

An Algorithm for Secure routed creation and Data Transfer in MANETs

B.Anantharaj¹, N.Satheeshkumar²

¹Department of CSE, Thiruvalluvar College of Engg. And Tech., Tamilnadu, India.

²Department of CSE, University college of Engineering Villupuram, Tamilnadu, India.

Email:nsatheesh8984@gmail.com

Abstract- Mobile ad hoc network is an emerging research area now days with practical applications oriented. MANETs are infrastructure-less networks used for communication between two or more nodes without a common access point. There are a number of Routing creations algorithms proposed in the recent scenario. Now we are proposed a secure route creation scheme for Pseudo-Random Number Generation using RSA Algorithm. In this security scheme we use a random bit series number function. In this function each node will generate random bit series number during signaling period and reverse the order of random bit series numbers after reaching the destination node. The merit of this security scheme is to protect from any intruder or outsider node to attack or capture the node of the wireless network. We use random bit series number function to make the network more secure for MANETs.

Key words: Wireless Ad hoc networks, MANETs, Security, routing protocol, routing creation.

I.INTRODUCTION

Security in MANETs is the most important concern for the basic functionality of network [1]. The availability of network services, integrity and confidentiality of the data can be achieved by assuring that security issues have been met. Mobil ad hoc networks often suffer from security attacks because of its features like open medium, shifting its topology dynamically, lack of middle monitoring and management, cooperative algorithms and no clear security mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

The Mobil ad hoc networks work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes Mobil ad hoc networks more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the Mobil ad hoc networks more susceptible to attacks, which make it simple way for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes inside within the range of wireless link can overhear and even participate in the network.

Mobil ad hoc networks must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the challenge of the day. In order to provide secure communication and transmission of the user, so must understand different types of attacks and their effects on the Mobil ad hoc networks. Attacks can be classified into two types [2]: Passive Attack and Active Attack (Komminos *et al.*, 2007). Passive attack is eavesdropping on transmission and it is complicated to detect. While active attack involves creating or modifying a fraudulent stream. Unfortunately, all types of Mobil ad hoc networks protocols have no security and can be easy vulnerable to any types of attack to face these attacks many new security protocols have been appeared to remove these endangered attacks and obtained Mobil ad hoc networks securities. These security protocols have to satisfy a few of the objectives, which are (Mouchataris and Anjum, 2007):

- **Availability:** Availability ensures that the network services area unit accessible.
- **Confidentiality:** It ensures that info content is hidid to unconstitutional entities.
- **Integrity:** It ensures that knowledge isn't changed throughout transmission.
- **Authentication:** Authentication ensures a node of the identity of the opposite party or parties that it's act with
- **Non-repudiation:** Guarantees that a celebration can not be false denying its action.

Since there are many attacks require defining the above objectives. It is complicated to have a universal protocol that can satisfy all the above security conditions. There are many protocols appeared to secure MANET routing and packet forwarding that it is focused on different types of the attack.

MANETs communication has two phases, route discovery and data transmission. Both phases are vulnerable to a variety of attacks. The main goal of the route discovery and securing routing in one node to another node.

II.CLASSIFICATION OF MANETs LAYERS ATTACKS

Attacks on network are classified into two categories [3] – Internal attack and External attack. In Internal attacks, the attacker wants to gain the ordinary access to the network and participate the network behavior, whichever by some malicious impersonation to get the access to the network as a new node, or by directly compromising a present node and using it as a basis to conduct its malicious behaviors. In External attacks, the attacker aims to cause jamming, propagate fake routing information or disturb nodes from providing services. Here we explain the different types of attacks against different layers [4]:

- **Application layer-** Repudiation, Data correction.
- **Transport layer** - Session hi-jacking, SYN flooding.

- **Network layer** - Wormhole, Black hole, Byzantine, Flooding, Resource Consumption, Location disclosure Attack.
- **Data link layer** - monitoring disruption MAC, Traffic analysis, WEP weakness.
- **Physical layer** - Jamming, interception, eavesdropping.
- **Multi-layer attacks** - DoS, impersonation, replay, manin- middle attack.
-

III. REVIEW OF ROUTING PROTOCOL

In MANETs, some variety of routing protocol is needed so as to dynamically notice the multi-hop ways through that packets may be sent from one node to a different [1]. There area unit primarily 2 classes of routing protocols for MANETs[16]:

1. Table Driven (Proactive): DSDV, GSR, WRP
2. Source Initiated On-Demand (Reactive): ABR, AODV, DSR, LAR

Much of the analysis has been done that specialize in the potency of the MANETs. There area unit quite a range of routing protocols that area unit wonderful in terms of potency. However the protection needs of those protocols modified the case and an additional elaborated analysis is presently afoot to develop secure unintentional routing protocols. MANETs area unit very liable to attacks thanks to their dynamically dynamic topology, absence of standard security infrastructures and open medium of communication, which, not like their wired counterparts, can't be secured. To deal with these considerations, many secure routing protocols are proposed: Secure economical Distance Vector Routing (SEAD), Ariadne, and echt routing for unintentional Networks (ARAN), Secure unintentional On-Demand Distance Vector Routing (SAODV), and Secure Routing Protocol (SRP). Though researchers have planned many secure routing protocols, their resistance towards varied styles of security attacks and potency area unit primary purpose of concern in implementing these protocols.

IV.ROUTING PROTOCOL ATTACKS IN MANETs

There are many attacks which might be mounted on the routing protocols and will disrupt the correct operation of the network. temporary descriptions of such attacks area unit given below[5]:

Routing Table Overflow: within the case of routing table overflow, the assaulter creates routes to nonexistent nodes[5]. The goal is to form enough routes to forestall new routes from being created or to overwhelm the protocol implementation. Within the case of proactive routing algorithms we want to find routing data even before it's required, whereas within the case of reactive algorithms we want to search out a route only if it's required. so main objective of such Associate in Nursing attack is to cause Associate in Nursing overflow of the routing tables, which might successively forestall the creation of entries cherish new routes to licensed nodes.

Routing Table Poisoning: In routing table poisoning, the compromised nodes gift within the networks send fictitious routing updates or modify real route update packets sent to alternative licensed nodes. Routing table poisoning could lead to sub-optimal routing, congestion in parts of the network, or maybe build some elements of the network inaccessible.

Routing Table Poisoning: In routing table poisoning, the compromised nodes gift within the networks send fictitious routing updates or amendment real route update packets sent to different approved nodes. Routing table poisoning could lead to sub-optimal routing, ECM in parts of the network, or maybe create some components of the network inaccessible.

Packet Replication: within the case of packet replication, associate degree assailant replicates stale packets. This consumes further information measure and battery power resources on the market to the nodes and conjointly causes supernumerary confusion within the routing method.

Route Cache Poisoning: within the case of on-demand routing protocols (such because the AODV protocol [11]), every node maintains a route cache that holds info concerning routes that became renowned to the node within the recent past. just like routing table poisoning, associate degree person may also poison the route cache to realize similar objectives.

Rushing Attack: On-demand routing protocols that use duplicate suppression throughout the route discovery method square measure liable to this attack [12]. associate degree assailant that receives a route request packet from the initiating node floods the packet quickly throughout the network before different nodes that conjointly receive a similar route request packet will react. Nodes that receive the legitimate route request packets assume those packets to be duplicates of the packet already received through the assailant and therefore discard those packets. Any route discovered by the supply node would contain the assailant jointly of the intermediate nodes. Hence, the supply node wouldn't be able to realize secure routes, that is, routes that don't embrace the assailant. It's extraordinarily troublesome to observe such attacks in accidental wireless networks.

V. PROPOSED WORK

Securing Routing Discovery Protocols :In the securing routing protocols [2] the routes discovered between the source and destination must be protected from any malicious nodes attempt to fabricated, forge, disrupted the route and replayed. There are 2 classes of routing protocols exist in the mobile ad hoc networks world. The first class, reactive protocols

acquire routes on demand through flooding a route request and receiving a route reply. Another class of MANET routing protocols is proactive; it ensures that all nodes at all times have sufficient topological information to construct routes for all destinations in the network through periodic message exchange.

Table-driven: Table driven routing protocols basically use proactive schemes. They conceive to maintain consistent up-to-date routing info from every node to each alternative node within the network. These protocols need every node to keep up one or additional tables to store routing info and any changes in configuration have to be compelled to be mirrored by propagating updates throughout the network so as to keep up a standardized network read.

On demand: a special approach from table driven routing is source-initiated on-demand routing. this kind of routing creates routes only desired by the supply node. Once a node needs a route to a destination, it initiates a route discovery method at intervals the network. This method is completed once a route is found or all potential route permutations are examined

Routing Discovery: The route discovery method consists of a route-request message (RREQ) that is broadcasted. If a node features a valid route to the destination, it replies to the route-request with a route-reply (RREP) message. In addition, the replying node creates a therefore known as reverse route entry in its routing table that contains the address of the source node, the quantity of hops to the source, and also the next hop's address, i.e. the address of the node from that the message was received.

Route Maintenance: The periodic routing updates square measure sent to all or any the nodes. If any link on a source route is broken, the source node is notified employing a route error (RERR) packet. The source removes any route victimisation this link from its routing table. A brand new route discovery method should be initiated by the source if this route remains required. The Routing Discovery example shown in figure 1.

Secure Routing Protocol (SRP): Secure Routing Protocol (SRP) can be applied as an extension of DSR (Dynamic Source Routing protocols) (Papadimitratos and Haas, 2002; Papadimitratos *et al.*, 2002; Papadimitratos, 2005) [2]. The necessity for SRP protocol is the existence of a SA (Security Associated). It applied security associated only at the end nodes and no need for any cryptographic methods at midway nodes. For each route request (as well as reply), SRP used two numbers to identify the request to improve the security; First one is a sequence number that is increased periodically. Another one is a random Identifier. The only possible attacks against the protocol would be if two or more nodes colluded during single route discovery and middle man attack .So avoids middle man attackers, to applied security associated with the each node using unique ID and Secure Pseudo-Random Number Generation using RSA algorithm in Secure Routing creation.

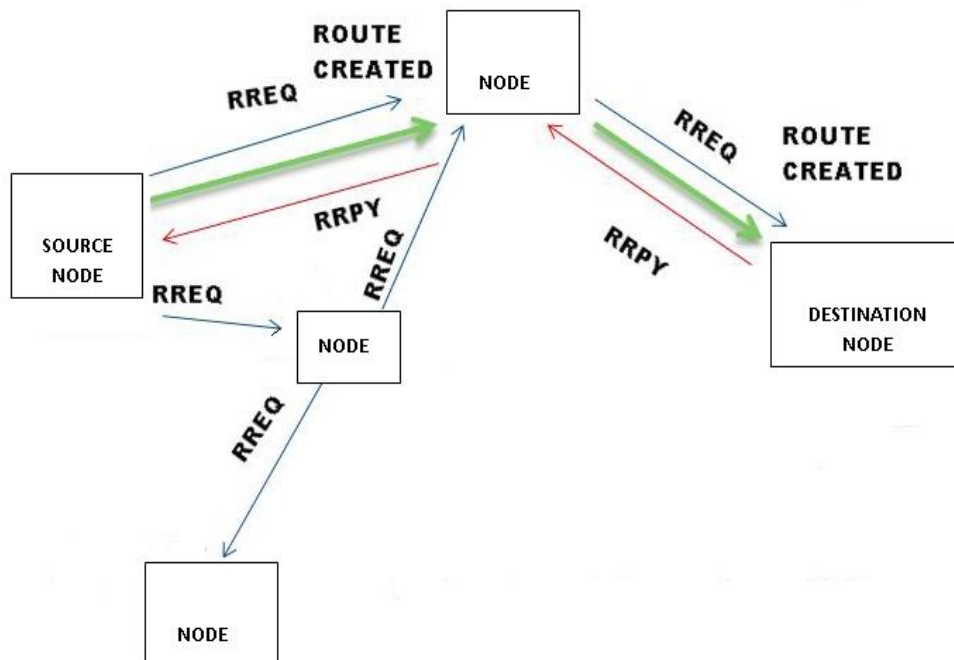


Fig 1: Example applications of MANETs.

The new idea is discussed in the (figure 2) shown blow. In this concept each node is assigned a unique ID before creating a wireless network for communication between nodes .when a wireless network is established and node (S) wants to communicate with node (D) in the network topology. The node (S) acts as a transmitting node, it will send a message during signaling period with unique node ID and generate a random bit number for example when this message is broadcast to its neighbors. Receiving node for (E) first verify that is has an ID of transmitting node in its routing table. If it already in the routing table it will accept the message from the transmitting node. If receiving node (E) is not the destination then it broadcast the message again. The node (E) will transmit a message with its unique ID and it knows that node (S) generated a random bit number (a_1), so after computation using random bit number it will generate a bit number (a_2).

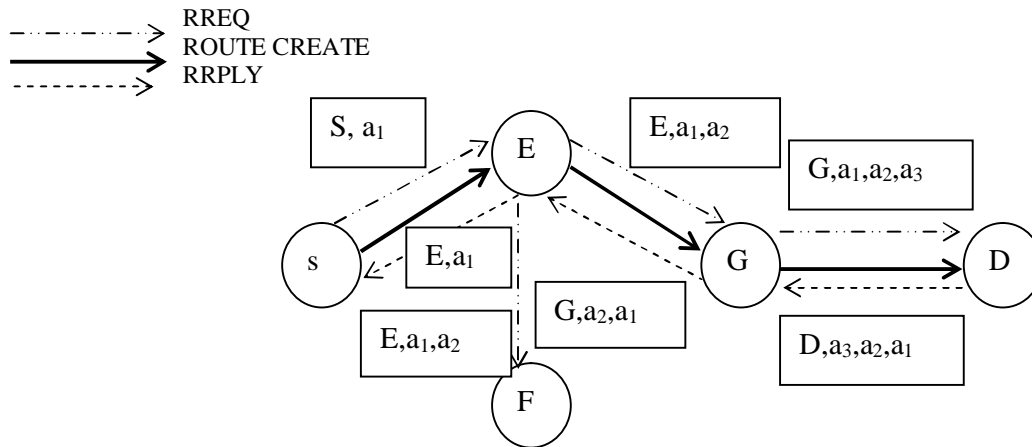


Figure 2: Secure based route creation

When the destination node (D) will receive the unique ID with a random bit series ($a_1, a_2, a_3, \dots, a_k$). The destination node (D) will send back and reverse back the order of all the random bit series number generation. When the destination node(D) sends its unique ID and generate an random bit series number which was generated by node G. Node (G) knows that it generated an random bit series number a_3 then it will accept it .Same procedure is followed in the whole network till it reaches to the source node (S). After this signaling process route is established between the source nodes to the network node in secured environment. In this algorithm data is transmitted safely without any intruder attack.

VI.CONCLUSION AND FUTURE WORK

Routing security in Mobile ad hoc networks appears to be a nontrivial problem that cannot easily be solved. It is impossible to find a general idea that can work efficiently against all kinds of attacks, since each attack has its own distinct characteristics. In this article we study the routing security issues of MANET, The proposed mechanisms until now have solved many security issues related to routing security and this algorithm data is transmitted safely without any intruder attack.

In future, we will propose to design a protocol that uses minimal public key cryptography to avoid overload on the network and uses shared key cryptography extensively to provide security.

REFERENCES

- 1) Irshad Ullah,Shoaib Ur Rehman "Analysis of Black Hole attack onMANETs Using different MANET routing protocols" Master Thesis, Electrical Engineering,*Thesis no: MEE 10:62, September, 2010.*
- 2) Salwa Aqeel Mahdi, Mohamed Othman, Hamidah Ibrahim, Jalil Md. Desa and Jumat Sulaiman" Protocols For Secure Routing And Transmission In Mobile Ad Hoc Network: A Review" Journal of Computer Science 9 (5): 607-619, 2013.
- 3) Sarvesh Tanwar, Prema K.V." Threats & Security Issues in Ad hoc network: A Survey Report" ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
- 4) Amandeep Kaur, Hardeep Singh"A Study of Secure Routing protocols" International Journal of Application or Innovation in Engineering & Management, ISSN 2319 – 4847 Volume 2, Issue 2, February 2013.
- 5) Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay" Different Types of Attacks on Integrated MANET-Internet Communication" International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3),
- 6) Uma Mani, Ramasamy Chandrasekaran and V.R. Sarma Dhulipala "STUDY AND ANALYSIS OF ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORK"Journal of Computer Science 9 (11): ISSN: 1549-3636 1519-1525, 2013.

- 7) Hongmei Deng, Wei Li, and Dharma P. Agrawal "Routing Security in Wireless Ad Hoc Networks" IEEE Communications Magazine • October 2002
- 8) Aggarwa, A., S. Gandhi, N. Chaubey, P. Shah and M.Sadhwani, 2012. AODVSEC: A novel approach to secure Ad Hoc on-Demand Distance Vector (AODV) routing protocol from insider attacks in MANETs. Int. J. Comput. Networks Commun., 4: 191-210. DOI: 10.5121/ijcnc.2012.4412
- 9) Kulasekaran, S. and M. Ramkumar, 2011. APALLS: A Secure MANET Routing Protocol. In: Mobile Ad-Hoc Networks: Applications, Wang, X. (Ed.), InTech, ISBN-10: 9789533074160.
- 10) C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April, 2010.
- 11) C.Parkins, E.B.Royer, S.Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: <http://www.faqs.org/rfcs/rfc3561.html>. [Accessed: April. 10, 2010]
- 12) Y.F.Alem, Z.C.Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May, 2010.
- 13) Mobile ad hoc networks http://en.wikipedia.org/wiki/Mobile_ad_hoc_network
- 14) Pro active protocol preview <http://www.soi.wide.ad.jp/class/20030000/slides/05/47.html>
- 15) Routing overview, Motorola mobility <http://networking.ringofsaturn.com/IP/Routing.php>.
- 16) Rajneesh Narula, Kaushal, Sumeer Khullar, Anish Arora " Security Issues of Routing Protocols in MANETs" International Journal of Computers & Technology, ISSN: 2277-3061 Volume 3 No. 2, OCT, 2012