nodes that are far apart have to rely on intermediary nodes or routers to relay messages. Dynamic topology changes occurred here. Movement of nodes invalidates topology information. Several application areas are now emerged in adhoc networks like military, law enforcement and rescue missions and conference room communications etc, the cost to set up an ad hoc network is low, it is a very attractive option for commercial uses. But communication medium is open which causes attacks like passive eavesdropping malicious injection etc so here ensuring security is the critical scenario.

A. *Classification of Routing Protocols*

The nodes in an ad hoc network also function as routers to discover and find paths to other nodes in the network. The primary goal of an adhoc routing protocol is to establish a valid, efficient and secure route between a pair of nodes so that messages may be delivered in a timely manner. If it fails, the entire network is affected. Thus, routing security plays an important role in the network. Routing in MANET depends on various factors like topology, selection of routers and resource availability of nodes. The computational resources are vital parts in these networks so an optimal routing scheme is needed. In wireless ad-hoc network there is no particular design to monitor the traffic and accessibility, which allows malicious users to enter into the network. Infrastructure less and dynamic behaviour of these networks can lead to develop new routing criteria's especially for these networks.

Routing protocols are classified into three types

i) Proactive Routing Protocols

These routing protocols maintain the neighbouring hops information in a routing table. The destination route is stored in the table so there is no need for route discovery before starting the communication. Various proactive routing protocols are FSR, DSDV and OLSR.

ii) Reactive/Ad hoc Based Routing protocols

These routing protocols do not maintain the routing table. When a node wants to communicate with each other then only route discovery starts. Each node broadcasts the route request packet into the network for getting the destination route. Examples for various types of reactive routing protocols are AODV, DSR and TORA.

iii) Hybrid Protocols

The hybrid protocols are used to overcome the drawbacks of proactive routing protocols and reactive routing protocols i.e. It reduces the control overhead of proactive routing protocols and the delay due to initial route discovery in reactive routing protocols. E.g. ZRP, HARP.

Various security attacks are there in adhoc networks. Packet transmission is in the form of multihop relay manner, but selfish nodes are there in the path. Involving autonomous and self-interested nodes in packet relay and the broadcast nature of radio transmission make the network highly vulnerable to serious security and privacy violation attacks. Attackers may analyze the network transmissions to learn the user's communication activities, which affects the user's privacy. Due to the open environment and the shared wireless medium, an attacker can intercept all the transmissions within the reception range of his radio receiver so there is no need to physically manipulate a node. Attackers may impersonate users or

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

manipulate route establishment packets i.e. they, may advertise false routing information to attract nodes towards them.

B. Security issues

- Insecure channel: - Channel is open radio broadcasting one so messages can be eavesdropped and fake messages can be injected or replayed into the network, without the need to access the network components.
- Insecurity of the nodes: - Nodes may not be physically protected, and more vulnerable to attacks. If an attacker accesses a node, it can change its behaviour, or corrupt the hardware
- Absence of infrastructure: - Adhoc networks have no fixed infrastructure. So security mechanisms used for normal wired scenario will not be applied for the adhoc scenario.
- Dynamically changing topology: - The topology of a wireless networks is quickly changing.
- Quality of Service: Due to the dynamic nature of the medium the Quality of service will not be ensured completely.

C. Attacks

Attacks can be classified into passive and active attacks. A passive attack does not disrupt the operation of a routing protocol, but only monitors valuable information by intruding into the traffic so it becomes very difficult to detect. An active attack is an attempt to change the data. Active attack can be further divided into external attacks and internal attacks. An external attack is one caused by nodes that do not belong to the network i.e. an outsider node. An internal attack is from compromised nodes that belong to the network i.e. an insider node. Internal attacks are more difficult to detect so new mechanisms should be needed to identify them.

Different types of attacks affected at different layers of communication model. Packet dropping attacks are the major types of attacks present in the adhoc network.

- Wormhole attack:-In Wormhole attack the colluding attackers build tunnel between the two nodes for forwarding packets by ensuring that it isthe shortest path between the nodes then the entire data flow is through this malicious tunnel.
- Black hole attack: - In Black hole attack a routing protocol has been used by malicious node reports itself stating that it will provides shortest path. The goal of the malicious node in this attack is to drop all packets that are directed to it instead of forwarding them as a result the amount of retransmission consequently increases leading to congestion.
- Resource consumption attack: - In the resource consumption attack, a malicious node can try to consume more battery for route discovery, or by passing unwanted packets to the source node.
- Denial of Service (DoS):- DoS is one of the most well known attack on computer communication networks. This kind of attack is critical in Wireless adhoc networks because they have less computational resources so it should be effectively utilized. Here a large number of RREQs are sent to a destination node on the network that is non-existent. As there is no reply to these RREQs, they will flood the entire network leading to a consumption of all of the node battery power, thus will eventually leads to denial-of-service.

D. Security Requirements

For security sensitive applications like adhoc networks, we consider the following attributes.

- Availability: - Only authorized entities should be allowed to access the information created and stored by an organization.
- Confidentiality:-Ensures that unauthorized entities should not access the sensitive information.
- Integrity: -To ensure that transmitted message is not altered during transmission.
- Authentication:-When two parties are communicating with each other they must be identify each other. This will prevent gaining unauthorized access to resources.
- Non-repudiation: -Ensures that the sender cannot deny later at a time the message is sent by him.

Cryptography can be used to provide security in routing protocol there by achieving confidentiality, integrity, authentication and non-repudiation. Cryptographic algorithms, in general, are divided into the following

- Symmetric key algorithms: These algorithms share the same key for encryption and decryption. Examples are Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES).
- Public key algorithms: These algorithms use pair of keys for encryption and decryption: public key and private key. Public key is used for encryption and private key is used for decryption. Examples include Digital Signature Algorithm (DSA) and the Rivest-Shamir-Adleman (RSA) algorithm.
- Elliptic curve algorithms: The basis of elliptic curve algorithm is based on computing discrete logarithms. Examples are Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) etc.
- Hash: These algorithms transform input string into fixed length value or key. An important property of hash algorithms are irreversibility and collision resistance. Examples of hash functions are SHA-1, SHA-256, SHA-384, MD5 and HMAC.

E. Security in AODV

The reactive routing protocol AODV is assumed here. One advantage of using reactive protocol is that the route for data transfer is established based only on demand, this saves the computational resources of ad hoc mobile nodes.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Here the nodes allowed to send messages through their neighbours to the destined nodes placed beyond their communication range with which they cannot directly communicate. This can be achieved via Route Discovery phase by sending the Route Request Messages. Outcome of this phase is a shortest and loop free communication path. But this protocol still has many weaknesses. In original AODV there are no security mechanisms by default. It is vulnerable to the attacks like Black hole, Wormhole, Denial of Service, Packet Dropping attacks, Packet Modification attacks etc. These attacks can occur during Route Discovery process and Data Transmission phases. Effective security mechanisms should be added to the existing AODV to withstand these types of attacks.

This paper is organized as follows. Section 2 overviews the related works. Section 3 discusses the proposed solution. Section 4 describes the performance comparison. Section 5 summarizes concluding remarks.

II. LITERATURE REVIEW

Zapata, Manel Guerrero [1] proposed a major security enhancement over AODV is the Secure AODV (SAODV). It considers resource- limitation in AODV. It uses digital signature and one-way hash chain to protect the packet with no digital certification i.e. no Certification Authority. If digital certificate, is not used there is a possibility for impersonation attack. This method uses hash chain to protect hop counts, but payload integrity is not assured. SAODV also does not have well designed encryption or key-management system. Many research works are done based on SAODV to avoid the Black Hole Attack.

Ms Darshana Patel, Ms Vandana Verma [2] proposed an encryption algorithm with public key used to secure AODV messages. This mechanism calculates signature using appropriate encryption algorithm for all the fields of an AODV message. It also calculates signature with public key and then both signatures will be transmitted along with the AODV messages. It uses secure hash algorithm (SHA) to generate signature. Integrating encryption algorithm with basic AODV routing protocol is efficient of handling both unauthorized and malicious nodes' attacks. RaviKumar M Inamathi and S. V. Saboji [3] describes security enhancement in AODV routing protocol by detection and tolerance of attacks using secure message transmission (SMT) protocol. In proposed algorithm enhancement of AODV made with secure message transmission using SMT Agent. It enables multicast operation (MAODV) with many groups. SMT agent sends ACK to tolerate from detected attacks. After getting the RREPs forward data using single path and forward data using multiple paths. Due to presence of multicast and queues, MAODV show better performance for detecting attacks using SMT Agent. Since frequent routing information updation and multicasting it can cause, performance degradation in MAODV with attacks as number of connections increases.

Amol Bhosle [4] proposed AES algorithm for encryption and decryption for secure data transfer, MD-5 and RSA public key algorithm to generate the digital signature to achieve user authentication, data integrity and non-repudiation. In VESS, Jung T. Chang, Sreedeepthi Gundala, Teng- Sheng Moh, and Melody Moh [5] ,four different modes of communication Encryption applied for MANET: Open Mode, User Mode, Lightweight Mode, and Strong Mode. In open mode no encryption is used, all data are sent out in the open channel. In Lightweight Mode a version of encryption designed for nodes that are keen on performance. In strong mode: data packets are heavily encrypted and demand more computation power and process time. In user mode, users can customize their own balance of encryption strength and performance. Another mode known as data-integrity mode is introduced in VESS. S.S. Zalte, Prof. (Dr.) Vijay R. Ghorpade and D.Y. Patil [6] propose secure token by using cryptographic algorithm AES and hashing algorithm SHA2. In the proposed method, they use secure token to provide the security to the non-mutable fields in the RREQ and RREP messages. Secure token is used to authenticate between each two neighbor nodes by agreeing on a secret key: first digest of the message is calculated using sha2 and the digest is encrypted using AES encryption thus forming a digital signature. It uses the Diffie Hellmann key exchange algorithm prior to key predistribution. Each intermediate node verifies the signature to authenticate node.

Songbai Lu et al. [7] proposed another variation to AODV which prevent the black hole attack in a MANET This protocol directly verifies the destination node by exchanging random numbers. In addition to RREQ and RREP packets in AODV it uses SRREQ and SRREP to avoid the black hole attacking node. The source sends the SRREQ packet with a random number to the Destination. After verifying the SRREQ the Destination will send SRREP with another random number then the source send the data if SRREP is valid, not malicious reply. Jassim et al [8] incorporated a trust mechanism to enhance the reliability of the AODV protocol. When request and reply messages are generated and forwarded by the nodes in the network, each node appends its own trust value and updates its routing table with all the information in the control messages based on this trust. Lack of trust will lead the possibility of the node to perform a packet drop attack. The use of R-AODV provides a higher percentage of successful data delivery.

Sharma et al [9] designed trusted routing protocols using trust frameworks and intrusion detection system. This information is updated directly through the monitoring neighborhood. When performing trusted route discovery, the recommended opinions are combined to make a routing judgment. This model shows that the malicious nodes are separated from the trusted nodes. Sonali Bhargava and Dharma P. Agrawal [10] have identified certain misbehaviours in Ad Hoc On-Demand Distance Vector (AODV) protocol; describe the Intrusion Detection and Intrusion Prevention Model to prevent them. The Intrusion Detection Model present on all the nodes. It constantly monitors the behaviour of its neighbours and analyzes it to detect the neighbours' behaviour whether it is compromised or not. In Intrusion Response Model a node identifies that a node has been compromised then

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

propagates this information to the entire network by transmitting a special packet. N. Bhalaji, A. Shanmugam [11] proposed a trust model used to prevent the grey hole attack. Here Route reply from more than one node is considered for observation. The nodes are classified into three categories i.e. companion, known and unknown nodes. Companion node is the most trusted node, RREP from the companion node if any is first selected and RREP from unknown is considered as malicious. Radha Krishna Bar et al [12] measures trust value mainly depending on the nodes' packet forwarding ability. Here a path with more trusted nodes is generated instead of a shortest path and also a dynamic trust value generation method is used which avoids the black hole attack.

III. PROPOSED SECURITY SOLUTION

Different types of security measures can be applied to enhance the security of adhoc Routing Protocols. Security parameters applied during Route Discovery Phase and Data Transmission phase. The criteria should address the problems in Routing Security, Data Security and consider the node features like battery energy, bandwidth utilization, processing power etc. Cryptographic mechanisms are better solutions to ensure security. Usage of Light weight cryptographic mechanisms like SHA and AES will increases efficiency. Node Trust is an important factor here i.e. if the forwarding node is a trusted one, the chance of an attack to be affected should be less. In the proposed method each node finds out the trust of neighbouring nodes and establishes a secure path for the dataflow. Then send the data along this path in an encrypted fashion and also check the integrity of message at the destination to detect packet modification attack.

IV. PERFORMANCE COMPARISON

Performance of two network scenarios has been studied, standard network scenario and black hole packet dropping scenario and measure the parameter throughput. In a normal network scenario an adhoc network with twenty number of nodes are selected some nodes are mobile and others are fixed. Attackers are not considered here, so the network throughput and packet delivery ratio should be high i.e. all intermediate node forwards all the send packets through the path. In a black hole attack scenario a black hole attacking node is considered and measures the above parameters. From the analysis it shown that the network throughput in attack scenario is less than the standard scenario since there is a black hole node in the path which drops the packets sends through it.

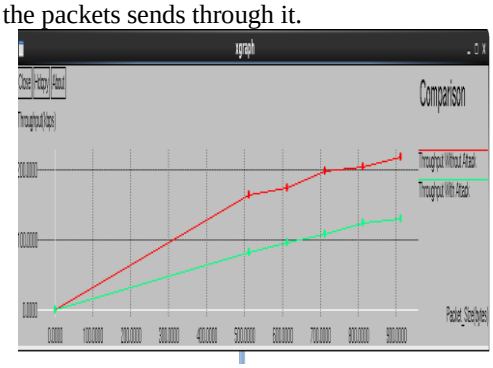

Fig 2: Throughput versus Packet size

V. CONCLUSION

Wireless Ad hoc network is a group of wireless or mobile computers for temporary communication. Due to their ease of use and Deployment they are widely used, but the factors like dynamic topology, selfish nodes, multihop packet relay and security attacks will restrict their benefits a lot. Adding Security enhancements to the routing protocols can reduces the level of problems.

ACKNOWLEDGMENT

In this paper I would like to thank Dept of Computer Science, LBSITW Poojappura for their support and providing necessary guidance for the work.

REFERENCES

[1] Zapata, Manel Guerrero, "Secure Ad hoc On-Demand Distance Vector Routing" , *Mobile Computing and Communication Review*. 6 (3) pp. 106-107.

[2] Ms Darshana Patel, Ms Vandana Verma, "Security Enhancement of AODV Protocol for Mobile Ad hoc network*" International Journal of Application or Innovation in Engineering & Management* Volume 2, Issue 1, January 2013, ISSN 2319 – 4847.

[3] RaviKumar M Inamathi and S. V. Saboji, " Security Enhancement in AODV Routing Protocol", *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)*, Volume 2, Issue 8, August 2013, ISSN: 2278 – 909X

[4] Amol Bhosle, "Improving Performance and Securing data in Manet with AES ", *International Journal of Research in Advent Technology (IJRAT)*, Vol. 1, No. 1, August 2013, ISSN: 2321–9637.

[5] Jung T. Chang, Sreedeepthi Gundala, Teng- Sheng Moh, and Melody Moh, "VESS: a Versatile Extensible Security Suite for MANET Routing", *2009 IEEE*, pp 944-950.

[6] S.S. Zalte, Prof. (Dr.) Vijay R. Ghorpade and D.Y. Patil, "Secure Token for Secure Routing of Packet in MANET," *International Journal of Computer Science and Information Technologies*, Vol. 5 (6) 2014, pp 6916-6919.

[7] Songbai Lu, Longxuan Li, Kwok-Yan Lam, Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack" , *International Conference on Computational Intelligence and Security* IEEE Computer Society 2009, pp 421-425.

[8] Jassim, H. S. H., Tiong, S. K., Yussof, S., Koh, S. P., & Ismail, R. "Scenario based performance analysis of reliant ad-hoc on-demand distance vector routing (R-AODV) for mobile ad-hoc network", *Journal of Engineering and Computer Innovations*, Vol, 2(5), 78-89, 2011.

[9] Sharma, P, Jain .Y.K.,"Trust based secure aodv in manet", *Journal of Global Research in Computer Science*, 3(6), 107-114, 2012.

[10] Sonali Bhargava and Dharma P. Agrawal, "Security Enhancements in AODV protocol for Wireless Ad Hoc Networks", *IEEE 2001*.pp 2143-2147.

[11] N. Bhalaji, A. Shanmugam, "Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Adhoc Networks", *International Conference on Communication Technology and System Design 2011*, Elsevier- Procedia Engineering 30 (2012) 881 – 888.

[12] Radha Krishna Bar, Jyotsna Kumar Mandal and Moirangthem Marjit Singh, "QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack", *International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA) 2013*, Elsevier- Procedia Technology 10, 2013 (530 – 537).