Congestion Control Using Secure Channel in MANET

Harsh Dubey[1], Prof. Ratnesh Dubey[2], Dr. Vineet Richhariya[3]
Department of Computer Science & Engineering LNCT, Bhopal
[1]harshdubey88[AT]gmailD[DOT]com, [2]ratneshdub[AT]gmail[DOT]com,[3]vineetrich100[AT]gmail[DOT]com

Abstract— *Mobile ad hoc network (MANET) is a collection of mobile nodes and every node has capacity to send and receive the packet which means that every node behaves like router host. The mobile ad hoc network can form or destroy the network. Due to dynamic behavior of MANET there are different security and congestion issues in the network. At the point when the offered load on the system exceeds congestion happens, which prompts packet losses. There are such a large number of proposed conventions that are versatile to clog and deals with congestion. In this paper, we propose secure channel algorithm to prevent the network from congestion. The experimental analysis of the proposed algorithm is done using network simulator NS-2.34 and the comparative analysis of propose algorithm is done between performance measuring parameter PDR, routing load and throughput*

Keywords—*Ad hoc network, Congestion, Network Simulator, PDR, Throughput.*

I. INTRODUCTION

Mobile ad hoc (MANETs) are wireless mobile network framed suddenly. Not at all like in the conventional wireless networks, correspondence in such a decentralized organize is commonly multi-hop, with the nodes utilizing each different as hand-off switches with no settled infrastructure. This type of network is exceptionally adaptable and appropriate for applications for example, transitory data partaking in a gathering, military activities and disaster rescues. Be that as it may, multi-hop routing, arbitrary development of portable nodes and other features special to MANETs prompt gigantic control overhead for route discovery and support. In a few situations, the routing maintenance overhead may expend so much resource that it truly bargains long term effectiveness. Besides, contrasted and the conventional systems, MANETs experience the ill effects of the resource limitations in energy, computational limits and bandwidth. These make steering in MANETs an exceptionally difficult issue. In recent days, home or small office networking and collaborative computing with laptop computers in a small area (e.g., a conference or classroom, single building, convention center) have emerged as other major areas of potential application. In addition, people also recognize that ad hoc networking has obvious potential application in all the traditional areas of interest for mobile computing.

1.1 MANET Characteristics

Autonomous and infrastructure-less: Each mobile node is an independent node, which could function either as a host or as a router. *Multi-hop routing:* When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes. *Dynamic Network Topologies:* The nodes in MANETs are free to move independently in any direction. The network's wireless topology may change frequently and randomly at unpredictable times and primarily consists of bidirectional links. *Limited Battery Power:* The nodes or hosts operate on small batteries and other exhaustible means of energy. So, energy conservation is the most important design optimization criteria. *Scalability:* Due to the limited memory and processing power on mobile devices, the scalability is a key problem when we consider a large network size. Networks of 10,000 or even 100,000 nodes are envisioned, and scalability is one of the major design concerns [1] [2].

1.2 LIMITATIONS OF MANETS

There is a current and future need for dynamic Ad hoc networking technology. This highly adaptive networking technology, however, still faces various limitations. The limitations of MANETs are as follows:

- **Bandwidth constraints**: As mentioned above, the capacity of the wireless links is always much lower than in the wired links. Several Gbps are available for wired LAN nowadays while the commercial applications for wireless LANs work typically around 2 Mbps.
- **Processing capability**: Most of the nodes of the MANET are devices without a powerful CPU. The network tasks such as routing and data transmission cannot consume the power resources of the device, intended to play any other role, such as sensing functions.
- **Energy constraints**: The power of the batteries is limited, which does not allow infinitive operation time for the nodes. Therefore, energy should not be wasted and that is why some energy conserving algorithms have been implemented.
- **High latency**: In a power maintaining design, nodes are napping or inactive after they do not have to send each data. After the data transactions amid two nodes go across nodes that are napping, the stay could be higher if the routing algorithm decides that these nodes have to awaken up.
- **Transmission errors**: Attenuation and interferences are other effects of the wireless links that increase the error rate.
- **Security analyses**: some of the vulnerabilities and aggressions MANET can suffer. The authors tear the probable aggressions in passive ones, after the attacker merely endeavors to notice priceless data by listening to the routing traffic; and alert aggressions, that transpire after the attacker injects arbitrary packets into the web alongside a little proposition like disabling the network. This is main limitation of MANET.

- **Location**: The addressing is the another problem for the network layer in MANET, since the information about the location the IP addressing used in fixed networks offers some facilities for routing that cannot be applied in MANET**.**
- **Roaming**: The continuous changes in the network connectivity graph involve that the roaming algorithms of the fixed network are not applicable in MANET, because they are based on the existence of guaranteed paths to some destinations.
- **Commercially unavailable**: MANET is yet far from being deployed on large-scale commercial basis.

Figure 1 Mobile ad hoc network

1.3 Problem Statement

In this section, we have tried to point out the problems of using TCP congestion control mechanism for classifying the type of losses to control in mobile ad hoc networks. Standard congestion control cannot detect link failure losses which occur due to mobility and power Scarcity in multi-hop Ad-Hoc network (MANET). Congestion control is the most controversial parts of TCP which degrades performance when encounters non-congestion loss in MANET. Congestion control assumes all loss induced by congestion.

II. CONGETION IN MANET

In mobile ad hoc networks, a message sent by a mobile node may be received simultaneously by all of its neighboring nodes. Messages directed to mobile nodes not within the sender's transmission range must be forwarded by neighbors, which thus act as *routers.* Due to mobility it is not possible to establish fixed paths for message delivery through the network. Mobile Ad hoc networks are composed of mobile stations communicating solely through wireless links [3]. Routing protocols are classified as *proactive or reactive,* depending on whether they keep routes continuously updated, or whether they react on demand. The routing protocols [4] can also be categorized based on congestion-adaptive versus congestion-un adaptive routing. The congestion unawareness in routing in MANETs may lead to the following issues. *Long delay:* This holds up the methodology of locating the congestion. At the point when the congestion is more careful, it is better to choose an interchange way. Anyway the predominating on demand routing protocol defers the route looking for process. *High overhead:* More handling and correspondence attempts are preferred for another route exposure. In the event that the multipath directing is used, it wants extra effort for maintaining the multi-ways paying small mind to the being there of interchange route. *Many packet losses:* The congestion control method activities to reduce the overload in the system by also reducing the sending rate at the sender part or by dropping the packets at the center nodes or by executing both the procedure. This causes increased packet loss rate or least throughput. The organization of paper is done as follows: Section II presents the Routing Protocols in MANET. In section III former work done by different author/researcher is presented. Congestion control technique is presented in section IV and last section gives overall conclusion and future work of the research work.

III. RELATED WORK

VarshaBais, Amit Sinhal et al. [5] In mobile ad hoc web (MANET), congestion is one of the most vital constraint that deteriorate the presentation of the finished web and routing skill of AOMDV protocol. Multi-path routing permits the formation of several trails amid a solitary basis and solitary destination node. Multi-path routing can balance the burden larger than the solitary trail routing in ad hoc webs, thereby cutting the congestion by dividing the traffic in extra than two paths. This research presents a new way of rate manipulation established buffer enhancement congestion manipulation mechanism for circumventing congestion in web contact flows. Mobile nodes in a MANET deeds as a both host and router relaying traffic on behalf of supplementary nodes in the web, that describe MANET by easy of exploitation in each where. On the supplementary hand, mobile node has restricted computational capacities like bandwidth and buffer suspect. Additionally, mobile nodes link and depart the web vibrantly that leads to topological changes. The demands for quality established multi-path routing have arose in substantial attention by researchers in the span of burden balancing in MANET. There is a tendency in established Mobile ad hoc routing protocols to use intermediate nodes for colossal number of paths.

Manveer Kaur, Ambrish Gangal et al. [6] in this paper, the mobile ad hoc web is the self configuring and decentralized kind of network. The web has not fixed topology as mobile nodes can move freely in the network. Due to vibrant kind of topology and self configuring nature of mobile ad hoc web countless subjects become increased that are routing, protection, quality of services and countless more. In this paper, assorted kinds of routing protocols are studied alongside their gains and disadvantages. The routing protocols are usually categorized as proactive, reactive and hybrid protocols. In these routing protocols power and burden balancing are main issues. This paper is concentrated on disparate routing like Proactive routing protocol (DSDV, OLSR and WRP), Reactive routing protocol (DSR, TORA, AODV) and a little trials in MANET. Across data transmission there is a setback of link wreck in MANET that cuts web presentation and reliability. In the preceding kind assorted methods had been counseled for burden balancing. The most elevated and power effectual method is multipath routing. In Upcoming to remove the link wreck setback in AOMDV protocol Instituted on the novel method.

Navneet Kaur, Rakesh Singhai et al. [7] in this paper, we examine the main factors altering presentation in ad hoc webs and debate countless normal enhanced congestion manipulation approaches. Web presentation of these disparate ways is discussed. The limitations of disparate ways are additionally remarked and the counseled method for congestion manipulation employing web coding is discussed. Ad hoc web is a multi-hop provisional self-organized web encompassing of countless mobile nodes lacking each infrastructure. The continuing routing protocols counseled for MANETs have precise limitations. Router assisted congestion manipulation way and conclude to conclude rate established flow manipulation creates intricacy at routers. Hop-by- Hop Congestion Domination ways induces scalability problem. Subsequently a well balanced congestion manipulation arrangement is to be retained for the stability and optimized presentation of the wireless network. Adaptive Web coding reliant on the channel conditions is counseled to ascertain the setback of congestion in the network. The routing protocol will be adjusted to cope up alongside the dynamics of Mobile Ad hoc web and furnish larger presentation of the network.

Anju et al. [8] aim of the congestion control is to assure that system is running at its rated capability even in worst condition (overload situation). By controlling the rate with which packets are injected in the network, the amount of information that reaches the data sinks minimizes. This fact can jeopardize the purpose of the network. Moreover, network connectivity issues arise since in most cases, this approach utilizes the shortest path from source to sink. Thus, in case of heavy data burden, this path of nodes can easily become power exhausted. To achieve this, author take advantage of the fact that mobile nodes are frequently redundantly and/or densely deployed. In this thesis, author focus on congestion detection and prevent the congestion using Ad hoc on demand routing protocol (AODV) using MATLAB.

Andreas Pitsillides et al. [9] have reviewed existing literature on IP and ATM congestion control. We have presented an illustrative example of using CI intelligence to control congestion using Fuzzy Logic. This and the literature we review on CI methods applied to ATM networks show that CI can be effective in the control of congestion. There is no doubt that we will see more and more use of these techniques, including their use in the IP world. We also expect that, as in other commercial products, CI techniques will finally make it into real products in this area, and we expect with tremendous success.

Dewariya et al. [10] proposed work the performance the existing compound TCP for wireless scenario is improved upgrade TCP give satisfactory result in high speed huge network. Upgrade TCP is a TCP for fast speed and huge network. Upgrade TCP execute congestion control with the help of a combination of open congestion window or delay based method, for transmission data or packet or mutual understanding among all sender or receiver we apply synchronization in TCP handshaking mechanism. In our propose work, we explain working of upgraded TCP. The simulation depicts that, the results of proposed approach is better than base approach. The congestion window of proposed approach is better and the good put of proposed approach is higher than base good put.

Youssef Bassil et al. [11] proposed a TCP congestion control scheme comfortable for wireless as well as system atmospheres. It is created by using any particular minute of the reticent minutes of the TCP legend to designate the variety of the connection above which a construction is recognized. If the connection is bound, the TCP reticent bit is fixed to 0 signifying a bound way; while, if the connection is wireless, the minute is fixed to 1 signifying a wireless way. Moreover, the system usages the SNR (Signal-to-Noise) part of perceiving the consistency of the association. In wired mode, any recreation is reflected a cramming defeat; and hence, cramming is evaded by exhausting the usual TCP start-slow procedure.

Aalam et al. [12] this research directs the problems in routing of CRAHNS; particularly this research provides the optimum solution for traffic management in CRAHNS. Obtaining the optimum solution this work analyzes Jackson and Feiler theorem equations further to make it more efficient, the Lagrangian multiplier approach is utilized, and some unique mathematical expressions are derived for computing the minimum value of the congestion of the available paths of the CRAHNs. The MATLAB simulation is conducted and the results show that the proposed expressions are obtained optimum congestion value and the best path is opted based on the vale for transferring of data.

IV. PROPOSED METHODOLOGY

4.1 Proposed Methodology

In the proposed methodology ACK scheme is modified for authentication of node in AODV protocol. By this type of approach it facilitate some misbehave activities of suspicious node in entire network. Before it various author proposed ACK-Based scheme but there was a common problem like overhead of huge amount of packets and node ambiguity. But in the proposed scheme secure channel control a generation of additional packets and also improved the AODV protocol performance. In the next section ACK-Based scheme, and its combine modified secure channel approach is discussed, which gives the high performance to the AODV protocol. 4.2 ACK-Based Approach In here, when power transmission is used then ACK based scheme overcome the restriction of passive feedback technique, for this an authentication mechanism is used to prevent the next hop from sending a forged ACK packet on behalf of the intended two hop neighbor. The chief shortcoming of this format is the enormous overhead. In order to decrease the overhead, the authors have proposed in [13] that each node asks its two hop neighbor to send back an ACK randomly rather than incessantly. Similarly, this extension also is unsuccessful when the two hop neighbor refuses to send back an ACK. In such circumstances, the requester node is unable to differentiate who is the malevolent node, its next hop or the requested node. The proposed technique has a reasonable overhead induced by the ACK sent back by the destination during preferred intervals of data transfer period. Throughout the data packets transmission, a flow of individual packets is transmitted at indiscriminate interims alongside the information. The reaction of these exceptional parcels summons the destination to convey an ACK from side to side various ways. The ACK bundles take numerous courses to gather the likelihood that all ACKs being dropped by the noxious hubs, furthermore to record for plausible misfortune because of softened courses or blockage up persuaded hubs. On the off chance that the source hub does not get any ACK parcel, then it gets to be aware of the vicinity of aggressors in the sending way. As a response, it shows a rundown of suspected malignant hubs to isolate them from the system. Every one of the hubs running an illustration in light of affirmation need to keep up a timeout (To) esteem. This timeout compares to an upper bound of the time that the sender hub needs to sit tight for the ACK to show up. The determination of this timeout worth is basic since a little esteem affects an expansive number of fake allegations and an extensive quality upgrades the memory required to store the active bundles for further correlations. Figure depicts a sample of the lower bound of the timeout worth kept up by hub A for the gathering of two jumps ACK from hub C. The timeout quality ought to be more noteworthy than the assessed edge (Th) esteem which can be calculated ascertained as follows:

$$Th= T1-T2 \qquad (1)$$

Where, T1 and T2 are the sending (reception) time of the packet (ACK) respectively. This threshold is estimated for a successful transmission at MAC layer without any retransmission, which is not a realistic assumption in MANETs, thus the timeout value should satisfy the following condition

$$To > Th + (AV\ G\ RT \times 1\ hop\ delay)\ldots\ldots\ldots\ldots\ldots.. \ (2)$$

Where AV G RT is the normal number of retransmissions of a bundle at MAC layer and 1 jump deferral is the one bounce transmission delay which incorporates parcel transmission delay, irregular Bakeoff postponement at the MAC layer and the preparing deferral.

4.2.1 Modified ACK-Based Scheme

In the modified scheme we also reduced the unnecessary 2 ACK, due to this there was a huge packets generated and they create ambiguity for the requested node and affect to the QOS, but in the proposed modified secure routing algorithm they maintain a state of node as well as a path state due to given request and response for maintaining a request packet ACK.

4.2.2 Secure Channel

Communication sessions in which a pair of parties begins by successively legitimated key-exchange protocol to acquire a shared session key, and afterward secure successive data transmissions among them through an authenticated encryption method based on the session key. We demonstrate that such a communication session congregates the notion of a secure channel protocol proposed by Canetti and Krawczyk [14] if and only if the underlying authenticated encryption mechanism meets two novel, easy definitions of security that we initiate, and the key-exchange protocol is secure. In other words, we diminish the secure channel requirements of Canetti and Krawczyk to effortless to utilize, stand-alone security requirements on the underlying authenticated encryption scheme. Additionally, we communicate the two new notions to existing security notions for authenticated encryption methods. We consider communication sessions in which a pair of parties begin by running an authenticated [14] key-exchange (KE) protocol to obtain a shared session key, and then secure successive data transmissions between them via an authenticated encryption scheme, a shared-key-based encryption scheme whose objective is to present both privacy and legitimacy, based on the session key.

4.3 Secure Channel Algorithm

```
Step 1: Set Source Node = $S_i$
Step 2: Start Route discovery with RREQ.
Step 3: Traverse with own identifier random query
identifier (RQI-SQNO).
Step 4: Share key between $S_i$ to $R_i$ nodes.
Step 5: Sender start sending a message
authentication code (MAC) to Receiver
    Active: (RQI-SQNO + SHKY);
    MAC = # (Si, Ri, RQI-SQNO, SHKY);
Step 6: MAC: secure packets and route.
Step 7: Accumulate IP address of intermediate
nodes.
Step 8: Traversed packet from intermediate node.
    IF (Traversed packet! = $S_i$ || Traversed
packet! = $R_i$) THEN;
      Start Route discovery and Intermediate
nodes switch route request RREQ.
Step 10: Update routing table and maintain
information.
Step 11: Store RQI-SQNO via $I_i$.
    $I_i$ node = RQI-SQNO+SHKY;
Step 12: Change previous RREQ;
    Flash: previous RREQ;
    GOTO step 10;
Step 13: IF (packets > 1) THEN //received via
different path.
Step 14: Receiver generate MAC and that will
verified by Sender
Step 15: Route reply from intermediate nodes ($I_i$
..........$I_n$)
Step 16: Receiver will count total MAC.
Step 17: $R_i$: Revert ACK to $S_i$ via different route.
Step 18: Packets transmission and broadcasting till
end of simulation.
```

V. EXPERIMENTAL RESULTS AND ANALYSIS

5.1 Network Simulator

Network Simulator (NS-2) NS2 [15] is an open-source event-driven simulator designed specifically for research in computer communication network. As its inception in

1989, NS2 has continuously gained tremendous interest from industry, academic world, and government. Having been under regular investigation and enhancement for years, NS2 now contains modules for several network components such as routing, transport layer protocol, application, etc.

5.2 Result Analysis

The analysis of the proposed work is performing by using the performance measuring parameter such as Routing load, Packet delivery ratio and Throughput. The experimental results of proposed work for packet delivery ratio with existing method is depicted through table and shown in graph. The comparison of proposed work and existing one is analyzed using packet delivery ratio performance metrics in which observed that the result generated by proposed methodology is much better than the existing ones it means PDR of proposed system is much better than other. The graph of the system is shown in fig.2.

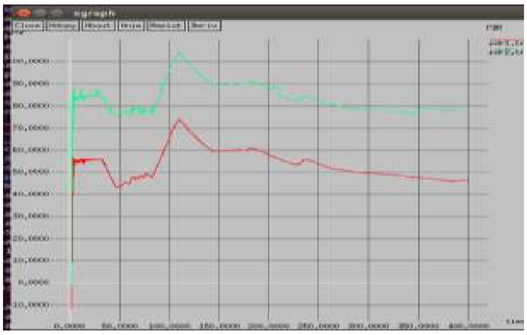

Figure 2 Graph of PDR between existing and proposed method.

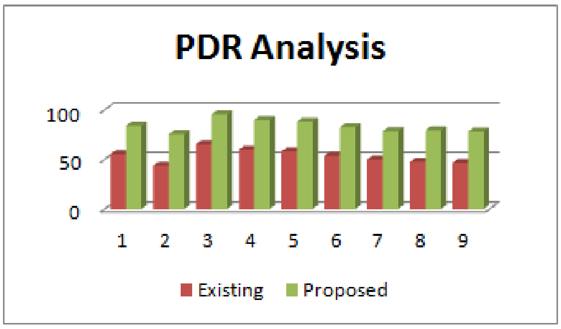

Figure 3 PDR analysis chart

Table1. PDR comparison table

Time	Existing	Proposed
10	55.22	83.96
50	43.75	75.49
100	65.35	95.5
150	59.71	89.86
200	58.02	88.17
250	53.7	82.44
300	49.8	78.54
350	47.51	79.26
400	46.47	78.22

Similarly the analysis of our work is perform on performance metric routing load for this metric our methodology also outperform than the other approach. The simulation result of proposed for routing load is depicted through graph shown in fig.4.

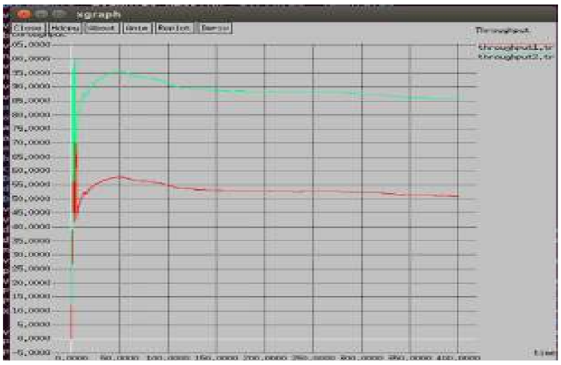

Figure 4 Graph of routing load between existing and proposed method.

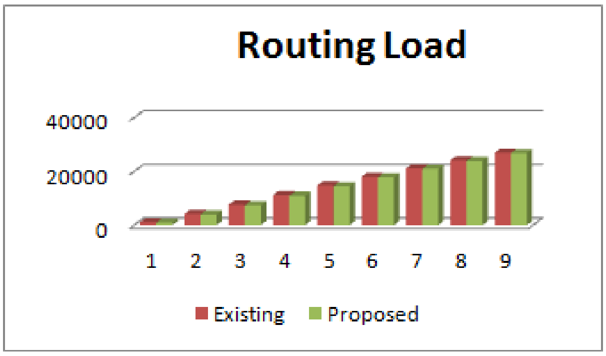

Fig.5 Routing load analysis chart

Table2. Routing load comparison table

Time	Existing	Proposed
10	1157	911.5
50	4248	4000.5
100	7674	7428.5
150	11209	10963.5
200	14821	14575.5
250	18057	17805.5
300	21191	20945.5
350	24122	23878.5
400	26999	26796.5

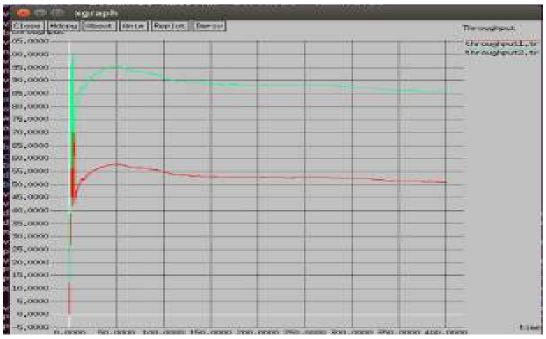

Fig.6 Graph of throughput between existing and proposed method.

We also perform simulation analysis of proposed system on performance metric throughput which is also more than other system about 37%. The simulation result for throughput of proposed system is depicted through graph in fig.6.

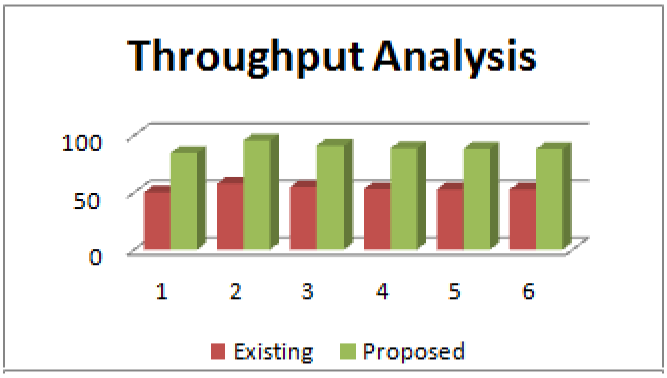

Fig.7 Throughput analysis chart

Table3. Throughput comparison table

Time	Existing	Proposed
10	50.26	84.63
50	57.86	95.58
100	54.77	91.12
150	53.09	88.71
200	52.81	88.31
250	52.69	88.14

VI. CONCLUSION

Mobile ad hoc network is dynamic in nature and because of its behavior any node starts transmitting of the packet which creates congestion over network due to this packet loss and overhead occurs. To prevent or control this problem in this use ACK based scheme and design secure channel algorithm to deliver the packet in this manner which prevent the packet loss and overhead. The experimental outcomes of our proposed scheme gives improved result than the existing approach. The analysis of the proposed scheme is done between PDR, routing load and throughput in which our scheme generates better results than the existing method.

REFERENCES

[1]. Muhammad Qasim Akbar, “Mobile Ad-Hoc Networks Applications and Its Challenges”. Scientific Research Publishing, Communications and Network, July 2016, Volume 8, Pages 131-136.

[2]. Prabhleen Kaur, “An Overview on MANET-Advantages, Characteristics and Security Attacks”. International Journal of Computer Applications, 4th International Conference on Advancements in Engineering & Technology (ICAET 2016).

[3]. G.S. Lauer, Packet-Radio Routing, in: Routing in Communications Networks, Editor: M.E. Steenstru Prentice-Hall, 1995), Ch. 1, 35, 1-396.

[4]. S. Ramanathan and M.E. Steenstrup, “A Survey of Routing Techniques for Mobile Communications Networks, Mobile Networks and Applications”, Vol. (1996), 98-104.

[5]. Bais, Varsha, Amit Sinhal and Bhupesh Gour, “Rate base Congestion Control in Multipath Routing Strategies under MANET”. International Journal of Computer Applications 112, no. 13 (2015).

[6]. Kaur Manveer, and Ambrish Gangal, “Comparative Analysis of Various Routing Protocol in MANET”. International Journal of Computer Applications118, no. 8 (2015).

[7]. Kaur Navneet and Rakesh Singhai, “Review on Congestion Control Methods for Network Optimization in MANET”. International Journal of Computer Applications 121, no. 7 (2015).

[8]. Anju, Sugandha Singh, “Modified AODV for Congestion Control in MANET”. International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June-2015, pg. 984-1001.

[9]. Andreas Pitsillides, Ahmet Sekercioglu, “Fuzzy logic based congestion control”.

[10]. Vinita Dewariya and Neha Bhardwaj “Enhanced TCP for Congestion Control in MANET”. IJCSNT Vol.5, No.1, 2016, ISSN 2053-6283.

[11]. Youssef Bassil, “TCP Congestion Control Scheme for Wireless Networks based on TCP Reserved Field and SNR Ratio”. International Journal of Research and Reviews in Information Sciences (IJRRIS), ISSN: 2046-6439, Vol. 2, No. 2, June 2012.

[12]. Saleem Shiek Aalam, R. Manimarn, Syed abuthahir, Deepak Kumar Nayak “Determining Congestion Control In Cognitive Radio Ad Hoc Networks”. International Conference on Green Engineering and Technologies (IC-GET) 2016.

[13]. Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang, IEEE 2010.

[14]. Secure Channels based on Authenticated Encryption Schemes: A Simple Characterization Chanathip Namprempre August 29, 2002.

[15]. Amitabh Mishra and Ketan M. Nadkarni, “Security in Wireless Ad hoc Networks”. In volume the instruction book of ad hoc Wireless Networks, CRC Press LLC, 2003.