Securing AODV for MANETs using Message Digest with Secret Key

Mr. Kamaljit Lakhtaria[1], Prof. Bhaskar N. Patel[2], Mr. Satish G. Prajapati[3], Dr. N. N. Jani[4]

[1] (Ph.D. Research Scholar), Lecturer, MCA Department, Atmiya Institute of Technology & Science, Rajkot Gujarat, India, Email: kamaljit.ilakhtaria@gmail.com

[2] Head of Department, Computer & Information Technology Department, B.S.Patel Polyetchnic, Ganpat Vidyanagar,Kherava, Gujarat, India, Email: er_bhaskarpatel@yahoo.com

[3] Lecturer, Computer Department, B.S.Patel Polyetchnic, Ganpat Vidyanagar, Kherava, Gujarat, India, Email: sgp_it001052@yahoo.com

[4] Director, Kadi Vishvadiva Vidyalaya (Deemed University), S K Patel Institute of Management & Computer Science, Gandhinagar, India, Email: drnnjanicsd@gmail.com

Abstract– Due to lack of the infrastructure, open peer-to-peer architecture, shared wireless medium, limited resource constraints and highly dynamic topology, MANETs (Mobile Ad-hoc Networks) are frequently established in insecure environments, which make them more vulnerable to attacks. These attacks are initiated by sharing malicious nodes against different services of network. The binding force in these networks is routing protocol, which is a common target of malicious nodes. MANETs routing protocols are being developed without having security in mind. Ad-hoc On-Demand Distance Vector (AODV) is one such widely used routing protocol that is at present undergo extensive research and development. AODV is based on distance vector routing, but here the updates are shared not on a periodic basis but on an as per demand basis. The control packets contain a hop-count and sequence number field which recognizes the freshness of routing. These fields are editable, so it creates a possible susceptibility that is frequently abused by malicious nodes to advertise false better routes. As well as, transmission of routing updates in form of clear text also reveals crucial information about the network topology, which is again a probable security danger. In this paper we are presenting a novel and practical security mechanism for securing the AODV routing protocol that protects against a number of attacks carried out in MANETs. We will present message digest with secret key mechanism to secure AODV messages, which is very effective, and less power consuming security solution for MANETs.

Keywords— Security, Routing Protocol, Message Digest, Mechanism, Malicious, Secret Key

I. INTRODUCTION

MANET is a collection of independent mobile users that communicate over relatively bandwidth and power constrained wireless links [1]. MANET has capability to establish networks at anytime, anywhere. These networks are built, work and maintained by its own because each node performs dual role of host and router. By and large, these nodes have a limited transmission range and so each node search for the support of its neighboring nodes in forwarding packets. In order to establish routes between two nodes, which are away from each other than a single hop, special routing protocols are already designed. This unique feature is responsible to route the message in spite of dynamic topology of network [2]. These networks don't depend on extraneous hardware, which makes them an ideal candidate for military services and operations. For example battle field ad hoc network, in such a network we would surely be first concerned with the efficient and in time delivery of the message but with this, we will have to be more concerned about the strong privacy or secrecy of the information also. These kinds of scenarios, where we want to transmit private and secure information very rapidly, motivate us to make use of message digest with secret key in security context. In this paper we consider advantage of message digest with secret key to hide the information of all the fields of message by using different message digest functions.

II. PREVIOUS WORK

To protect MANET against various possible attacks a routing protocol must fulfill a set of requirements [3] to confirm that the determined path from source to destination works correctly in the presence of malicious nodes. These requirements are:

1) Authorized nodes should perform route computation and discovery,
2) Minimal exposure of network topology,
3) Detection of spoofed routing messages,
4) Detection of fabricated routing messages,
5) Detection of altered routing messages,
6) Avoiding formation of routing loops, and
7) Present redirection of routes from shortest paths.

Many secure routing protocols have been recently developed that conform to most of the requirements. Some of them are as under:

1. SAODV (Secure Ad-hoc On-Demand Distance Vector)

SAODV [8] is an extension of AODV routing protocol. It provides authentication, message integrity and non-repudiation in ad-hoc networks by using one-way hash chain and digital signature. It needs the use of Key Management Scheme. The main disadvantage with the protocol is the use of Public Key Cryptography that requires considerable amount of processing power and slows down the process to some extent.

2. ARAN (Authenticated Routing for Ad-hoc Networks)

ARAN [3] 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 trusted certification 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.

III. AODV ROUTING PROTOCOL

AODV [2] is a distance vector routing protocol that has been naturally build for MANETs. It is an on demand protocol and reactive in nature as it searching the routes only when required. It makes use of basic route establishment and maintenance mechanisms from the DSR protocol and hop-to-hop routing vectors from the DSDV protocol. AODV makes widespread use of sequence numbers in control packets to avoid the problem of generation of routing loops. When a source node is interested to communicate with a destination node whose route is unknown, it broadcasts a RREQ (Route Request) packet. Each RREQ packet contains a Request ID, source and the destination node IP addresses and sequence numbers along with a hop count and flags. The Request ID field uniquely identifies the RREQ packet; the sequence numbers gives information regarding the freshness of control packets and the hop-count maintains the number of nodes between the source and the destination. Recipient node of the RREQ packet that has not find the Source IP and ID pair or doesn't maintain a fresher (larger sequence number) route to the destination rebroadcasts the same packet after incrementing the hop-count. Such intermediate nodes also create and preserve a REVERSE ROUTE to the source node for a certain time.

When the RREQ packet arrived at the destination node or any intermediate node that has a fresher route to the destination a RREP (Route Reply) packet is generated and sent back to the source. RREP packet contains the destination node sequence number, the source and the destination IP addresses, route lifetime along with a hop count and flags. Intermediate node that receives the RREP packet, increments the hop count, establishes a Forward Route to the source of the packet and transmits the packet on the Reverse Route. AODV makes use of HELLO messages periodically to find link failures to nodes that it considers as its immediate neighbors. When a link failure is detected for a next hop of an active route a RERR (Route Error) message is sent to its active neighbors that were using that particular route.

The key vulnerabilities [2] present in the basic AODV routing protocol are:

1) Deceptive incrementing of Sequence Numbers
2) Deceptive decrementing of Hop Count

Value	Hash Function
0	Reserved
1	MD5
2	SHA1
3-127	Reserved
128-255	Implementation Dependent

Table 1: Possible values for Hash_Function field

IV. SECURING AODV USING MESSAGE DIGEST AND SECRET KEY MECHANISM

There is a Message Digest with Secret Key mechanism used to secure AODV message. This mechanism calculates message digest using appropriate hash function for all the fields (mutable as well as non-mutable) of an AODV message in addition with secret key. And then message digest and hash function value will be transmitted along with the AODV message.

The Message Digest with Secret Key mechanism algorithm is as follows:

➢ Every time a node originates a RREQ, a RREP or a RERR message, it performs the following operations:
- It chooses suitable value of hash function h that is to be used to make message digest, from all available possible values shown in Table 1.
- Sets Hash_Function field by value of chosen h.
  Hash_Function = h

  Where, h is the value of hash function.

- Get the value of Secret Key, and add it to values of all the fields of message.
- Calculates Message_Digest by passing the values of all the fields with added secret key to hash function h.
  Message_Digest = h (values of all the fields with added secret key)

  Where, h is a hash function.
  h(x) is the result of applying the function h to x.

➢ In addition, every time a node receives a RREQ, a RREP or a RERR message, it performs the following operations in order to verify the valid message:
- Get the value of Secret Key, and add it to values of all the fields of received message.
- Applies the hash function h to the values of all the fields of received an AODV message with added secure key except Hash_Function and Message_Digest fields, and verifies that the calculated message digest is equal to the value contained in the Message_Digest field of received an AODV message.
  Message_Digest = = h (values of all the fields with added secure key except Hash_Function and

Message_Digest fields), Where, a = = b reads: to verify that a and b are equal.

- Before rebroadcasting a RREQ or forwarding a RREP or a RERR, a node will perform the following:
  - It once again chooses suitable value of hash function h (may be different of earlier value of h) that is to be used to make message digest.
  - Sets Hash_Function field by value of chosen h. Hash_Function = h
  - Get the value of Secret Key, and add it to values of all the fields of message.
  - Calculates Message_Digest by passing the values of all the fields to hash function h. Message_Digest = h (values of all the fields with added secret key)

V. EXTEDED MESSAGE FORMATS

Type	J	R	G	Reserved	Hop Count
RREQ ID					
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Originator Sequence Number					
Hash Function			Message Digest		

Figure 1: Secure AODV RREQ Message Format

Type	R	A	Reserved	Prefix sz	Hop Count
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Lifetime					
Hash Function			Message Digest		

Figure 2: Secure AODV RREP Message Format

Type	N	Reserved	Dest Count
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Destination IP Address (if needed)			
Additional Unreachable Dest. Sequence Number (if needed)			
Hash Function	Message Digest		

Figure 3: Secure AODV RERR Message Format

As shown in Fig. 1, Fig. 2 and Fig. 3, the extended fields namely Hash Function and Message Digest (shown in gray color) are added in AODV messages [13], in order to make them secure according to our proposed mechanism.

VI. MESSAGE DIGEST WITH SECRET KEY MECHANISM

In our proposed secure mechanism, we assumed that there exists a central key management system, which distributes secret key to all legitimate nodes in advance before they participate in system called a team key or a group key or anything else. How key management system handles, distribute and share the secret key among legitimate nodes is out of scope for this paper.

The node which wants to send AODV message, first selects appropriate hash function and then gets secret key and adds secret key to the message data and then applies hash function on message data with added secret key to create message digest, after creating message digest it will send message digest and hash function value along with AODV message to the next node.
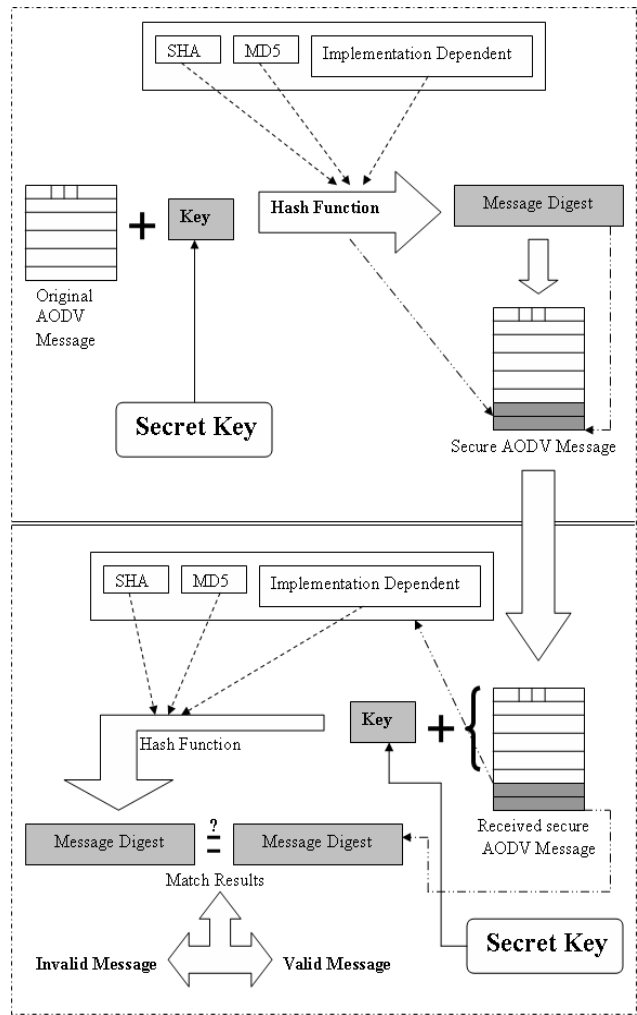

Figure 4: Message digest with secret key mechanism

The node which receives AODV message first obtains hash function from received hash function value and then gets secret key and adds secret key to the message data of received message and then applies that hash function on message data of received message with added secret key and creates message digest. After creating message digest it will compare created message digest with received message digest, if both message digests are equal it will accept that valid message and

process it, but if they are not equal it will not accepting that invalid message and simply drops it. The detail secure Message digest with secret key mechanism works as shown in Figure 4.

VII. SECURITY ANALYSIS

Here we discuss how the presented message digest with secret key security mechanism defies possible attacks in MANET and satisfies the seven requirements of any secure routing protocol:

1) *Authorized nodes should perform route computation and discovery*

All authorized nodes are having unique system wide secret key and different secure hash function by using which they are generating message digest for route computation and discovery while unauthorized nodes does not have secret key and any knowledge about hash functions and so that they cannot participate in network.

2) *Minimal exposure of network topology*

Mechanism allows passive eavesdropping by any adversary regarding network topology, but main punch of mechanism is it will not let any malicious node to misuse that eavesdropped information, because adversary cannot alter or fabricate routing message, as they do not have secret key.

3) *Detection of spoofed routing messages*

Spoofing of information does not give any benefit to the adversary until it has secret key and different hash functions available to use that spoofed information.

4) *Detection of fabricated routing messages*

Malicious nodes cannot inject fabricated routing messages into the network as they have not secret key, required to generate messages.

5) *Detection of altered routing messages*

All routing message data produces single and unique message digest so that it is not possible by any malicious node to alter it without secret key, and if malicious node alters it then legitimate node can easily find out that alteration when it compares message digest.

6) *Avoiding formation of routing loops*

This mechanism confirms that routing loops cannot be formed through any malicious action. Since routing loops mainly occurs if a malicious node is able to spoof, alter or fabricate legitimate routing packets [2].

7) *Present redirection of routes from shortest paths*

Generally, shortest paths are created by decrementing the number of addresses in the routing protocol. The mechanism is designed in such a manner that routing packets are only accepted from authenticated immediate neighbors. This ensures that an adversary cannot inject such routing packets unless an authorized node first authenticates it [2].

Following are the attacks that can be launched against the AODV routing protocol [12]:

1) *Message tampering attack*

This mechanism confirms that if malicious node tampers message in between the route, it can be easily detected by destination node.

2) *Message dropping attack*

This mechanism confirms that if malicious node drops invalid messages to the destination or to the intermediated node, it can be easily detected.

VIII. SIMULATION AND RESULTS

We have successfully implemented message digest mechanism to secure AODV routing protocol using NS-2.28 [9, 10] on Fedora core 4 Linux version and concluded that it is very secure mechanism which fulfills all security requirements without consuming much power of nodes and gives almost same performance as AODV gives without using mechanism.

The main aim of simulation is to prove proposed mechanism is properly securing AODV with all security aspects. For simulation, we have considered 3 different mobile nodes, namely node 0, node 1 and node 2. The TCP traffic connection is established between nodes 0 to node 1.

Total simulation time is 150 sec. All network components of mobile node are considered their default values. (E.g. Link Layer, Interface Queue, Mac Layer etc.) Agent, Router and Movement traces are kept ON and Mac trace is kept OFF for all three mobile nodes.

Following tables are showing the result of our simulation that proves proposed mechanism is securing AODV.

Routing Protocol: AODV				
Case: With or without malicious node				
Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	3934	3931	0	7837
Node 1	3923	3920	0	7848
Node 2	6	6	7827	7845

Table 2: AODV with or without malicious node/s

Routing Protocol: AODV with proposed mechanism				
Case: Without malicious node				
Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	3934	3931	0	7837
Node 1	3923	3920	0	7848
Node 2	6	6	7827	7845

Table 3: AODV with proposed mechanism and without malicious node/s

Routing Protocol: AODV with proposed mechanism

Case: With malicious node 0

Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	12	12	0	5
Node 1	0	0	0	6
Node 2	0	0	0	9

Table 4: AODV with proposed mechanism and with malicious node 0

Routing Protocol: AODV with proposed mechanism

Case: With malicious node 1

Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	12	12	0	18
Node 1	8	8	0	14
Node 2	9	9	0	13

Table 5: AODV with proposed mechanism and with malicious node 1

Routing Protocol: AODV with proposed mechanism

Case: With malicious node 2

Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	5540	5535	0	11046
Node 1	5518	5502	0	11047
Node 2	15	15	0	17

Table 6: AODV with proposed mechanism and with malicious node 2

Next we will consider the power consumption of nodes and showing the result of our simulation. We considered energy model for all three nodes with initial energy 10 joules and 0.1 W energy consumed when node receives AODV message and 0.2 W energy consumed when node transmits AODV message.

Routing Protocol: AODV

Case: With or without malicious node

Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	3067	3048	0	6069
Node 1	3020	3017	0	6037
Node 2	2	2	5692	5694

Table 7: AODV with or without malicious node/s

Routing Protocol: AODV with proposed mechanism

Case: Without malicious node

Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	3067	3048	0	6069
Node 1	3020	3017	0	6037
Node 2	2	2	5692	5694

Table 8: AODV with proposed mechanism and without malicious node/s

Routing Protocol: AODV with proposed mechanism

Case: With malicious node 0

Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	12	12	0	5
Node 1	0	0	0	6
Node 2	0	0	0	9

Table 9: AODV with proposed mechanism and with malicious node 0

Routing Protocol: AODV with proposed mechanism

Case: With malicious node 1

Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	12	12	0	18
Node 1	8	8	0	14
Node 2	9	9	0	13

Table 10: AODV with proposed mechanism and with malicious node 1

Routing Protocol: AODV with proposed mechanism

Case: With malicious node 2

Node	Packets			
	Generated	Sent	Forwarded	Received
Node 0	4652	4652	0	9278
Node 1	4634	4626	0	9268
Node 2	4	4	0	5

Table 11: AODV with proposed mechanism and with malicious node 2

Table 2 and Table 7 shows that simple AODV routing protocol cannot detect any malicious node/s and generate, send, forward and receive same amount of packets in both the cases of present and absent of malicious node/s.

Table 3 and Table 8 shows that AODV routing protocol with proposed mechanism and without any malicious nodes in system will generate, send, forward and receive same amount of packets as AODV will generate, send, forward and receive.

Table 4 and Table 9, shows AODV routing protocol with proposed mechanism and with malicious node 0 that can easily detect malicious node. Here node 2 recognizes that node 0 is malicious and will not forward any of the message sent by node 0 to node 1.

Table 5 and Table 10, shows AODV routing protocol with proposed mechanism and with malicious node 1 that can easily detect malicious node. Here node 2 recognizes that node 1 is malicious and will not forward any of the message sent by node 0 to node 1.

Table 6 and Table 11, shows AODV routing protocol with proposed mechanism and with malicious node 2 that can easily detect malicious node. Here node 0 is recognizing that node 2 is malicious and sends all the messages directly to node 1 by passing node2.

Table 7 and Table 8 shows that proposed mechanism generate same amount of messages, it means that mechanism does not consume more power even if it is secure.

Above results easily illustrates that proposed mechanism is very efficient, secure and can easily find malicious node/s within system, and provide good security overall without loosing extra energy in spite of security.

IX. CONCLUSION

In this paper we have presented a message digest with secret key mechanism for securing the AODV routing protocol used in MANET. Research in the field of networks has shown that Public Key Cryptography and its related algorithms are very slower and power consuming than the Symmetric Key Cryptography. Our proposed mechanism uses symmetric key cryptography and generates very less overhead of calculations and saves power consumption of nodes significantly which is most important and attractive feature. This mechanism does not use any kind of encryption or decryption techniques so that the performance of secure routing protocol is remain almost same. The entire security strength of this mechanism is relies on how frequently key management scheme is changing the secret key of all nodes. For ensuring greater security, we can have the concept of "One Time Pads" or "Key of the Day" etc. Moreover, the military networks which perform very sensitive operations where we have to spread private information very securely, we are mainly concern about privacy or secrecy along with efficient and in time delivery of the message. Such a kind scenarios motivate us to use message digest with secret key, which is very secure as well as efficient.

X. FUTURE WORK

The same kind of mechanism we would like to design for other routing protocols of MANET like DSR, DSDV, TORA etc.

We would like to enhance proposed secure mechanism by adding concept of "set of secret key", in which each node will maintain couple of secret keys instead of single unique key, in order to make mechanism very strongly secure.

REFERENCES

[1] Junaid Arshad, Mohammad Ajmal Azad, "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks", *(2006) IEEE,* pp. 971-975.

[2] Asad Amir Pirzada, Chris McDonald, "Secure Routing with the AODV Protocol", *(2005) Asia Pacific Conference on Communication, Perth, IEEE,* p.p. 57-61.

[3] B. Dahill, B.N. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks", *Proceedings of the international conference on Network Protocols (ICNP),* p.p. 78-87, 2002.

[4] Tuulia Kullberg, "Performance of the Ad hoc On demand Distance Vector Routing Protocol", *HUT T-110.551 Seminar on Internetworking.*

[5] Manel Zapata, N. Asokan, "Securing Ad hoc Routing Protocols" (2002), *WiSe-02, September 28,2002, Atlanta, Georgia.* (ACM)

[6] H Yang, H.Y. Lue, F Ye, S.W. Lu and L Zhang, "Securing in mobile as hoc networks: challenges and solutions" (2004) *IEEE wireless communications* 11(1), pp. 38-47.

[7] Jean-Pierre, Levente Buttyan, Srdan Capkun, "The Quest for security in mobile ad hoc networks". *(2001)* ACM.

[8] Manel Zapata, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, *INTERNET DRAFT (September 2006)* draft-guerrero-manet-saodv-06.txt

[9] Ns homepage - http://www.isi.edu/nsnam/ns/

[10] Ns manual - http://www.isi.edu/nsnam/ns/

[11] Konrad Wrona, "Distributed Security: Ad Hoc Networks & Beyond", *PAMPAS Workshop, RHUL, September 16-17, 2002.*

[12] Lin, Rad, Wong, Song, "Experimental Comparisons between SAODV and AODV Routing Protocols", *WMuNeP, October 13, 2005.* (ACM)

[13] Perkins, Belding-Royer and Das, "Ad hoc on-demand distance vector (aodv) routing", *IETF RFC 3591, 2003.*