Review based on Public Key Cryptography in Wireless Network

***Ratnkant Jain**
****Ashish Mandloi**
*****Piyush Chouhan**

Abstract

Networks are being employed in various areas and also the mobile ad-hoc network (MANET) is that the network in Laptops, smart phones. Manet could be a dynamic network without the mounted infrastructure because of their wireless nature and topology and changes because of their dynamic nature. In Manet varied routing protocols are used, AODV routing protocol is one in all them and therefore the AODV has the various characteristics, AODV is that the reactive routing protocol and drawbacks of DSDV routing protocol is overcome by AODV. The failure of the link can degrade its characteristics as once the error message is distributed back to source and also the method gets repeated. During this work, we are proposing a technique once nodes or links fails to receive the information packets. Cryptography technique is additionally used here to secure the network.

Key Words: *Mobile Ad-hoc networks, security, NS2, Reactive routing protocol, SHA algorithm*

*Shree vaishnav Polytechnic college, Indore, ratnkant@rediffmail.com
**Shree vaishnav Polytechnic college, Indore, mandloi2000@yahoo.com
***Shree vaishnav Polytechnic college, Indore, pchouhan06@yahoo.com

Introduction

Wireless system operates with the help of a centralized structure like an access point. These access points assist the wireless users to stay connected with the wireless system, once they roam fro m one place to different. In wireless system the device communicate via rad io channel to share resource and data between devices. Because of presence of a fixed structure, limits the ability of wireless system, thus this generation of wireless system is needed simple and fast preparation of wireless network. Recent advancement of wireless technologies like Bluetooth, introduced a replacement form of wireless system referred to as Mobile ad-hoc network (MANETs) [1], that operate within the absence of central access point.

It provides high quality and device portability‟s that modify to node connect network and co mmunicate to every other. It permits the devices to keep up connections to the network additionally as simply adding and removing devices within the network. User has great flexib ility to style such a network at price-effective} cost and minimu m time.

Mobile ad hoc network consist large number of node, it type temporary network with dynamic topology. during this network every node communicates with one another through radio channel with none central authority. In MANETs every node operates during a distributed peer-to- peer modes, is an independent router to forward message sent by different nodes.MANETs has shows distinct characteristics, such as:

- Weaker in Security
- Device size limitation
- Battery life
- Dynamic topology
- Bandwidth and slower information transfer rate

A part from these limitation MANETs has several intensive application like: Military application, Natural d isaster, Medical service. In ad hoc network there are often node which will attempt to disrupt the right functioning network. These nodes are often malicious or selfish. they try to disrupt network perform by modifying packets, injecting packets or making routing loops. So, security is a very important task, because MANETs has characteristics such as; dynamic topology, infrastructure less. There are massive nu mbers of secure routing protocols planned by several researchers they fulfill completely different security needs and prevent specific attacks. they are divided into 3 categories: Reactive routing protocol [5, 6], Proactive routing protocol [5] and hybrid routing protocol [6].In reactive routing protocol the route is discovered once it needed, in proactive every node maintain network informat ion concerning to network property and route informat ion to any or all others node inside the network and proactive is one that is neither reactive nor proactive.

Now, the foremost of the solution uses cryptography mechanis m to observe selfish, malicious behavior of nodes and securing data from different varieties of attacks. The mechanisms that are employed by totally different secure routing protocol to observe malicious and selfish node have address individually in several protocol. No secure mechanism has been planned till date that may address to detection malicious and selfish node conjointly. we tend to planned a mechanis m, Extended Public key Cryptography (EPKCH) [12] that ready to discover the malicious nodes and selfish nodes conjointly so as to achieving security goals such as; Authentication, Integrity, Confidentiality. Also, we tend to planned a routing protocol named demonstrate and Secure Routing protocol for mobile ad hoc Network (AMSRP). We tend to implemented EPKCH mechanis m in monitor mode of AMSRP to securing MANETs. to style of this protocol follows the table-driven approach, during which every node maintain the information rmation, regard ing to network structure and route from a selected source to its all possible destination in its node information table. AMSRP could be a reactive secure routing protocol.

Security Drawback with Exis Ting Ad Hoc Routing Protocols

The main assumption of the previously given ad hoc routing protocols is that each one collaborating nodes do therefore in straightness and while not maliciously disrupting the operation of the protocol [7]. However, the existence of malicious entities can not be forgotten in

any system, particularly in open ones like ad hoc networks. In ad hoc network the routing perform is discontinuous by internal or external attackers. An inside attacker will be any legitimate participant of the routing protocol. An external assaulter is defined as the other entity. Cryptological solutions will be employed to forestall the impact of external attackers by mutual authentication of the collaborating nodes through digital signature schemes [9]. However, the underlying protocols ought to even be thought-about since an attacker might man ipulate a lower level p rotocol to interrupt a security mechanis m during a higher level. Internal attackers having capability to comp lete access the communicat ion link they are ready to advertise false routing informat ion at can and force arbitrary routing selections on their peers.

Types of Attack

Many attacks are attainable on the manet. There are in the main two forms of attack they are internal attacks and external attacks.

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

External attacks: The attacker attacks from outside the network during this kind, because of congestion within the network traffic by propagating non significant messages throughout the network, thereby disturb the complete communication of the network.

A. Impersonation

This type of attack is fall within the class of the foremost severe attacks. The attacker will act as an innocent node and be part of the network during this form of attack. Similar method, once many this kind of nodes be part of the network, they gain the complete management of the network and conduct malicious behavior. They spread fake routing data and that they additionally gain access to confidential information. A network is at risk of such attacks if it does not use a correct authentication mechanism.

B. Denial of Service

This type of attack is initial ensuring that a selected node is not accessible for service. Therefore the entire service of the network could be disturbed because of this attack.

C. Eavesdropping

The main goal of the attacker is to induce some non-public data during this form of attack, whereas it is being transferred from one node to the opposite. This attack is extremely a lot of advanced search out and also the secret data like private and public key password etc of the nodes will get compromised because of this attack.

D. black hole attack

A black hole is made with the opponent at the most Centres. The opponent traps the traffic of the network near a compromised during this form of attack. Primarily the attacker offers an attractive path to the neighboring nodes. This attack also can be paired with different attacks like packets dropping, denial of service, replay of data, selective forwarding.

E. wormhole attack

Here the opponent connects 2 distant elements of the network and convey messages received in several a part of the network to the opposite. A lower latency link is employed to pass the messages during this kind of network.

F. Sybil attack

In this variety of an attack, a selected node within the network tries to own many completely different fake identities; therefore this manner helps the malicious node to realize more and more specific data concerning the network. The validity of fault tolerant schemes like; multipath topology in routing, distributed storage, maintenance etc includes a great decrease.

Cryptography

A wide simplified which means of cryptography is encryption. Plaintext, or clear text is that the data or message itself and encryption is that the method of coding the data in such the simplest way that its that means is hidden. Decryption is that the reverse method of encryption. Encryption and decryption sometimes create use of a Key, and therefore the coding methodology is in such the way that decryption will solely be performed knowing the correct key. Today's cryptography is over encryption and decryption. Cryptography has developed to provide:

Confidentiality: The prevention of unauthorized revelation of knowledge.

- Integrity: The prevention of erroneous modification of knowledge.
- Availability: The prevention of unauthorized withholding of knowledge or resources.
- Authentication: the method of verificatory that users are who they claim to be once logging onto a system.
- Authorization: the method of allowing solely approved user’s access to sensitive data.
- Privacy ensures that the sole the sender and supposed recipient of an encrypted message will scan the contents of the message that are transmitted from one place to a different and can't be understood by any intermediate parties that will have intercepted the information stream.
- Non-repudiation provides a technique to ensure that a party to a transaction cannot incorrectly claim that they failed to participate in this transaction.

Literature Review

There are several works focalized on performance analysis of multicast routing protocols over Manet. The foremost of these connected works take in consideration solely the most effective effort traffic. In planned work, our basic contribution is that the comparative performances analysis of Manet routing protocols for security purpose.

1) 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 it will handle higher approach at the time of nodes or links failure. in conjunction with it presents the performance of AODV Reactive routing protocol and analysis of various attacks which will be potential on AODV. It additionally describes 2 layer signature security schemes which has secure hash algorithmic rule that geared toward improving traditional AODV performance.

Proposed Work: To propose techniques to hold forward the information packet once 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: during this paper, the most aim is to reduce the various attacks like false distance vector, false destination sequence, wormhole attacks, Routing data hiding exploitation the distance vector routing protocols. Each host receiving this packet can examine its route entry to the destination host. If the sequence variety is larger than the present sequence in INVALID packet, the presence of an attack is noted. Subsequent hop to the destination are additional into this host's blacklist.

Proposed Work: To develop a quick response mechanism (local repair) in proactive protocols to scale back packet drop cause by route changes. Study the joint responses to discover attacks and determine intruders. The results can cause a secure routing protocol for mobile ad hoc networks, a whole 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 connected works in Manet and therefore the basic operations of AODV routing protocol and its security flaws.

Proposed Work: a technique to secure ad hoc on-demand distance vector (AODV) routing protocol. The planned methodology provides security for routing packets and may with efficiency prevent the attacks like black hole, modifying routing data and impersonation. The planned methodology uses hashed message authentication code (HMAC) performs that provides quick

message verification and sender also as intermediate nodes authentication. Simulation and Comparison of the planned methodology with original AODV and secure AODV (SAODV) protocol exploitation 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: algorithmic rule scales to massive populations of mobile nodes and analysis methodology and simulation to verify operations.
Proposed work: Nodes stores solely routes that are required, want for broadcast is reduced, reduces memory necessities.

Conclusion and Future Work

For the additional security here we are exploitation Cryptography technique to secure the manet. Consistent with results, analysis parameters are going to be studied and therefore the attack are going to be created which attack is implemented exploitation Network simulator II. Exploitation the cryptological based mostly advanced routing protocol the impact of attack are going to be reduced.

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.