Intellectual Routing Mechanism for Improving Qos in Manets for Secure Data Transmission

Raja Rao PBV
Associate Professor,
BVCEC (A),
Odalarevu, Allavaram Mandal
rajaraopbv@gmail.com

Dr. Neeraj Sharma,
Associate Professor,
Dept of CSE-SSSUTMS, Sehore, M.P.

Abstract

A Mobile Ad Hoc Network (MANET) is a consistently self-arranging, infrastructure less system of nodes associated without wires. Every gadget in a MANET is allowed to move autonomously toward any path, and will accordingly change its connects to different gadgets regularly. The essential test in building a MANET is outfitting every gadget with the ability to protect the data eternally for legitimate route support. With the development and expansion of these gadgets in each part of society, the requirement for such gadgets to discuss in a consistent way is getting progressively fundamental and important. Additionally, as MANETs has mobility nature security needs to be improved for secure data transmission avoiding malicious tasks. Continuous applications strengthened by MANETs have strict Quality of Service (QoS) parameters, for example, proficient transmission capacity use, least delay, least loss of packets, great throughput and so on. Giving QoS is a troublesome task in MANETs because of an absence of unified framework based framework, restricted transfer speed accessibility, consistent development of nodes, argument for channel allocation and the exceptionally unique topology of the remote system. In this manuscript an Intellectual Routing Method (IRM) is proposed for improving the QoS in MANETs that decreases the packet loss and increases the throughput of the system. The proposed method is compared with the traditional methods and the results show that the proposed method is exhibiting better performance.

Keywords: Data security, Quality of Service, packet loss, malicious activities, routing method, secure data transmission, network delay

1. Introduction

MANETs are independent frameworks of fixed or portable remote nodes with routing capacities that may work in an independent manner or in heterogeneous system. In spite of the fact that their improvement was at first determined by the necessities of military networks, they are required to hold onto business frameworks too, particularly with the advancing utilization of individual correspondence administrations frameworks. It is imagined that future applications won't be constrained to the necessities of the military applications, however will incorporate a few non military personnel applications also. For example, they can be conveyed in shared system situations, where singular clients need to share or transfer data without relying upon nearby systems [1]. They are a suitable arrangement in circumstances of disasters and rescue activities where the framework based system may not be accessible [2].

The ongoing advances in scaling down, and the proposition of open principles for remote correspondence, have extraordinarily encouraged the arrangement of ad hoc systems and backing for further developed capacities [3]. This enables a node to go about as a remote terminal just as a router and still be sufficiently reduced to be versatile. A self arranging versatile collection of such gadgets associated with remote connections is said to be an ad hoc network [4]. A remote system is ordinarily a decentralized system. The system is ad hoc in light of the fact that every node is eager to transfer information for different nodes, thus the assurance of which nodes forward information is made powerful [5]. The structure of a MNET is depicted in figure 1.

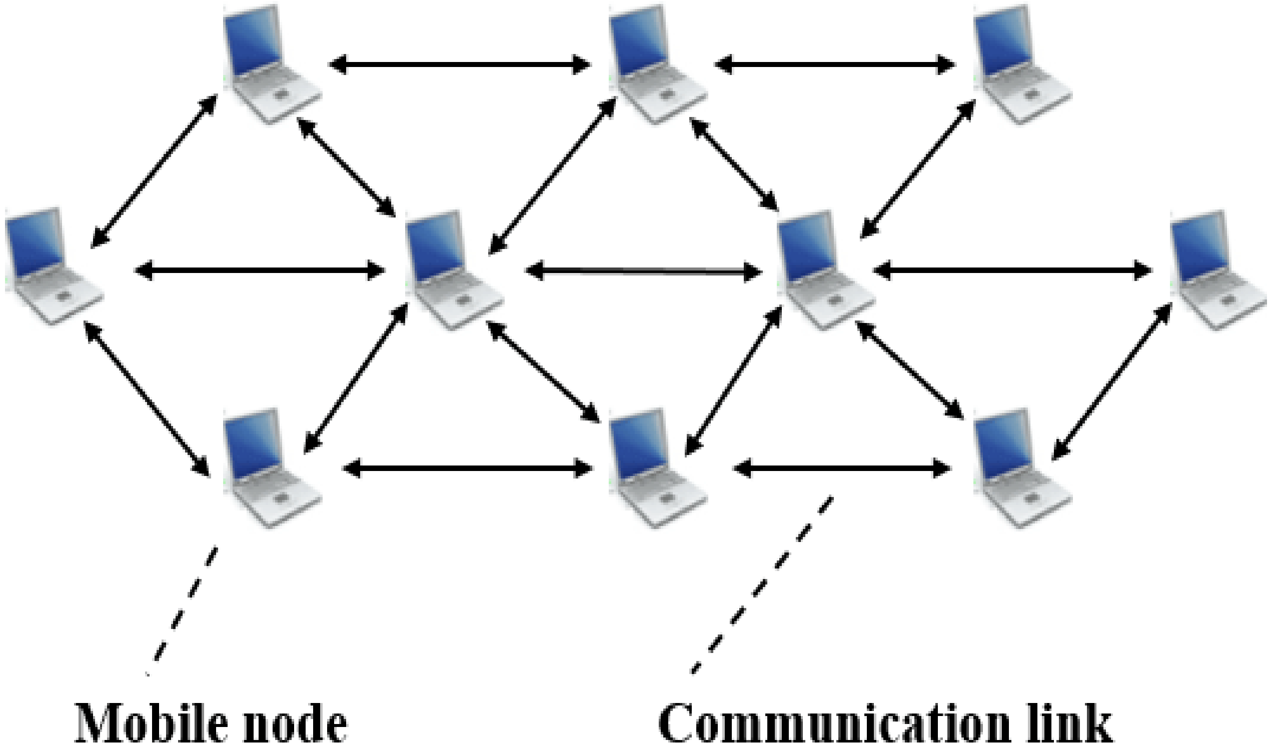

Fig 1: MANET Structure

Different MANET applications incorporate military organizations, rescue tasks, disaster recovery activities, development of system in gatherings and meetings, electronic study halls and so forth. MANETs can be utilized viably where no fixed framework is accessible however ongoing, dependable and interactive media correspondence is required [6]. To give a solid MANET set up that stick to certain QoS parameters, it is important to guarantee that an ideal and strong route is found among source and destinations however because of dynamic nature of MANETs, the issue of routing is significantly more convoluted when contrasted with wired systems [7]. Other than finding an secured route, it is likewise up and coming to give different QoS parameters like great throughput, least delay, least loss of data packets and so on in such systems. Numerous interactive media and constant applications like document sharing, video conferencing, versatile learning and so forth require high data transfer capacity and have severe delay, and data loss prerequisites [8]. Giving continuous applications in MANETs with QoS ensures is a significant testing task as these applications request high data transfer capacity and less delay. Besides, the characteristic idea of MANETs is described by route breakages and failure of nodes because of which QoS in such systems turns out to be still progressively troublesome.

Malicious activities in the network needs to be strictly monitored as some malicious nodes intentionally drops the packets or modifies the contents[9]. Some nodes involve in fake routing also to redirect the data towards malicious nodes, thus increasing the packet loss. Strong routing method need to be designed for secured data transmission with less packet loss and delay[20]. The nodes in the network has to choose a secure path that avoids malicious nodes and the data transfer rate needs to be increased[21]. The delay in the network has to be reduced by transferring the data to the respective nodes successfully.

2. Literature Survey

A Vasilakos et.al.in [1] introduced Quality of Service in MANET. In this method author had exhibited a thought regarding nature of administration in MANET, layered design of QoS, QoS parameters and limitations, QoS provisioning and QoS routing in MANET. Abid M.A et.al.in [2] proposed different difficulties and advances in QoS Routing conventions in MANET. Additionally a review of QoS routing conventions in MANET is projected.

Ankita Sharma and Sumit Vashistha in [2] concentrated on AOMDV-QoS which is adjustment of existing AOMDV utilizing drop minimization under MAC error control strategy like impact minimization and dynamic line plot and so forth. The proposed multipath QoS routing convention dependent on AOMDV improve the system execution.

Chlamtac et al [5] projected AODV routing convention with secured route if there should arise an occurrence of connection failure. On the off chance that one of the route is lost, at that point other is accessible. On the off chance that this route additionally comes up short, at that point another route is accessible. Consequently in this manner improves execution by choosing various secured routes.

Kumar M et al [8] exhibited another convention QAMR dependent on ANT COLONY OPTIMIZATION calculation which gives conceivable way from numerous ways for information transmission. QoS is estimated utilizing measurements, for example, delay, throughput, packet loss.

L Liang et al [9] exhibited a routing convention dependent on AODV. In AODV-QoS the nature of AODV convention for routing has been improved to upgrade the ability of route identification. In this technique the trust limit is considered for route selection nodes participated in communication for increasing the packet delivery rate.

Lindeberg M et al. [11] proposed a AntOR convention depends on Ducatalle calculations. The framework was set up for inadequate settings. Throughput and bundle delay accomplished were found to be superior to AntHocNet however estimation of packet loss was seen as less. AntOR was not contrasted and other routing conventions are not effective when compared to this method. Another burden was that if there should arise an occurrence of littler set up, no improvement was accomplished in overhead routing.

S. Marwaha et al [15] proposed a improved Ant Colony Optimization technique. The greatest test in MANETs with dynamic topology is to discover a way between source node and destination node that fulfills QoS necessities in spite of regular failures in route. An Multiobjective optimization method with respect to QoS Routing calculation (AMQR) is proposed for portable specially appointed systems. In this method, a medium measured framework is considered.

3. Proposed Method

QoS models for MANETs ought to consider the difficulties caused by such frameworks such like unique topology, essential in resources and secured data transmisisons. At first, Internet Protocol (IP) was viewed as the best exertion convention and it was intended to transfer data to destinations accurately. Even accuracy is high, packet delivery rate is low as malicious nodes are more. As the popularity of MANETs are increasing day by day because of no central administration and no infrastructure, special care need to be maintained on the MANETs for providing strong routing mechanism and strong methodology for avoiding malicious nodes in the network.

To improve Quality of Service, a strong routing method is introduced in the proposed method that reduces the packet loss rate and improves the packet delivery rate and also reduces the delay in the data transfer between nodes. The proposed method validates every node involved in the network and checks its behavior for identification of malicious activities. Multiple routes are identified in the proposed method and then stored in the routing information. Because of mobility nature, if any node leaves the network, then another new route is identified and communication is done without any delay.

Algorithm: Intellectual Routing method

```
Step-1:  INPUT: Total Nodes in network N, Text Message TM, Converted Text CT, Source S, and
         Destination D, simulation Time T.
Step-2:  Establish network using N nodes.
Step-3:  Select a Node as Network Head NH.
Step-4:  When nodes want to transfer data, the Source node will send Data Transfer (DT) message
         along with destination id to all the nodes in the network.
```

Step-5: A node which receives DT message, if has a route to destination transfers the DT message till it reaches destination.

Step-6: The NH node will continuously monitor all the activities in the network.

Step-7: A node which DT message first reaches the destination, the route is considered for data communication. Other available routes are also maintained by the NH.

Step-8: When a route is identified, the NH generates the secret key pair as

$$\text{Keys} = \text{set} (\{\text{Public key}(PUK_i) : \text{Private key}(PRK_i)\})$$

Where PUK is the public key and PRK is the private key.

Here keys must be used as pair for both encryption and decryption. After finding the route, the source node has to send PUK request to the NH. The NH verifies the routing table information and then sends PUK to sender and PRK to destination.

Step-9: By using public key, data is encrypted and when it reaches destination, private key is used for decrption.

Step-10: When transaction is completed, the NH calculates the data loss occurred at every node and then marks the nodes as malicious if data lost at particular node is high. The data loss is calculated as

Data Lost at Node (DLN_{LR}) = Data Received by neighbor Node (DR_L) – Data transferred to next neighbor node (DT_L).

Step-11: If the DLN_{LR} > 15%, then the node is considered as malicious node.

Step-12: The entire communication need to be completed within the time T to reduce delay in the network. Otherwise network is removed and new communication is initiated.

Step-13: If there is any delay in the data transmission, it is considered as link/node failure and a new route is selected from the route table available at NH.

The proposed technique contains three stages which are

(a) Limit setting,

(b) Route identification.

(c) Data loss verification.

In the proposed method, every node is verified by the NH node for its behavior in terms of malicious activities. The node which receives the data from neighbor node has to transfer the data immediately to its next node in the routing table for avoiding delay in the network.

4. RESULTS

The QoS method is implemented by setting a MANET using NS2.35. The proposed method improves the quality of service of the network by improving the throughput, packet delivery rate, security levels in the route and reducing the packet loss ratio and delay in the network. The proposed method considers the parameters listed in table 1 for setting up a MANET.

Table 1: Parameters used for creating MANET.

Simulator Used	NS-2.35
Number of nodes	50
Dimension of simulated area	800m×600m
Routing Protocol	AODV
Simulation time	100
Traffic type	CBR(3pkts/s)
Packet size	512 bytes
Number of traffic connections	4 / 25
Node movement at maximum Speed (m/s)	random
Transmission range	250m
Threshold value	10 J
Transmit power	1.5 mJ
Receiving power	1.0 mJ
Idle power	.17 mJ
Sleeping power	.047 mJ

The Proposed method establishes a MANET and a node is selected as Network Head NH nodes which has huge computational capabilities. The selection of NH node is depicted in Figure 2.

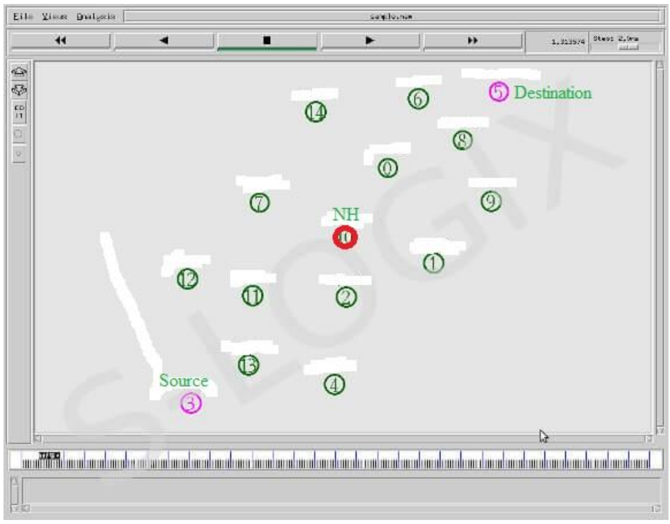

Fig 2¨NH node in MANET

The Proposed IRM method is compared with the traditional Improved AODV (IAODV) method and the results show that the proposed method is exhibiting high packet delivery rate than the existing method. Figure 3 shows the packet delivery rate in the proposed and existing methods.

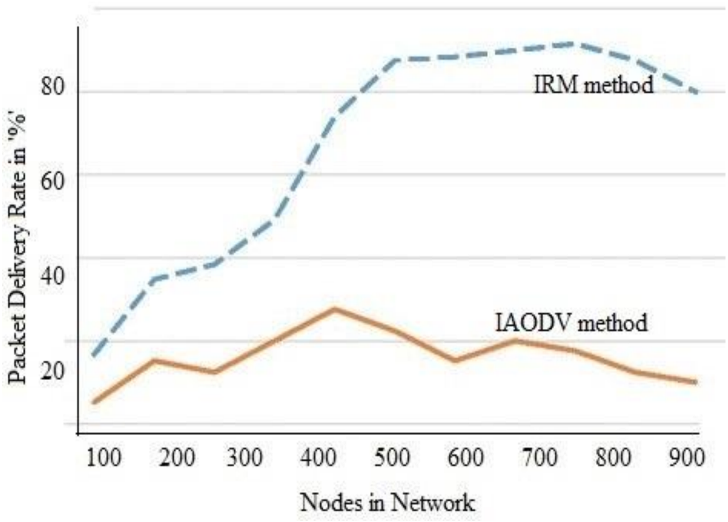

Fig 3: Packet delivery rate

The packet loss ratio is less in the proposed method as malicious nodes are strictly identified and removed from the network. Figure 4 represents the packet loss ratio in the proposed and existing methods.

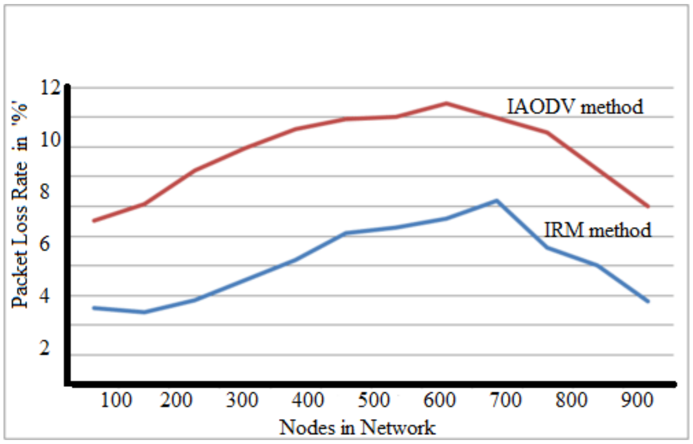

Fig 4 : Packet Loss Ratio

The data in the proposed method is securely transferred to the destination as NH node will monitors all the data levels. Figure 5 illustrates the security levels in the proposed and existing methods.

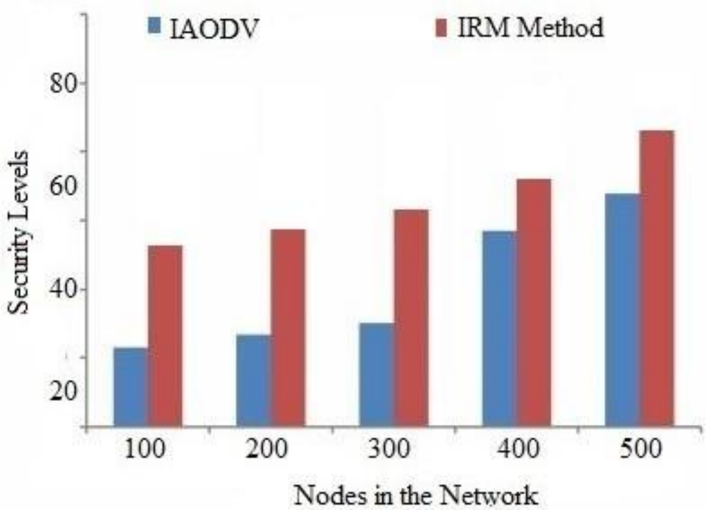

Fig 5: Security Levels

The throughput of the proposed method is high when compared to the existing method. Figure 6 depicts the throughput levels.

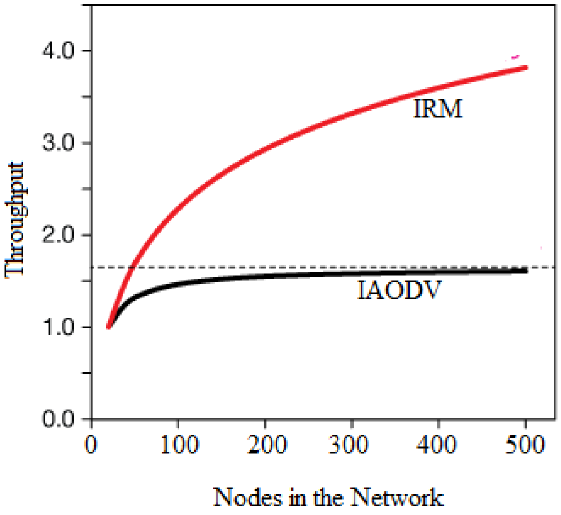

Fig 6 : Throughput Levels

5. Conclusion

QoS prerequisites are particularly significant on account of applications which are utilized in MANETs. These applications necessitate that the framework must stick to certain QoS parameters regarding less packet loss and high packet delivery rate and great throughput. Additionally, routing is incredibly testing in MANETs particularly in a unique topology. Because of continuous change in position of nodes, even the proficient nodes may get unusable or wasteful. To guarantee stable routing it is important to refresh routing data consistently and also to select multiple routes. Be that as it may, this in itself can represent an issue as it brings about more control overhead which should be stayed away from because of constrained assets accessibility. The issue is more when the MANETs are dynamic and medium or huge estimated. The proposed IRM method effectively identifies the malicious nodes in the network and improves the packet delivery rate. In future, the proposed method can be extended by considered only specific nodes to involve in route identification process.

References

[1]. A Vasilakos, MP Saltouros, AF Atlassis, W Pedrycz, Optimizing QoS routing in hierarchical ATM networks using computational intelligence techniques. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. 33(3), 297–312 (2003)

[2]. Abid M.A., Belghith A., (2011). Stability routing with constrained path length for improved routability in dynamic manets, Personal and Ubiquitous Computing, Springer-Verlag, Vol.5, No. 8, 799-810.

[3]. C Busch, R Kannan, A Vasilakos, Approximating congestion + dilation in networks via "quality of routing" games. IEEE Trans. Comput. 61(9), 1270–1283 (2012)

[4]. C.E. Perkins, E.M. Royer, S.R. Das, Ad hoc on demand distance vector routing (DSR). Proceedings of IEEE workshop on mobile computing systems and applications 1999: 90–100

[5]. Chlamtac I., Conti M., Liu J.N., (2003). Mobile ad hoc networking: imperatives and challenges, Ad Hoc Networks, Elsevier, Vol. 1, Issue 1, 13-64.

[6]. Farkas K., Wellnitz O., Dick M., Gu X., Busse M., Effelsberg W., Rebahi Y., Sisalem D., Grigoras D., Stefanidis K., Serpanos D.N., (2006). Real-time service provisioning for mobile and wireless networks, Computer Communications, Elsevier, Vol. 29, Issue 5, 540-550.

[7]. Lakshman Narayana Vejendla and Bharathi C R,(2017),"Using customized Active Resource Routing and Tenable Association using Licentious Method Algorithm for secured mobile ad hoc network Management", Advances in Modeling and Analysis B, Vol.60, Issue.1, pp.270-282.DOI: 10.18280/ama_b.600117

[8]. Kumar M., Rashmi M., (2012). An overview of manet: history, challenges and applications, Indian Journal of Computer Science and Engineering, Vol. 3, 121-125.

[9]. L Liang, Y Song, H Zhang, H Ma, A Vasilakos, Physarum optimization: a biologyinspired algorithm for the Steiner tree problem in networks. IEEE Trans. Comput. 64(3), 818–832 (2015)

[10]. Lee K., (2012). A backup path routing for guaranteeing bandwidth in mobile ad hoc networks for multimedia applications, Multimedia Tools and Applications, Springer Science + Business Media, Vol. 57, No. 2,439-451.

[11]. Lindeberg M., Kristiansen S., Plagemann T., Goebel V., (2010). Challenges and techniques for video streaming over mobile ad hoc networks, Multimedia Systems, Springer-Verlag, Vol. 17, No.1, 51-82.

[12]. P Li, S Guo, S Yu, A Vasilakos, Reliable multicast with pipelined network coding using opportunistic feeding and routing. IEEE Trans. Parallel Distrib. Syst. 25(12), 3264–3273 (2014)

[13]. P. Li, S. Guo, S. Yu, A. Vasilakos, CodePipe: an opportunistic feeding and routing protocol for reliable multicast with pipelined network coding. IEEE INFOCOM 2012: 100–108

[14]. Reddy T.B., Sriram S., Manoj B., Murthy C.S.R., (2006). MuSeQoR: Multi-path failure-tolerant security-aware QoS routing in ad hoc wireless networks, Computer Networks, Elsevier, Vol. 50, Issue 9, 1349-1381.

[15]. S. Marwaha, D. Srinivasan, C.K. Tham, A. Vasilakos, Evolutionary fuzzy multiobjective routing for wireless mobile ad hoc networks. Evolutionary Computation, 2004. CEC2004. Congress on 2, 1964-1971, 2004

[16]. SS Chaudhari, RC Biradar, Survey of bandwidth estimation techniques in communication networks. Wirel. Pers. Commun. 83(2), 1425–1476 (2015)

[17]. T Meng, F Wu, Y Zheng, G Chen, A Vasilakos, Spatial reusability-aware routing in multi-hop wireless networks. IEEE Trans. Comput. 65(1), 244–255 (2016)

[18]. XM Zhang, Y Zhang, F Yan, A Vasilakos, Interference-based topology control algorithm for delay-constrained mobile ad hoc networks. IEEE Trans. Mob. Comput. 14(4), 742–754 (2015)

[19]. Ye Z., Srikanth V. K., Tripathi S.K., (2004). A routing framework for providing robustness to node failures in mobile ad hoc Networks, Ad Hoc Networks, Elsevier, Vol. 2, Issue 1, 87-107.

[20]. Lakshman Narayana Vejendla and Bharathi C R,(2017),"Identity Based Cryptography for Mobile ad hoc Networks", Journal of Theoretical and Applied Information Technology, Vol.95, Issue.5, pp.1173-1181. EID: 2-s2.0-85015373447.

[21]. Lakshman Narayana Vejendla and Bharathi C R,(2017),"Using customized Active Resource Routing and Tenable Association using Licentious Method Algorithm for secured mobile ad hoc network Management", Advances in Modeling and Analysis B, Vol.60, Issue.1, pp.270-282. DOI: 10.18280/ama_b.600117.

[22]. Yen Y.-S, Chang R.-S., Chao H.-C., (2009). Flooding-limited for multi-constrained quality-ofservice routing protocol in mobile ad hoc networks, IET Communications., Vol. 2, No. 7, 972-981.

[23]. Y-S Yen, H-C Chao, R-S Chang, A Vasilakos, Flooding-limited and multiconstrained QoS multicast routing based on the genetic algorithm for MANETs. Math. Compute. Model. 53(11-12), 2238–2250 (2011)