A Secured Routing Protocol for MANETs

A.Jayanand[#], Prof.Dr.T.Jebarajan[*]

[#]*Principal, Maria Polytechnic College, Attoor, India*
(Research Scholar, MSU)

[*]*Principal, Kings Engineering College, Sriperumpudur, India.*

***Abstract*— Security is one of the major concern in MANET routing. A large number of secured routing protocols exist however they are either insecure for some types of attacks or they consume much computational power which reduces their quality of service. In this paper we present a new secured routing protocol which is simple yet powerful. We name this new protocol as JJ model. The new protocol uses flooding technique just like AODV and SAODV, but much different from those protocols. Its ability to discover the route without identity of source and destination nodes makes it a unique design.**

***Keywords*—** MANET, MANET routing, MANET routing security, AODV, SAODV**.**

INTRODUCTION

A Mobile Ad hoc Network (MANET) is a dynamic wireless network that can be formed infrastructure-less connections in which each node can act as a router. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different mechanisms have been proposed using various cryptographic techniques to countermeasure the routing attacks against MANET.

Secured routing protocols are designed to secure MANETs from various attacks. But in order to achieve security, these protocols use complicated encryption techniques and additional information in the routing packets which reduces overall efficiency. Some secured routing protocols uses lengthier routing tables which require more space and more computational power. Almost all routing protocols (both secured and non-secured) transmit identity of source and destination nodes in the RREQ/RREP packets which makes them more vulnerable. The routing tables transmitted along with the packets also become a destination of attackers. Simply, the design of routing protocols itself makes them more vulnerable.

In this paper we present a new design which doesn't transmits identities of source node or destination node. It doesn't transmit routing table. It uses neither complicated encryption techniques nor lengthier routing table. We name this protocol as JJ model which is simple, yet powerful.

Before seeing how it works, let us analyse some existing routing protocols.

I. EXISTING ROUTING PROTOCOLS

A. AODV [2]

The Ad Hoc On demand Distance Vector Routing Protocol (AODV) is a source initiated, on demand driven, routing protocol. Since the routing is on demand, a route is only traced when a source node wants to establish communication with a specific destination. The route remains established as long as it is needed for further communication. Furthermore, another feature of AODV is its use of a destination sequence number for every route entry. This number is included in the RREQ (Route Request) of any node that desires to send data. These numbers are used to ensure the freshness of routing information. For instance, a requesting node always chooses the route with the greatest sequence number to communicate with its destination node. Once a fresh path is found, a RREP (Route Reply) is sent back to the requesting node. AODV also has the necessary mechanism to inform network nodes of any possible link break that might have occurred in the network.

B. SAODV[2]

The Secure Ad hoc On-Demand Distance Vector Routing Protocol (SAODV) is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation. SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. Achieving this is the job of the key management scheme. Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). This is because for the non-mutable information, authentication can be performed in a point-to-point manner, but the same kind of techniques cannot be applied to the mutable information. Route error messages are protected in a different manner because they have a big amount of mutable information. In addition, it is not relevant which node started the route error and which nodes are just forwarding it. The only relevant information is that a neighbour node is informing to another node that it is not going to be able to route messages to certain destinations anymore. Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole message and that any neighbour that receives verifies the signature.

C. Ariadne [4]

Ariadne is an on-demand routing algorithm based on the Dynamic Source Routing (DSR) protocol. There are several variants of Ariadne, depending on which mode of authentication is used to protect route requests: one uses digital signatures, one TESLA, and one uses MACs. The MAC version has an optimized variant that uses iterated MAC computations instead of several independent MACs. In addition to being more efficient, the iterated MAC version has superior security characteristics when compared to the non-optimized version, as noted in. We describe this version below.

A typical route request that reaches an intermediate node X_j, $1 \le j \le p$, on the route $S = X_0, X_1, \ldots, X_p, X_{p+1} = T$ is of the form

msgS,T,rreq = (rreq, S, T, id,X1,…,Xj, $mac_{SX1\ldots Xj}$),

where $mac_{SX1\ldots Xj}$ is the MAC computed by Xj with a key it shares with T on the route request received from X_{j-1}:

(rreq, S, T, id,X1,…,Xj, $mac_{SX1\ldots Xj-1}$)

The target T, on receiving the last request from Xp, is able to recompute all intermediate MAC values, since it shares a key with each one of the intermediate nodes, and then iteratively reconstruct that sequence up to the last value that should match the MAC received from X_p. If the verification succeeds, with overwhelming probability (given by the security of the MAC construction) all intermediate MACs were correctly computed by the nodes included in the route. The route reply of T is

$msg_{S,T,rrep}$ = (rrep, S, T, id,$X_1,\ldots,X_p$, mac_T);

where mac_T is an MAC computed by T with a key shared with S on the message field that precedes it: (rrep,S,T,id,$X_1,\ldots,X_p$). This is unicast upstream to S via the nodes $X_p, X_{p-1},\ldots, X_1$. Intermediate nodes must check that their label appears on the route adjacent to two of their neighbors.

D. EndairA[4]

This is a variant of Ariadne, designed to address the hidden channel attack. In endairA, the route replies of intermediate nodes Xj are protected, rather than the route requests as in Ariadne. A typical route request broadcast by a node Xj, $0 \le j \le p$, on route $S = X_0, X_1, \ldots, X_p, X_{p+1} = T$, is of the form

msgS,T,rreq = (rreq, S, T, id,X1, . . .,Xj);

while the route reply unicast by Xj, $1 \le j \le p + 1$, is

msgS,T,rrep = (rrep, S, T, id,X1, . . .,Xp, sig_T , . . . , sig_{Xj}),

where sig_{Xj} is the digital signature of Xj on the message field preceding it.

II. ANALYSIS OF EXISTING ROUTING PROTOCOLS

In the research work [5] the authors argue that routing security of mobile adhoc networks can be precisely defined using a mathematical model. They proved that the secured routing protocol Ariadne is insecure for specific attacks. They also designed a new routing protocol called EndairA which they claim to be secure.

In the research paper [4] the authors analysed the secured routing protocols Ariadne and EndairA. Also they have proved that the security proof for endairA is flawed and that this routing algorithm is subject to a hidden channel attack.

In the research work [6], the authors present a route discovery protocol that mitigates the detrimental effects of malicious behavior, as to provide correct connectivity information. They claim that their protocol guarantees that fabricated, compromised, or replayed route replies would either be rejected or never reach back the querying node. Furthermore, they claim the protocol responsiveness is safeguarded under different types of attacks that exploit the routing protocol itself. The sole requirement of the proposed scheme is the existence of a security association between the node initiating the query and the sought destination. Specifically, no assumption is made regarding the intermediate nodes, which may exhibit arbitrary and malicious behavior. They say that the scheme is robust in the presence of a number of non-colluding nodes, and provides accurate routing information in a timely manner.

In the research paper [7], the authors say that the security increase is often obtained with a quality of service (QoS) decrease. In this paper they propose a solution that provides at the anonymity, security to Ad Hoc network with a limited impact on QoS in multi-path routing of MANETs. They claim that their method could be efficient against some viral attacks. They also give some security proofs of their solution for Ad Hoc networks.

In the research work [8], the authors analysed various security threats for MANET routing and different secured routing protocols. They concluded that no existing routing protocol is a complete model against all threats.

In the research paper [3], the authors show that the security proof for the route discovery algorithm endairA is flawed, and moreover, that algorithm is vulnerable to a hidden channel attack. They also analyze the security framework that was used for route discovery and argue that composability is an essential feature for ubiquitous applications.

From the research work done by various researchers and their reports, it was clear that the secured routing protocols Ariadne and EndairA are proved to be vulnerable. Even though some researchers suggest enhancements for existing security protocols, they are proved to provide security for a few types of attacks only.

III. NEW SECURED ROUTING PROTOCOL (BASIC MODEL)

Main features

- No identity of source node in routing packets
- No identity of destination node in routing packets
- No identity of intermediate nodes in routing packets
- Single record entry (only three fields) stored in each node (local table)
- No encryption in intermediate nodes.
- Packet size is always same (no accumulation of data).
- Multi-path ability.
- No HELLO messages
- Simple, fast and secure

In this paper, we explain only the basic model. However enhancements may be made which is out of scope of this paper.

The new protocol works on the principle of FCFS (First Come First Serve) basis of packets to ensure quick delivery of packets. The complete working of basic model is as below.

A. Assumptions

It is assumed that there is a key management sub-system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network.

B. RREQ (Routing Request) process

Source Node : Generates a Session_ID, which is a random string. It also generates a RREQ_ID, which is another string encrypted with destination node's public key. Another random string is generated as the Transmission_ID. The three values combine to form the RREQ packet. The routing table is appended with Session_ID and Transmission_ID values and the Reception_ID field is left blank.

SAMPLE RREQ PACKET TRANSMITTED

Session_ID	RREQ_ID	Transmission_ID	Flag
423JK3	Encrypted message	JK785G	RR

SAMPLE ROUTING TABLE ENTRY

Session_ID	Reception_ID	Transmission_ID
423JK3		JK785G

The string used in RREQ_ID is a string which must be understandable by the destination node. That is, while decryption by the destination node by its private key, it must understand that it is the authorized recipient of the packet. Any identification of destination node in the packet may lead to attacks. Therefore, a common rule must be followed by all the nodes to identify the packet.

Sample rule (simple): Only prime numbers must be used in the message.

In the above example, any large prime number is encrypted by the source node using the destination node's public key. The authorized recipient receives only prime number by decryption of RREQ_ID using its private key whereas an attacker won't.

Proper common rule must be selected since this is the heart of this protocol and its security.

Intermediate nodes : Routing table is searched for Session_ID. If found, the packet is dropped. Otherwise, RREQ_ID is decrypted with its own private key. If a valid message is found, then current node is the destination node and RREP process starts. If the decrypted message is not valid, routing table is appended with Session_ID. The Reception_ID of the local routing table is replaced with Transmission_ID of the received packet. A new random string is generated as Transmission_ID. The new Transmission_ID is stored in the routing table. The received packet is transmitted by replacing existing Transmission_ID with the new Transmission_ID.

SAMPLE RREQ PACKET RECEIVED

Session_ID	RREQ_ID	Transmission_ID	Flag
423JK3	Encrypted message	JK785G	RR

SAMPLE RREQ PACKET TRANSMITTED:

Session_ID	RREQ_ID	Transmission_ID	Flag
423JK3	Encrypted message	LK36MV	RR

SAMPLE ROUTING TABLE ENTRY:

Session_ID	Reception_ID	Transmission_ID
423JK3	JK785G	LK36MV

Destination node : Routing table is searched for Session_ID. If found, the packet is dropped. Otherwise, RREQ_ID is decrypted with its own private key. If a valid message is found, then current node is the destination node and RREP process starts. The routing table is appended with Session_ID. The Reception_ID field of the local routing table is replaced with Transmission_ID of the received packet and the Transmission_ID field is left blank.

SAMPLE RREQ PACKET RECEIVED

Session_ID	RREQ_ID	Transmission_ID	Flag
423JK3	Encrypted message	LK36MV	RR

SAMPLE ROUTING TABLE ENTRY:

Session_ID	Reception_ID	Transmission_ID
423JK3	LK36MV	

C. RREP (Route Reply) process

Destination node : A RREP_ID is created by encrypting the received RREQ_ID number with source node's public key. A new RREP packet is created by combining Session_ID, encrypted RREP_ID and Transmission_ID for the corresponding Session_ID from the table. The RREP packet is then transmitted.

SAMPLE RREP PACKET TRANSMITTED

Session_ID	RREP_ID	Transmission_ID	Flag
423JK3	Encrypted message	LK36MV	RA

SAMPLE ROUTING TABLE ENTRY:

Session_ID	Reception_ID	Transmission_ID
423JK3	LK36MV	

Intermediate nodes : The routing table is searched for Transmission_ID of the packet received. If not found, the packet is dropped. Otherwise, the Reception_ID field of the current record is checked for emptiness. An empty Reception_ID field represents a source node and data transmission session is started. If it is not empty, the packet is transmitted by replacing Transmission_ID of the packet with Reception_ID of current record in the routing table.

SAMPLE RREQ PACKET RECEIVED

Session_ID	RREP_ID	Transmission_ID	Flag
423JK3	Encrypted message	LK36MV	RA

SAMPLE RREQ PACKET TRANSMITTED:

Session_ID	RREP_ID	Transmission_ID	Flag
423JK3	Encrypted message	JK785G	RA

SAMPLE ROUTING TABLE ENTRY:

Session_ID	Reception_ID	Transmission_ID
423JK3	JK785G	LK36MV

Source Node: The routing table is searched for Transmission_ID of the packet received. If not found, the packet is dropped. Otherwise, the Reception_ID field of the current record is checked for emptiness. An empty Reception_ID field represents a source node and data transmission procedure is started.

SAMPLE RREQ PACKET RECEIVED:

Session_ID	RREP_ID	Transmission_ID	Flag
423JK3	Encrypted message	JK785G	RA

SAMPLE ROUTING TABLE ENTRY:

Session_ID	Reception_ID	Transmission_ID
423JK3		JK785G

D. Data forwarding process

Once a route is discovered, the data transmission begins. Each data packet consists of Session_ID, Message and Transmission_ID. The data transmission process is as below.

Source Node: The same Session_ID used for route discovery is used. The packet is assembled with session_id, encrypted message and Transmission_ID.

Intermediate nodes: Receives the packet. Checks for Session_ID in the routing table. If not found, the packet is dropped. Else Transmission_ID field is checked. An empty Transmission_ID field indicates that the current node is the authorized recipient of the packet. If the Transmission_ID field is not empty, then the packet is transmitted.

Destination node : Receives the packet. Checks for Session_ID in the routing table. If not found, the packet is dropped. Else Transmission_ID field is checked. An empty Transmission_ID field indicates that the current node is the authorized recipient of the packet.

IV. SECURITY ANALYSIS FOR VARIOUS ATTACKS

The detailed analysis using mathematical models and simulation tools are out of scope of this paper. However, an outline of possibility of various attacks are analysed in this section.

A. Possible modification attacks on the RREQ/RREP packets and its effects.

1) Modification of Session_ID

Any modification in Session_ID will make the RREP packet to get dropped at the current node because, no more forwarding is possible. This initiates a fresh RREQ.

2) Modification of Transmission_ID

Any modification made in Transmission_ID also will make the RREP packet to get dropped at the current node because, no more forwarding is possible. This initiates a fresh RREQ.

3) Modification of RREQ_ID/RREP_ID

Any tampering in the RREQ_ID/RREP_ID makes the packet invalid and can't be identified by the recipient.

B. Other attacks.[1]

4) Eavesdropping

Eavesdropping is a kind of attack that aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

In the proposed design, no such data is transmitted. Therefore it is fully secure against such attacks.

5) Traffic Analysis & Monitoring

Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

In the proposed design, neither source nor destination is exposed. Therefore, there is no possibility of such attack.

6) impersonation / Spoofing

Impersonation attacks are also called spoofing attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes.

In the proposed routing protocol, the attacker needs the private key of the spoofed node to read the content. This protocol is strong enough to defend against such attacks.

7) Flooding Attack

This type of attack exhausts network resources, overall bandwidth, and individual nodes resources of computational and battery power. In AODV attacking node A sends out a large number of RREQs for a route to a non-existent node.

There is no provision to stop this type of attack in the basic model; however such provision may be added with the advanced version by using statistical analysis to detect varying rates of flooding.

8) Blackhole Attack

In this type of attack, the attacking node returns fake routing information, causing the source node to choice a route through it. The attacker can then misuse or drop messages as it sees fit.

The new protocol works on the basis of FCFS of packets. Any node found to delay or drop routing packets will be discarded from the route.

9) Link Withholding Attack

In this type of attack, the attacker does not advertise a link to a specific node or group of nodes.

The new protocol doesn't carry the identity of any node, thus safe from this kind of attack.

10) Replay Attack

In this type of attack, the attacker records another node's control messages and resends them later. Can be used to spoof another node or just disrupt routing.

In the new protocol, control messages changes each time. Also, the Transmission_ID changes with every node. Therefore, the new protocol is strong enough against this type of attack.

11) Wormhole Attack

In this type of attack, an attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole

The proposed protocol doesn't send the identity of source/destination. This nature of the proposed protocol prevents it from wormhole attack.

V. CONCLUSION AND FUTURE WORK

The protocol explained in this paper is just a basic model. Additional features such as 'time to live' mechanism, authentication info, mechanism to detect packet collision, mechanism to transmit 'low battery power' info, multi path transmission, etc. are not included in this paper. Advanced model of this protocol will contain all these features which will make this model the most simple and secured protocol.

REFERENCES

[1] K.P.Manikandan, Dr.R.Satyaprasad and Dr.K.Rajasekhararao *A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks*(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011

[2] Lu Jin, Zhongwei Zhang, Hong Zhou *Performance Comparison of the AODV, SAODV and FLSL Routing Protocols in Mobile Ad Hoc Networks*

[3] S.Gowsiga and V.K.Manavalasundaram *A Mechanism with Security for Route Discovery in MANETs* Proceedings of the International Conference , "Computational Systems and Communication Technology", 5th May 2010

[4] Mike Burmes and Breno de Medeiros, *On the Security of Route Discovery in MANETs* IEEE transactions on mobile computing, vol. 8, no. 9, september 2009

[5] Gergely A´ cs Levente Buttya´n Istva´n Vajda *Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks* IEEE Transactions on Mobile Computing (impact factor: 2.65). 12/2006

[6] Panagiotis Papadimitratos and Zygmunt J. Haas *Secure Routing for Mobile Ad hoc Networks* In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio

[7] Herv´e Aiache, Fran¸cois Haettel, Laure Lebrun and C´edric Tavernier *Improving Security and Performance of an AdHoc Network through a Multipath Routing Strategy* Journal in Computer Virology, 2008, pp.267-278.

[8] YIH-CHUN HU, Berkeley and Carnegie Mellon *A Survey of Secure Wireless Ad Hoc Routing* Security & Privacy, IEEE May-June 2004 Volume: 2 , Issue: 3 Page(s): 28 – 39