http://www.jctjournals.com

ISSN(ONLINE):2278 - 3814

Volume-11, Issue-8, August, 2022

JOURNAL OF COMPUTING TECHNOLOGIES (JCT)

International Journal

Page Number: 01-07

Enhancing Security in The Mobile Ad hoc Network By using SHA-1 and ECC

Suman Rathore[1], Dr. Neha Singh

[1]M.Tech Scholar, [2]Associate Professor,

[1,2]Department of Computer Science Engineering

[1,2]IASSCOM Fortune Institute of Technology, Bhopal (M.P), INDIA,

***Abstract*— In earlier work to optimize the delay, in data transmission of multimedia traffic is main concern for the research, for transmission of multimedia data in MANET it always face some difficulties like poor quality, more delay because it required high data rate and need more time to transmission due to larger size of file. Dynamic nature of MANETs creates problem. To overcome these problem of MANETs, proposed a new mechanism in which delay is minimize by in-order delivery of packet. Knapsack algorithm is used to fill the packets in the memory by optimizing the buffer utilization. Buffer is leaky bucket where some packets are remain stored in the buffer because of sequence out-of-order and in order packets are sent to directly reach to destination through intermediate nodes or make packets in-order in buffer within a specified time of transmission. In previous work author uses dynamic approach for solving Knapsack but this dynamic approach required $O(n^3)$ time delay to overcome this time delay problem in our proposed work we used branch and bound for solving 0/1 knapsack ,our main goal is to maximize the in-order capability of packets and at the same time minimize the random packet transmission in the buffer. This approach is very useful to reduce and optimize the delay and increase the throughput by avoiding out-of-order packets delivery. This is more suitable to the multimedia data communication with good QoS for multimedia transmission in MANETs.**

***Keywords*— MANETs, Knapsack, Branch and Bound, Delay optimization, Multi-Media Traffic etc.**

I. INTRODUCTION

Three-way Portable systems over local nodes are very useful for both the military and the regular citizen world. While they were initially implied for improving military interchanges in the front line or in territories hit by regular fiascoes, remote systems have discovered their way into nonmilitary personnel life. To-day individuals are utilizing these systems as a part of bistros, eateries, shopping centers, colleges, and open social events, for example, gatherings.

Force is additionally vital in remote systems, particularly in portable impromptu systems, as the "fuel" keeps the system alive. Along these lines, preserving power draws out system life. Besides, vitality protection prompts littler, more lightweight gadgets and diminishes natural dangers by minimizing disposed of batteries [2].

There are two unmistakable sorts of remote systems: base based remote systems and versatile impromptu systems (MANETs). In base based remote systems, the portable nodes depend on stationary nodes, generally called access focuses, with sufficient AC energy to course their parcels through the system. For the most part, for this situation, the entrance point arranges and courses traffic between nodes. In MANETs, the portable nodes depend on each other for parcel conveyance and traffic coordination. This kind of coordination structures what is called multi-hop connections. In impromptu systems, the undertaking of bundle conveyance and traffic coordination puts a great deal of weight on the individual nodes' vitality sources. As the nodes expend vitality from their energy sources, the system can get to be apportioned. This can hurry the "passing", i.e. the time when the system can no more satisfy its planned capacities, of the system.

1.2 Types of Wireless Ad-hoc Network

1) MANET (Mobile Ad Hoc Network)
2) VANET (Vehicular Ad hoc Network)
3) SANET (Wireless Sensor Network)

ISSN(ONLINE):2278 - 3814

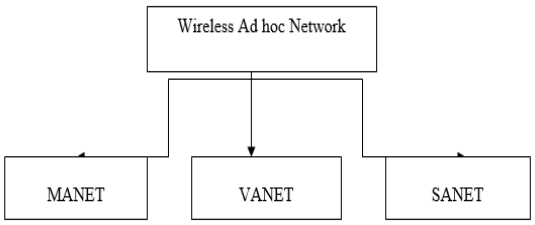


Figure 1.1: Classification of Ad hoc network

1.2.1 Mobile Ad Hoc Network (MANET)

Portable Ad hoc Networks (MANET) is a correspondence system framed by the union of self-ruling accumulation of versatile nodes (PCs, mobiles, PDAs and so forth.) and interfacing remote connections. The system is demonstrated as a discretionary correspondence chart.

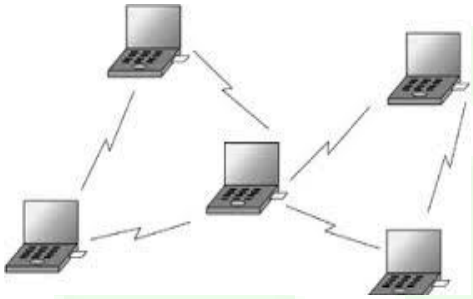


Figure 1.2: Mobile ad hoc network

1.2.2 Vehicular Ad-Hoc Network (VANETs)

VANET is a type of advert hoc network, it is used to offer communications among cars and nearby roadside regular tool. In a vehicular advert hoc network (VANET) automobiles are mobile nodes used to create a cell community. A VANET movements every taking component car right right into a Wi-Fi router or node, allowing automobiles approximately a hundred to 3 hundred metres of each other to connect with create a community with a tremendous variety. The primary objective of vanet is to offer safety and comfort for passengers. A unique virtual tool is placed indoors each vehicle that lets in you to offer ad hoc network connectivity for the passengers. The network has a tendency to perform with none fixed infrastructure.

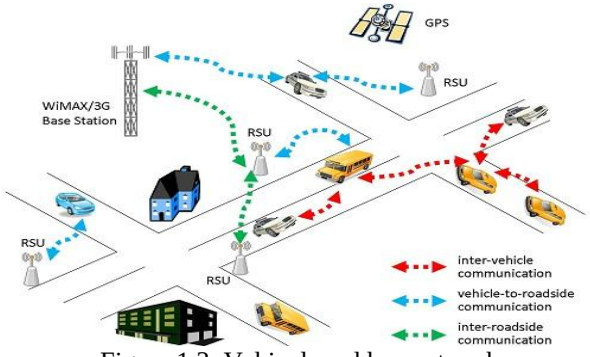


Figure 1.3: Vehicular ad hoc network

For the duration of the previous couple of years vehicular communiqué is attracting growing interest from both instructional and commercial factor of view. This is because of programs starting from road protection to traffic manipulate and as much as infotainment.

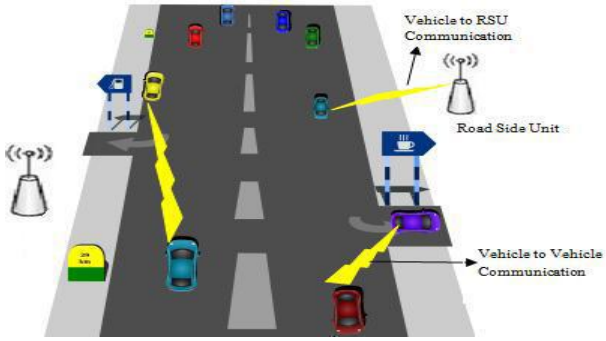


Figure 1.4 Overview of VANET

1.2.3. Wireless Sensor Network [4]

A sensor network made of multiple stations called sensor nodes. These sensor nodes are very small in size, light in weight, and it can be move from the one place to another place. The WSN is created by the few nodes. WSN network size can be few hundred; it can be few thousand as well. Node are connected to each other by the wireless link. Every wireless sensor node has a transducer to generate the electrical signal, microcontroller for make network operative. It store and process the data. WSN has a transceiver mainly used for data transmission and data reception.

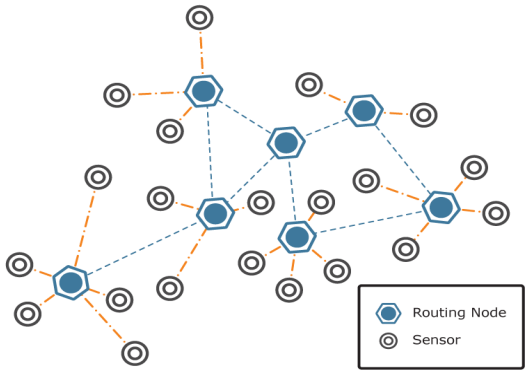


Figure 1.5: Wireless sensor Network

II. LITERATURE SURVEY

In mobile ad hoc network security and reliability is very important and challenging task due to its dynamic nature and absence of centralized control mechanism. MANIT is highly vulnerable to the attack. Any malicious node can easily penetrate the security and it can easily perform malicious activity and steel the confidential information [23]. Attack in MANET is mainly categories in the two categories such as active and passive attack. An active

attacks are those first receive packet from the network then they modified or dropped it and they may be insert their own packet in the network. On the other hand passive attacker only listen or steal information from the network without any disturbances in the network [24][25].

Various attack are present in the MANET such as wormhole attack, sink hole, flooding attack, routing table overflow attack, Denial of Service (DoS), and black hole [26][27][28][29][42].MANET is more vulnerable to these attacks because node are communicate on the mutual trust and any node can join the network without any permission and restriction [30].

V. Arora et al. [31] proposed a self-authentication and key management protocol for MANET. It mainly work in the one hop communication based on the RSA algorithm.P. Bansal et al. [32] present the study of black hole and neighbor attack on the MAODV routing protocol. They also measure the performance off network on the metrics like network throughput, packet delivery, and network delay.M. Raju et al. [33] developed a novel elliptic curve cryptography based security in the MANET.

H. S. Chiu and K.S. Lue [34] introduced a method to detect both hidden and exposed wormhole attacks. In DELPHI, the sender gets all the disjoint paths between a sender and a receiver. After that, sender calculates the number of hops count and delay for each hop, the information is used to detect the wormhole attacks in the network. A path that has wormhole links will have a larger delay per hop value.

X. Wang and J. Wong [35] proposed an end-to-end detection of Sybil attack (EDWA) in mobile ad-hoc networks. In this method detection of Sybil made based on hop count if hop count is very less compared to establish count then that path has Sybil attack. The result of detection is broadcast into the network to aware the other nodes in the network. After detection and identification of the Sybil the source node could select a shortest path from the set of legalize paths. The main drawback of this method is that it does not work well when the source and destination are too far away.

Su et at. [37] Proposed modified AODV routing protocol called WARP to find out the attack in the network. WARP adopts link-disjoint multiple routing path from source and destination during the route discovery process. To avoid the malicious nodes, WARP provides a larger path selection but finally uses only one path for data transmission. In WARP, each node collects anomaly values of its neighbors. Wormhole nodes have great ability to grab the route from source to destination; if the occurrence of one links exceeds the threshold value then neighbors of this node will discard all requests-forming route containing that node in the path.

M. natu and A. Sethi [38] proposed an intrusion detection system to detect a wormhole using fault location techniques to defend against wormhole attack. Passive monitoring, proving, and event correlation tools have used to detect wormhole attacks in the network. In this method, two types of anomalies have focused to identify the nodes involved in a wormhole attack: end-to-end delay and hop-per delay.

Choi, Kim, lee and Jung [39] proposed wormhole attack preventive (WAP). The WAP detects the false route in the discovery phase. In WAP, all nodes monitor their neighbor's behavior during the route request RREQ messages to the destination. When source node receive route replay packet from the destination, first check whether path is belong to wormhole or not.

Y. Singh, A. Khatkar, P. Rani [40] in this method, existing DSR protocol is modified for detecting and preventing the wormhole attacks in the network. The proposed method detects such nodes and the routers are those involved in the wormhole attack and simply discard into the routing table of the DSR so that in future, nodes are not used in any communication. In this method, for evaluating the network performance three parameters throughput, end-to-end delay and jitter have been used.Sultana et al.[41] proposed a system for black hole attack to study the performance of they consider MAODV protocol. For securing network connections, Elliptic curve Cryptography technique is used.

III. PROBLEM DEFINITION

In above literature review several security techniques has been proposed by the researchers and at some stand they perform efficiently in terms of network performance but mobile ad hoc network is still having many security issues due to the lack of centralized control and lack of administration and in MANET topology are fully dynamic any node can join and leave network at any time without any authentication. Mobile ad hoc network has following major security issues:

1. Data transmission in the network is on the air and it can be received by the any node within direct range of the transmission.
2. Routing protocol in the MANET does not have any security check. So the security is depends on the individual node truthiness and reliability.
3. Mobile ad hoc network does not have authentication and access control mechanism.

IV. RESEARCH METHODOLOGY

In this research work, we have proposed a new approach to address the security issues in the mobile ad-hoc network (MANIT). In the proposed method standard MAODV routing protocol is modified, Elliptic curve cryptography and secure hash algorithm (SHA) is introduced. To overcome the problem of authentication and data infertility in the network. It also handle the attack like Man in middle attack, denial of service attack. This additionally improved network security and privacy.

ISSN(ONLINE):2278 - 3814

The proposed SHA and ECC based algorithm provides the secure access of the network. It overcome the problem of node authentication in the mobile ad hoc network and provides the access control over the malicious node. In figure 5.1 depicted the block diagram of the proposed algorithm framework. As we can see our proposed method is combined with MAODV routing protocol.

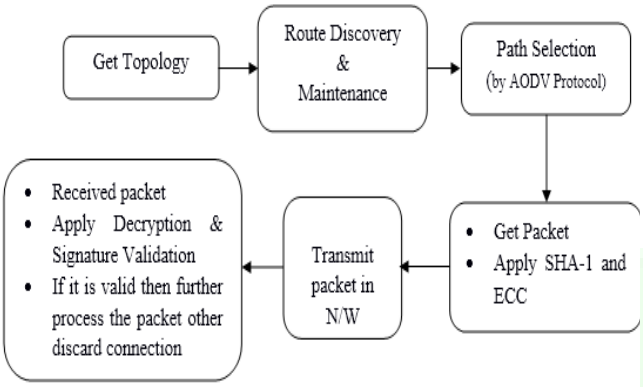


Figure 4.1 Block diagram of proposed methodology

4.1 Secure Hash Algorithm

Secure Hash algorithm (SHA-1) is very commonly used algorithm. It is a mathematical function that mainly used to get authentication by the digital signature. SHA-1 is very popular method for the authentication. It produces 160 bit hash code.

Figure 5.2 shows the block diagram of hash code generation. To generate the hash code following steps are follows:

1. Take packet from the sender.
2. Apply SHA-1 algorithm. It gives 160 bit SHA-1 hash
3. Then encryption is applied by using sender`s private key.
4. At the receiver, receiver first compute the hash code by using sender`s public key and validate the hash code
5. If hash code is valid then it receives the packet otherwise it will discard the packet and stop the communication.

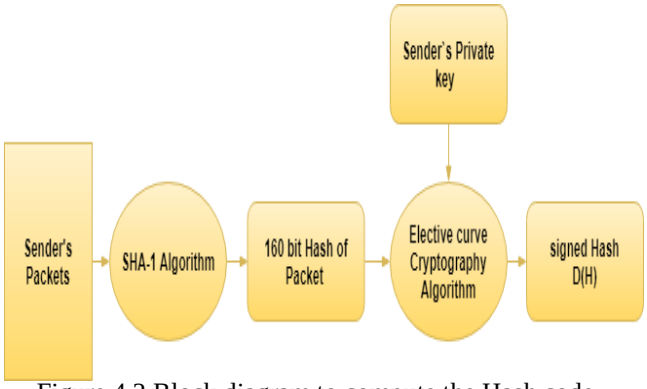
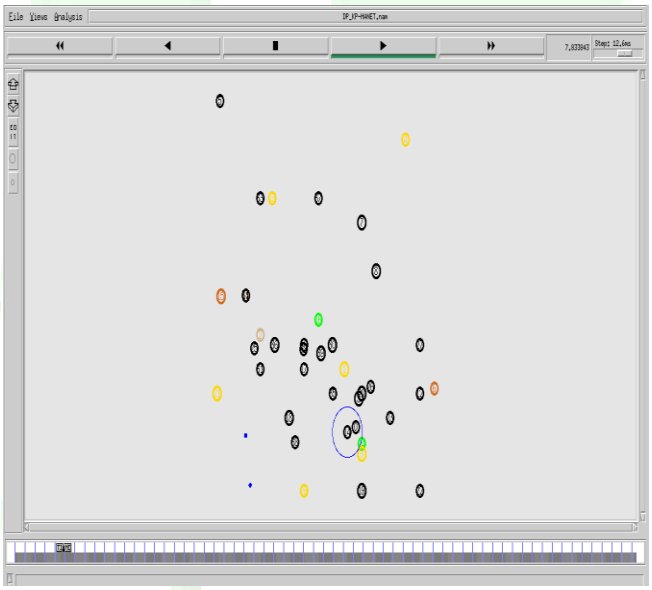


Figure 4.2 Block diagram to compute the Hash code.

V. SIMULATION AND RESULT

5.1 Implementation

To evaluate and study the enhancement for energy conservation, a series of simulations and measurements are carried out using modified and unmodified versions of two existing MANET routing protocols. We test the enhancements with a reactive protocol AODV. We study the effects of the enhancement primarily on the network lifetime under deferent mobility scenarios and network topologies. We also study the side effects of the enhancement on network performance metrics such as delay and percentage of packets delivered to the application. The testing performed on single-hop and multiple-hop ad hoc networks. Moreover, we implement the same scheme on a proactive routing protocol and compare and contrast the relative performance under stationary and mobile scenarios. Initial experiments were conducted on sparse and dense static ad hoc networks. We ran the experiments until the communicating nodes stopped communicating due to battery power exhaustion in the intermediate nodes, then gathered the information needed for the metrics under study. Each experiment was repeated four times with different number of node to determine any



effects of randomness.

Figure 5.1 Network Topology

5.2 Simulation Scenario

In this dissertation work all the implementation work is performed in NS-2. For implementation of existing and proposed method 40 mobile nodes are created. Simulation time was taken 100 seconds. We pick Min speed = 1 m/s, Max speed = 30m/s. Table 6.1 shows the simulation parameter of the network.

Table 5.1: Simulation Parameter

ISSN(ONLINE):2278 - 3814

Simulator Used	NS-2.35
Number of nodes	40
Dimension of simulated area	800m×800m
Routing Protocol	MAODV
Simulation time	100 sec.
Traffic type (TCP & UDP)	CBR (3pkts/s)
Node movement at maximum Speed (m/s)	random
Transmission range	550.5 m
Antenna Height	150 m

5.3 Simulation Results

Results are evaluated of original AODV and proposed rate control scheme with MAODV. In order packet delivery scheme is implemented and performance analysis of proposed method is measures on the following parameters discussed here.

A. Packet Delivery Ratio (PDR) Analysis

Packet delivery ration is ratio between the successfully packet received to packet transmitted in the network. The comparison between exiting work and proposed work is shown in the figure 6.2. In the figure we can observed that PDR is better for the proposed method.

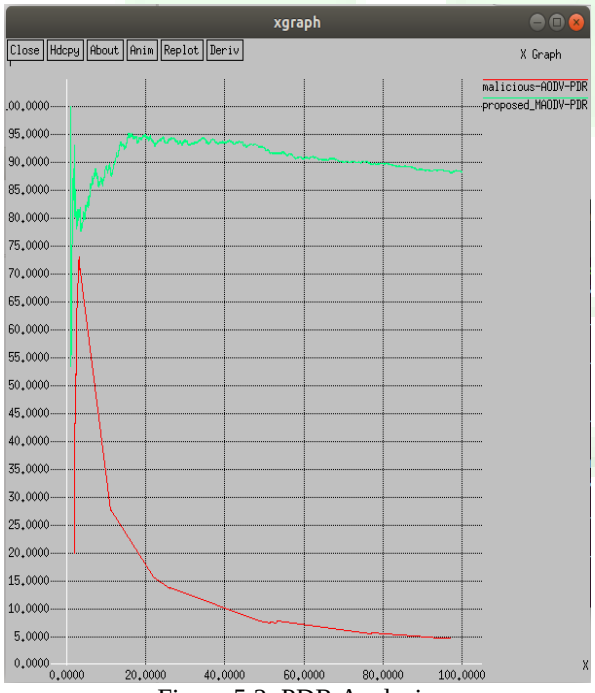


Figure 5.2: PDR Analysis

B. Routing Load Analysis

Number of packets required for management of routing is called routing load. For route management such as route discovery and to maintain router required to communicate with node by using extra packets. Figure 6.3 shows the comparison between old and proposed work.

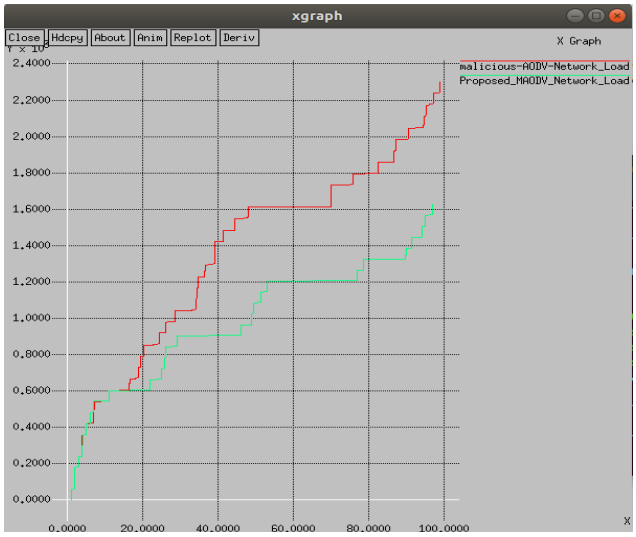


Figure 5.3: Routing Load Analysis

C. Throughput Analysis

Successful packets received by receiver in per unit time is called network throughput. The throughput analysis in this research is measured in number of packets transmitted per second in the network. The throughput is shown in figure 6.4 and graph shows the better results in case of proposed algorithm based method with compare to existing method.

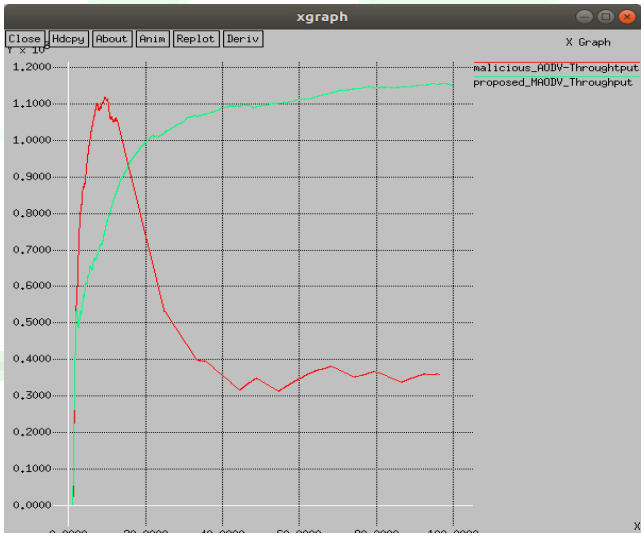
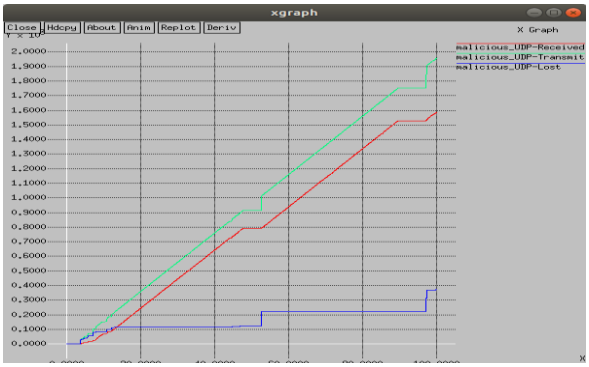


Figure: 5.4: Throughput Analysis

D. UDP packet Analysis

In the figure 6.5a and figure 6.5b shows the UDP packet analysis in the suspicious (malicious node) network as well as in the proposed SHA based network. In the figure we can see that packet loss in the suspicious network is more with compare to proposed network.

ISSN(ONLINE):2278 - 3814



(b)Figure 6.5 UDP packet analysis; (a) In Suspicious Network, (b) In Proposed system.

VI. CONCLUSION AND FUTURE WORK

Conclusion

Security in the mobile ad hoc network is very challenging task due the open communication and without centralized control. To other the problem of security and reliability in the MANET we have proposed a group SHA based routing protocol which provides authentication and secure communication. Proposed hash code method each node able to authenticate the packet before received. In this work we have solve the problem of man in middle attack and denial of service attack. Man in middle attack is now not possible because if middle man is not able to generate the hash code and denial of service attack is solved as that the only authenticated node as able to communicate. We tend to simulate the proposed approach with the assistance of network machine in static and dynamic situations, wherever we tend to analyzed the efficiency of transmitted packets (i.e., throughput, packet loss, in-order packets and out-of-order packets). Our approach will increase the transmission reliability and reduces the packet loss chance in comparison to existing approaches.

Future Work

Proposed SHA based technique gives good results as seen in the simulation results like give network throughput, minimize network load and give improved packet delivery ratio but as universal true that every where is an some area where the improvement are possible. Proposed framework is needed to test in the highly vulnerable environment such as attack like wormhole, black hole, Sybil attack etc. in future different encryption algorithm will also combine with digital signature.

Reference

[1] Vanita Rani PG Student, Dr.RenuDhir, "A Study of Ad-Hoc Network: A Review" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue3,March 2013

[2] DivyaChadha,Reena, "Vehicular Ad hoc Network (VANETs): Areview" International Journal of Innovative Research in Computer and Communication Engineering" Vol. 3, Issue3,March2015.

[3] Soundararajan**, S.** and R.S. Bhuvaneswaran "Multipath Load Balancing & Rate Based Congestion Control for Mobile Ad Hoc Networks (MANET)" 978-1-4673-0734-5/12/$31.00 ©2012 IEEE.

[4] Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." Computer networks 38.4 (2002): 393-422.

[5] Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", Volume 3, Issue 5, May 2013.

[6] Qin, F. and Y. Liu, 2009. Multipath based QoS routing in MANET. J. Netw., 4: 771- 778.

[7] Goyal, Priyanka, VintiParmar, and Rahul Rishi. "Manet: vulnerabilities, challenges, attacks, application." IJCEM International Journal of Computational Engineering & Management 11.2011 (2011): 32-37.

[8] Ivascu, G.I., S. Pierre and A. Quintero, 2009. QoS routing with traffic distribution in mobile ad -hoc networks. Comput. Commun., 32: 305-316, 2008.

[9] Qin, F. and Y. Liu, 2009. Multipath based QoS routing in MANET. J. Netw., 4: 771-778.

[10] Sivakumar, P. and K. Duraiswamy, "A QoS routing protocol for mobile ad hoc networks based on the load distribution", Proceedings of the IEEE InternationalConference on Computational Intelligence and Computing Research (ICCIC), IEEE Xplore Press, Coimbatore, pp: 1- 6, 2011.

[11] Perkins and Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (Dsdv) For Mobile Computers, "Proceedings OfAcmSigcomm 1994, Pp. 233-244," August 1994.

[12] Murthy, Shree, and Jose Joaquin Garcia-Luna-Aceves. "An efficient routing protocol for wireless networks." Mobile Networks and applications 1.2, 183-197, 1996.

