Prof.Ravi Verma, Prof. Navneet Tiwari / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com

Vol. 2, Issue 1,Jan-Feb 2012, pp. 631-638

Comparative Study of Routing Mechanism for Ad Hoc Network

[1] Prof.Ravi Verma, [2] Prof. Navneet Tiwari

[1](Department of MCA, Mahakal Institute of Technology & Sciences, India)
[2](Department of MCA,Mahakal Institute of Computer Science & Technology,india)

Abstract-

As we knew that the current working routing protocols for ad hoc network are use shortest path routing .it include On Demand routing protocols such as DSR and AODV it provides Qos for traffic management but it cannot support Quality of Services for timely and guaranteed transmission of data packet. Ad hoc network is dynamic in nature therefore we cannot directly use wire line protocol and algorithm so that we have been designed a natural time management scenario for routing the data. Exiting work in routing in a ad hoc networks is presented in(1),where protocol manage the delay and delay and bandwidth constrained in routing, To make the decision it will uses the deterministic model for choosing the routing decision but this paper use a periodic time scheduled for making the routing communication fast and timely with no data loss. Due to the dynamic nature of ad hoc networking it is necessary for an organization that communication performance major should be there for reliability and network management so that performance major for finding routs (path) based on least cost routing using hop count performance will be major. In this paper we are handling the time quantum at each and every node of the ad hoc network it making the overheads but provide the services of confidentially reliable communication.

***Keyword*: DSR, AODV, Quality of Services, Ad Hoc Network, Time Quantum.**

I. INTRODUCTION TO NETWORK MODEL

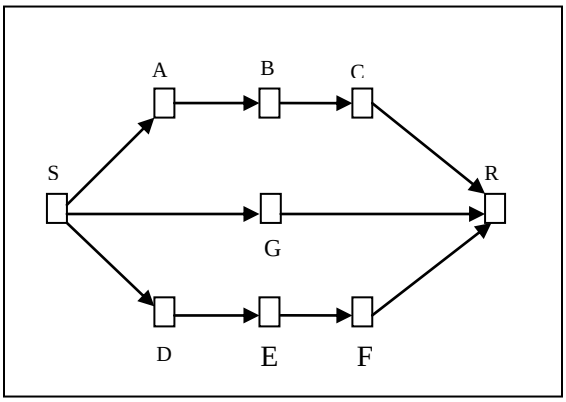
In the area of network management it is necessary to travel data packet as reliable as possible because we all know that how the reliable path and cost management can affect the network management system specially when we are working or making the confidential communication for an organization we have been designed a special time scheduled routing scheme to achieve the higher level of reliability maintenance in Ad Hoc Network but the difference between the existing mechanism is that this scheme will remain provides the major degree of reliability from the source to destination, its guarantees that data packet must be reach at the destination end in a timely manner because all the available nodes will working in a time management schedule so that packet should be reach in a less timely way no node will Longley wait for getting the rout all the host will perform the buffering to achieve the full duplex communication .

We can imagine that all the exiting routing algorithm and techniques provides the periodically transmission of data packet but if the rest of the node has no data item and packet to send then also the timer will be work for all the nodes available in the network as working it by default, it causes the time complexity higher which makes the network unreliable.

The timely transmission of data packet is the major requirement of each and every organization to get this aim we need to initialize node buffer in periodic manner after getting the buffer size they need to initialize the nodes. If node's buffer size is higher to the assigned time limit then data packets will be divided in time slot and sanded the packet as its time comes. The Networked model suggested for the requirement will work on the basis of the buffer size available at each node.

The proposed routing model will initialize the timer, buffer, node_event_bit at each source to destination node as:

```
initialize node (timer t, buffer b, event_bit b)
    {
    float min_timer=0, max_timer=60;
    float min_buffer=0,
    char node_event_bit;
    }
```



Figer1.1: 3 props to send data from S to R node(S →R)

In this network scenario each node will keep the buffer and timer parameter to take decision for sending the request to feasible node available at that time, when node S will send data to R ad hoc network will follow the routing as:

1. Initialize the entire available node with buffer size and according to the available buffer the timer will be initialized.
2. Node S found A, G, D as intermediate nodes.
3. Node S will use probabilistic model to choose the next node. In figure1.1 by the way of hop count technique the least cost route will S to G and G to R will be the best route to send data packet to node R but what happened if node G has already engaged with other transmission then source node S will check the buffer size of available node A and D :

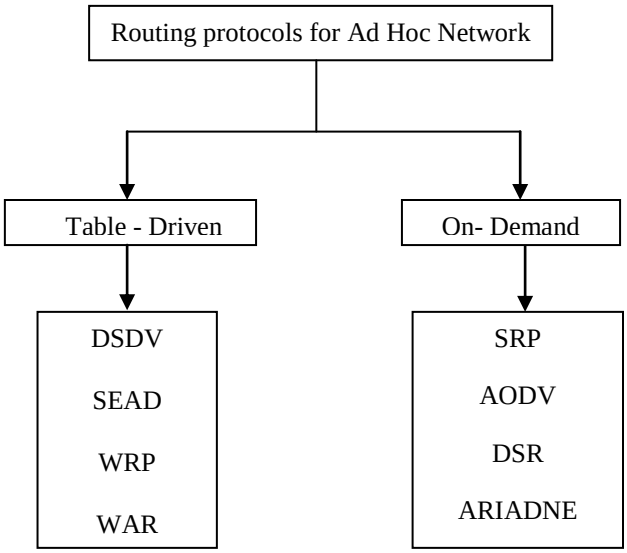
- If A's buffer Data < D's buffer Data then Node A will be the next node and Node_event_bit is set to A (Available).

  Else

- Node D will be the next node to send the data packet coming from Node S destined to Node R.

II. RELATED WORK

In the same scenario if we looking backward there are so many protocols work for routing in an Ad hoc network. We can have a practical example like "Routing in Manets" it's wonderful to work with Table Driven an On demand routing mechanism



In Table Driven to exchange routing information periodically to make consistent rout for routing with every other node in the network.

Ex: Dynamic Source routing(DSR)[2] is the implementation of Table Driven ad hoc routing it is similar to the connectionless approach to forward the data packets like UDP and IP here routing is completely relies on the routing information available on the routing table. It will not be in case

of On – Demand routing protocols. On-Demand creates a request called as Route Discovery whenever it needs to reach at Destination it create route accordingly to single time use. ADOV(Ad hoc On Demand Vector routing) [3] In On Demand routing techniques when an On demand protocol desires a new route for a new destination .it will have to wait until such a route can be discovered. On the other hand, because routing information is constantly propagated and maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed. This type of protocols maintains fresh lists of destinations this type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are –

1. Respective amount of data for maintenance.

2. Slow reaction on restructuring and failures.

On the other hand, the Reactive protocols find a route on demand by flooding the network with Route Request packets.

The main disadvantages of such algorithms are –

1. High latency time in route finding.

2. Excessive flooding can lead to network clogging.

A. Secure Routing Protocol (SRP)

It is proposed by Papadimitratos and Haas. SRP is applied as an extension of a multitude of existing RPs such as DSR [11] and ZRP [12]. This protocol counters the malicious behavior that guarantees the acquisition of correct topological information in a timely manner [10]. The protocol is proven robust against a set of attacks that attempt.
To compromise the route discovery. It provides the correct routing information regarding a pair of nodes provided they have prior security association. The source node initiates the route discovery by sending a Route Request (RREQ) packet (identified by a pair of identifiers, a query sequence number & a random query identifier) to the destination and replies are sent back strictly through the same route. SRP can only handle Black Hole attacks and not Worm Hole attacks. However, it can nevertheless prevent them.

B.Secure Efficient Ad-hoc Routing (SEAD)

It is a Distance Vector Routing Protocol based on Destination Sequences Distance Vector (DSDV) Ad Hoc Routing [13]. It is a lightweight secure routing protocol presented by Hu, Johnson & Perrig [9]. The designers of SEAD used efficient one-way Hash functions to provide authentication for both the sequence number and metric field

in each routing entry. They avoid asymmetric cryptography to protect against DoS attack and to overcome limited CPU processing capability. The receiver of the achieved either through Message Authentication Certificate (MAC) [14] or some broadcast authentication mechanism. It is too susceptible to Worm Hole attacks like SRP.

C. ARIADNE

It is another On-Demand Routing Protocol presented by Hun, Johnson & Perrig [2] based on DSR. It maintains authenticity on end-to-end basis, using symmetric key cryptography. It can authenticate routing messages using either shared secret keys, digital signatures or shared secrets
in combination with broadcast authentication like TESLA [15]. The Protocol enables the destinations to authenticate the Route Request sent by source node. The RREQ contains MAC which can be easily verified by the destination node. A per-hop hashing technique is used to verify that no node is missing from the node list [16]. Route maintenance is done using Distance Secure Routing (DSR) mechanism. However, Ariadne is very much immune to Worm Hole attacks through Clock synchronization between nodes, but not in all cases.

D.Authenticated Routing for Ad-hoc Network (ARAN)

It is presented by Dahill. It relies on a trusted certificate server. Every node forwarding a Route Request or Reply is required to sign the packet. It detects and protects against malicious actions carried out by 3rd party and peers [1]. It uses public key cryptography to obtain a public key
certificate from TCA. ARAN introduces authentication, message integrity and non-repudiation to an ad hoc environment as a part of a minimal security policy. The route maintenance is done through special error messages. The source code initiates and the route discovery packet that is verified by the destination before the RREQ is sent back. It prevents impersonation attacks by providing end-to-end and hop-to-hop authentication of route discovery & reply messages. It is also not capable to handle wormhole attacks

and the uses of asymmetric cryptography makes it more valuable to DoS attacks. All the routing messages are authenticated at every hop from source to destination as well as on reverse path from destination to source.

Ad Hoc On-Demand Distance Vector is based on On-demand mechanism that relieves nodes from frequently generating and storing route entries, but introduces a delay caused by the Route Discovery procedure [18, 19]. It finds routes only when required and hence is reactive in nature.

The major vulnerabilities present in AODV protocols are: Deceptive increase of sequence number and Deceptive decrease of hop count. Zapata [17] applies security extensions to AODV using one-way hash functions to serve metric fields in Route Request (Route Discovery). He Introduced Secure-AODV (SAODV) [18] where he suggests using digital signatures to authenticate non-mutable data in an end-to-end manner. Hash chains are used to secure mutable fields such as hop count. It is an extension to AODV Routing Protocol. It is used to protect Route Discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation.

Table1.1
Comparison of Main Ad Hoc Routing Protocols

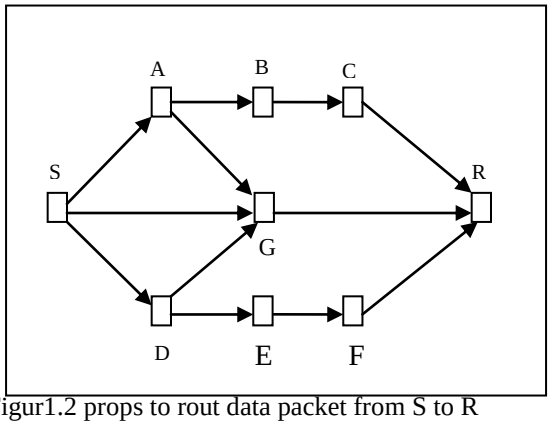
Parameters	DSDV	AODV	DSR
Reactive	No	Yes	Yes
Multiple Routes	No	No	Yes
Loop Free	Yes	Yes	Yes
Distributed	Yes	Yes	Yes
QoS Support	No	No	No
Periodic Update	Yes	Yes	No
Multicast	No	Yes	No

III. PROBABILISTIC MODEL FOR ROUTING DECISION

As we have discuss all the above mention protocols that no one will support the quality of services in Ad Hoc Routing as in table 1.1

All the protocols have been provides the services commonly used for routing but here we are proposing the "Decision Making Model" Named as probabilistic model for making the decision on the basis of QoS in Ad Hoc Network it provides:

- Time Slot Management among the entire available node in Ad Hoc Network.
- In the case of congestion it reduces the long term wait for travel the data packet.
- Probabilistic model takes the decision based on the Node's buffer size and assigned time slot to the node for routing.
- Route the data packet basis the routing table made by probabilistic model.
- This model compute the time and space complexity better than others available protocols of O(n).
- Periodically it updates the table after making the buffer computation.



Figur1.2 props to rout data packet from S to R

As fig 1.2 show that when hop S will send data packet destined to R they need to analysis his rout table, table contains the best route for the point of view of buffer size and allocated time slot.

Here our probabilistic model is working as a router to taking the best route for delivery basis on the computation of buffer

size. fig 1.3 shows that Hop S has three routes for sending the data packet to R that is:

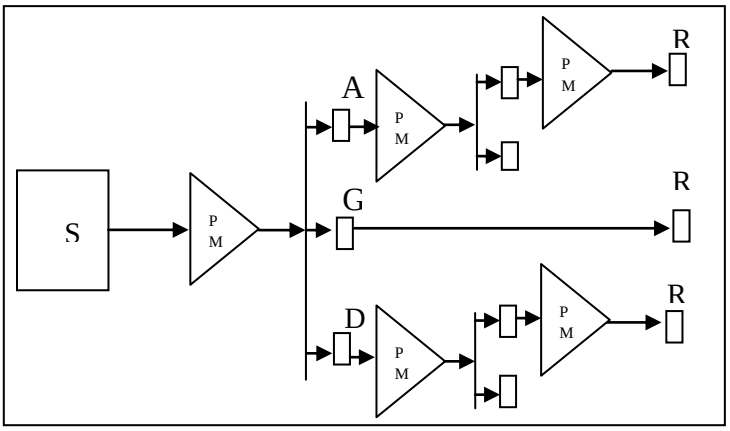
- S →A, A→B, B→C, C→R.
- S→G, G→R.
- S→D,D→E,E→F,F→R

I. The Source Node S will choose Node A as the next node if and only if the buffer size of A's is less than the buffer size of node G & D. i.e. Buffer of A<buffer of G and D.

II. Similarly if Node S found G and D will have lower buffered then A, it will deliver accordingly.

III. In the case of contention if S found the entire node's are busy with higher amount of delivery request then S follow the Hop count technique to choose the next node as

IV. Fig.1.2 shows node G will be chosen.

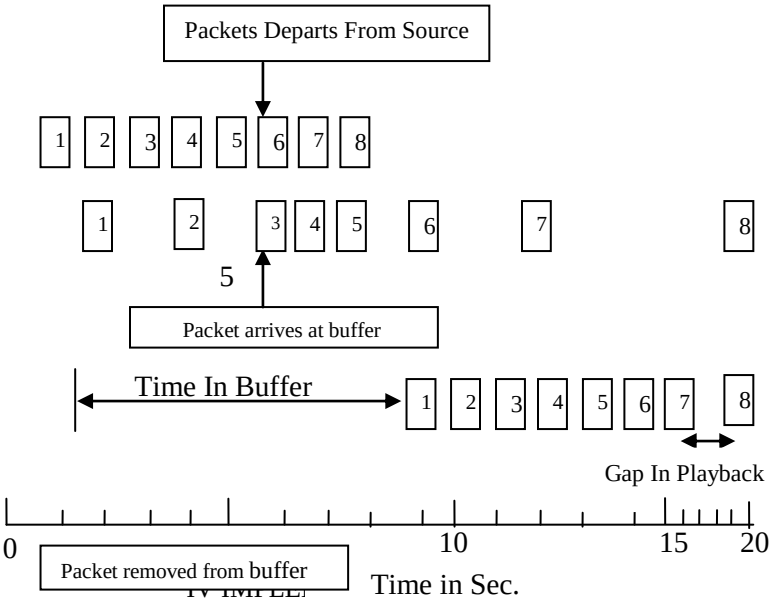


Figur1.3 Probabilistic Model

Here PM= Probabilistic Model, S= Source Node R= Destination Node

Buffering: Flows can be buffered on the receiving side before being delivered. Buffering then does not affect the reliability or bandwidth and increases the delay, but it smoothes the jitter. For audio and video on demand jitter is the main problem so this technique helps us out.

In following figer1.4 we see a stream of packets being delivered with substantial jitter. Packet 1 is sent from the server at t = 0 sec and arrive at the client at t = 1 sec Packet 2 undergo more delay and takes 2 sec to arrive. As the packet arrives, they are buffered on the client machine.



Figer1.4 Buffering of Data Packets

Here we are presenting the policy for the implementation of the proposed paper, it will describes the introductive point of view for both of the side either it is sender or receiver. Sender modules follows the steps as following and initialize the entire upcoming node who can be the next or best node's for routing.

```
#define Max_Seq 1
Typedef enum {frame_arrival,cksum_err,timeout}
event_type
#include"protocol.h"
Void sender (void)
{
Send_ne next_frame_to_send;
Frame s;
Packet buffer;
Event_type event;
Next_frame_to_send=0;
From_network_layer(&buffer);
While(true)
{
s.info=buffer;
```

```
s.seq=next_frame_to_send;
to_physical_layer(&s);
start_timer(s.seq);
wait_for_event(&event);
if(event==frame_arrival)
        {
        From_physical_layer(&s);
        if(s.ack==next_frame_to_send)
        {
        Stop_timer(s.ack);
        From_network_layer(&buffer);
        Inc(next_frame_to_send);
        }
        }
}
}
```

After the completion of the above procedure sender will be relaxed and call the initialize_node () subroutine to initialize all the other route node, now our proposed probabilistic module will perform buffer computation for all the available node and select as a next node who has less buffer then other ,if any case it found more than one node have same less size buffer then it perform hop

Counting techniques between those nodes's. Following steps will used in the beginning of the connection establishment.

```
Initialize node (double c,timer t, buffer b, event_bit b)
{
If (b<available_buffers) then
c=count(buffer b);
goto void receiver();
endif
}
```

When sender system will found the best node for the point of view of time and space complexity by performing the probabilistic computation data will be sanded to the required destination system with the quality of service support which is not available in any protocol mentioned in Table 1.1.

Now the receiver system will use the following code to get the data packet from the source system.

```
Void receiver(void)
{
Seq_nr frame_expected;
Frame r,s;
Event_type event;
Frame_expected-0;
While(true)
{
Wait_for_event(&event);
If(event==frame_arrival)
        {
        From_physical_layer(&r);
        If(r.seq==frame_expected);
        {
        To_network_layer(&r.info);
        Inc(frame_expected);
        }
        s.ack=1-frame_expected;
        to_physical_layer(&s);
        }
}
}
```

V. CONCLUSION

Traditional routing algorithm and protocol as mentioned in table 1.1 can't meet the need of Routing with Qos support .Our research is different from the traditional mechanism by performing the buffer size computation and the allocation of time slot on the bases of buffer computation discussed in implementation policy, it will meet the requirement of reliable routing in "Ad Hoc Network". Actually Ad Hoc Network can be the part of any intranet also requires contentionless routing without long delay means Qos is essentially required, to make it possible we have present the buffering mechanism in "Probabilistic Model" provides routing with Qos in Ad Hoc Network.

In probabilistic model every time source node will perform the buffer computation and make routing table basis on the result of computation, Node contain less buffer size will be the first priority node for the source node, similarly until the data packet should not reach to the correct destination node the same computation will be done by each and every mediator node to make the routing efficient.

REFERENCES

[l] S. Chen, and K Ndustedt. "Distributed *QoS* Routing in ad hoc Networks." IEEE joumal on Selected Areas in Communication, August 1999.

[2] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2002.

[3] Janne Lundberg, Routing Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security,

[4] Y.C. Hu, D.B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," IEEE, Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), 0-7695-1647-5, 2002.

[5] 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), Jan 2002.

[6] D.B. Johnson, D.A Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," Ad Hoc Networking, C.E. Perkins, Ed., Addison-Wesley, 2001, 139-172.

[7] Z. J. Haas, M. Perlman, "The Performance of Query Control Schemes of the Zone Routing Protocol" IEEE/ACM Transactions on Networking, vol. 9, no. 4, pp. 427-438, Aug 2001.

[8] C.E. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) for Mobile Computers," Proc. ACM Conf. Communications Architectures and Protocols (SIGCOMM'94), London, UK, August 1994, pp. 234-244.

[9] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, February1997.

[10] Vesa Karpijoki. Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security.

[11]http://citeseer.nj.nec.com/karpijoki01securityhtml.2000. G.V.S. Raju and Rehan Akbani, "Some Security Issues in Mobile Ad-hoc Networks," in proceedings of the Cutting Edge Wireless and IT Technologies Conference, November 2004.

[12]http://citeseer.nj.nec.com/karpijoki01security.html.2000. G.V.S. Raju and Rehan Akbani, "Some Security Issues in Mobile Ad-hoc Networks," in proceedings of the Cutting Edge Wireless and IT Technologies Conference, November 2004.

[13] Manel Guerrero Zapata. "Secure ad hoc on-demand distance vector (SAODV) routing". IETF MANET Mailing List, Message-ID3BC17B40.BBF52E09@nokia.com,

[14]ftp://MANET.itd.nrl.navy.mil/pub/MANET/2001-10.mail, October 8,2001.M. Zapata, N. Asokan, "Securing ad hoc routing protocols",WiSe'02, ACM 1-5813-585-8, September 28, 2002, pp.1-10.

[15] C.E Perkins, E.M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.

[16] Young-Bae Ko and Nitin Vaidya. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In *Proceedings of the Fourth ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98)*, pages66–75, October1998.

[17] John Kohl and B. Clifford Neuman. The Kerberos Network Authentication Service (V5). RFC 1510, September 1993.

[18] B. Kumar. Integration of Security in Network Routing Protocols. *SIGSAC Review*,11(2):18–25, 1993.

[19] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, and Jorjeta G.Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In *Proceedings of the Fourth ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98)*, pages 85–97, October 1998.

[20] Michael Brown, Donny Cheung, Darrel Hankerson, Julio Lopez Hernandez, Michael Kirkup, and Alfred Menezes. PGP in Constrained Wireless Devices. In *9th USENIX Security Symposium*, pages 247–261, August 2000.

[21] Steven Cheung. An Efficient Message Authentication Scheme for Link State Routing. In *13th Annual Computer Security Applications Conference*, pages 90–98, 1997.

[22] Steven Cheung and Karl Levitt. Protecting Routing Infrastructures from Denial of Service Using Cooperative Intrusion Detection. In *The 1997 New Security Paradigms Workshop*, pages 94–106, September 1998.

[23] Tom Clark. Tom Clark's Totally Accurate Clock FTP Site. Greenbelt, Maryland. Available at ftp://aleph.gsfc.nasa.gov/GPS/totally.accurate.clock/.

[24] D. Coppersmith and M. Jakobsson. Almost Optimal Hash Sequence Traversal. In *Proceedings of the Fourth Conference on Financial Cryptography (FC '02)*, Lecture Notes in Computer Science, 2002.

[25] Bridget Dahill, Brian Neil Levine, Elizabeth Royer, and Clay Shields. A Secure Routing Protocol for Ad Hoc

Networks. Technical Report UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan, August 2001.

[26] T. Dierks and C. Allen. The TLS protocol version 1.0. RFC 2246, January 1999.

[27] Eran Gabber and Avishai Wool. How to Prove Where You Are: Tracking the Location of Customer Equipment. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pages 142–149, November 1998.

[28] Ralf Hauser, Antoni Przygienda, and Gene Tsudik. Reducing the Cost of Security in Link State Routing. In *Symposium on Network and Distributed Systems Security (NDSS '97)*, pages 93–99, February 1997.

[29] Andy Heffernan. Protection of BGP Sessions via the TCP MD5 Signature Option. RFC 2385, August 1998.

[30] Yih-Chun Hu and David B. Johnson. Caching Strategies in On-Demand Routing Protocols for Wireless Ad Hoc Networks. In *Proceedings of the Sixth Annual IEEE/ACM International Conference on Mobile Computing and Networking (MobiCom 2000)*, pages 231–242, August 2000.

Er. Ravi Verma: He has completed his MCA from Vikram University Ujjain India and M. Tech from Singhaniya University Jaipur Rajasthan , India in Computer Science and Engineering .Now he is doing Phd. In Computer Science and Engineering. My interested research area is Ad Hoc Network. Presently He is working as a lecturer at MITS Ujjain India.