International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 1 Issue: 12 896 – 899

Asymmetric Prevention Based Techniques In Ad-Hoc Networks

Budesh Kanwer
Assistant Professor
Maheshwari College Of Commerce & Arts
E-mail: budesh82@gmail.com

Abstract —A mobile ad hoc network is a infrastructure-less and autonomous network where so cooperation among nodes is important since in such networks nodes depend on each other for forwarding packets. However, cooperation in such operations consumes nodes energy and recourses. Therefore, it is necessary to design incentive mechanisms to enforce nodes to forward packets when the source and destination of the packet are other nodes in the network. Routing is a key issue in wireless networks and it has been the topic of extensive research in the last few years. Prevention Techniques provides solutions that are designed such that malicious nodes are originated from actively initiating attacks. The prevention mechanisms need encryption techniques to give authentication, integrity, confidentiality and non repudiation of routing information. Among all of the recent preventive approaches, few proposals utilize symmetric algorithms, few utilize asymmetric algorithms, however the others utilizes one-way hashing, each particular having distinguish trade-offs and goals.

Keywords: *ad hoc network, encryption, one-way hashing, malicious nodes.*

*****

1. INTRODUCTION

There are basically two approaches used these days to provide solutions to the security issues in ad hoc networks.

- Prevention Techniques in MANETs
- Detection and Reaction Techniques in MANETs

Prevention Techniques provides solutions that are designed such that malicious nodes are originated from actively initiating attacks. These prevention mechanisms need encryption techniques to give authentication, integrity, confidentiality and non repudiation of routing information. Among all of the recent preventive approaches, few proposals utilize symmetric algorithms, few utilize asymmetric algorithms, however the others utilizes one-way hashing, each particular having distinguish trade-offs and goals. In this paper we are going to discuss prevention using asymmetric cryptography.

The figure 1 depicts the communication in any ad hoc network:

1. Sender node sends the signal to the neighboring nodes within the vicinity.
2. Neighboring nodes communicate with the sender node
3. Sender node sends the message to the destination node.
4. If destination node is within the vicinity then message received by the destination node else an intermediate node receives the message.
5. Restart the process of forwarding the message from step no 1 till the destination node is reached.

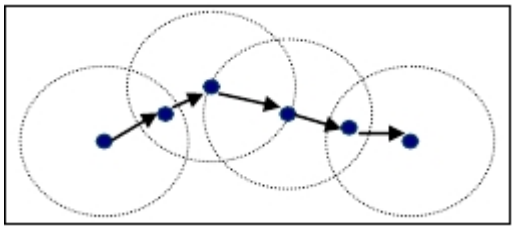

Figure1. Communication in Mobile Ad hoc Network

2. PREVENTION USING ASYMMETRIC CRYPTOGRAPHY

These asymmetric cryptography techniques give the underlined basic methodology of operation of protocols under this category. A secure wired network is needed to distribute public keys on digital certificates in the ad hoc networks. In mathematical terms, a network with n nodes would demands n public keys stored in the network. Two protocols SAODV and ARAN [1] [2] are defined in this category.

2.1 Secure Ad hoc on-demand Distance vector routing (SAODV)

It is an extension to AODV routing protocol which support public key cryptography. SAODV functionality work under in security the AODV protocol by authenticating the unchangeable fields of the routing messages using digital signatures. This protocol gives an end-to-end authentication and node-to-node verification of the messages. It is an easy process. There routing messages i.e. RREQs, RREPs and RERRs are digitally signed to agreement their integrity and authenticity. A node that develops a routing message signs it with its private key. While the nodes that accept this message check the signature using the sender's public key.

Because of this reason SAODV must be incremented at every hop count so that hop counts can not be signed by the sender. So, to prevent it; means this is not allow malicious intermediate nodes to decrement it, a mechanism is used that is based on hash chains. In SAODV basic form, this constitutes it impractical for intermediate nodes to reply to RREQs if they have a route regarding the destination for the reasons that the RREP message must needs be signed by the destination node. Therefore, to secure the cooperation mechanism of AODV, SAODV enclose a kind of Trust worthy feature that permits intermediate nodes to reply to RREQs messages. This mechanism named as *double signature*. In *double signature* when a node A produce a RREQ message, in terms to the regular signature, which is estimated on a fictitious RREP message regarding to A itself. Intermediate nodes can store this second signature and the other routing information related to node A in their routing table. If any one of these nodes then acquires a RREQ toward node A, it can respond on behalf of A with a RREP message, and similar is happen with regular AODV. To do this operation, the intermediate node produces the RREP messages, encloses the signature of node A that is formerly cached, and then signs the message with its personal private key. With respect to AODV, SAODV does not need additional messages. However, SAODV messages are significantly bulky because of the reason of digital signatures. SAODV needs heavy weight asymmetric cryptographic operations: every time a node produces a routing message, it must need to generate a signature, and every time it acquires a routing message, it must needs to verify a signature. This achieves deficient when the double signature is applied ,for this reason it mmay need the production or conformation of two signatures for a single message. SAODV permits to authenticate the AODV routing data in the SAODV operations. Basically two operations: *hash chains* and *signatures* are used to achieve this
[5].

2.1.1 SAODV Signature operations

When computing signatures, because of the reason that it is a changeable field the hop count field is always zero. In the case of signature for Route reply packet field of the RREQ Double signature extension, so the question is that what is signed in the forthcoming RREP message that nodes might forward back in reply to the RREQ. To develop this message it utilizes the values of the RREQ and the Prefix size. R and A flags are also in the case of RREPs. 'A' flag is changeable and if an attacker changes it, it can only tend to some sort of DOS. Every time a node creates a RREQ it determines if it should be signed with a Single Signature Extension or either with a Double Signature Extension. All implementations need to supports RREQ Single signature Extension and must support RREQ Double Signature Extension. A node that creates a RREQ with the unnecessary RREP flag set need to sign the RREQ with a Double Signature Extension. A node requires that it never creates a RREQ without adding a Signature Extension. When a node accepts a RREQ, first check the signature before generating or modifying a reverse route to that host. Only if the signature is checked, it will store the route. If the RREQ was accepted with a Double Signature Extension, therefore the node will also store the signature. It also stores the lifetime and the Destination IP address for the RREP in the route entry. If a node accepts a RREQ without a Signature Extension it must drop it. An intermediate node will respond to a RREQ with a RREP only if completes the AODV needs to do so, and the node has the represent signature and the old lifetime and old originator IP address to place into the 'Signature', 'Old Lifetime' and 'Old Originator IP address' fields of the RREP Double Signature Extension. Otherwise, it will broadcast again the RREQ. When a RREQ is acquired by the destination itself, it will respond with a RREP only if completes the AODV requirements to do so. This RREP will be forward with a RREP Single Signature Extension. All implementations need to support RREP Single Signature Extension, and must support RREP Double Signature Extension. A node needs that never create a RREP without adding a Signature Extension. This also uses to unnecessary RREPs. When a node accepts a RREP, first checks the signature before developing or modifying a route to that host. Only if the signature is checked, it will keep the route with the signature and the lifetime and the originator IP address of the RREP. If a node accepts a RREP without a Signature Extension it must drop it. Each node, creating or sending a RERR message, utilizes digital signatures to sign the whole message and any neighbor that accepts verifies the signature. In this way it can check that the sender of the RERR message is really the one that claims to be. And however destination sequence numbers are not signed by the corresponding node, a node must be never modifying any destination sequence number of its routing table supported a RRER message. However nodes will not believe destination sequence numbers in a RERR message, they will utilize them to decide whether they should invalidate a route or not [3] [6].

2.1.2 SAODV Hash Chains Operation

Hash chains are utilized in SAODV to authenticate the hop count of the AODV protocol routing messages but by any node that accepts one of those messages. Each time a node wants to forward a RREQ or a RREP it creates a random number. Choose a Maximum Hop Count. Maximum Hop Count must be set to the TTL value in the IP header, and need that never above its configuration parameter Net Diameter. The Hash field in the Signature Extension is arranging to the random number. The Top Hash field is arrange to the Random number hashed Max Hop Count times. Each time a node receives a RREQ or a RREP it confirms the hop count by hashing Max Hop Count times the Hash field, and analyzing that the resultant value is the identical than the Top Hash. If the check is not works, the node must be drop the packet. Before broadcasting again a RREQ or sending a RREP, a node hashes one time the Hash field in the Signature Extension. The function utilized to calculate the hash is arranged in the Hash Function field. While this field is signed, a sending node will only be able to utilize the same hash function that the creator of the routing message has chooses. If anode cannot conform or send a routing message because of the reason that it does not back up the hash function that has been used, then it drops the packet.

2.1.3 Features of SAODV

- This protocol can be utilized to prevent the route discovery mechanism of the AODV by giving security features such as integrity, authentication and non-repudiation.
- In this protocol, the ownership of certified public keys changes intermediate nodes to authenticate all in-transit packets.
- SAODV works only by using the new extension message with the AODV protocol.

Issue

There is only one mutable field in this protocol is the hop-count value. To prevent from wormhole attacks this protocol determines a hash of the hop count field [1] [2].

2.2 Authenticated Routing for ad hoc networks (ARAN)

It is an on-demand routing protocol that makes use of cryptographic certificates to provide routing security. This is a preliminary certification process that uses a route instantiation process that guarantees end-to-end authentication. It detects and protects against malicious actions by third parties and also peers in ad-hoc

infrastructure. This protocol introduces message integrity, authentication and non-repudiation to an ad-hoc environment. Basically ARAN[4] includes two distinct stages. In the first stage of ARAN protocol, it needs extra work from peers beyond traditional ad hoc protocols however this stage is very simple. On the other hand, nodes that have choice of second stage specify secure shortest route.

Before moving in to ad hoc network, ARAN protocol wants the use of a trusted certificate server T, where each node has to quest a certificate signed by T. The certificate includes the IP address of the node, a timestamp, its public key of when the certificate was developed and a time at which the certificates run out along with the signature by T. Here all nodes are expected to hold unused certificates with the trusted server and must remember T's public key.

The motive of the first stage of ARAN protocol is for the source to check the specified destination was reached. As with other secure system that is based on cryptographic certificates, the key issue that has to be turn to be the revocation, in order to make confirm that expired i.e. runs out or revoked certificates do not permit the holder to access the network. In ARAN protocol when certificate requires being revoked i.e. recall then the trusted certificate server T forwards a broadcast message to the ad hoc group that announces the revocation. Any node that is acquiring this message rebroadcasts to its neighbors. Revocation notices require to be gathered until the revoked certificate would have run out normally. Any particular neighbor of the node with the revoked certificate requires redeveloping routing as compulsory to ignore transmission through the now untrustworthy node. Therefore, this case is not failsafe. But in some cases, the untrustworthy node its own certificate revoked may be the sole connection between portions of the ad hoc network. In this particular case, the untrustworthy node might not send the notice of revocation for its certificate, which resulting in a separation of the network, as nodes that have acquired the revocation notice will no longer send messages through the untrustworthy node, however all other nodes based on it to reach the rest of the network. This only lasts as long as the untrustworthy node's certificate would rather been valid, or until the untrustworthy node is no longer the sole connection the two partitions. At the time that the revoked certificate should have run out, the untrustworthy node is not able to renew the certificate and also the routing across that node ceases. As well as, to find out this situation, to look sharp the propagation of revocation notices, when a node

sees a fresh neighbor, it can exchange a result summary of its revocation notices with the neighbor. If the result summary is not match then the real signed notices can be send and broadcast again to start up again propagation of the notice [4] [6] [7].

2.2.1 Features of ARAN

- This protocol prevents against exploits using fabrication, modification and impersonation.
- Because of the reason that ARAN protocol uses asymmetric cryptography, this makes it a very expensive protocol to use in terms of energy usage and CPU.

Issue:

- Major issue of ARAN protocol is the requirement of a certificate server i.e. the integrity of that server is necessary. This is by although only a design issue and as it is intended for securing communication over a managed-open-environment, it shouldn't be considered a big issue.
- These two protocols, SAODV & ARN do not address wormhole attacks. ARAN provides both node-to-node and end-to-end authentication while SAODV provide only end to-end authentication [1] [4] [7].

CONCLUSION AND FUTURE WORK:

In this paper we have discussed about secure routing based on prevention technique where it has been explained about various algorithms such as SAODV, ARN also methods, features and issues of them. Prevention technique are used to prevent malicious transmission, on the other side detection approaches specifies solutions that try to identify clues of any unauthorized activity in the network and take appropriate action against such node. Future work involves the implementation of proposed methods in existing WLANs and the development of adaptive mobile applications so that *ad-hoc* mobile computing can be better supported. Further research will be on symmetric preventive methods for secure routing and detection techniques to make the working easier, cost effective and efficient.

REFERENCE

[1] Perkins C.E. and Royer E.M. , "Ad-hoc On-Demand Distance Vector Routing," Second IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, February1999

[2] TIRTHANKAR GHOSH, NIKI PISSINOU and KAMI (SAM) MAKKI, "Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks", October 2005

[3] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, Joo-Han Song, "Experimental Comparisons between SAODV and AODV Routing Protocols" WMuNeP'05, October 13,2005, Montreal, Quebec, Canada. Copyright 2005 ACM 1-59593-183-X/05/0010

[4] C. Perkins, "Ad-hoc on-demand distance vector routing," Internet draft RFC, 1997.

[5] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In CRYPTO, pages 513–525, 1997.

[6] Mehdi Kargar and Mohammad Ghodsi, "Truthful and Secure Routing in Ad Hoc Networks with Malicious and Selfish Nodes" 2009

[7] K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in proceedings of IEEE ICNP, 2002.