Review Paper on Cryptography Based Secured Advanced on Demand Routing Protocol in MANET's

[1]Prachi D. Gawande,[2] Yogesh Suryavanshi,[3] Sandeep Kakde
Department of Electronics Engineering
Yeshwantrao Chavhan College of Engineering,
Nagpur, Maharashtra, India

***Abstract* – Networks are being used in various areas and the mobile ad-hoc network (MANET) is the network in Laptops, smart phones. MANET is a dynamic network without the fixed infrastructure due to their wireless nature and topology and changes due to their dynamic nature. In MANET various routing protocols are used, AODV routing protocol is one of them and the AODV has the different characteristics, AODV is the reactive routing protocol and disadvantages of DSDV routing protocol is overcome by AODV. The failure of the link will degrade its characteristics as when the error message is sent back to source and the process get repeated. In this chapter, we are proposing a method when nodes or links fails to receive the data packets . Cryptography technique is also used here to secure the network.**

***Index terms* - Mobile Ad-hoc networks, security, NS2, Reactive routing protocol, SHA algorithm.**

I. INTRODUCTION

Adhoc networks come into existence when two or more wireless mobile nodes agree to pass packets for each other. Ad hoc on demand distance vector (AODV) is one of the frequently used routing protocol and network is established. Network popularity has motivated the development of Mobile Ad hoc Networks (MANETs). MANETs provide communication between the nodes in the network without the presence of a central node which is normally found in the cellular and other networks. Fast changing network is created by this system. Different attacks that can be possible on AODV will be analyzed. Normal AODV performance will be improved. We are proposing an extended version to secure AODV protocol and the working of AODV routing protocol studied. In this paper we are going to decide evaluation parameters or performance parameters and attack analysis will be done. Cryptographic based security solution provided and the analysis of proposed protocol or algorithm in term of decided evaluation parameters will be performed. Using SHA AODV's security with network performance improved. Performance factor and security factor is checked by network simulator NS2.

II. TYPES OF ATTACK

Many attacks are possible on the MANET.

There are mainly two types of attack they are Internal attacks and external attacks.

Internal attacks: The attacker acts one of the nodes from the containing nodes and gains direct access to the network and can do the malicious activity.

External attacks: The attacker attacks from outside the network in this type, due to congestion in the network traffic by propagating non meaningful messages throughout the network, thereby disturb the entire communication of the network.

A. Impersonation

This type of attack is fall in the category of the most severe attacks. The attacker can act as an innocent node and join the network in this type of attack. Similar way, when several this type of nodes join the network, they gain the full control of the network and conduct malicious behavior. They spread fake routing information and they also gain access to confidential information. A network is vulnerable to such attacks if it does not employ a proper authentication mechanism.

B. Denial of Service

This type of attack is first making sure that a specific node is not available for service. So the entire service of the network might be disturbed due to this attack.

C. Eavesdropping

The main goal of the attacker is to get some private information in this type of attack, while it is being transferred from one node to the other. This attack is very much complex to find out and the secret information like private and public key password etc of the nodes can get compromised due to this attack .

D. Black hole attack

A black hole is created with the opponent at the main Centre. The opponent traps the traffic of the network close to a compromised in this type of attack. Basically the attacker offers an attractive path to the neighboring nodes. This attack can also be paired with other attacks like packets dropping, denial of service, replay of knowledge, selective forwarding.

E. Wormhole attack

Here the opponent connects two distant parts of the network and convey messages received in different part of the network to the other. A lower latency link is used to pass the messages in this type of network.

F. Sybil attack

In this type of an attack, a particular node in the network tries to have several different fake identities. Thus this way helps the malicious node to gain more and more specific information about the network. The validness of fault tolerant schemes like; multipath topology in routing, distributed storage, maintenance etc has a great decrease.

III. CRYPTOGRAPHY

A widely simplified meaning of cryptography is encryption. Plaintext, or clear text is the information or message itself and encryption is the process of coding the information in such a way that its meaning is hidden. Decryption is the reverse process of encryption. Encryption and decryption usually make use of a Key, and the coding method is in such a way that decryption can only be performed knowing the proper key. Today's cryptography is more than encryption and decryption. Cryptography has developed to provide:

Confidentiality: The prevention of unauthorized disclosure of information.

- Integrity: The prevention of erroneous modification of information.
- Availability: The prevention of unauthorized withholding of information or resources.
- Authentication: The process of verifying that users are who they claim to be when logging onto a system.
- Authorization: The process of allowing only authorized users access to sensitive information.
- Privacy ensures that the only the sender and intended recipient of an encrypted message can read the contents of the message that are transmitted from one place to another and cannot be understood by any intermediate parties that may have intercepted the data stream.
- Non-repudiation provides a method to guarantee that a party to a transaction cannot falsely claim that they did not participate in that transaction.

IV. LITERATURE REVIEW

There are many works focalized on performance analysis of multicast routing protocols over MANET. The most of those related works take in consideration only the best effort traffic. In proposed work, our basic contribution is the comparative performances analysis of MANET routing protocols for security purpose.

1) Brijesh Soni, Biplab Kumar Sarkar, Arjun Rajput, "Improvising the Ad hoc on Demand Distance Vector Routing Protocol When Nodes or Links Fails," in Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE2012) © Springer India. [2]

Concept of Paper: Build an AODV routing protocol such that it can handle better way at the time of nodes or links failure. Along with it presents the performance of AODV Reactive routing protocol and analysis of different attacks that can be possible on AODV. It also describes two layer signature security schemes which includes secure hash algorithm which aimed at improving normal AODV performance.

Proposed Work: To propose a method to carry forward the data packet when nodes or links fail from the last node it receives.

2) Weichao Wang, Yi Lu, Bharat Bhargava, “On Security Study of Two Distance Vector Routing Protocols for Mobile Adhoc Networks”, (IEEE) 2003, 0-7695-1893- 1/03. [4]

Concept of Paper: In this paper, the main aim is to minimize the different attacks like false distance vector, false destination sequence, Wormhole attacks**,** Routing information hiding using the distance vector routing protocols. Every host receiving this packet will examine its route entry to the destination host. If the sequence number is larger than the current sequence in INVALID packet, the presence of an attack is noted. The next hop to the destination will be added into this host’s blacklist.

Proposed Work: To develop a fast response mechanism (local repair) in proactive protocols to reduce packet drop cause by route changes. Study the joint responses to detect attacks and identify intruders. The results will lead to a secure routing protocol for mobile ad hoc networks. A complete system to implement intruder identification.

3) International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011 DOI: 10.5121/ijnsa.2011.3518 229 Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism. [5]

Concept of Paper: Network security attacks and related works in MANET and the basic operations of AODV routing protocol and its security flaws.

Proposed Work: A method to secure ad hoc on-demand distance vector (AODV) routing protocol. The proposed method provides security for routing packets and can efficiently prevent the attacks such as black hole, modifying routing information and impersonation. The proposed method uses hashed message authentication code (HMAC) function which provides fast message verification and sender as well as intermediate nodes authentication. Simulation and Comparison of the proposed method with original AODV and secure AODV (SAODV) protocol using network simulator tool (NS2).

4) Ram Ramanathan and Jason Redi, “A brief overview of Ad-hoc Networks: Challenges and Directions”, IEEE Communications Magazine May 2002, pp. 20-22. [6]
Concept of Paper: Algorithm scales to large populations of mobile nodes and evaluation methodology and simulation to verify operations.
Proposed work:
Nodes stores only routes that are needed, need for broadcast is minimized, reduces memory requirements.

V. CONCLUSION AND FUTURE WORK

For the more security here we are using Cryptography technique to secure the MANET. According to results, Evaluation parameters will be studied and the attack will be created and that attack can be implemented using Network simulator II. Using the cryptographic based advanced routing protocol the effect of attack will be minimized.

VI. ACKNOWLEDGMENT

Author takes this opportunity to express my sincere and deep regards to my guide Prof. Mr. Yogesh Suryavanshi sir for his constant guidance and encouragement. I am grateful for his cooperation. I would like to thank all my concerned lecturers and friends who supported and helped us.

VII. REFERENCES

[1] Asad Amir Pirzada, Chris McDonald, and Amitava Datta, Member, IEEE “Performance Comparison of Trust-Based Reactive Routing Protocols” IEEE Transaction On Mobile Computing, vol. 5, no. 6, June 2006.

[2] Brijesh Soni, Biplab Kumar Sarkar, Arjun Rajput, "Improvising the Ad hoc on Demand Distance Vector Routing Protocol When Nodes or Links Fails," in Proceedings of All India Seminar on Biomedical Engineering 2012 (AISOBE2012) © Springer India.

[3] Christopher Lott and Demosthenis Teneketzis “Stochastic Routing in Ad-Hoc Networks” IEEE Transactions On Automatic Control, vol. 51, no. 1, January 2006.

[4] Weichao Wang, Yi Lu, Bharat Bhargava, “On Security Study of Two Distance Vector Routing Protocols for Mobile Adhoc Networks”, (IEEE) 2003, 0-7695-1893- 1/03.

[5] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011 DOI: 10.5121/ijnsa.2011.3518 229 Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism.

[6] Ram Ramanathan and Jason Redi, “A brief overview of Ad-hoc Networks: Challenges and Directions”, IEEE Communications Magazine May 2002, pp. 20-22.

[7] Morli Pandya, Ashish kr. Shrivastava, Rajiv Gandhi Proudyogiki Vishwavidyalaya “Improvising the Performance with Security of AODV Routing Protocol in MANETs” 2013 Nirma University International Conference on Engineering .

[8] Fei Xing, Student Member, IEEE, and Wenye Wang, Member, IEEE “On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures” IEEE Transactions On Dependable and Secure Computing, vol. 7, no. 3, July-September 2010.

[9] Mohamed Elsalih Mahmoud and Xuemin (Sherman) Shen, Fellow, IEEE “ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multihop Wireless Networks” IEEE Transactions on Mobile Computing, vol. 10, no. 7, July 2011.

[10] Zhiguo Wan, Kui Ren, and Ming Gu “USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks” IEEE Transactions on Wireless Communications, vol. 11, no. 5, May 2012.

[11] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc on-demand distance Vector (aodv) routing,” IETF RFC 3591, 2003.

[12] A. A. Pirzada and C. McDonald, “Establishing trust in pure ad-hoc networks,” Proceedings of the 27th Australasian Computer Science Conference (ACSC), vol. 26, no. 1, pp. 47–54, 2004.