International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.104.19

Encryption Based Authenticated Routing Protocol for Ad-Hoc Network

Mahendra Prasad Sharma[1], D.K Chauhan[2], Sanjay Pachauri[3]

[1]*Research Scholar –Computer Science & Engineering, Director-CRS, H.O.D-IT, Noida International University, Gr.Noida-India*

[2,3]*Research Scholar, Prof. –Computer Science & Engineering, Director-CRS, H.O.D-IT, Noida International University, IIMT College of Engineering, Gr.Noida3*

Abstract- The working range of Ad-hoc network will spread in coming future due to dynamic nature. However, there will be the risk of spreading wrong routing information, packet dropping and selective forwarding in the network which further leads to special kind of attacks [1]. Existing authenticated routing protocols for Ad-hoc network fails to detect and defend against such kind of attacks in the mobile ad hoc network. Thus, if malicious node hack the packets and make the modifications , intentionally drop control or data packets, the current specification of existing routing protocols cannot detect or defend against such authenticated selfish nodes.This weakness in ARAN specification will result in the disturbance of the ad hoc network and the waste of the network bandwidth. In this research paper, a solution is proposed to account for this type of attacks.

Key Words: AHN- Ad-hoc network, ARAN- Authenticated Routing Protocol for Ad-hoc Network, TTP- Trusted Third Party, RDP- Route Discovery Packet, REP- Route Reply Packets.

I. INTRODUCTION

Ad hoc networks (AHNs) are wireless multi-hop packet networks without any fixed infrastructure. An AHN network is formed solely by its terminals so that each terminal connected to the network provides also relaying service for others i.e. acts as a router [2]. Advantages of such system are rapid deployment, robustness, flexibility and inherent support for mobility. AHN can work as a stand-alone autonomous network providing internal connections for a group. Demand for such networks could arise in the contexts of shared desktop meeting, disaster recovery, or in various military applications [5].

The problems and their solutions considering packet routing are closely related to those widely studied in the case of ordinary fixed networks, but also completely new fundamental challenges have emerged due to the peculiar features of AHNs, such as [7,8]:

- Dynamic network topology and Structure
- Limited bandwidth
- Constrained power
- Broadcast nature of transmission

II. SECURITY ISSUES

Ad hoc networks are particularly prone to malicious behavior. Lack of any centralized network management or certification authority makes these dynamically changing wireless structures very vulnerable to infiltration, eavesdropping, interference etc. Security is often considered to be the major "roadblock" in ad hoc network technology [15].

Security requirements depend naturally on the application where they are needed. In cases where all the terminals are "on the same side", such as military or emergency rescue applications, it is enough to get protection against outside interference. In civilian, especially commercial, applications even mere lack of cooperation may be enough to bring the network on its knees. The nodes enter and leave the networks as they wish and links may be using nodes that should not have access to data. How to define membership in ad hoc networks, how to classify nodes to the trusted and the not-trusted ones [14]?

Traditional methods of protecting the data with cryptographic methods face a challenging task of key distribution and refresh [12].

Accordingly, the research efforts on security have mostly concentrated on secure data forwarding. However, many security risks are related to the peculiar features of ad hoc networks.

The most serious problem is probably the risk of a node being captured and compromised. This node would then have access to structural information on the network, relayed data, but it can also send false routing information which would paralyze the entire network very quickly.

III. TUNNELING

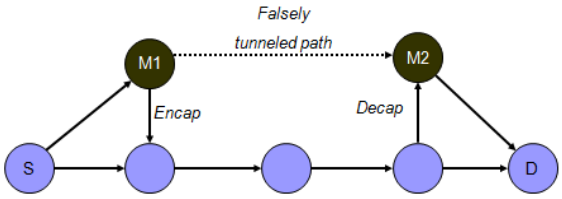

Fig: 1 Tunneling

When M1 receives a RDP from S, M1 encapsulates the RDP and tunnels it to M2 through an existing data route, in this case {M1->A->B->C->M2}.When M2 receives the encapsulated RDP, and it forwards the RDP on to D as if it had only traveled {S -> M1 -> M2 -> D}. Neither M1 nor M2 update the packet header to reflect that the RDP also traveled the path {A->B->C}. After route discovery, it appears to the destination that there are two routes from S of unequal length: {S->A->B->C->D} and {S- >M1->M2->D}. If M2 tunnels the RREP back to M1, S would falsely consider the path to D via M1 a better choice (in terms of path length) than the path to D via A. In our assumption, node A wants to get a route to node D.

IV. ASYMMETRIC CRYPTOGRAPHIC SOLUTIONS

Protocols that use asymmetric cryptography to secure routing in mobile ad hoc networks require the existence of a universally trusted third party (TTP).

V.ARAN

ARAN or authenticated routing protocol detects and protects against malicious actions by third party and peers in ad hoc network.

Two distinct stages of ARAN consist of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. ARAN makes the use of cryptographic certificate to accomplish its task.

(a) Route Initiation Step:

Stage 1

Each node, before attempting to connect to the ad hoc network, must contact the certification authority and request a certificate for its address and public key.

5.1 cert A= [IPA, KA+ ,t, e]KTThe→T

Certificate contains the IP address of A (IPA), the public key of A (KA+), a timestamp k of when the certificate was created, and a time e at which the certificate expires.. These variables are concatenated and signed by KT-. The protocol assumes that each node knows a priori the public key of the certification authority.

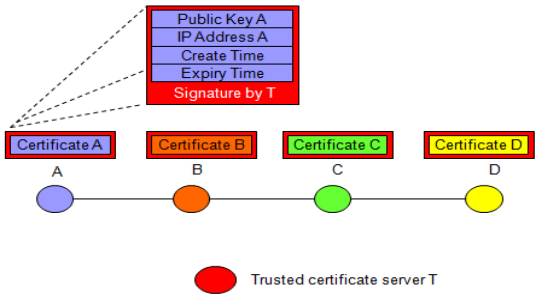

Fig 2: ARAN – Initial Setup

Initially each node has its own certificate produced by trusted certificate server T.Each node also has a copy of T's public key, so they can verify other certificates.

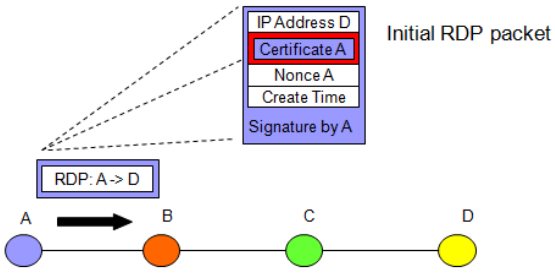

Fig 3: ARAN – Route Discovery

Node A generates a RDP request packet for node D. Node A includes its own certificate, and then signs the RDP packet with its private key. Node A then broadcasts this packet to its neighbors. Clearly each neighbor can verify the packet truly came from node A.

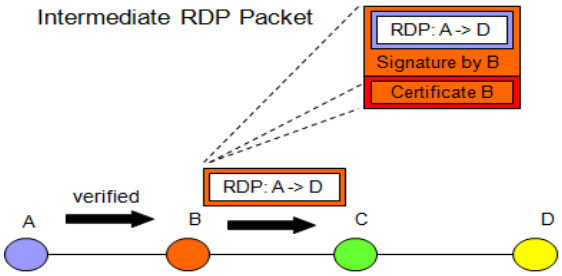

Fig 4: ARAN – Route Discovery

Upon receipt of the RDP packet, node B first verifies the packet. If passes the test, then node B takes the packet, signs it, appends its certificate, and forwards it on to each of its neighbors.

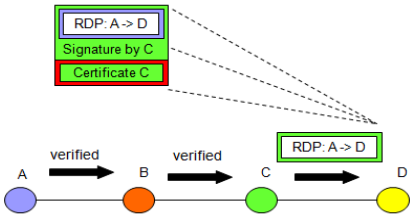

Fig 5: ARAN – Route Discovery

Again, at each step along the RDP request path, we validate the previous node's signature, remove the previous node's certificate and signature, record the previous nodes IP add (e.g. AODV reverse path), sign the original message contents, append our own certificate, and forward broadcast the message.

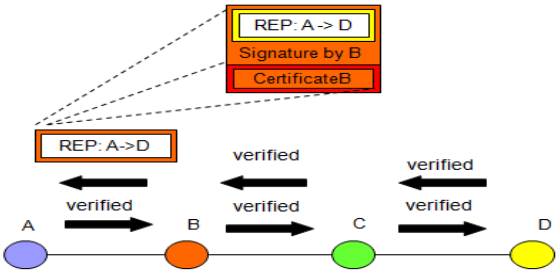

Fig 6: ARAN – Route Setup

Destination replies to first RDP packet received. Although this may not be shortest hop packet, it means RDPs don't get modified en-route, allowing both signature process and avoiding hop count = 0 attacks by malicious nodes. Reply packet is effectively similar to initial RDP packet.

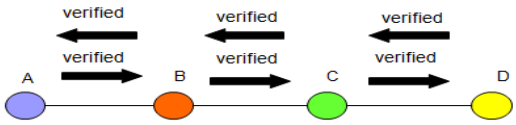

Fig 7: ARAN – Route Complete

Stage 2
The second operational stage of the protocol ensures that the intended destination was indeed reached. Each node must maintain a routing table with entries that correspond to the source-destination pairs that are currently active. The route discovery of the ARAN protocol begins with a node broadcasting a route discovery packet (RDP) to its neighbors.

5.2 brdcst: [RDP, IPX, NA] KA-, CertA→A
The RDP includes a packet type identifier ("RDP"), the IP address of the destination X (IPX), A 's certificate (cert A) and a nonce NA , all signed with A 's private key.
Note that the RDP is only signed by the source and not encrypted, so the contents can be viewed publicly. The purpose of the nonce is to uniquely identify an RDP coming from a source. Each time, A, performs route discovery it monotonically increases the nonce.

5.3 Route maintenance
When no traffic has occurred on an existing route for that route's lifetime, the route is simply de-activated in the route table. Data received on an inactive route causes nodes to generate an Error (ERR) message. Nodes also use ERR messages to report links in active routes that are broken due to node movement. All ERR messages must be signed. For a route between source A and destination X}, a node B generates the ERR message for its neighbor C as follows:

5.4: [ERR, IPA, IPX, Nb] KB- , certb→B

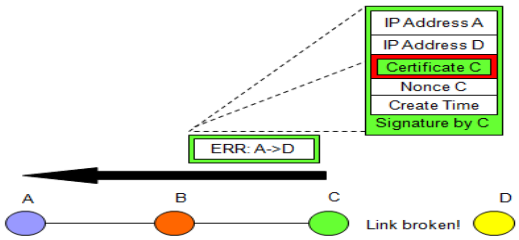

Fig 8: ARAN – Route Maintenance

Potential problem: fabrication of ERR messages – at least malicious node cannot create ERR messages for other nodes. "A node that transmits a large number of ERR messages, whether the ERR messages are valid or fabricated, should be avoided."

5.5 Key Revocation
In the event that a certificate needs to be revoked, the trusted certificate server, T, sends a broadcast message to the ad hoc group that announces the revocation. Calling the revoked certificate cert X, the transmission appears as:
brdcst : [revoke, certT] K TAny→T
node receiving this message re-broadcasts it to its neighbors. Revocation notices need to be stored until the revoked certificate would have expired normally. Any neighbor of the node with the revoked certificate needs to reform routing as necessary to avoid transmission through the now un trusted node.

VI. ANALYZING SECURITY OF –ARAN

ARAN specifies that the RDP is only signed by the source and not encrypted, so the contents can be viewed publicly. The purpose of the proposed scheme is all fields of RDP and REP packets remain unchanged between source and destination.

Since the initiating node signs both packet types, any alterations in transit would be detected, and the altered packet would be subsequently discarded.
Repeated instances of altering packets could cause other nodes to exclude the errant node from routing, though that possibility is not considered here. Thus, modification attacks are not prevented.
However, capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. Does not account for attacks that are conducted by authenticated selfish nodes as these nodes trust each other to cooperate in providing network functionalities.

VII. ENCRYPTION AND DECRYPTION OF PACKETS

Encryption Algorithm
Step 1: Activate and Initialize the Packet Pi
Step 2: Generate a Random Key KR by analyzing number of 0s (Zero) in Packet.
(a) Develop a routine to count bits in the Data Packet
(b) Set N := Count(Pi) // Count Number of 0's in the Data Packet.
(c) Set KR: =N // Store N in Random Number KR
Step 3: Apply XOR (Exclusive-OR) Operation
(a) Set EK: = Pi KR
(b) Perform: XOR Operation to generate Encrypted Packet EK .
(c) Set PEK: =EK // Utilize EK as Encrypted Packet
Step 4: Packet equipped for Transmission
Encryption Routine
Suppose we have a Data Packet with Bit
Stream – 11101010
The packet is represented as a 1 Byte or 8 Bits Data Packet.
Numbers of 0"s in Data packet is: 3, Binary Equivalent of 3 is: 0011
Bitwise XOR Operation for Encryption of Packet
Actual Packet: 11101010, Key: 00000011
Encrypted Packet: 11101001
Decryption Algorithm
Step 1: Receive the Encrypted Packet PEK
Step 2: Check the Front PFi and Rear End
PRi of Packet
if (PFi = PRi)
Accept PFi
Set KR := PFi
else
goto Step 5
Step 3: Generate the Binary Equivalent of KR
PBi = Binary (KR)
Step 4: Perform XOR Operation
if (PBi = PEK)
Decryption Successful
Accept the Packet
else
goto step 5
Step 5: Insert the Record of Corrupt Packet in Forensic Database
Key: 00000011, E- Packet: 11101001
Actual Packet: 11101010

VIII. ACKNOWLEDGMENT

This proposed method focuses on the two most important issues in mobile ad hoc networks, performance and security and performed effectively encryption and decryption with unique cryptographic technique without any complexity.
However, there are still many issues that deserve further investigation such as: Scalability, Address configuration, Quality of service (QoS), Power control.

IX. REFERENCES

[1] R. Hauser, A. Przygienda and G. Tsudik, "Reducing the cost of security in link state routing", In Symposium on Network and Distributed Systems Security (NDSS ″97), San Diego, California, Internet Society, pp 93–99, February 1997.

[2] A. Kush, "Security Aspects in AD hoc Routing" , Computer Society of India Communications, Vol. 3 No 2 Issue 11, pp 29-33, March 2018.

[3] A. Kush, "Security And Reputation Schemes In Ad-Hoc Networks Routing" International Journal of Information Technology and Knowledge Management, Volume 2, No. 1, pp 185-189, June 2009.

[4] T. Karygiannis and L. Owens, "Wireless Network Security", NIST Special Publication, pp 800-848, November 2002.

[5] Yonguang Zhang and Wenke Lee, "Intrusion detection in wireless ad-hoc networks", In 6th International Conference on Mobile Computing and Networking (MOBICOM″00), pp 275– 283, August 2000.

[6] A. Kush, C. Hwang and P. Gupta, "Secured Routing Scheme for Adhoc Networks" International Journal of Computer Theory and Engineering (IJCTE), Volume 3, pp 1793-1799, May 2009.

[7] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[8] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure message transmission in mobile ad hoc networks", Elsevier Journal of Adhoc network, Ad Hoc Networks 1, pp 193–209, 2003.

[9] Fei Hu and Neeraj K. Sharma, "Security considerations in ad hoc sensor networks" Elsevier Journal of Ad hoc Networks, Ad Hoc Networks 3, pp 69–89, 2005.

[10] B. Dahill, B. N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", Technical Report UM-CS-2001-037, University of Massachusetts, Department of Computer Science, August 2001.

[11] Y. C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Technical Report TR01-383, Rice University, December 2001.

[12] A. Perrig, R. Canetti, D. Song and D. Tygar, "Efficient and secure source authentication for multicast", In Network and Distributed System Security Symposium (NDSS″01), February 2001.

[13] D. B. Johnson et al., "The dynamic source routing protocol for mobile ad hoc networks (DSR)", Internet Draft, MANET working group, February 2002.

[14] R. Perlman, "Fault-tolerant broadcast of routing information", In Computer Networks, No. 7, pp 395–405.

[15] Animesh Kr Trivedi1, Rishi Kapoor1, Rajan Arora1, Sudip Sanyal1 and SugataSanyal , " RISM - Reputation Based Intrusion Detection System for Mobile Adhoc Networks" Available from link profile.iiita.ac.in/aktrivedi_b03/rism.pdf.

[16] Sameh R. Zakhary and Milena Radenkovic ,"Reputationbased security protocol for MANETs in highly mobile disconnection-prone environments" in International conference on Wireless On-demand Network Systems and Services (WONS), PP. 161 – 167, Feb. 2010.

[17] Ns2 - www.isi.edu/nsnam/ns/ns-tutorial/tutorial-02.