IJETST- Volume||01||Issue||05||Pages 579-584||July||ISSN 2348-9480 2014

International journal of Emerging Trends in Science and Technology

HASH Mechanism to Secure the AODV Protocol in MANETs

Authors

Sudarsanan. D[1], Megha. J [2]

[1]Assistant Professor, Department of ISE,
Acharya Institute of Technology, Bangalore,
sudarsanan@acharya.ac.in
[2]M.Tech (STUDENT) Department of ISE,
Acharya Institute of Technology, Bangalore
megha.mtcn.12@acharya.ac.in

Abstract

Mobile ad-hoc networks are self forming network without any fixed infrastructure. An ad hoc network does not have fixed infrastructure, it means a network without the standard routing infrastructure like fixed routers and routing backbones. Since the network is self configuring it is prone to security problems [19]. One such aspect is Routing .The most widely used protocol for ad-hoc networks is DSDV and AODV. The routing protocol Ad hoc On Demand Distance Vector has been built without considering any security mechanisms. In AODV the updates are generated as per demand not on a periodic basis. The freshness of routing in AODV is recognized by the control packet which contains hop-count and sequence field. As the fields are editable, it creates a possible vulnerability that is recurrently abused by malicious nodes to advertise false enhanced routes. To improve the security there are some new mechanisms like hash chains and digital signature. To verify the correct functionality of the protocol it is implemented on NS2 simulator and performed extensive simulations and performance evaluations. This experimentation considers parameters such as packet delivery ratio, control overhead and throughput.

Keywords*: AODV,Hashchain,Security,Routing,DigitalSignature*

1 .INTRODUCTION

MANET is formed by independent mobile users that communicate over relative bandwidth and power constrained links. MANET has capability to establish networks at anytime, anywhere. Every node does not operate as a host but it acts as a router and is responsible for transferring packets to other mobile nodes.

Mobile Ad-hoc Network topology is composed of nodes that enter into or exit from network dynamically [19]. There is no central controller or a stable structure to support configuration or reconfiguration of the network .Each nodes has a limited transmission range and so each node search for the transmission range to forward packets to neighbors. 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.

Each network is designed to provide numerous applications. Ad-hoc networks are having widespread applications which are part of day life as we can connect any mobile node to the network and can perform required tasks like an accessing the Internet without having the fixed infrastructure.

MANET networks are used to connect soldiers in battlefield. As MANET can be used for Military purposes it can also be used for secured online Transaction and hence the main requirement is to make it secure or attack free so that malicious node cannot enter this Network and hence the information will be secure.

The AODV is dynamic algorithm which enables multihop routing to establish and maintain an ad hoc network. The route to the destination is obtained quickly by AODV .the nodes which are not in the active communication need not maintain routes to destination. The link breakages and changes in the network topology are updated by AODV in timely manner. MANETs have certain unique characteristics that make them vulnerable to several types of attacks. Since they are deployed in an open environment where all nodes co-operate in forwarding the packets in the network, malicious nodes are difficult to detect. Hence, it is relatively difficult to design a secure protocol for MANET, when compared to wired or infrastructure-based wireless networks.

2. RELEATED WORK

2.1 Ad-Hoc on Demand Distance Vector Routing (AODV)

As the name suggests it is an on demand routing protocol. It is a Source-Initiated On-Demand or Reactive Routing Protocol. When a source node desires to send a packet to the destination node for which the path is not established, a route discovery Process is initiated. There are three kinds of routing messages which are generated by this routing protocol during the establishment of route from source to destination they are:

-RREQ (Route Request).
-RREP (Route Reply).
-RERR (Route Error).

When a source node need to send some data to another node and if path is not established then it starts a route discovery process in order to establish a route towards destination node by sending route request message (RREQ) to all its neighbors[11]. Request is received by the Neighboring nodes, hop count is incremented and then message is forwarded to neighbors. As the RREQ message is broadcasted it is called as flooding. The objective of RREQ message is not only to find a path to destination but also making other nodes learn about a route toward source node (reverse route). When a RREQ message is received by the intermediate node, then it has a reverse route to node S through A with path length equals to hop count field of RREQ [12]. Finally, when destination node receives the RREQ message, route reply message (RREP) is generated in response. The unicast RREP is sent, using the path towards the source node established by the RREQ. Finally when the route discovery process is done then, packets can be delivered from the source to the destination node and vice versa [2]. A route error (RERR), allows nodes to notify breakage of link between any two nodes or information about those nodes which are unreachable at present.

In AODV it is not necessary that always a RREQ should reach the destination node. If path already exists towards the destination node RREP messages need not forwarded further. Quicker replies are generated and it limits the flooding of RREQs [16]. The freshness of routing information is identified by the sequence number. Each node maintains its own the sequence number is incremented before sending any new RREQ or RREP message by every node [5]. These sequence numbers are included in the routing messages and also stored in routing tables. In AODV preferences is given for the fresh or new information, thus routing table is updated if the node receive a message with a sequence number higher than the last recorded one for the destination.

2.2 VULNERABILITIES IN AODV

The AODV is very efficient as a network service but as it is having lots of vulnerabilities this protocol can be easily attacked. AODV is not so secure. AODV is designed without considering malicious node. AODV protocol with no malicious nodes is the most efficient one but malicious node in the network will be present in one or the other way [3]. Malicious nodes may be present in the network and performs unauthorized activity on the network [11]. In AODV when RREQ messages or RREP is received the following changes is seen.

1. Sequence numbers can be modified.
2. Hop Counts can be modified. (Main attack is looping in the network).
3. Modification of source routes (Black hole attack, divert the route).
4. Tunneling.
5. Spoofing.

2. Nodes in the network have capabilities for creation public and private keys.

6. Fabrication of Error messages (greedy node capture the data if Error message is not reached to Destination).

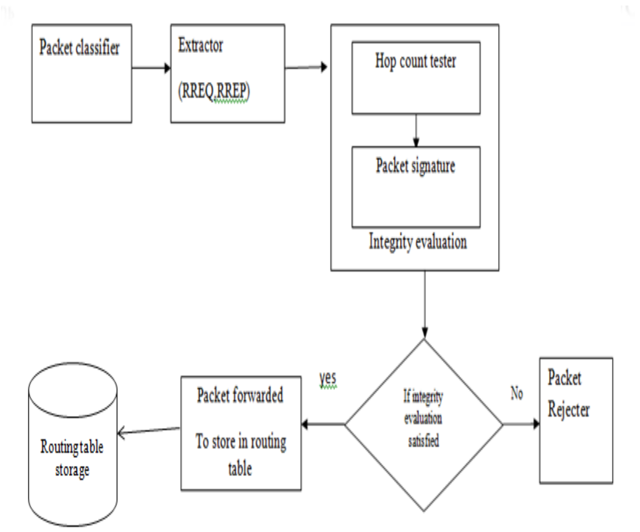
3. SECURING AODV

In MANET the public keys are obtained from other nodes of the network. Each ad hoc node is capable of securely verifying the identity of a given MANET node and the public key of that node by the key management sub-system.

Node to obtain public keys from the Depending on the key management scheme this can be achieved [1][2]. To secure the AODV messages two mechanisms are used:

1. The non-mutable fields of the messages are authenticated by using Digital signatures.
2. To secure the hop count information Hash chain used (the only mutable information in the messages).

To the non-mutable information, an end-to-end authentication is performed, but it the same kind of techniques cannot be applied to the mutable information [7]. Hash chains and the signatures are transmitted with the AODV message as an extension message.



The model contains packet classifier, extractor, integrity evaluation, packet rejecter and packet forwarder. The type of packet is identified by the packet classifier to determine whether is RREQ /RREP which arrives at the system. Based on the request the packets are extracted by extractor and the integrity evaluation is performed and the hop count verifications evaluated on extracted packets .The two modules hop count tester and packet signature will handle these tasks. If integrity evaluation fails the packet is rejected by the packet rejecter. If evaluation and verification are succeeded then the packet information can be stored in routing table.

Security requirements and Assumption

1. The destination node can authenticate packets from the source and each of the receiving nodes can authenticate packets from previous hops.

3. Each node has only one pair of keys. The digital signature algorithm is well known by all nodes in the network.

3.1 EAODV HASH CHAIN

To authenticate the hop count of the AODV routing messages Hash chains are used in EAODV. A random number (seed) is generated when the node wants to send a RREQ or a RREP. Max Hop Count is selected and it is set to the TTL value in the IP header [2]. In the Signature Extension format The Hash field is set to the seed. The Max Hop Count is set to the seed hashed times of the Top Hash field. Whenever a node receives RREQ or a RREP hop count is verified by hashing Max Hop Count Hop Count times the Hash field. Obtained resultant value is compared with the Top Hash. If the comparison fails, then the packet is discarded. A node hashes one time the Hash field in the Signature Extension before rebroadcasting a RREQ or forwarding a RREP [3].
Hash Function field indicates which is to be used to compute hash. The same hash function will be used by a forwarding node that the originator of the routing message has selected due to the field which is already signed. If a the hash function is not supported by the node then forwarding routing message Packet is dropped.

The calculations are as follows:

1. Generates a random number (seed)

2. Sets field

Max_Hop_Count = TTL

3. Sets field

Hash = seed

4. Sets field

Hash_Function = h,

5. Top_Hash field is calculated by hashing seed Max_Hop_Count times.

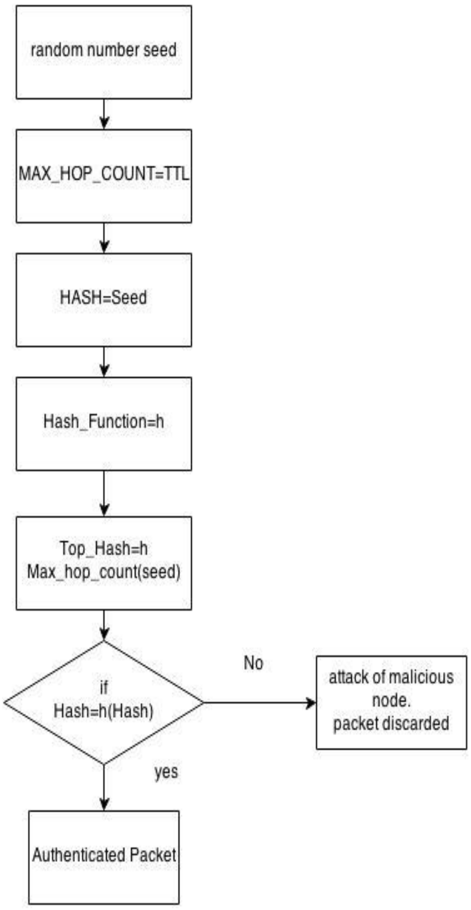
Top_Hash = h Max_Hop_Count (seed)

- hi(x) is the result of applying the function h to x i times.

4. When a node receives a RREQ or a RREP message, is compared with
5. Top_Hash == h Max_Hop_Count – Hop_Count (Hash)

- Hop Count refers to number of hops

7. Before rebroadcasting a RREQ or forwarding a RREP, a node performs Hash = h (Hash)



3.2 EAODV DIGITAL SIGNATURE

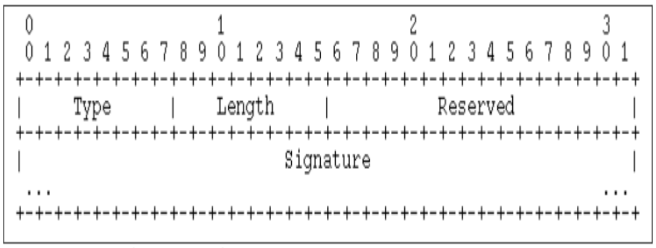
Digital signatures protect the integrity of the non-mutable data in RREQ and RREP messages. When a node receives a RREQ, it first verifies the signature before creating or updating a reverse route to that host. Only if the signature is verified, it stores the route [7]. Otherwise, RREQ is rebroadcasted. When a RREQ is received by the destination itself, it will reply with a RREP only if the AODV's requirements are satisfied. This RREP will be sent with a RREP Single Signature Extension. When RREP, it first verifies the signature before creating or updating a route to that host. Only if the signature is verified, it stores the route which is received by the node the signature of the RREP and the lifetime. The format of signature extensions is given below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     | Hash Function | Max Hop Count |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Top Hash                            |
 ...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Signature                           |
 ...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Hash                              |
 ...                                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: RREQ/ RREP SINGLE SIGNATURE

3.3 EAODV ERROR MESSAGES

Route error messages have to be protected as they contain mutable information. The route error is not concerned with which node is the originator of error. Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole message and that any neighbor that receives verifies the signature. Destination sequence numbers are not trusted by the nodes. RERR message is used to decide whether they should invalidate a route or not. Malicious node are not considered.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Signature                           |
 ...                                                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: RRER message format

SIMULATION AND RESULTS

All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83GHz machine using Ubuntu 12.4.0 with 2 GB RAM and the network simulator NS2 version NS-2.35. Table 1 provides the parameters considered during the simulation

Table 1: simulation parameters

parameters	value
Simulation area	1500*1500
Channel	wireless
No of nodes	50
Protocol	AODV
Malicious node	1
Packet size	512 bytes

Experiment 1: Number of Packets Calculated

It gives the original AODV, Malicious and the EAODV sent received and the dropped packets scenario.

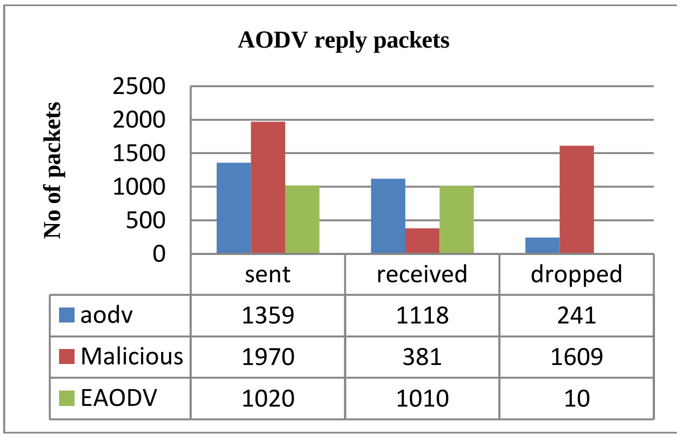


Figure 4: Number of Packets Calculated

Experiment 2: Packet Delivery Ratio

It is the ratio of packets delivered to that generated by the traffic generator. It is given by received packets/sent packets. The packet delivery ratio is directly influenced by packet loss, due to network faults.

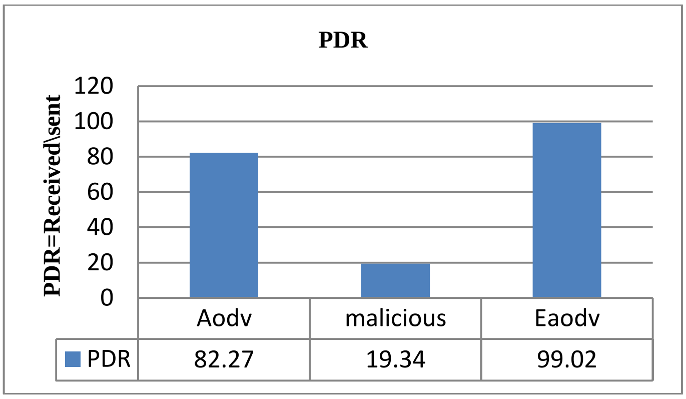


Figure 4: Packet Delivery Ratio

Experiment3: Throughput

Throughput is the ratio of total amount of data received at the destination from sender in receiving the last packet. It is measured in bits per second or packets per seconds.

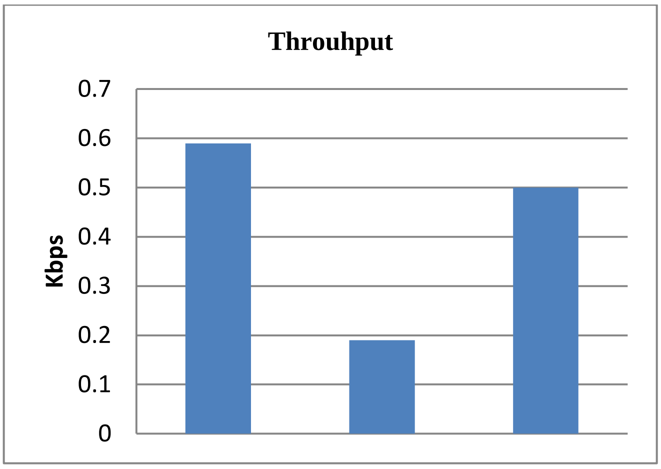


Figure 5: Throughput

Experiment4: Average End to End Delay

The delay experienced by packet from the time it was sent by a source till the time it reached the destination. During route discovery it includes all possible delays caused by buffering latency, queuing at the interface queue, retransmission delays at the MAC and propagation and transfer times. For each packet sent, calculate the send time and receive time, then average it.

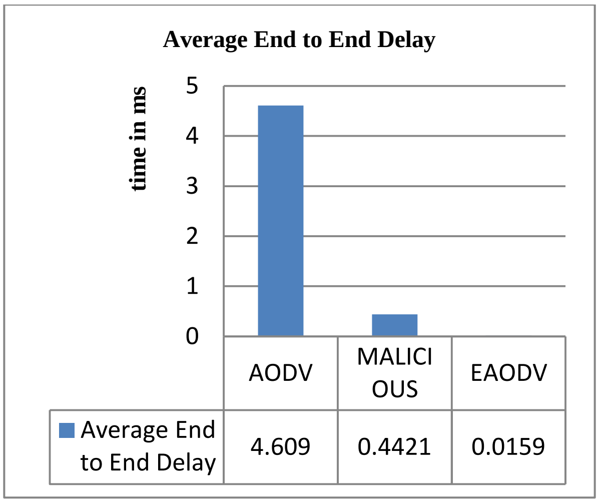


Figure 6: Average End to End Delay

Experiment5: Control Overhead

When a number of node increases the control over head also increases. this is due to as a number of nodes increased their by causing frequent link breaks when the link is broken the node sent more control packets to source so that the control overhead is increased.

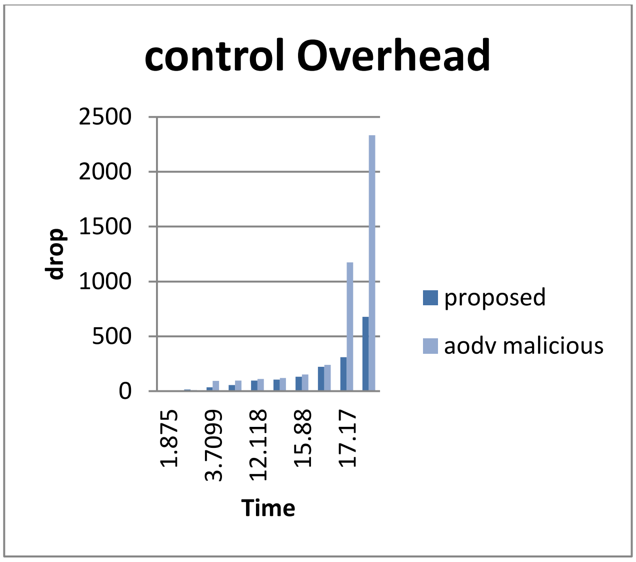


Figure 7: Throughput

CONCLUSION

Securing AODV is still an open area for research work. The proposed scheme proves to be more efficient in securing AODV routing protocol in defending against malicious nodes. Enhanced AODV improves the AODV message format by including the security parameter for securing the routing messages. When comparing to some current secure AODV protocols like ARAN, SAODV and SRAODV, our solution expands the security scope of them and provides more security service. The simulation results prove the feasibility of secure routing protocols. According to the simulations that were performed in NS2, the newly proposed security scheme, built on top of normal AODV routing protocol, achieves an overall good results.

Future Enhancement

For future work, the proposed protocol can be designed to secure other routing protocols like DSR, DSDV etc. and Intrusion detection scheme is not solved by this algoritm.

REFERENCES

[1] Er. Kamaljit Kaur*, Er. Amanpreet Kaur Chela "Simulation and Review of SAODV NS2 Simulation", IJESRT, [Kaur, 3(2): February, 2014.

[2] Sunil J. Soni, Suketu D. Nayak "Enhancing Security Features & Performance of AODV Protocol under Attack for MANET", 2013 International Conference on IntelligentSystems and Signal Processing (ISSP).

[3] Madhavi, S. and K. Duraiswamy "Flooding attack aware secure aodv" 2013.

[4] Er. Kamaljit Kaur, Er. Amanpreet Kaur Chela "Simulation and Review of SAODV NS2 Simulation",IJESRT. February, 2014.

[5] J Rajeshwar, Dr G Narsimha "A Comparative study on secure routing algorithms SAODV and A-SAODV in Mobile Ad hoc Networks (MANET)– The Enhancements of AODV, International Journal of Computers and Technology Volume 3 No 2, December 2012.

[6] Alekha Kumar Mishra, Bibhu Dutta Sahoo "A modified adaptive-saodv prototype for performance enhancement in manet", , April '09 – September '09, (IJ-CA-ETS).

[7] Durgesh Wadbude, Vineet Richariya "An Efficient Secure AODV Routing Protocol in MANET ",, (IJEIT) Volume 1, Issue 4, April 2012 **.**

[8] Savithru Lokanath, Aravind Thayur "Implementation of AODV Protocol and Detection of Malicious Nodes in MANETs", (IJSR**),** Volume 2 Issue 11, November 2013.

[9] Mr. Suketu D. Nayak, Mr. Ravindra K. Gupta "Sec.AODV for MANETs using MD5 with Cryptography", IJCTA | July-Aug 2011.

[10] V.K.Taksande, Dr.K.D.Kulat, "Performance Comparison of DSDV, DSR, AODV Protocol with IEEE 802.11 MAC for Chain Topology for Mobile Ad-hoc Network using NS-2", IJCA Special Issue on 2nd National Conference- Computing,

Communication and Sensor Network" CCSN, 2011.

[11] Basavaraj, Sannakashappanavar, C R. Byrareddy, Ravikumar M. Inamathi "Security Enhancement in AODV Routing Protocol for MANETs", , Int. J. on

[12] Sandhya Khurana Neelima Gupta Nagender Aneja "Reliable Ad-hoc On-demand Distance Vector Routing Protocol", 2006 IEEE.

[13] The Network Simulator – NS2. (http://www.isi.edu/nsnam/ns/index.html).

[14] The NS Manual, http://www.isi.edu/nsnam/ns.

[15] MANET,.http://www.ietf.org/html.charters/manet charter.

[16] Yuxia Lin, A. Hamed Mohsenian Rad,Vincent W.S. Wong, Joo-Han Song WMuNeP'05,"Experimental Comparisons between SAODV and AODV Routing Protocols, , October 13.

[17] Eitan Altman, Tania Jimenez; NS Simulators for Beginners; lecture notes 2003-2004.

[18] Mustafa Jasim AL-Jubori, Prof. S. S. Pawale,Prof. S. R. Shinde "Efficient Ad-Hoc On-demand Distance Vector Routing Protocol using Link State Algorithm", Vol 26– No.2, July 2011.

Author profile

Sudarsanan. D M.Tech (Ph.D) from Acharya Institute Of Technology Dept of ISE. 15 years of teaching experience. Published three international papers on different domain.

Megha J M.Tech in CNE from Acharya Institute Of Technology . published 3 papers in international journals on different domains.