ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

A SECURITY SURVEY OF AUTHENTICATED ROUTING PROTOCOL (ARAN)

Ravi Raval[1], Ketan Sarvakar[2]

P.G. Student, Department of Computer Engineering, U.V Patel College of Engineering, Ganpat University, Kherva, Mehsana, Gujarat, India[1]

Assistant Professor, Department of Information Technology,U.V Patel College of Engineering, Ganpat University, Kherva,Mehsana,Gujarat, India[2]

Abstract: Communication happens in ad hoc networks through multiple hops if the destination node is not in the direct wireless transmission range of sender. Many proposed routing protocol for ad hoc networks. On demand routing protocolsare quite less expensive in terms of network overhead and fortunatelyquicker reaction time than other type of routing schemes which are based on periodic protocol. However varieties of attacks have been identified which targets routing protocols. The attacker attacks the routing protocol to soak up network traffic packets. Later on an attacker maypush intothe path in between source and destination, and hence control network traffic. There are so many routing protocols developed which can deal with this type of attack. This paper analyzes specially the security features of a commonly used routing protocol, i.e. ARAN

Keywords*:* AODV, ARAN, RREQ, RREP, Network Security

I. INTRODUCTION

MANETs are the mobile ad hoc networkswhich do not have anyinfrastructure.Sogenerally they have no routers like wired networks and all nodes have their own movement and can be connected dynamically but arbitrary manner. There are various routing protocols have been proposed and available in use in MANET. Numerous of them are not secure. Ad-hoc On Demand Distance Vector (AODV) is one of the commonly used protocol in an Ad-hoc network environment. [1] The AODV has the capability to deal with the network in which frequent changes occurs dynamically and it also performs well. However it has only some security features.The MANETs are now used insensitive business applications, transfers of military information and online banking. So security becomes extremely important in such an environment. Therefore from this aspect any security must possess following criteria.

A. **Isolation:**A protocol should be able to recognize misbehavior of nodes in the network and should be able to avoid them from interfering in communication.
B. **Certain discovery:**For a given network if a path exists between any two points then it must be able to discover it. Moreover, whenever any node request for a path, it should possess a capability of finding a path to the intended node only.
C. **Lightweight computations:** Generally nodes in this type of network carries battery which has limited power storage in nature, also limited computational capability. So it would be unfair to think of a node performing an extensive computation. If functions ofasymmetric key cryptography or shortest path algorithms for very large networks is the requirement, then they should be restricted to the less number of nodes as possible; preferably only the path endpoints at its creation time.
D. **Location privacy:** The information carried in message headers is equallyimportantjust as the message contents. The routing protocol must protect location information about the nodes in a network and the network topology too.

E. Byzantine robustness: It should be able tofunction properly even if some participating nodes inrouting are intentionally obstructing its operation. Byzantinerobustness can be thought as self-stabilizationproperty's severe version. The routing protocol must not onlyautomatically recuperate from an attack; it should not cease itselffrom functioning even during the attack.

F. Self-stabilization. This propertysays that a routing protocol should possess a feature to automatically recuperateitself from any possible problematic event in a fix amount of time without human mediation. It means, there must not be any possible way to permanently disable the network by admitting a small number of badly formed packets. Self-stabilizing protocol helps to locate an attacker easily when an attacker who may wishes to inflict continuous damage must remain in the network and continue sending malicious data to the nodes

The term Security implies identification of threats, attacks andvulnerability in a given network system. Various attackstargeting on routing in a network layer have been identified.The attacks can be classified into two different categories: One is passive and other is active type of attacks. In passive attacks, the attackeraims to obtain the information in transits. It means theattacker neither modifiesnor harms the system. However in active attacks the attacker may modify or harm the system. So as far asauthentication and integrity features are concerns active attacks can be considered as dangerous. Here certain common types of active attacks are listed here:

a) Packet dropping attacks
   - I.) Black hole attack: An attacker drops all the thieved packets including data and control packets too. Asany intermediate node responds to the RREQmessage if it has a fresh enough path, themalicious node easily disrupts the proper functioning of the path protocol and make atleast part of the network crash.
   - II.) Gray holes: In this attack, an attacker is dropping selected packetsi.e. dropping data packets but not control packets for example.

b) Modification of Protocol message attack: The malicious nodes may participatedirectly in the path discovery process and it might be possible that they may intercept andfilter routing protocol packets to interrupt communication. If malicious nodes alter this field then alteration can causeredirection of network traffic and DOS [2].
   - I.) Redirection with modified Hop count: Here, The malicious node may get success in diverting all thetraffic to a specificintended point (i.e. some destination) through itself by showing a shortest path (by help of very low hop count)to that destination. Now if the malicious node hasbeen able to insert itself between the twocommunicating nodes even for once, it will be able to do anythingwith the packets which are passing in between them. So now itis easy for an attacker to select and drop packets to perform a denial ofservice attack, or instead it usesa particular place on thepathjust like in the first step of a man-in-the-middleattack.
   - II.) Denial of service (DoS): The malicious node may generate frequent uselesspath requests so the network resources will be unavailable to othernodes.

c) Impersonation Attacks: A malicious node may enact another node while sending the controlpackets for creating an anomaly update in the routing table [12, 13].

d) Fabrication Attacks: These type of attacks are classifiedinto further two types:
   - I.) Falsifying path error message: A maliciousnode can getsuccess in propelling a DoS attack against a gentle node by sending falsepath error messages against this node.
   - II.) Routing table overflow: The attackertries to create paths to fake nodes (nonexistent nodes).The attacker aims to have necessarypaths so that creationof new paths is hindered or the routing protocol implementation is overwhelmed. AODV isless vulnerable to this attack.Because AODV is reactive ratherthan proactive.

e) The wormhole attacks: In the wormhole attacks [3], theattacker decides to receive packets at one specific point in the networkand after receiving now tunnels them to another part of the network.Afterwards the attacker willreplay them in the network from that tunneled point onwards.The attacker need not to haveany knowledge of the cryptographic keys in this type of attack.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

II.SECURE AD HOC ROUTING PROTOCOL

The protocol AODV is not satisfying the requirements of discovery, isolation or Byzantine robustness. Therefore secure routing protocol for ad hoc networks was developed, in order to provide protection against such attacks. These proposed solutions are either a brand new independent protocol, or in some cases they contain just modifications in security mechanisms into some existing protocols (DSR and AODV for example). All the proposals concentrated on a commondesign principle and that is thetradeoff in between performance providing by the protocol and the security. Proper care must be taken since routing is anecessary function in any ad hoc network, so the integrated security functions should not slow down its operation. Another important consideration in analysis is the inspection of the assumptions was kept and the requirements for which each solution depends. Though a protocol may pass certain security constraints, however its operational requirements might prevents its successful employment. There arefive common categories of the secure routing protocol: the solutions based on public key cryptography; solutions based on private key cryptography; reputation-based solutions;category of mechanisms which provides security for ad hoc routing and hybrid solutions. In this paper we have chosen one of the most common plus efficient ARAN to analyze its security aspects from asymmetric cryptographic solution. This paper introduces a short description of ARAN first, then it will briefly describe the analysis of protocol by help of all discussed attacks consideration.

PUBLIC KEY CRYPTOGRAPHIC SOLUTIONS

The Protocols that use public key cryptography as a base for routing security in mobile ad hoc networks require the existence of an entity calleduniversally trusted third party (TTP).

AUTHENTICATED ROUTING PROTOCOL (ARAN)

The authenticated routing protocol (ARAN) detects and defends against malicious activities by third party and peers in an ad hoc network. There are two different stages of ARAN consists of a preparatory certification process and then it performs a path instantiation process which assures and guarantees end-to-end authentication. ARAN is accomplishing use of cryptographic certificate to function. The code for the protocol ARAN is publically available [17].

a) Path Initiation Step

Stage I: The first of ARAN is each node have to go to the trusted certification authority andask for a certificate by giving its address and public key before attempting to connect to the ad hoc network. This step can be shown as follows:

$T \rightarrow A$: $Cert_A = [IP_A, K_{A+}, t, e]K_{T-}$

Where, IP_A is the IP address of node A contained in the certificate. K_{A+} is the public key of node A, k is the timestampof certificate creation, and e is the certificate expiration time. Thesevariables are concatenated and signed by K_{T-}. The protocolhas the assumption that each node knows a priori the public key of thecertification authority.

Stage 2: This stage is operational stage of the protocol which ensures that the intended destination was indeed reached. Each node must have to maintain a routing table which contains entries of correspondingpairs of source-destination which are currently active. If a node want to initiate route discovery it will begin the route discovery process by broadcasting a route discovery packet (RDP) to its neighbors.

$A \rightarrow$brodcast: $[RDP, IP_X, N_A]\ K_{A-}$, $Cert_A$

The RDP contains a packet type identifier (“RDP”), the IP address of the destination node X (IP_X), A 's certificate ($Cert_A$) and a nonce N_A , all of them signed with A's secret key. Here one thing to note is the RDP is only signed by the source and not encrypted, so its contents can be viewed publicly. The purpose for adding the nonce N_A is to uniquely identify each RDP coming from a source. So it does mean thatnode A will monotonically increases the nonce when node A will perform route discovery.

Afterwards each node would be able to validate the signature with the certificate, updates its routing table with the neighbor from which it got the RDP, signs it, removes the signature and certificate of the previous node (but not the initiator's signature and certificate) and then finally forwards that packet to its neighbors.
Now, let'shave a B be a neighbor that has received the RDP broadcast from A, which will be rebroadcasted subsequently.
B→brodcast: [[RDP, IP_X, N_A] K_{A-}] K_{B-}, $Cert_A$, $Cert_B$
Upon receiving the RDP, B's neighbor C will validate thesignatures for both the node B and the RDP initiator, the neighbor who received the RDP from, using the certificates in the RDP. Now node C then removes B's certificate and signature as well, and then it records as its predecessor node, then it will signs the message content which was originally broadcasted by A and appends $Cert_C$its own certificate then rebroadcasts the RDP.
C→brodcast: [[RDP, IP_X, N_A] K_{A-}] $K_{C-\_}$, $Cert_A$, $Cert_C$
Finally, the message is received by the destination node X,so the process of sending a reply back is same but in reverse order. The Node X replies to the first RDP that it receives for a source anda given nonce. The RDP need not have traveled along thepath havingleastnumbers of hops.Unfortunately it might be possible that the least-hop path mayhave a greater delay, because of it was legitimately or maliciouslymanifested either. However in the case whensometimes a non-congested, non-least-hop path is likely to be selected to a congested least-hoppath because the delay will be reduced. One significant advantage here is that hop count or specific recorded source route are not containing in RDP,because each hop sign the message upon receiving, so maliciousnodes have no choicesleft to redirect traffic.
When the RDP will be received, the destination unicasts a REply Packet (REP) will be send back to the source along same path but in reverse. Letthe first node that receives the REP sent by X is node D.
X→D: [REP, IP_A, N_A] K_{X-}, $Cert_x$
The Reply packet contains four things. The address of the source node, thedestination's certificate, the associatedtimestamp and a nonce. Now the destination node will sign the REP first and then transmit it. The REP is forwarded back to the initiatingnode by following the same process similar to the one which we discussed for thepath discovery. It is required to mention here that the REP is unicasted along thereverse path.
Let node C be the next hope to the source for node D.
D→C: [[REP, IP_A, N_A] K_{X-}] K_{D-}, $Cert_X$, $Cert_D$
The D's signature will be validated by C on the received message,removes the certificate and signature, and signs the contents of the message. After that, it will appendits own certificate and unicast the REP to B.
C→B: [[REP, IP A, N_A] K_{X-}] K_{C-}, $Cert_X$, $Cert_C$
Now each node will check the signature and nonce of its previoushop during the REP is returned from the destination to source. When the sourcewill receive the REP, first it will do verification of the destination's signature andthe nonce sent back by the destination.

b) Route maintenance

The path will be de-activated in path table when there isn't any traffic has occurred on the existing path for thatpath's lifetime. If data will be received for such non-active path then Error packet (ERR) will be generated. These ERRmessages can be used by nodes to report broken links in active pathsbecause ofmobility of nodes. It is must to sign all ERR messages. Let say for apath in between a source node A and the destination node X, ERR messages will be generated by a node Bfor its neighbor C as follows:
B→C: [ERR, IP_A, IP_X, N_b] K_{B-}, $Cert_b$
The message is sent along the path towards to the sourcewithout any modification. A nonce will ensurethe freshness of ERR message. It would beseverelyhard to detect whenERR messages are fabricated for those links which are indeed activeand not broken. However, ARAN is providing non-repudiation by the use of signature on the message and henceprevents impersonation attacks. Anode should be avoided if it transmits a huge number of ERR messages,no matters the ERR messages are valid or fabricated.

IJIRSET

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

Key Revocation

When a need to revoke a certificate is arises, thetrusted certificate server, T will broadcast a message tothe ad hoc group member nodes which implies the revocation. Let say therevoked certificate $Cert_T$, the transmission appears as:

T→brodcast: [revoke, $Cert_T$] K_{T-}

The node who will receive this message will re-broadcasts it to itsneighbors. It is required to store revocation notices until therevoked certificate will expire normally. A node will have to reform routing with the revoked certificate as necessary to avoid transmission thorough the now untrusted node.

III.SECURITY ANALYSIS

a) The nodes can drop packets for without any reason, as there isn't any mechanism exist to prevent from this attack scenario. In fact a genuine node can drop.
b) ARAN specifies that all REP and RDP packetfields remain untouched between source and destination. The starting node signs both REP and RDP, so any alterations will be detected in transit, and fortunately the altered packet would be discarded subsequently. The offending node could be excluded from routing if it does alteration repeatedly to packets, but this possibility is not considered here anymore. So, modification attacks are prevented. This will prevent the attacks in which routing messages are altered while in transit or routing loops creation.
   I.) In general only destination address are contained in ARAN packets, plus packets do not contain hop-count field, which prevents it from the attack of redirection by modifying hop-count value.
   II.) The Denial-of-service attacks are possible by nodes with or without valid ARAN certificates. In the certificate less scenario, the unsigned route requests are dropped because thistype of attack is limited to the attacker's immediate neighbors. More severe attacks can happen at physical layer and MAC layer than ARAN is providing. Some effective attacks can be initiated by nodes with valid certificates, however, by sending many unnecessary route requests.A widespread congestion and power-loss to all nodes can be created by attacker in the network. The attacker can cause as these are forwarded and broadcasted across the network.
c) The certificate of the source node contained in path discovery packets which will be signed with the source's private key. In similar way, the destination node's certificate and signature contained in reply packets whichensures that only the destination can respond to path discovery. So fortunately it prevents impersonation attacks.
d) ARAN guarantees non-repudiation and hence preventsspoofing and unauthorized participation in routing. Because during routing all routing messages must have to include the sending node's signature and certificate, However fabrication of routingmessagescannot be prevented by ARAN, but it does offer a discouragement by ensuring nonrepudiation.A node will be excluded from future route computation phase if it continuously attempts to admit falsemessages into the network.[4]
e) Securing the shortest pathwould not be done by any means except by physicalmetrics like a timestamp in routing messages itself.According to this, ARAN does not provide any guarantee for a shortest path,but ARAN offers a *quickest* path. ARAN offers quickest path which is chosen by the RDPitself which reaches the destination first. The packet processing time could be saved by malicious nodes by not verifying theprevious hop's signature on the RDP packet, so it would results in increasing chances of being on the quickest route.However if it is executed by more than one malicious node on a path then and only such an attack is likely to happen, if a malicious node is present in one of the quickest path then also this type of attack is likely to be happen. Moreover the path length is measured from time of a path so it might be possible that malicious nodes can delay REPs as they propagate, even in the worstcase they can drop REPs packets, as well as delaying routingafter path instantiation too. At last, malicious nodes can elongate all the routes by conspiracy butone, forcing the source and destination to pick theunaltered route.[5]

IV.CONCLUSION

This paper has presented the authenticated routing protocolfor securing the routing protocols of mobile ad hoc and other wireless networks. Thestudy has shown thatdeficiency of network infrastructure and rapidly changing topology are the in inherent characteristics of any adhoc network, which causes difficulties to already complex problem under routing security [6]. Moreover, diverse application scenarios are enabled by suchflexible networks to be deployed. This in turn,each application has its own security demands and requirements which are to be placed on theunderlying routing protocol. Hence, the application scenario that is going to be protected, and how well the protocol can manage and handle scenarios different than the one for whom the design has been placed and so it would be the additional difficultyin a secure protocol designing. It would be preferable forapplications to took help of some alreadyexisting infrastructure as for obtaining certificates ARAN requires trusted third party.ARAN protocol is basically Ad hoc on demand distancevector routing protocol. So due to its reactive nature it has the benefits of high network performance andlow operational cost.In this paper, active attacks on AODV is presented.This paper discusses 5 possible active types of attacks.In general, by use of stringer authentication methods the active attacks can be avoided.We have firstly presentsthe complete working of ARAN. As nothing comes as a free of cost, always a price to be paid for gaining any advantage, ARAN cannot deal with black hole type of attacks,wormhole attack &Denial of service attack.

V.FUTURE SCOPE

In this paper we identified different possible attacks onAuthenticated Routing Protocol (ARAN). ARAN has solution forsome attacks but it is also has deficiency of security mechanisms to deal with some attacks likeblack hole attacks, denial of service (DoS) attacks etc. This would be an open research gap to make ARAN robust to defend against this type of attack.The trustestablishment [7, 8, 9, 11, 12], nodes thatmaliciously do not forward packets [14], key generation [10] and securityrequirements for forwarding nodes [13] are the explored areas in secure ad hoc network routing. These areas arebeyond the scope of this paper. Routing protocol intrusion detection has been studied in wired networks as a mechanism for detecting misbehaving routers. Cheung and Levitt [15] and Bradley et al [16] propose intrusion detection techniques for detecting and identifying routers that send bogus routing update messages.

REFERENCES

[1] Mobile Ad -hoc Networks (MANET). URL: http://www.ietf.org/html.charters/manet charter.html.

[2] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, A secure routing protocol for ad hoc networks, in: Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November 2002.

[3] Y.-C. Hu, A. Perrig, D.B. Johnson, Wormhole detection in wireless ad hoc networks, A Technical Report TR01-384, Rice University Department of Computer Science.

[4] K. Sanzgiri *et al.*, "A Secure Routing Protocol for Ad hoc Networks," *Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02)*, IEEE Press, 2002, pp. 78–87.

[5] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks," *Proc. 2nd ACM Symp. Mobile Ad Hoc Net and Comp. (Mobihoc'01)*, Long Beach, CA, Oct. 2001, pp. 299–302.

[6] E. M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks," *IEEE Per Commun.*, vol. 2, no. 6, Apr. 1999, pp. 46–55.

[7] Dirk Balfanz, D. K. Smetters, Paul Stewart, and H. Chi Wong.Talking To Strangers: Authentication in Ad-Hoc Wireless Networks. In *Symposium on Network and Distributed Systems Security (NDSS2002)*, February 2002.

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: ASecure On-Demand Routing Protocol for Ad Hoc Networks. In*Proceedings of the Eighth Annual International Conference onMobile Computing and Networking (MobiCom 2002)*, pages 12–23,September 2002.

[9] Jean-Pierre Hubaux, Levente Butty´an, and Srdjan Cˇ apkun. TheQuest for Security in Mobile Ad Hoc Networks. In *Proceedings of theThird ACM Symposium on Mobile Ad Hoc Networking andComputing (MobiHoc 2001)*, Long Beach, CA, USA, October 2001

IJIRSET

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

[10] Stefano Basagni, Kris Herrin, Emilia Rosti, and Danilo Bruschi.Secure Pebblenets. In *ACM International Symposium on Mobile AdHoc Networking andComputing (MobiHoc 2001)*, pages 156–163,Long Beach, California, USA, October 2001.

[11] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. MitigatingRouting Misbehaviour in Mobile Ad Hoc Networks. In *Proceedingsof the Sixth Annual International Conference on Mobile Computingand Networking (MobiCom 2000)*, pages 255–265, Boston MA, USA,August 2000.

[12] Frank Stajano and Ross Anderson. The Resurrecting Duckling:Security Issues for Ad-hoc Wireless Networks. In *Security Protocols,7th International Workshop*, edited by B. Christianson, B. Crispo, andM. Roe. Springer Verlag Berlin Heidelberg, 1999.

[13] Seung Yi, Prasad Naldurg, and Robin Kravets. Security-Aware Ad-Hoc Routing for Wireless Networks. Technical Report UIUCDCS-R-2001-2241, Department of Computer Science, University of Illinois atUrbana-Champaign, August 2001.

[14] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. Secure EfficientDistance Vector Routing in MobileWireless Ad Hoc Networks. In*Fourth IEEEWorkshop on Mobile Computing Systems andApplications (WMCSA '02)*, June 2002.

[15] Steven Cheung and Karl Levitt. Protecting Routing Infrastructuresfrom Denial of Service Using Cooperative Intrusion Detection. In *The1997 New SecurityParadigms Workshop*, September 1998.

[16] Kirk A. Bradley, Steven Cheung, Nick Puketza, BiswanathMukherjee, and Ronald A. Olsson. Detecting Disruptive Routers: ADistributed Network Monitoring Approach. In *Proceedings of theIEEE Symposium on Research in Security and Privacy*, pages 115–124, May 1998

[17] Authenticated Routing Protocol (ARAN) Implementation, http://moment.cs.ucsb.edu/~kimaya/aran-code.tgz

BIOGRAPHY

Ravi Raval have completed diploma in computer engineering from Technical Exam Board, Gandhinagar, India in 2008. He hasreceived his B.Tech degree from Ganpat University, Mehsana, India, in 2011. He has an experience of 13 months in academics ashe was a lecturer in Ganpat University from 2011 to 2012. Currently his M.Tech in computer engineering is pursuing in the same university. His research area includes security analysis of routing protocol.

Ketan Sarvakar received his B.E degree and M.Tech degree in computer science and engineering. He is currently working as an assistant professor in the department of Information Technology at U.V Patel College of Engineering, Kherva, Mehsana, India. His research area includes data mining and wireless networking.