An Efficient Secured Routing Protocols for MANETs

Shwetha T.R
Department of CSE
EWIT
Bangalore,India
Shwetha.shwe24@gmail.com

Dr.ArunBiradar
HOD Department of CSE
EWIT
Bangalore,India
hodcsea@gmail.com

Abstract - Mobile Ad-hoc Network (MANET) consists of a collection of wireless mobile hosts without the required intervention of any existing infrastructure or centralized access point such as base station. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Wireless MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. So security in MA NET is a complex issue. There are many routing protocols that establish the routes between the nodes in the network. The control towards the management of the nodes in the MANET is distributed. This feature does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security.

In this paper, therefore, we attempt to focus on analyzing and improving the security of one of the popular routing protocol for MANET viz. the Adhoc On Demand Distance Vector (AODV) routing protocol. Our focus specifically, is on ensuring the security against the BlackholeAttack. The proposed solution is that capable of detecting and removing black hole nodes in the MANET at the initial stage itself without any delay.

Keywords-Mobile Ad-hoc Network, Ad-hoc On demand Distance Vector (AODV), BlackHole attack, Security

1. Introduction

An ad-hoc network is a collection of wireless mobile hosts forming a impermanent network without the assistance of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-configuring and self-organizing multi-hop wireless networks. Each node in mobile ad hoc networks is set up with a wireless transmitter and receiver, which permits it to communicate with other nodes in its communication range only. Nodes communicating usually share the similar physical media; they transmit and get signals at the same frequency band, and follow the same hopping sequence or spreading code. If the destination node is not inside thetransmission range of the source node, thesource node takes help of the intermediate nodes in order to communicate with the destination node by

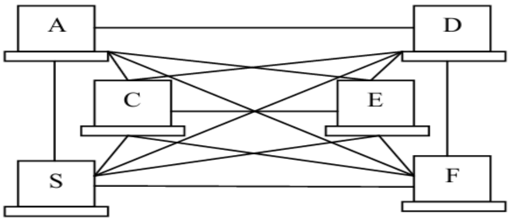


Figure-1 A mobile Ad-hoc Network

The nodesare free to move inany direction and organize themselves arbitrarily. They can join or leave the network at any time. Due to the frequently change in the network topology there is a significant change in the status of trust among different nodes which adds the complexity to routing among the various mobile nodes. The self-organization of nodes in ad hoc networks may tend to deny providing services for the advantage of other nodes in order to keep their own resources acquaint new security that are not addressed in the infrastructure-based networks.

2. Related Work

2.1 Security Aware Ad hoc Routing (SAR)

SAR protocol integrates the trust level of a node and the security attributes of a route to provide the integrated security metric for the requested route. A Quality of Protection (QoP) vector used is a combination of security level and available cryptographic techniques. It uses the timestamps and sequence numbers to stop the replay attacks. Interception and subversion threats can be prevented by trust level key authentication. Attacks like modification and fabrication can be stopped by verifying the digital signatures of the transmitted packet. The main drawbacks of using SAR are that it required excessive encrypting and decrypting at each hop during the path discovery. The discovered route may not be the shortest route in the terms of hop-count, but it is secure [2] and [7].

2.2Trusted Ad-hoc On-demand distance vector Routing (TAODV)

TAODV is secure routing protocol which uses cryptography technologies recommended to take effect before nodes in the establish trust relationships among one another. The main salient feature of TAODV is that using trust relationships among nodes, there is no need for a node to request and verify certificates all the time.

TAODV (Trusted AODV) has several salient features:

(1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them;

(2) A node that performsmalicious behaviors willeventually be detected and denied to the whole network.

(3) The performance of the System is improved by avoiding requesting and verifying certificates at every routing step.

That protocol greatly reduces the computationoverheads. Assume that the keys and certificates needed by these cryptographic technologies have been obtained through some key management procedures before the node performs routing behaviors. Some extranew fieldsare added into a node's routing table to store its opinion about othernodes' trustworthiness and torecord thepositive and negative evidences when it performs routing with others. The main advantages of embedding trust model into the routing layer of MANET, save the consuming time without the trouble of maintaining expire time, valid state, etc. This is important in the situation of high node mobility and invalidity. Trusted AODV are mainly three modules in the whole TAODV system: basic AODV routing protocol, trust model, and trusted AODV routing protocol. Based on trust model, the TAODVrouting protocol contains such procedures as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating [1] and [6] and [9].

2.3 ARAN (Authenticated Routing for Ad-hoc Networks)

ARAN provides authentication, message integrity and non-repudiation in ad-hoc networks by using a preliminary certification process which is followed by a route instantiation process that ensures end-to-end security services. But it needs the use of trustedcertification server. The main disadvantage with the protocol is every node that forwards a route discovery or a route reply message must also sign it, which is very power consuming and causes the size of the routing messages to increase at each hop.

It is clear from the above mentioned security analysis of the ARAN protocol that ARAN is a secure MANET routing protocol providing authentication, message integrity, confidentiality and non-repudiation by using certificates infrastructure. As a consequence, ARAN is capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. However, erratic behavior can come from a malicious node, which will be defended against successfully by existing ARAN protocol, and can also come from an authenticated node. The currently existing ARAN secure routing protocol does not account for attacks that are conducted by authenticated selfish nodes as these nodes trust each other to cooperate in providing network functionalities. This results in that ARAN fails to detect and defend against an authenticated selfish node participating in the mobile adhoc network. Thus, if an authenticated selfish node does not forward or intentionally drop control or data packets, the current specification of ARAN routing protocol cannot detect or defend against such authenticated selfish nodes. This weakness in ARAN specification willresult in the disturbance of the ad hoc network and the waste of the network bandwidth [8] and [10].

3. Proposed work

3.1 Block Hole attack:

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

In this method we are detecting the BlackHole attack during route discovery phase, mainly during route reply phase. When the malicious node sends the route reply saying that it has fresh enough routes to destination and it advertise the source node by including high destination sequence number in RREP packet. When the malicious node sends the RREP packet, its previous node has to check the destination sequence number present in RREP packet and the threshold value. If the value present in the RREP packet is greater than the threshold value the previous node will note its ID and consider it as malicious node. Otherwise the previous node will forward the RREP packet to its previous node and the process will continue.

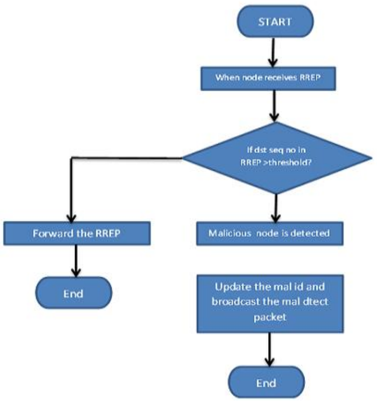

START
When node receives RREP
If dst seq no in RREP >threshold?
Forward the RREP
End
Malicious node is detected
Update the mal id and broadcast the mal dtect packet
End

Figure 5.Flow chart for detection of BlackHole attack

3.2 Secure AODV:

AODV protocol would be the center of ourproposed work. Route Requests messages (RREQs), Route Replies messages (RREPs) and Route Errors messages (RERRs) are the message types defined by AODV. The designed protocol includes the routing method and exchange of security constraints in a single step. In general the overall concept of process would be based on the utility of digital certificates issued by trusted CA (Certification Authority). It is supposed that a trust relationship exists between CA and all participating nodes.

Our proposed work encompasses following initiatives:

1) For the exchange of session key the concept of asymmetric cryptography (public key and private key cryptography) will be used.

2) Certificates will be used to attach asymmetrickeys (public and private keys) to the nodes.

3) Certificates ofsource and destination are attached with RREQ and RREP messages.

4) Our proposal scheme uses the concept of asymmetric cryptography for exchange of session key only as it is resource intensive and could be considered as unsuitable choice for MANETs..

5) We propose use of a symmetric cryptographic techniques such as Triple Data Encryption Standard(3DES) for data encryption

providing more reliable and secure data transmission.

6) Certificates can be issued to all participating nodes in relation to unique identity of respective users . Following symbols will be used in the proposed scheme, source (S), destination (D), session key (Ks), encrypted session key (Ke). Kaxpublic keyof x, Kbx private key of x, where X is either source or destination. Ekencryption using key K, Dkdecryption using key K.

3.3Working

Source generates RREQ message, attaches its certificate, along with a request for the sessionkey and sends it for route discovery of destination. The intermediate nodes rebroadcast the RREQ message according the operation of AODV protocol. On receipt of RREQ message, thedestination node verifies the certificate of source and on authorization generates a session key. The destination encrypts the session key first through its private key and then encrypts Ke1 with the publickey of the source as

Ke1= Ekbd (Ks))

Ke = Ekas (Ke1).

4. Conclusion

MANETs require a reliable, efficient, scalable and most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. AODV is prone to attacks like modification of sequence numbers, modification of hop counts, source route tunneling, spoofing and fabrication of error messages. AODV does not specify anyspecialsecurity measures. The proposed scheme uses the concept of mutual authentication in which both sender and receiver authenticate each other with respective

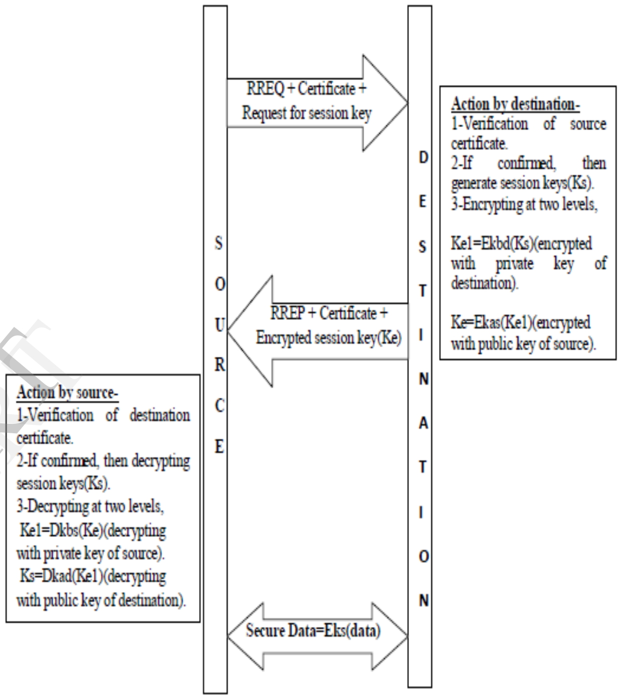
Destination act in response with RREP message attach its certificate and encrypted session key Ke. On receiving, the source confirms the authenticity of destination from its certificate, decrypts the session key first through its private key and then through public key of destination as

Ke1= Dkbs (Ke)

Ks= Dkad (Ke1) respectively.

Finally session key is achieved that will subsequently be used for secure data exchange.

3.4 Flow Diagram


RREQ + Certificate + Request for session key
Action by destination-
1-Verification of source certificate.
2-If confirmed, then generate session keys(Ks).
3-Encrypting at two levels,
Ke1=Ekbd(Ks)(encrypted with private key of destination).
Ke=Ekas(Ke1)(encrypted with public key of source).
DESTINATION
SOURCE
RREP + Certificate + Encrypted session key(Ke)
Action by source-
1-Verification of destination certificate.
2-If confirmed, then decrypting session keys(Ks).
3-Decrypting at two levels,
Ke1=Dkbs(Ke)(decrypting with private key of source).
Ks=Dkad(Ke1)(decrypting with public key of destination).
Secure Data=Eks(data)

certificates and the recipient also encrypts the generated session key with its private key (ensuring its authentication for the sender) and further encrypts the session key with the public key of the sender thus confirming the authentication of the sender. Data confidentiality and integrity can be accomplished by data encryption using powerful symmetric key algorithm such as 3DES.Thus the proposed scheme results in successful delivery of messages, despite of the presence of challenges almost importantly, the low end-to-end delay clues on the ability of the protocol to support QoSfor real-time traffic in MANET

REFERENCES

[1] IEEE Computer Society, “IEEE 802.11 Standard, IEEE Standard for Information Technology”,1999.http://standards.ieee.org/catalog/olis/lanman.html.

[2] S Corson and J. Macker.Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. Internet Request for comment RFC 2501, Jan 1999.

[3] P. Papadimitratos ,Z.J. Haas, “Secure Routing for Mobile Ad Hoc Networks”in Proceedings of the SCS Communication Networks and Distributed SystemModeling and Simulation Conference(CNDS 2002),San Antonio,TX,Jan 27-31,2002.

[4] P. Papadimitratos ,Z.J. Haas, and P. Samar “The Secure Routing Protocol(SRP) for Ad Hoc Networks” Internet Draft,draft-papadimitratos-secure-routing-protocol-00.txt,Dec.2002.

[5] C. E. Perkins, S. R. Das, and E. Royer, “Ad-hoc Demand Distance Vector (AODV)”, http:/www.ietf.org/internet-draft/draft-ietf-manet- aodv-05.txt, Mobile Ad Hoc Networking Group,IETF.

[6] Gustav J. Simmons. Symmetric andAssymetricencryption. ACM Computing surveys (CSUR). Volume 11, Issue 4 pp 305-330, Dec 1979.

[7] BruceSchneir: Applied Cryptography. John Wiley and sons inc, 1996.

[8] Wenjing, W., X. Fei, et al. 2007, TOPO: Routing in Large Scale Vehicular Networks, IEEE 66th Vehicular Technology Conference, and VTC-2007.

[9] Wenjing, W., X. Fei, et al. 2007, An Integrated Study on Mobility Models and Scalable Routing Protocols in VANETs. 2007 Mobile Networking for Vehicular Environments.