ISSN 2047-3338

Secure Analysis for Secure Routing Protocols over MANET

Pradnya Patange and S.P. Medhane

***Abstract*— Security is one of the important aspects in mobile ad-hoc network (MANET). Also routing algorithm in MANET is dissimilar than traditional routing. This paper provides limits of traditional routing protocols if used to MANET. This paper also describes routing protocols at this time used in MANET and place focus on security analysis of routing protocol over quite a lot of possible security attacks such as Attacks by means of alteration, Denial of Service attacks, Wormhole attacks, Impersonation attacks, Attacks by means of fabrication, Rushing Attacks etc. lastly this paper emphasis on requirement for more robust protocol to identify wormhole attacks.**

***Index Terms*— MANET, Routing Algorithms, Security Analysis, Secure Routing Protocol and Network Lifetime**

I. INTRODUCTION

MOBILE Ad-hoc Network (MANET) is a group of self configurable mobile node linked through wireless links.

In MANET a large amount of the study has been completed focusing on the effectiveness of the system. There are quite a number of routing protocols that are outstanding in terms of effectiveness. But the protection requirements of these protocols altered the condition and a more detailed study is at present underway to build up protected ad hoc routing protocols. MANETs are more susceptible to attacks due to their dynamically altering topology, nonexistence of usual safety infrastructures and public medium of communication, which, not like to their wired parts, may not be protected.

In wireless network many types of attacks can be initiated but most of them are relative easy to detect because of their property of dramatically altering the network statistics but one different type of attack i.e. wormhole attack we have considered. It is very significant when considering security issues of network, is wormhole attack, which is not easy to identify & can harm by directing significant information to unauthorized nodes. Throughout the path detection process, a wormhole can relay route request and response messages between distant nodes, making the appearance of shorter paths to destinations. Since the wormhole can be anyplace along a path, a source will have to identify its existence anywhere along the path when a node sets up the path (on-demand).

Pradnya Patange is Student of M.Tech (IT) Bharati Vidyapeeth College of Engineering Pune, India, (Email: pradnya11@gmail.com)

S. Medhane is Assistant Professor with the Department of Information Technology Bharati Vidyapeeth College of Engineering, Pune, India, (Email: sampat.medhane@gmail.com)

II. ANALYSIS OF SECURE ROUTING PROTOCOLS

Security protocols for MANET's can be primarily divided in two main categories [1], [2]:

Prevention: This mechanism involves protocols which prohibit the attacking node to initiate any action. This advancement requires encryption method to verify the privacy, integrity, non-repudiation of routing packet data.

Detection and Reaction: Detection as well as Reaction method as the name advise will recognize any malicious node or activity in the network and take right act to keep up the proper routing in the network.

A. ARAN: Authenticated Routing For Ad Hoc Network

Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz as well as Elizabeth M. Belding-Royer searched Authenticated routing for Ad hoc Network based on AODV [3] by means of Certificates with a Central Certification Authority. Authenticated Routing for Ad hoc Networks (ARAN) [4] routing protocol, is based on Cryptographic Certificates as well as depend on a central trusted Certification Server (T). Every node entering into the network has to get a certificate signed by T. The certificate contains the IP address of the node, its public key, and time stamp when the certificate was issued and when it will expires. ARAN protocol in its route discovery sends a Route Discovery Packet (RDP) to its neighbor nodes. RDP includes destination IP (d), Source certificate Cert(s), nonce N(s) that is a time stamp for the packet life and the current time 't'. And the complete packet is signed by source's private key K(s) [4].

ARAN uses public key cryptography with a central certification authority server for node authentication as well as neighbor node authentication in path detection.

Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbor node authentication through certificates. Participating nodes broadcast needless path requests across the network. An attacker can effect blocking in the network, there by compromising the working of the network.

Spoofing attacks are prohibited by ARAN by node level

signatures. Every packet in the system is signed by its private key previous to broadcasted to the next level and checked for the verification. So spoofing the uniqueness of node is hampered by ARAN. Due to the well-built cryptographic characters of ARAN, malicious nodes may not contribute in at all type of attack patterns. Only compromised nodes can participate in any attack pattern. Wormhole attack is possible in ARAN. Two compromised neighbor nodes can collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. Rushing attack is not possible in ARAN. Table overflow, black hole attacks are impossible due to node level authentication with signatures.

B. SAR: Security- Aware Routing Protocol

Seung Yi, Prasad Naldurg and Robin Kravets developed SAR [5]. SAR based on AODV [3] & uses Security as on of the Key Metrics in its route discovery and maintenance.

SAR uses Security as one of the Key Metrics in its route discovery and maintenance.

The framework and attributes of the security metrics are detailed in [8]. This framework also uses different levels of security for different level of applications.

Each node in the network is associated with a level of trust metric, based on which route will be followed according the security requirements of the application. SAR extends on-demand ad hoc routing protocols (like AODV or DSR) in order to incorporate the protection metric into the path request messages. The originator broadcasts a path request (RREQ) with an extra field (RQ_SEC_REQUIREMENT) that indicates the necessary safety level of the path that needs to find out. A neighboring node that receives the packet, checks whether it can satisfy the security requirement. If the node can provide the required security then it can participate in the requested route and re-broadcasts the packet to its own neighbors setting a new field called RQ_SEC_GURANTEE to indicate the maximum level of security it can provide. If a node is not secure enough to participate in the requested route it simply drops the RREQ. Therefore, when the destination node receives the RREQ it can be sure that a route to the source node exists and that this route satisfies the security requirements defined by the initiator. The destination sends a path reply (RREP) packet with an extra field (RP_SEC_GUARANTEE) that indicates the highest level of protection of the found path. The RREP message travels back along the reverse path of the intermediate nodes that were allowed to participate in the routing, and each node updates its routing table according to the AODV specification including the RP_SEC_GUARANTEE value. This value is used in order to permit middle nodes with cached routes to respond to a request of a path with a specific safety prerequisite.

SAR was developed using a trust-based framework. Every node in the system is assigned with a trust level. Consequently the attacks on this structure can be analyzed based on trust level as well as message integrity. Rushing attack, Routing table modification and Black hole attacks is not possible in SAR but Wormhole attacks and Denial of- service attacks are possible in SAR.

C. SRP: Secure Routing Protocol

Secure Routing Protocol (SRP), was proposed by Papadimitratos and Hass [5]. SRP is based on DSR [6]. DSR is an on-demand routing protocol, which finds the route as and when required, dynamically. The major difference between AODV and DSR is that DSR uses source routing in which a data packet carries the complete path to be traversed where as in AODV the source node and intermediate nodes store the next hop information for each data packet transmission.

SRP is implemented over DSR [11], by means of an underlying Security Association (SA) connecting the source with destination nodes. Key created by the SA is used to encrypt and decrypt the data by the two nodes.

Secure routing protocol (SRP) was developed based on Destination Source Routing (DSR). The middle nodes including in the path detection measure the frequency of queries received from their neighbors and keep up a priority ranking inversely proportional to the query rate. Consequently the malicious compromised nodes including in the network are known least priority to deal with. Rushing attack, Routing table alteration, Denial of-service Attacks and Black hole attacks is not possible in SRP but Wormhole attack is feasible in SRP.

D. SEAD: Secure Efficient Ad Hoc Distance Vector Routing Protocol

SEAD is planned based on top of the DSDV (Destination Sequenced Distance Vector) protocol. SEAD was developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig [7]. Destination Sequenced Distance Vector routing protocol is one of the first protocol proposed for ad hoc wireless networks. It was developed based on the distributed Bellman-Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. It's a table driven routing protocol. Paths to all destinations are readily accessible at each node at every time. The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology. When there is a alteration in the system topology, the table entries are modernized.

SEAD was developed based on DSDV and incorporates One-Way Hash function to authenticate in the routing update mechanism in order to improve the path safety. Securing a table driven protocol is difficult than securing an on demand protocol due to the existence of already defined paths. Distance vector protocols encapsulate the path information into a hop count value as well as a next hop. An attacker cannot generate a valid path with a bigger sequence number that it got due to the characteristics of hash function.

As SEAD includes neighbor verification through Hash functions, an attacker cannot cooperate any node. Routing table overflow attacks are feasible in SEAD, as SEAD is searched based on a table driven approach. A compromised node can announce paths to nodes which are not in the network and there by fill in the gap allocated in the routing table with false node paths. Spoofing attack is possible through

compromised node acting like a destination node in the route discovery process by spoofing the identity of the destination node that can cause path damage. Black hole attack is also possible through a compromised node advertising the shortest roots to non-existing nodes in the network. Wormhole attack is also feasible for the period of compromised nodes. Rushing Attack as well as Denial of-service attack is not feasible. Table driven protocols are much more prone to security threats.

E. ARIADNE

Ariadne is a secure routing protocol developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig based on the Dynamic Source Routing protocol (DSR) [6].

Ariadne[7] uses the basic path mechanism of DSR and uses TESLA [12] broadcasting verification protocol. Ariadne gives ides point-to-point authentication of a path message using a message authentication code (MAC) and a shared key between the pair of communicating nodes. In Ariadne a route request packet (RREQ) includes eight fields: RREQ, initiator, target, id, time interval, hash chain, node list, as well as MAC list.

Ariadne was developed based on an on demand protocol, Destination Source Routing (DSR). Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime.

Ariadne prevents spoofing attacks with time stamps. The use of source paths prevents loops, because a packet passing during only legitimate nodes will not be forwarded into a loop due to time stamps. Rushing attack, Routing table alteration, Denial of-service Attacks as well as Black hole attack is not feasible in Ariadne but Wormhole attack is feasible in Ariadne.

F. SLSP: Secure Link State Routing Protocol

A The Secure Link State Routing Protocol (SLSP) [9] has been developed to create protected proactive routing for mobile ad hoc networks. It secures the detection and the sharing of link state information both for locally and network-wide scoped topologies. SLSP can be working as stand-alone clarification for proactive link-state routing, or joint with a reactive ad hoc routing protocol forming a hybrid framework. The Secure Link State Routing Protocol (SLSP) is used to secure the discovery and the distribution of link state information. This protocol makes use of asymmetric key for the security purpose. Participating nodes are identified by the IP addresses of their interfaces. SLSP can be logically divided into three major steps which are as follows:

• *Public key distribution:* SLSP does not use any central server for key allocation. Distribution of public key is done by the node to the nodes within its own surrounding area. This distribution of the key is called as public key distribution (PKD).

• *Neighbour discovery:* Link state information of the node is broadcast periodically using Neighbour Lookup Protocol (NLP). Hello message contains sender's MAC address and IP address of the network. These packets are also signed. NLP can be used for verifying the discrepancies or the malicious node.

• *Link state updates (LSU):* Link state update (LSU) packets are verified by the IP address of the originating node as well as contains a 32-bit sequence number for providing updates. Middle nodes LSU validate the attached signature using a public key they have previously catched in the pubic key distribution phase of the protocol. The hops traversed field of the LSU is updated to hashed hops traversed, the TTL is decremented and at the end the packet is broadcasted again.

To guard against denial of service attacks, SLSP nodes preserve a priority ranking of their neighboring nodes based on the rate of control traffic they have observed. High priorities are given to nodes that generate LSU packets with the lowest rate. This functionality enables the neighbors of malicious nodes that flood control packets at very high rates to limit the effectiveness of the attack.

SLSP provides a proactive secure link state routing solution for ad hoc networks. SLSP offers protection against individual malicious nodes by securing the neighbor discovery process and using NLP as a way to detect discrepancies between IP and MAC addresses. As it is mentioned by the authors, SLSP is susceptible to colluding attackers that fabricate non-existing associations between themselves and flood this data to their adjacent nodes. Rushing attack, routing table alteration, Denial of-service Attacks and Black hole attack is not feasible in SLSP but Wormhole attack is feasible in SLSP.

G. SAODV: Secure Ad Hoc On-Demand Distance Vector Routing

SAODV is a secure routing protocol developed based on AODV. SAODV was developed by Manel Guerrero Zapata, N. Asokan [10]. SAODV in its implementation assume that there is already a central key management system through which every node can obtain public keys. Digital signatures are used to authenticate the fields of the message and hash chains to secure the hop count information. SAODV uses hash chains to authenticate RREQ and RREP flows between neighbor nodes in the route discovery process. A hash chain is formed with a one-way hash function and random seed. Each time a node creates a RREQ or a RREP message, the maximum hop count field is put to the max time to live. The top hash value is calculated using the hash function 'h′ and the random seed to it. Every time RREQ or RREP are received by a node it verifies the hop count, [h (max hop) – hop count time] to check it with the value contained in the top hash value.

The intermediate node after the verification of its integrity and authentication creates a RREQ or RREP if it's the end node. The node puts the hash function to the hash value in the signature addition to account for the new hop. The hash function field indicates which hash function has to be used to compute the hash.

When a node initially got a RREQ, it first identifies the signature previous to creating or updating a reverse path to that host. When the RREQ go upto the destination node, RREP will be sent with a RREP signature extension. When a node got a RREP, it initially identifies the signature previous to genereating or updating a path to that host. If the signature is verified, it will save the path , the signature of the RREP with

lifetime. Once successful path detection is made, the sender and end nodes communicate along the discovered paths. If a connection break occurs in the topology a Route Error (RERR) message is created like in AODV. This RERR's are secured again with digital signatures.

SAODV is a mainly used protocol in industry due to its strong protection characteristics. SADOV uses a central key organization in its routing topology. Digital signatures are used to validate at node level as well as hash chain is used to prevent the altering of node counts. Wormhole attack is feasible through two compromised nodes. And Denial of-service Attacks is also feasible. But Rushing attack, Routing table alteration, and Black hole attack is not feasible.

H. Byzantine Algorithm

N This protocol is used to protect the network from Byzantine failures which include modification of packets, dropping packets, attacks caused by selfish or malicious nodes. Byzantine algorithm [11] consists of three different phases:

• *Route Discovery:* When a source node needs to deliver the message, it broadcasts a route request packet containing sender address, end station address, a sequence number, a weight list and the private key for authentication to its neighbors. On receiving the RREQ packet the intermediate node checks for RREQ entry in its own list. If there is no entry for the RREQ, it identifies the key for verification and appends it in the list and resends it to all every nodes. When the destination node is reached, it identifies the key and generates a route reply message (RREP). On getting the RREP packet, sender node confirms the private key. It also compares the received path and the existing path. If the received path is good than the existing one then update this path in its own table.

• *Fault Detection:* In this phase source node for every received packet. If quantity of unacknowledged packets moves more than some threshold value, a fault is identified on the path.

• *Link Weight Management:* This phase of the protocol calculates the weight of the links. If a link is identified as faulty by the fault detection phase its corresponding weight value gets doubled. In the route discovery phase link with lower weight value will be taken as better link.

This protocol is used to guard the network from Byzantine failures which contain alteration of packets, dropping packets, attacks created by selfish or malicious nodes. Rushing attack, Denial of- service and Routing table alteration attacks is not feasible in Byzantine Algorithm. But Wormhole attacks and Black hole attacks are possible in Byzantine Algorithm.

I. Core

The CORE (a collaborative reputation mechanism to enforce node cooperation in MANET) is a protocol which works on the co-operative behavior of the nodes. It takes use of Reputation Table as well as Watchdog method to recognize the co-operative or disobedient node. The reputation table component maintains a table of intermediate nodes and the associated reputation or ratings. The Watchdog component calculates the function and provides the Reputation value [12].

This protocol consists of a sender and one or more middle node. In this protocol, whenever an middle node rejects to co-operate with the sender node, CORE scheme will decrease the repudiation of middle node. This can lead to elimination of intermediate node from the network.

CORE is a protocol which works on the co-operative behavior of the nodes. It makes use of Reputation Table and Watchdog mechanism to identify the co-operative or misbehaving node. Rushing attack, Routing table modification Wormhole attacks and Black hole attacks are possible in CORE but Denial of- service attacks is not possible in CORE.

J. Confidant

The Confidant (Cooperation of Nodes: Fairness in Dynamic Ad hoc Networks) protocol is use to identify the non cooperative nodes. This protocol contains the monitor, the reputation system, the path manager and the trust manager. The monitor component is responsible for monitoring passive acknowledgements for each packet it forwards. The trust manager component deals with the sending and receiving of alarm messages. When a node detects that a node is disobedient, it sends an alarm message. These messages are exchanged between nodes that are pre-defined as friends. Alarms from other nodes are given substantially less weight [13].

The reputation system component keeps up a table of nodes in addition to the associated ratings. Ratings are updated according to a rate function that uses of small weights if an alarm is reported for a disobedient node and larger weights for direct observations. The path manager component manages all path information regarding addition, deletion, and updating of paths according to the feedback it received from the reputation system. If a rating falls under a certain threshold the path manager component is called in order to remove the path containing the identified malicious node.

The Confidant protocol is used to detect the non helping nodes. Rushing attack, Wormhole attacks in addition to Black hole attacks are not feasible in Confidant. But Denial of-service and Routing table modification attacks are feasible in Confidant.

K. Watchdog and Path rater

Number The watchdog and path rater protocol is used to find out the malicious nodes which deny forwarding the packets however they have agreed to forward it earlier. The role of Watchdog is to watch that the next node in the path is forwarding the data packet or not. If not then it will be taken as the malicious behavior. Role of path rater is to assess and discover the reliable path from the result created by watchdog [14].

When a node transmits a packet to the next node in the path, it tries to listen if the next node will also transmit it and also tries to find out that the next node do not modify the packet before forwarding it. If a node presents some malicious action such as denial of service or alteration of data packet, Watchdog will enhance its failure rating. This failure rating is helpful in discovery of the reliable path from start station to end station.

The watchdog and path rater protocol is used to discover the malicious nodes which reject forwarding the packets though they have accepted to forward it earlier. Rushing attack, Denial of- service attacks, Routing table alteration attacks as well as Black hole attacks are feasible in Confidant. Detection of Wormhole attack is not possible in Watchdog and path rater and approaches for detecting wormhole attacks are proposed in [15]-[18].

III. CONCLUSION

In this paper we analyzed secure routing protocols and their effectiveness to detect several possible security attacks on MANET environment. Most of the secure routing protocols are not effective to detect and mitigate wormhole attack. This paper emphasis on need for more robust routing algorithm to detect and mitigate wormhole attacks. Our feature work includes design of secure routing protocol to detect and mitigate wormhole attacks using public key cryptography.

ACKNOWLEDGMENT

Thanks to Bharati Vidyapeeth College of Engg. Pune,

REFERENCES

[1] Stallings W, Network Security Essentials: Security Attacks. Prentice Hall. , 2000 (pp. 2- 17)

[2] Parul Tomar, M. K. Soni and P.K. Suri "A Comparative Study for Secure Routing in MANET" from YMCA University, MRIU and Kurukshetra University, in International Journal of Computer Applications (0975 – 8887), Volume 4 – No.5, July 2010, pp. 17-22.

[3] C. Siva Ram Murthy and B.S. Manoj. Ad Hoc Wireless Networks, Architecture and Protocols: 2004 Pearson Education (pp. 321-386, 473-526)

[4] Kimaya Sanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), 2002.

[5] Seung Yi, Prasad Naldurg and Robin Kravets in the Dept. of Computer Science, University of Illinois at Urbana-Champaign.

[6] Basagni, S. Conti, M. Giordano, S. Stojmenovi & cacute (Edit). Mobile Ad Hoc Networking: September 2004 Wiley-IEEE Press. (pp. 1-33, 275-300, 330-354), 2004.

[7] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02).

[8] P. Papadimitratos and Z. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In IEEE Wksp. On Security and Assurance in Ad Hoc Networks, 2003.

[9] P. Papadimitratos and Z. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In IEEE Wksp. On Security and Assurance in Ad Hoc Networks, 2003.

[10] M. Zapata and N. Asokan. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. ACM Mobile Computing and Communications Review, vol. 3, no. 6, July 2002, pp. 106-107.

[11] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens. An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. WISE'02, Atlanta, Georgia, September 2002, pp. 21-30.

[12] P. Michiardi, R. Molva. Core: A Collaborative Reputation mechanism to enforrce node cooperation in Mobile Ad Hoc Networks. In Communication and Multimedia Security Conference, 2002.

[13] S. Buchegger, Jean-Yves Le Boudec. Cooperation of Nodes — Fairness in Dynamic Ad-hoc NeTworks. IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC).

[14] Sergio Marti, T.J. Giuli, Kevin Lai and Mary Baker.Mitigating routing misbehavior in mobile ad hoc networks. ACM MobiCom, 2000, pp- 255-265.

[15] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008, pp. 343-348.

[16] Wang, W.; Bhargava, B. Visualization of Wormholes in Sensor Networks. In Proceedings of the 2004 ACM workshop on Wireless Security (WiSe), ACM WiSE'04, Philadelphia, PA, USA, October 2004; pp. 51–60.

[17] W. Wang, B. Bhargava, Y. Lu, and X. Wu, Defending against wormhole attacks in mobile ad hoc networks: Research articles," Wirel. Commun. Mob. Comput., vol. 6,no. 4, pp. 483-503, 2006, 1144444.

[18] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. IEEE INFOCOM, Mar 2003.

Pradnya R. Patange has completed B.E.I.T. from Govt. College of Engg. Karad,Maharashtra in 2005. Currently getting MTECH (IT) degree from Bharati Vidyapeeth College of Engg., Pune.Main interest of study in MANET, (Email: pradnya11@gmail.com)

Sampat Medhane working as a Assistant professor in Department of Information Technology at Bharati Vidyapeeth College of Engg, Pune, (Email:sampat.medhane@gmail.com)