Performance Improvement of DYMO Routing Protocol using Gateway Authentication Technique

Rajesh Gargi
Associate Professor
IIET, KINANA(JIND)
Purusing PHD, GJUST(HISAR)

Yogesh Chaba
Prof. Department of CSE
GJUST, HISAR

R. B. Patel
Prof. & Head
G.B.P.E.C.
Pauri Garwal

ABSTRACT

A hybrid Mobile AdHoc Network (MANET) is provided by gateways (GWs), which connect the MANET to the Internet. Hybrid MANETs are vulnerable to more security threats while routing through the gateways. To guarantee secure hence efficient data routing and transmission, In this paper, we propose to design a data aware secure gateway selection technique for hybrid MANET. In our technique, gateway is classified into two categories as public gateway and protected gateway. Protected gateway can route both public and protected data. Conversely, public gateway can only route public data. Among multiple gateways, a gateway is elected using multi criteria gateway selection strategy. Protected gateway and mobile nodes are authenticated using Extensible Authentication Protocol (EAP). By simulation results, we prove the performance of our technique. This gateway authentication technique improves the routing performance of MANETs.

Key Words:

Hybrid MANETs, EAP, Protected gateway

1 INTRODUCTION

1.1 Hybrid Manet

Hybrid MANET is imparted by the gateways (GWs) connecting the MANET with the internet which also gives advanced communication, network scalability, and pervasive sustainable environments. Studies related to GW management, mobility management, addressing, and routing are undergone in the hybrid MANETs. Additionally, logical and technological developments are needed for robust interconnection [1].

With the fixed internet gateways (IGWs), the hybrid MANET provides internet access to the MANET nodes. It also exploits mobility capability of additional mobile nodes (mobile IGWs). The benefits of the proactive and reactive approaches are also balanced by the hybrid approach. The dynamic network topology leads to uncertainty in the connectivity of the mobile nodes with gateway nodes and mobile nodes with other active mobile nodes. In the local MANET, there is a delay in finding route to destination due to the mobility of mobile nodes. [2]

1.2 Gateway Selection

When a mobile node sends a data packet to fixed network, the packets are transmitted to the gateway, which acts as a bridge between a MANET and the Internet. On receiving RREQ, the gateway cross checks with the routing table for destination IP address which has been précised in the RREQ message. If the address is not found, then gateway sends RREP_I flag to the originator, else it unicast a normal RREP, but may also optionally send a RREP_I back to the originator of the RREQ. [3]

Proactive Gateway Discovery, Reactive Gateway Discovery, Hybrid Gateway Discovery, Adaptive Gateway Discovery, and Maximal Benefit Coverage are the various gateway discovery processes.

- **Proactive Gateway Discovery:** Gateway broadcasts a Gateway Advertisement message after each interval. Mobile nodes in the gateway's transmission range receive the advertisement and those without the route to the gateway, builds a route entry for it in their routing tables.
- **Reactive Gateway Discovery:** By performing expanding ring search, the node willing to communicate with the network will contact it within the ad hoc network. A new route is found towards the Internet, if there is no reply after the search.
- **Hybrid Gateway Discovery:** The TTL-limited messages are flooded by the gateways, which will be forwarding only up to few hops away from the gateway. Proactive approach has been carried out by the sources within flooding area and outside that, it acts as reactive.
- **Adaptive Gateway Discovery:** Information is easily provided by the gateway only if it is routing those datagrams that it would receive anyway. In addition, the number of hops of its active source location is maintained.
- **Maximal Benefit Coverage:** The overhead of flooding GWADV messages up to t hops plus the overhead associated to the discovery of gateways by sources at distances longer than t hops can be minimized by selecting a TTL t. When multiple nodes are discovered for internet access, the Internet gateway selection is used. We have to choose a metric for selecting the right gateway. [3]

1.3 Security Issues in Hybrid MANET

The characteristics of MANET such as mobility, dynamic topology changes and lack of infrastructure make security a challenging task. A wide variety of security risk namely eavesdropping, message modification attack, denial of service attack, insider attack paves way for a malicious node to threaten the network. Hence, an efficient security mechanism is essential to secure the MANET. In hybrid MANET, we can make use of gateway (GW) to implement the security mechanism. [4]

In hybrid MANET access network paradigm, one of the key attributes to maintain the infrastructure is authentication and authorization. Using authorization and authentication process, nodes that are authenticated are permitted to transmit and communicate bidirectionally with other network hosts. [5]

Lack of security can allow a malicious node in the network to forward the corrupted data, injecting of false or uncompleted information, overwhelms the network without forwarding the data packets and to fabricate the a route advertisement. [6]

Implementing security mechanism in hybrid MANET is a daunting task, as the network some times connected to the Internet and some times may be stand alone. That is the temporary hybrid behavior of the network brings difficulties in security. [7]

1.4 Problem Identification

A novel gateway selection protocol is proposed by Takeshi Matsuda et al. [4] Their routing protocol permits the source node to transmit sensitive data to the Internet through the secure/trusted GWs. They have considered these sensitive data have more possibility of susceptible risks such as information leak and data falsification. The main drawback of this paper is that the authors have only discussed of selecting the gateway but not about the secured gateway. Therefore, by applying the concept of paper [5] in the above concept we can overcome the drawback of security.

In this paper, a Secure Gateway Authentication Technique for Hybrid MANETs has been implemented.

2. RELATED WORKS

Takeshi Matsuda et al. [4] have proposed a novel gateway (GW) selection protocol in hybrid Mobile Ad hoc Networks (MANETs). Their routing protocol permits the source node to transmit sensitive data to the Internet through the secure/trusted GWs. They have considered these sensitive data have more possibility of susceptible risks such as information leak and data falsification. They have implemented their technique in Dynamic MANET On-demand (DYMO) protocol. They have assumed that the data is transmitted through the secure channel but they do not provide any secure mechanism to authenticate mobile nodes and secure gateways.

Rayala Upendar Rao et al. [8] have introduced a new secure mechanism. Their mechanism makes use of Elliptic Curve Cryptography (ECC) with DYMO routing protocol. By using ECC, their mechanism has incorporated access control mechanism and this ensures the confidentiality and authentication. Their mechanism also notifies the resource consumption attack and alleviates by informing to other routing AGENT node about its identity and bootstrapping time. Their mechanism requires less memory, provides great security and perfectly suitable for low power devices like mobile nodes

Pedro Miguel Ruiz Martinez et al. [5] have proposed a utility-based optimized control scheme for the selection of the gateways to pre-authenticate. Initially, their scheme finds a trade-off between the benefit of the pre-authentication and the cost in terms of control overhead. Their goal is to allow the Internet gateways to accept only authorized traffic without jeopardizing the overall network performance. They have proposed a preauthentication process to minimize the delay that occurs in authentication process.

Shahid Md. Asif Iqbal et al. [9] have proposed a new gateway discovery and selection scheme. In their scheme, the gateways in the network advertise gateway advertisement messages only on-demand. It contains the advertisements within a limit in order to make our scheme scalable. The authors have also considered the interface queue length and the total number of neighbors along a route in addition to the hop count to bypass the loaded and dense route to the gateways in order to reduce the delay and packet loss. The disadvantage of this paper is that if the current load is higher and new Internet traffic is directed towards this gateway by a gateway selection algorithm at the MANET nodes, which does not consider the current traffic at the gateway, the new Internet traffic at the heavily loaded gateway might increase serious congestion in the network.

Guofang Nan et al., [10] have presented a load-balancing strategy and security routing protocol for a multi-gateway architecture called dynamic gateway. Their dynamic gateway approach selects an optimal gateway and a foreign agent. Further, to assure secure operation they have also proposed secDSDV (Secure Destination Sequenced Distance Vector) authenticated routing protocol. Their proposed mechanism provide authentication to the transmission with the use of public-key cryptographic mechanisms.

3. SECURE GATEWAY AUTHENTICATION FOR HYBRID MANETS

3.1 Overview

In this paper, a technique named Secure Gateway Authentication for Hybrid MANETs have been modified. This technique differentiates the data as public and protected based on necessity of data. Correspondingly, gateway is categorized into two types namely, public gateway and protected gateway. Protected gateway can transmit both public and protected data. Conversely, public gateway can only transmit public data. Among multiple gateways, a gateway is elected using multi criteria gateway selection strategy. To transmit public data, the source and destination use puRREQ and puRREP messages for discovering the route. While transmitting public data, both protected and public gateway does not require any authentication techniques. For transmitting protected data, the source and destination makes use of prRREQ and prRREP messages. Before transmitting protected data, mobile nodes and private gateways are authenticated using Extensible Authentication Protocol (EAP). Upon successful authentication, protected data are transmitted over protected gateway.

3.2 Route Discovery Technique

In our approach, we differentiate the data into two types as protected and public data. This classification is performed concerning security. In the same way, we also categorize the gateways into two namely, protected gateway and public gateway. The information that requires privacy and confidentiality is known as protected data. This includes sensitive information such as emergency information, government records and medical records. On the other hand, general information such as news, weather and advertisements are known as public data. Protected data are transmitted in the hybrid network using protected gateway and public data are transmitted through public gateway.

Table – 1 IP Header

Version (4 bits)	Header Length (4 bits)	Type of Service (8 bits)	Total Length (16 bits)
Identification (16 bits)	Flags (3 bits)	Fragment Offset (13 bits)	
Time To Live (8 bits)	Protocol (8 bits)	Header Checksum (16 bits)	
Source Address (32 bits)			
Destination Address (32 bits)			
Options and Padding (Multiples of 32 bits)			

The transmitting data can be recognized using type of service field in IP header. This field is generally used in the IP header to prioritize the data packets. The format of IP header is given above in table-1.

Based on type of data transmitted we have also differentiated route discovery message packets. If the source needs to send protected data, it use prRREQ and the destination replies using prRREP messages. Alternatively, the source and destination use puRREQ and puRREP for transmitting public data. To distinguish the route discovery packet as public and private we append a binary bit in the route discovery packet. Bit 0 symbolize that the route discovery message is either puRREQ or puRREP and bit 1 denote the protected message discovery packets namely prRREQ and prRREP. The format of route request message is given below in table-2.

Table-2 Format of Route Request Message

Source ID	**Dest ID**	**Reqt ID**	**Source Seq No**	**Dest Seq No**	**Hop Count**	**Type of Data** **(0/1)**

While route discovery messages are traversed in the network, each intermediate node distinguishes the data using type of data field.

3.3 Gateway differentiation

As one considers the hybrid MANET, the network consists of multiple gateways. In that, during deployment some gateways are categorized as protected gateway (prGW) and others as public gateway (puGW). The prGWs can transmit both protected and public data and puGWs can transmit only public data. The architecture of hybrid MANET is shown below in figure-1,

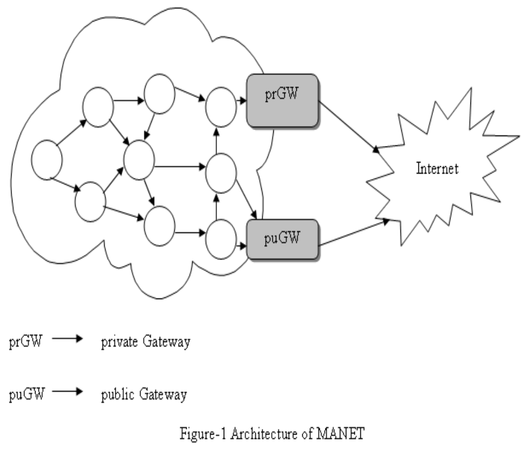

Figure-1 Architect of Manet

Transmission of public data through prGW does not require any authentication but transmission of protected data through prGW requires authentication phase. Authentication of prGW with mobile nodes is performed using preauthentication and utility function. For performing the authentication process, each prGW employs Extensible Authentication Protocol (EAP). The EAP contain a authenticate server that validates the nodes information. In preauthentication process, each node initiates the authentication process before it starts transmission.

The process of authenticating prGW and mobile nodes is as follows,

(i) Each prGW periodically broadcasts GW-HELLO message to all nodes in the network. The GW-HELLO message encompasses of network information such as gateway IP address, hopcount and EAP authenticator IP address. Hop count is the distance between mobile node and the gateway.

(ii) While receiving GW-HELLO message from internet gateways, each node creates the set of private gateways.

(iii) Once the gateway set has prGW> 1, the node starts preauthentication phase.

3.3.1 Preauthentication Process

During deployment, nodes that are declared as prGW take part in preauthentication process. Since, puGW transmits public data, they does not require any preauthentication process. The systematic process of preauthentication is as follows,

Step-1

The EAP authenticator in GW periodically sends GW-HELLO message to the nodes in the network. GW-HELLO message includes the gateway information.

Step-2

Nodes that accept GW-HELLO message reply back to the corresponding gateway by sending GW-REP message. GW-REP message enclose nodes information.

Step-3

Upon receiving the GW-REP message from the node, the authenticator forwards the node information to the authenticating server.

Step-4

From the derived information if gateway and node, the authenticator forwards Master Session Key (MSK) to the gateway and the node.

Step-5

By authenticating the MSK, both node and gateway receives two transient keys (TSK1, TSK2), which is used for further authentication.

Step-6

Each node stores MSK, TSK1 and TSK2 values of corresponding gateway

On completion of preauthentication process, each node has shared transient keys with corresponding prGW. These shared keys are used for authenticating a node and a gateway

3.4 Data Transmission

Consider that the source and destination are in different networks. When the source desires to transmit data to the destination, it first checks for the type of data to be transmitted. If the transmitting data belongs to public data, it selects a puGW from multiple puGW using multi criteria gateway selection strategy described in our previous paper. Through the selected puGW, the source discovers the route by flooding puRREQ message. The destination replies to the source using puRREP message. This transmission does not require authentication technique.

Algorithm

```
If (Type of Data = Public)
Then
    1 The node selects the puGW using multi criteria gateway selection strategy.
    2 The source use puRREQ message
    3 The destination use puRREP message
    4 Route discovery and data transmission are accomplished over selected puGW
Else if (Type of Data = Protected)
Then
    1 The node selects the prGW using multi criteria gateway selection strategy
    2 The source use prRREQ message
    3 The destination use prRREP message
    4 Route discovery and data transmission are accomplished over prG
End if
End if
```

Algorithm ends

When the data belongs to protected data type, the source selects the protected gateway multi criteria gateway selection strategy. Then it transmits gateway request to the selected prGW1, the source encrypts the gateway request using TSK1.

$$\text{The Source} \xrightarrow{E(GATEWAYREQUEST)} \text{prGW1}$$

On receiving gateway request, the prGW1 decrypts the gateway request using TSK2 and replies to the source node.

$$\text{The Source} \xleftarrow{GATEWAYREPLY} \text{prGW1}$$

The source discovers the route to the destination using prRREQ message. Each intermediate node transmits the prRREQ packet towards destination. The destination replies the source using prRREP. Here, route discovery and data transmission are performed through the authenticated prGW1. Thus, our technique provides security for gateway as well as protected (sensitive) information.

4. SIMULATION RESULTS

4.1 Simulation Setup

Efficient Secure Gateway Authentication DYMO (SGA-DYMO) extension protocol was evaluated through NS2 [11] simulation. NS2 version 2.28 with DYMO extension was used. A hybrid network deployed in an area of1200 X 1200 m was considerded. There are 15 mobile nodes in the MANET domain. There are 5 gateway nodes connected with a fixed internet host through a router (ref. fig 2).

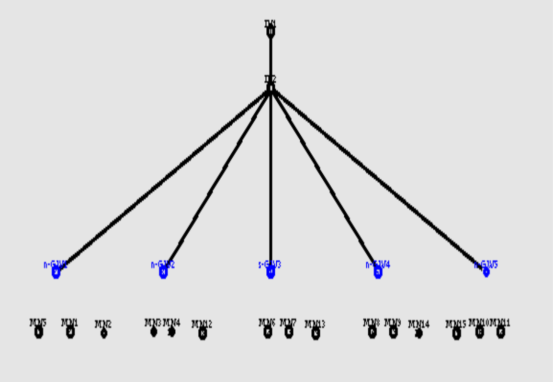

Figure 2: Simulation Topology

The simulated traffics are CBR and FTP. We have varied the traffic flows to increase the traffic load in the network. The following table summarizes the simulation parameters used.

Table 3: Simulation Settings

Mobile Nodes	15
MAC protocol	802.11
Propagation Model	TwoRayGround
Area Size	1200 X 1200
Simulation Time	50 seconds
Radio Range	250m
Wired Nodes	2
Gateway nodes	5
Traffic Source	CBR and TCP
Packet Size	512
Data Rate	250Kb

Mobility Model	Random Way Point
Speed	5m/s to 25m/s
Initial Energy	5.1 J
Transmit Power	0.66 Watts
Receiving Power	0.0695 Watts
Idle Power	0.035 Watts
Traffic Flows	1,2,3,4&5

4.2 PERFORMANCE METRICS

According to the following metrics the performance was evaluated

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Energy Consumption: It is the average energy consumption of all nodes in sending, receiving and forward operations

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Drop: It is the average number of packets dropped during the transmission.

SGA-DYMO protocol was compared with the normal DYMO protocol. The simulation results are given in the next section.

4.3 RESULTS

A. Based on Speed

A attack scenario was introduced in which a malicious node disturbs the normal flows by launching DDoS attacks and collision attacks. In order to validate the gateway selection process in terms of mobility, we vary the speed as 5,10,15,20 and 25 m/s.

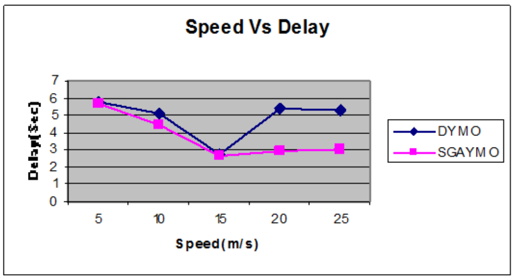

Fig 3: Speed Vs Delay

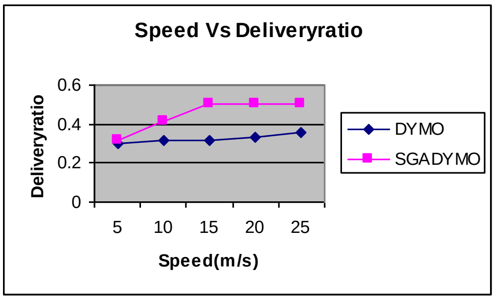

Fig 4: Speed Vs Delivery Ratio

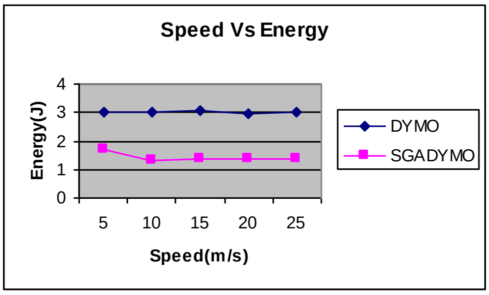

Fig 5: Speed Vs Energy

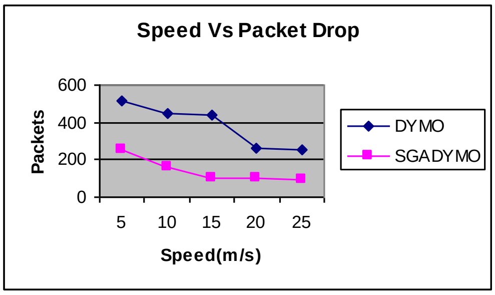

Fig 6: Speed Vs Packet Drop

Since SGADYMO involves secure authentication, attacks due to malicious nodes will be eliminated and hence the **packet drop** is very much reduced. As shown in Figure 6 the packet drop is less in SGADYMO when compared to DYMO. Since the packet drop is reduced, the **packet delivery ratio** is increased. Figure 4 shows the result packet delivery ratio for the proposed SGADYMO protocol is significantly more when compared with DYMO. Our protocol also performs better when compared in terms of **delay** as evident from figure3

Since **Residual Energy** is considered as one of the metrics for selecting the GW, the energy consumption in SGADYMO is less when compared with the normal DYMO protocol. One can observe this from Figure 5.

B. Based on Attacker

In order to see study the performance of the protocols in presence of attackers, we vary the number of attackers from 1 to 5.

As it can be seen from figure 8, when the no. of attackers is increased, the packet drop tends to increase. Since SGDYMO involves secure authentication, attacks due to malicious nodes will be eliminated and hence the packet drop is very much reduced, when compared to normal DYMO. The packet drop for SGDYMO is reduced up to 38% when compared to DYMO

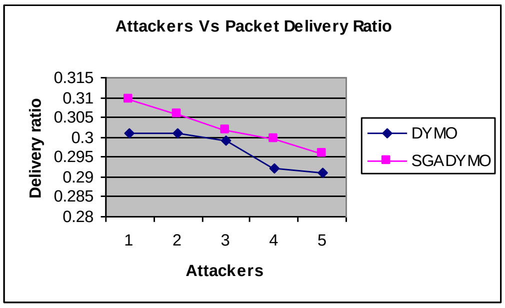

Fig 7: Attackers Vs Packet Delivery Ratio

Figure 7 shows the result of packet delivery ratio for the proposed SGADYMO and DYMO protocols. When the no. of attackers is increased from 1 to 5, the packet delivery ratio tends to decrease. The packet delivery ratio for the proposed SGADYMO protocol is 4.5% more when compared with DYMO.

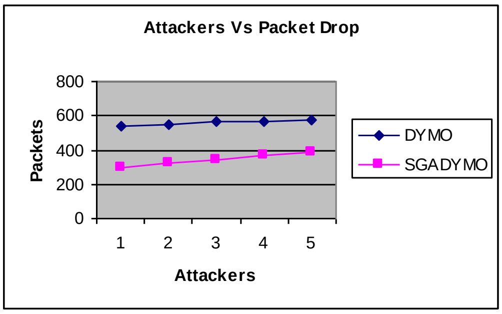

Fig 8: Attackers Vs Packet Drop

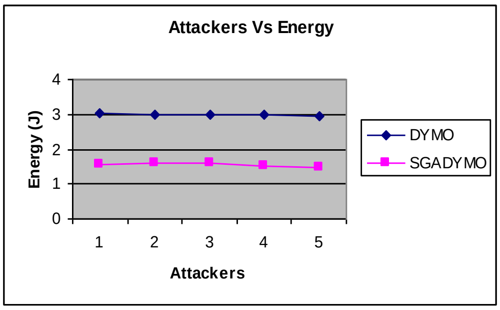

Fig 9: Attackers Vs Energy

Figure 9 shows the result of energy consumption for both DYMO and SGADYMO protocols when the attackers are increased. Since residual energy is considered as one of the metrics for selecting the IGW, the energy consumption in SGADYMO is 47% less when compared with the normal DYMO protocol.

5. CONCLUSION

In this paper, a Secure Gateway Authentication Technique for Hybrid MANETs have been proposed. While routing gateways are classified into two categories as public gateways and protected gateways. Gateways are selected using multi criteria gateway selection strategy. To transmit public data, the source and destination use puRREQ and puRREP messages for discovering the route. While transmitting public data, both protected and public gateway does not require any authentication techniques. For transmitting protected data, the source and destination makes use of prRREQ and prRREP messages. Protected gateway and mobile nodes are authenticated using Extensible Authentication Protocol (EAP). By simulation results, this protocol is evaluated using Packet Delivery Ratio, Packet Drop, Delay and Residual Energy. It is proved that our protocol performs better when we vary the speed and number of attackers. This improvement in performance can vary from 4.5% to 47% depending on the case under consideration. Hence the performance of this technique was proved.

6. REFERENCES

[1] Takeshi Matsuda · Hidehisa Nakayama, Xuemin (Sherman) Shen · Yoshiaki Nemoto, Nei Kato "Gateway Selection Protocol in Hybrid MANET Using DYMO Routing" Springer -Mobile networks and applications, May 2009.

[2] Velmurugan Ayyadurai1 and Rajaram Ramasamy "Internet Connectivity for Mobile Ad Hoc Networks Using Hybrid Adaptive Mobile Agent Protocol" The International Arab Journal of Information Technology, Vol. 5, No. 1, January 2008.

[3] Kamaljit I. Lakhtaria and Prof. Bhaskar N. Patel "Comparing Different Gateway Discovery Mechanism for Connectivity of Internet & MANET" International Journal of Wireless Communication and Simulation .2010

[4] Takeshi Matsuda · Hidehisa Nakayama · Xuemin (Sherman) Shen · Yoshiaki Nemoto · Nei Kato "Gateway Selection Protocol in Hybrid MANET Using DYMO Routing", Springer Science + Business Media, LLC 2009

[5] Pedro Miguel Ruiz Martinez∗,†, Rafael Marin Lopez, Francisco J. Ros and Juan A. Martinez "Enhanced access control in hybrid MANETs through utility-based pre-authentication control", Wireless Communications and Mobile Computing, 2008

[6] Yasir Abdelgadir Mohamed and Azween B. Abdullah, "Immune-Inspired Framework for securing Hybrid MANET", IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), October 4-6, 2009, Kuala Lumpur, Malaysia

[7] Jose L. Munoz, Oscar Esparza, Carlos Ganan and Javier Parra-Arnau, "PKIX Certificate Status in Hybrid MANETs", Proceedings of the 3rd IFIP WG 11.2 International Workshop on Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks, (WISTP '09), pp-153 – 166, 2009

[8] Rayala Upendar Rao and Daranasi Veeraiah "Secure Mechanism for DYMO Routing Protocol by using Elliptic Curve Cryptography in Mobil Ad-hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 31– No.11, October 2011

[9] Shahid Md. Asif Iqbal and Md. Humayun Kabir "Hybrid Scheme for Discovering And Selecting Internet Gateway in Mobile Ad Hoc Network", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011

[10] Jinhua Zhao, Ling Wang, Yoohwan Kim, Yingtao Jiang, Xiaozong Yang "Secure Dynamic Gateway to Internet Connectivity for Ad-hoc Network", International Journal of Information Technology Vol. 11 No. 2 ,2006

[11] Network Simulator, http://www.isi.edu/nsnam/ns

AUTHOR'S PROFILE

Dr Yogesh Chaba received the B.E. degree in Computer Sc. & Engg with DISTINCTION from Marathwada University, Aurangabad in year 1993. He obtained his MS degree in Software Systems from BITS Pilani and PhD degree from Guru Jambheshwar University of Science & Technology, HISAR. He is working as Associate Professor in Deptt of

Computer Sc. & Engg, Guru Jambheshwar University of Science & Technology, HISAR. He worked as Chairman, Deptt of Computer Sc. & Engg, Guru Jambheshwar University of Science & Technology, HISAR for three years. His Research areas are Computer Networks and mobile communication. He has published more then 75 papers in national and international journals and conferences of repute including IEEE, Springer and Science Direct Journals. He is Principal Investigator of two major research projects funded by All India Council for Technical Education and University Grants Commission, INDIA in the area of Network Security and Ubiquitous. He is also Deputy Coordinator of SAP project funded by University Grant Commission. He has vast international exposure as he has visited different universities and research institutions in USA, UK and China for academic assignments. He is also recipient of "Young Scientist Award" by International Academy of Physical Sciences for year 2002

Dr. R. B. Patel ,Dean ,Faculty of Information Technology & Computer Science ,Deenbandhu Chhotu Ram University of Science & Technology, Murthal. He received PhD from IIT Roorkee in Computer Science & Engineering, PDF from Highest Institute of Education, Science & Technology (HIEST), Athens, Greece, MS (Software Systems) from BITS, Pilani and B. E. in Computer Engineering from M. M. M. Engineering College, Gorakhpur, UP.He has two patents , numerous best paper awards and more than 100 publications to his credit. He is member of bodies like IEEE, ISTE.

Rajesh Gargi received the B.Tech. degree from Regional Engineering College , Kurukshetra. He obtained his M.Tech degree in Computer Sc. & Engg from Guru Jambheshwar University of Science & Technology, Hisar and perusing PhD from the same University. He is working as Associate Professor in Computer Sc. & Engg, Department at Indus Institute of Engineering and Technology Kinana,Jind. His Research areas are Computer Networks and Mobile Communication. He has published more than 10 papers in national, international journals and conferences of repute.