



## A Security Scheme for Mobile Ad-hoc Network with Reduced Routing Overhead

Tarun Kumar Mishra<sup>1</sup>, Bhupendra Singh<sup>2</sup>, Arun Kumar<sup>3</sup>*School of Computing Science & Engineering,  
Galgotias University, Greater Noida, Uttar Pradesh, India*

**Abstract-** A mobile ad-hoc network is collection of mobile nodes which are design to communicate each other without fix infrastructure and central coordination. Since in the MANET, routing protocols have no security mechanism. They are designed only to provide correct routing and have ability to adjust their dynamic changing condition. So MANET is more venerable due to their routing behavior. Routing protocols are more affected by two way, first one is attacks from private node that do not belongs to network and also disrupted by presence of compromise nodes. We can solve the issue of attacks from private nodes by authentication techniques that provide mutual trust between nodes. In this paper, we proposed digital signature scheme to provide mutual trust between nodes. We are choosing AODV routing protocols for study. Since AODV routing protocol provide route on demand and integrate many features designed to maximize performance at reduced routing overhead and cost of added complexity. We also proposed a solution for route availability and validation.

**Keywords:** ad-hoc network; attacks; routing security; routing protocols; routing overhead; AODV;

### I. INTRODUCTION

Security is essential things in mobile ad-hoc network because the mobile nodes in the network dynamically setup temporary paths among themselves to forwarding data packets due to existence of temporary network without any fix infrastructure and centralize management [1, 7]. Since ad-hoc network routing protocols have not include any security mechanism at all so main security threads comes their routing protocols such as AODV, DSR, DSDV and OLSR. It means ad-networks are more venerable due to their routing behavior and characteristics of network. In the ad-hoc network, mobile nodes are not bound to any centralize control like base stations. In such type of network mobile nodes work not only as a host but also as a router. In the ad-hoc network routing protocol, each nodes allow to find multi-hop path to any other nodes in the network. Flexibility in MANET technology offers much application such as emergency services, geographical or terrestrial situations where we can establish communication without any fix base station. But these flexibility or characteristics such as dynamic topology, open medium and distributed cooperation are reason to be venerability in mobile ad-hoc network. Since in MANET, routing has important role to provide the security for entire network. Most ad-hoc network routing protocols exchange information about change topology of network. Since topology changes dynamically and update messages about these changes require to be sent normally from one node to another. We know that these entire messages are sent through the open medium, so any private node could take action as malicious router, transmitting false routing information or avoid packets from being forwarded. Due this reason, packets will never reach at right destination and as a result, total failure of network [4].

In this paper in section II, we firstly analyze the various routing attacks, need of routing security in MANET, routing protocols of MANET and why, we choose AODV routing protocol. In section III, we describe the problem statement. And in section IV describe our proposed mechanism. Finally, the conclusions and future work are describes in last section V.

### II. ROUTING ATTACKS IN MANET

#### A. Attacks

A variety of attacks are classified in following two ways. First one is the passive attacks and second one is the active attacks. Passive attacks do not disrupt the operation of routing protocols, while active attacks disrupt the operation of routing protocols and engage modification, information interruption and fabrication.

TABLE 2.1 EXAMPLE OF SECURITY ATTACKS

Passive Attacks	Traffic analysis, Eavesdropping, Monitoring
Active Attacks	Modification, Spoofing, Jamming, Replaying, DoS( denial of services )

Further active attacks are classified in two ways. First one is external attacks and second one is the internal attacks. Some paper refers to outsider and insider attacks [7]. External attacks do not belong to domain of network. So these attacks also know as outsider attacks. External attacks come from node that does not have the authentication of network [1]. Internal attacks come from compromise nodes that have the legal private key of network. This compromise node can modify routing packets to disrupt the operation of routing protocols and generate the unnecessary routing information. Below table 2.2 show attacks on each layer of internet model. These attacks are categorized on basis of layers. Internal attacks are actually part of network.

TABLE 2.2 ATTACKS ON LAYERS

Layers	Attacks
Application layer	Data corruption, Repudiation
Transport layer	SYN flooding, Session hijacking
Network layer	Black hole, Byzantine, Flooding, Wormhole
Data link layer	Monitoring, Traffic analysis
Physical layer	Eavesdropping, Jamming, Interception
Multi layer	Impersonation, Replaying, Denial of services

External attacks can be prevented by providing authentication and encryption method. But challenging task is to prevent the internal attacks that come from a group of compromise nodes. In our scheme, we provide the authentication and integrity to prevent the private nodes. And route validation and availability are provided in our scheme which prevent from some internal attacks.

#### B. Need of routing security

Current routing protocols [1, 3, 4] are design in such way they provide solution to adjust well to dynamically changing conditions and provide a partial solution for making correct routing; they do not have any guarantee for security because they do not have any security mechanism in their routing protocols. Due to characteristics of MANET, mobile ad-hoc network need much harder security. MANET is more venerable due to their routing behavior. The primary goal of routing protocols is to establish the valid and available route for data transmission so that data can be transmitted timely at defined destination. Due to misdirect of routing, the entire whole network can be affected. So, routing security has an important role in security of whole network.

#### C. Routing protocols of MANET

Basically many routing protocols [3] are developed for mobile ad-hoc network which are designed to established route between sources to destination. But they are classified into two categories.

*Table driven or proactive routing protocols:* In proactive or table driven routing protocols each node have maintain up-to-date routing information to each and every other nodes in the network. These types of protocols need every node to keep one or more table to store information about its neighbor and dynamic change in network topology during routing.

*On demand:* In on demand or reactive routing protocols have each node have maintain routing information about active route only as when needed. These protocols are designed to reduce routing overheads in table driven protocols. On demand of route, when source node wants a route to destination for transmitting data packet, a route discovery process is initiated.

[3] There are mainly three routing protocols for a MANET, AODV (ad-hoc on demand distance vector), DSR (dynamic source routing), and DSDV (destination sequence distance vector). AODV [5] is reactive routing protocols in which route discovery process is initiated to create route from source to destination when they are needed. Maintenance process at each node is based on time in which if the routing entry is not recently used, it will be expire. DSDV proactive routing protocol is based on Bell- Ford routing algorithm. In this, every node maintain a routing table about all possible routes to destination. DSR maintain routes in its table of which it is aware in route cache.

#### D. Why, we choose AODV routing protocol?

AODV (ad-hoc on demand distance vector) is reactive and on demand protocol it initiated route discovery process when there is need. So due to this feature, it reduce routing overheads in table driven protocols. There are following packet send and receive during route discovery.

*Route discovery process:* When a source node want to send data then a route discovery process initiated. Source node transmits RREQ request message to its neighbors. If mid node have a route to destination then a reverse path is build and mid node set a life time for this reverse path. If mid node does not have route to destination then it send a RREP response message to source. This procedure will proceed until destination node find. If a node is destination node then its send a RREP message along reverse track to source. In case of link breakage or time out a RRER error message is send to the source. Source node sends a HELLO message to maintain the link breakage and remove the unnecessary information from routing table which reduces the routing overhead.

### III. PROBLEM STATEMENTS

The main challenging task of MANET i.e., to provide the security scheme in their routing protocols because routing protocols do not have any security mechanism. We proposed digital signature security scheme and route validations scheme

which protect from private users and some internal attacks. MANET is formed by mobile nodes that have limited battery and CPU power. Since there are no dedicated routers, every mobile node is expected to route (or relay) packets on behalf of other nodes. Nodes often transform their location in network. So, some fusty routes are produced in the routing table which leads to unnecessary routing overhead. So a HELLO message is being sent from source using AODV protocols to maintaining the link breakage and removing the unnecessary information from its routing table on occurring of ERROR messages.

CASE 1: In case first, when source node want to send a data to destination then there is need of routing protocols which is used to discover arouse to destination. We have chosen AODV routing protocol for estisblsiment of route to destination. It is initiated on demand of data by source when source want to send data to any destination. Source node sends request packets to their neighbors with a destination IP address. Intermediate node response when they receive their request otherwise sends an error message to source.

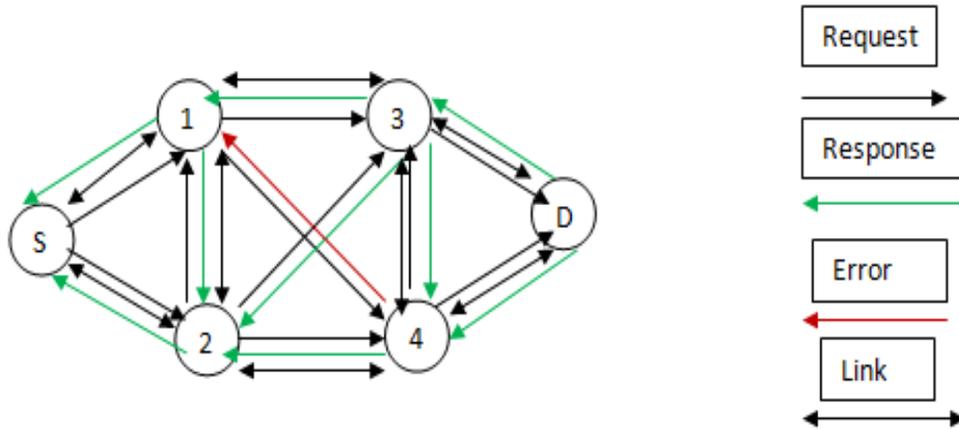


Figure 3.1 Route discovery process

Problem in case first, if every intermediate node response then every node has more routes to above case every node has extra routing overhead which decreases the network performance and routing delay.

*Solution of Case First*

When route discovery process is initiating the route between source to destination, a time interval, sequence number and hop count is append in the request packets. And send this packet to its neighbors. Following way is describing to find shortest path.

- a) *How to find shortest path:* A sequence number is sending with request packet which is mutable. If the receiving intermediate node receive packet first time then this record is update in neighbor routing table with packet information. Else discard the request and increase the sequence number in their routing table. If the receiving node is destination then receive all requests by destination and send a response message to source through existing route information in their routing table. When a source node receives the response message it check highest sequence no. and minimum hop- count. And delete all other route.

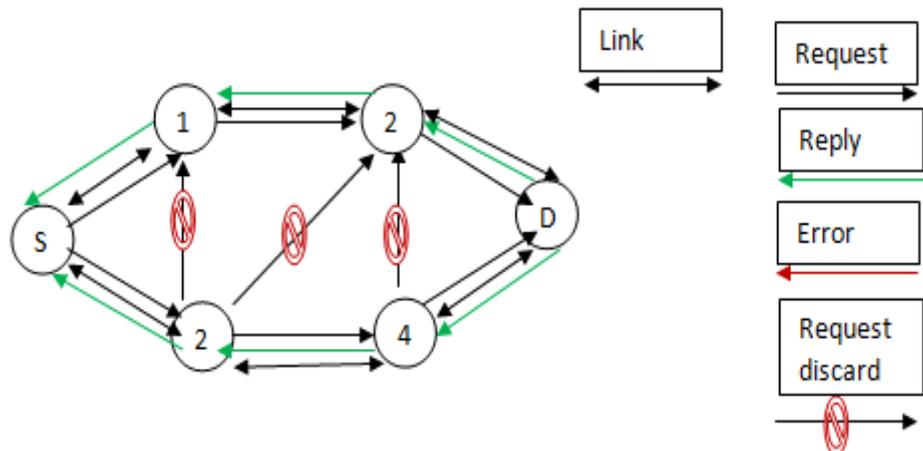


Figure 3.2 Route discovery process with discarding duplicate request

- b) *How to check route validation and availability:* In request packet, a time interval is set for response message to source when request is send by the source to destination. If response messages are received by source in this time interval with same hop-count in their routing table. Then route is valid and available else route is not valid. If time is out then an error message is send to source and source node choose another path with available highest sequence no. and minimum hop count.

If any alternative route is not available then route discovery process is initiated to find new route.

CASE 2: In the case link breakage due to unreachable of node or battery power down.

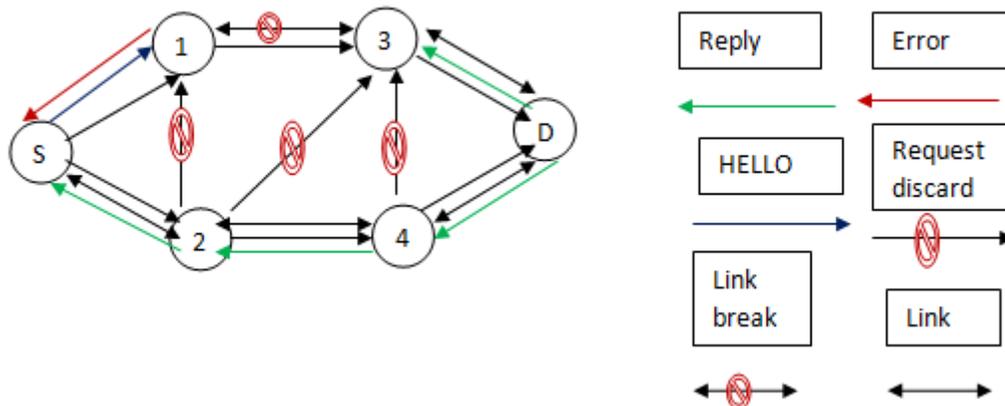


Figure 3.3 Route discoveries with link breakage

The neighbor active node send error message to the source. And source node send a HELLO message to maintain the route and remove the unnecessary information from the routing table which reduced the routing overhead. And if source node have not alternate route then route discovery process is initiated else not.

CASE 3: If malicious node enters in the network in network or compromise with any node in network then, how will we sure about the secure path? For fulfill this type of security we are proposing digital signature scheme. This digital signature is sending with the request packet in encrypted form. And every officer of team in the network has key to create the digital signature. If digital signature will not match, then node will not receive the request during request process. This same procedure will be follow during the response message through the destination.

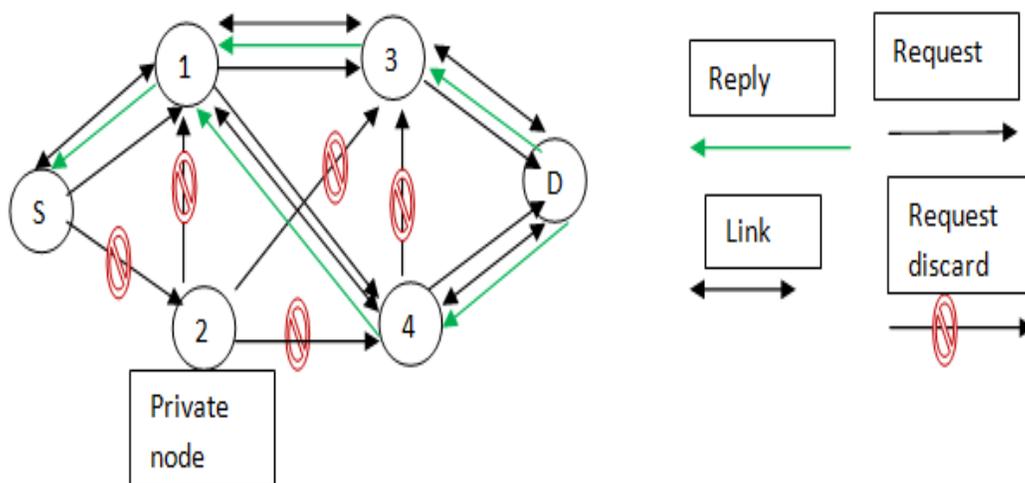


Figure 3.4 Route discovery process with private node

In the above figure, node 2 is private node which is malicious and request message is discarded due to non-verification of digital signature because private node does not know about private key. Only officers have key by which they create and verify the digital signature.

#### IV. PROPOSED WORK

In our scheme, a digital signature scheme and route validation scheme are proposed which secure from private user and some internal attacks. Shortest path mechanism is also proposed which reduce the routing overhead. When route discovery process is initiated a request is sent to its neighbors by source node. And intermediate node also sends it to its neighbors until a

destination node find. Table 4.1 below show request packet it sent to its neighbors by source node. Route availability validation is test on basis of hop count and time interval.

TABLE 4.1 REQUEST PACKET

Type count	Reserved	Hop-
	Broad cast id	
	Source IP address	
	Next hop	
	Pre hop	
	Destination IP address	
	Digital signature	
	Key	
	Sequence number	
	Time interval	

*Algorithm*

i) Security from private node (initially every officer knows about the key “rq\_k”)

a) *Generation of digital signature (encryption technique)*

- If (rq\_bcast\_id>rq\_k)
- {rq\_dgn=(rq\_bcast\_id-rq\_k)
- Else
- {rq\_dgn=(rq\_bcast\_id+rq\_k)
- }}

b) *Digital signature verification*

- If(rq\_dgn>2\*(rq\_k)
- {if(rq\_bcast\_id==(rq\_dgn+rq\_k)
- {forward((aodv\_rt\_entry\*) 0, p, NO\_DELAY);
- ELSE
- {drop(P, DROP\_RTR\_ROUTE\_LOOP);
- }}}
- ELSE
- If{(rq\_bcast\_id==(rq\_dgn-rq\_k)
- {forward((aodv\_rt\_entry\*) 0 P, NO\_DELAY);
- ELSE
- {drop(P, DROP\_RTR\_ROUTE\_LOOP);
- }}}

ii) For shortest path

- If receiving node is intermediate node and receives the packet first time add the record in routing table.
- Else intermediate node discards request and increase the sequence no. of sending node.
- If receiving node is destination node receive all requests to its neighbors and send response message to source by existing routing information in their routing table.
- If source node find response from multiple routes, data will be only the route have highest sequence number and minimum hop count.

iii) For route validation and availability.

- If response message have the same hop-count in defined time interval then I will ensure that this route is valid and available. Else I will decide that this route is not valid route.
- If time is out then send error message to source. In this case source node checks the availability of other route on basis of their highest sequence number and minimum hop-count.
- If alternate route option is available then data will be sent by this available route. Else route discovery process is initiated by the source node.

TABLE 4.2 RESPONSE PACKET

Type	Reserved count	Hop
Response test id		
Next hop		
Pre hop		
Destination IP address		
Source IP address		

A response packets are only send by the destination node which solve the black hole problem because in black hole problem intermediate nodes response to source generating false information to become a valid route with high sequence number.

#### V. CONCLUSION AND FUTURE WORK

In this paper we have proposed a security scheme for Mobile ad-hoc network with reduced routing overhead based on digital signature. In this scheme, a key is used by all offices in team member. This key generates digital signature using encryption technique and verifies the digital signature after decrypt the digital signature. This scheme provides the security from the private node in the network. A route validation scheme is also used to find the availability and validation of route on basis of hop count and time interval. This scheme protect from black hole attacks. In future, we improve my security scheme to provide security from some other internal attacks and detect the behavior of malicious nodes and analysis results of this scheme with various routing protocols at cost, throughput, complexity factors.

#### REFERENCES

- [1] L.Pengwei and X.Zhenqiang, *Security Enhancement of AODV against Internal Attacks*, International Conference on Information Science and Engineering (ICISE), Vol. 2, pp 584-586, 2010.
- [2] A.Das, S.S.Basu and A.Chaudhuri, *A Novel security scheme for wireless Ad-hoc network*, International Conference on Wireless Communication Vehicular Technology, Information theory and Aerospace and Electronic System technology, Vol. 2, pp 1-4, 2011.
- [3] DENG Hongmei, L I Wei and D P Agrawala, *Routing Security in Wireless Ad Hoc Networks*, International Journal of IEEE, Communication Magazine, Vol. 40(10), pp 70-75, 2002.
- [4] L. Venkatraman, D. P. Agrawal, *Strategies for Enhancing Routing Security in Protocols for Mobile Ad hoc Networks*, Journal of Parallel Distributed Computing, Vol. 63(2), pp 214-227, 2003.
- [5] V. Sesha Bhargwi, M.Seetha and S. Viswanand, *Design of A Scheme for Secure Routing in MANET*, International Conference of CS & IT,JSE-2012, Vol. 04, PP. 33-46.
- [6] N. Zhou, H. WuAlhussein ,A. Abouzeid, *Reactive Routing Overhead in Networks with Unreliable Nodes* , International Conference on Mobile Computing and Network, Vol. 9, pp 141-160, 2003..
- [7] Y.Xiao, X.Shen, and D.Z.Du (Eds.), *A Survey of Attacks and Countermeasures in MANET*, Wireless/Mobile Network Security, Springer, Vol. 12 pp 1-38, 2006.
- [8] Y.-B. Ko and N.H. Vaidya , *Location-Aided Routing (LAR) in mobile ad hoc networks*, International Conference on Wireless Network, Vol. 6, pp 307-321, 2000.
- [9] R. J. La and E. Seo, *Expected Routing Overhead for Location Service in MANETs Under Flat Geographic Routing*, IEEE Transactions on Mobile Computing, Vol. 10(3), pp 433-448, 2011.
- [10] J. Lopez, J. M. Barcelo and J. G. Vidal, *Analysing the Overhead in Mobile Ad-hoc Network with a Hierarchical Routing Structure*. [http://research.ac.upc.edu/XARXES/CompNet/papers/HETNETs\\_paper\\_23.pdf](http://research.ac.upc.edu/XARXES/CompNet/papers/HETNETs_paper_23.pdf) (access on 12/04/2013).
- [11] X. Wu, H. R Sadjadpour and JJ. Garcia-Luna-Aceves, *Routing Overhead as A Function of Node Mobility Modeling Framework and Implications on Proactive Routing*, Proceeding of IEEE MASS, pp 1-9, 2007.