A Survey on Provisioning of Quality of Service (QoS) in MANET

Tegegn Ayalew Hailu[1], Arappali Nedumaran[2]

[1,2]Department of Electrical and Computer Engineering, Kombolcha Institute of Technology-Wollo University, Ethiopia.
E-mail:ayalewtegegn2008@gmail.com[1], maran.van@gmail.com[2]

Abstract - Mobile Ad Hoc Network (MANET) applications such as multimedia applications, audio/video conferencing, VOIP and webcasting need uninterrupted, stringent and inflexible Quality of Service (QoS). The provision of QoS guarantees in MANET is more challenging and difficult than wired network because of node mobility, lack of centralized control and a limited power supply. A lot of researches have been accomplished and also ongoing so far to offer QoS guarantees by designing QoS models and protocols. In this paper issues and challenges of QoS, overview of QoS routing metrics, and various performance metrics have been discussed. In future, Mobile Ad Hoc Networks (MANETs) may provide access to services in the Internet. MANETs should therefore support diverse applications and data types. This introduces a need for QoS, a process of discriminating different data types to provide them with an appropriate level of service. However, QoS can be affected by nodes performing packet forwarding attacks, packet delivery, end to end delay, node mobility and bandwidth are the dominant concern of QoS. A critical analysis of the related literature shows that research into QoS and security has typically proceeded independently.

Keywords - Mobile Ad Hoc Network (MANET), Quality of Service (QoS), Nodes, VOIP and webcasting, Protocols.

I. INTRODUCTION

Ad Hoc Network: Ad Hoc means wireless and infrastructure-less network. It is classified as Mobile Ad-Hoc Network (MANEN), Vehicular Ad-Hoc Network (VANET) and Wireless Sensor Network (WSN). A Mobile Ad Hoc Network (MANET) is a collection of well-defined mobile nodes. This network is an infrastructure less network because such network does not have any fixed infrastructure. The mobile nodes are dynamically change the topology and paths between themselves to transfer the data packets from one node to another node and it is self-organizing network, Each and every mobile nodes are acts as a host and router .when Request (REQ)/Replay (REP)/Error (RERR) information from/to in the network and route determining and preserving routes other nodes in network in Fig 1.

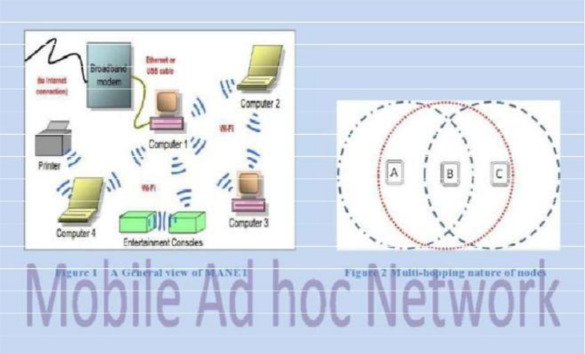

Fig. 1. Manets Structure

Its topology frequently keeps on changing with time, that ‘why, routing path are formed and deleted arbitrarily due to the node’s mobility. QoS guarantee is much more challenging task in wireless multi-hop networks than wire line networks because of its mainly multi-hop communication, frequently varying topology, interference, distributed on-the-fly nature and channel access contention. Some of the features of MANET are compared with one of the other wireless ad hoc network (Sensor Network) in Table 1 [16].

Free-space optical communication (FSO) is a technology that uses light which propagates in free space to send data wirelessly for communications. “Free space” means air. The technology is useful where the physical channel is not possible due to high costs. FSO is a technology which is used mainly for high bandwidth and in wireless communication links.

TABLE 1: COMPARISON OF FEATURES OF MANETS AND AD HOC SENSOR NETWORKS.

Features	MANET	Ad Hoc Sensor Networks
Mobility	Varies (slow To fast)	Limited
Decentralized	Yes	Yes
Energy deficient	Yes. But this is of secondary importance as battery packs can be replaced	Yes, it is of Primary importance
Bandwidth deficient	Yes	Sometimes
Data rate	High	Low [1-1000 Kbps]
Flow of data	Bi-directional	Mostly Unidirectional [sensor to sink]
Fault tolerance	Needed is mobility increases	Needed only if Nodes exhaust available energy or are moved
Main Goal	To optimize QoS and high bandwidth efficiency	Prolonging the Life of the network through aggressive energy management, to prevent connectivity degradation.
Traffic	Multimedia rich	Statistical and Multimedia
Basic features of Routing protocol	Loop free, energy and bandwidth efficient, secure, Provides QoS, fault tolerant and reactive instead of proactive, and distributed in nature	Most of the same features as for MANETs, but with Less emphasis on mobility and more emphasis on energy efficiency, scalability, and multipath connectivity.
Redundancy in data	No	Very few
QoS	Highly needed	Lesser as compared to MANET

In FSO, an optical transceiver is placed on each side of a transmission path to establish a network link [14].The transmitter is an infrared (IR) laser or LED that emits a modulated IR signal. Link availability can be maintained under utmost weather conditions (except heavy fog, heavy rain has little effect) [14]. Most of the mobile devices are equipped with single transceivers and it operates in single-channel mode hence more amount of bandwidth is wasted. To mitigate this problem, all mobile nodes have to be equipped with multiple transceivers. Enhancement of the present MAC protocol can give better performance on multichannel with single transceiver. In such networks the main challenged task is how to design MAC protocol with the following futures. Here Carrier séance media access (CSMA) based medium accesses control protocol for multi-hope wireless network is proposed.[13]. In which channel selection is based on signal to interference and noise ratio at the receiver. Although this method increases the throughput up to 50% there is delay in performance due to high packet transmission. Before discussing the term and definition of QoS, explanation about the different types of classifications of MANET protocols and their perspective nature of QoS is presented.

A. Classification of Routing Protocols in MANET

Routing protocols can be classified into proactive routing, reactive routing, and hybrid routing in the MANETs [2].

1). Proactive or Table-driven Routing Protocol: A proactive routing is called a “table-driven” routing protocol [3]. In proactive routing protocols, the routes to all the destinations (or parts of the network) are determined at the start-up and maintained by using a periodic route update process. Examples are:

- Destination-Sequenced Distance Vector (DSDV),
- Optimized Link State Routing (OLSR) Protocol,
- Wireless Routing Protocol (WRP) ,
- Topology Broadcast Reverse Forwarding (TBRF) ,
- Fisheye State Routing (FSR) [2].

All such type of protocols has setup delay performance problem and flow control congestion problems when each protocols applied alone itself.

2) Reactive or On-Demand Routing Protocol: Reactive routing protocols for mobile ad hoc networks are also called “on-demand” routing protocols. In this type of protocol connections are made when needed [2]. Ste-up delay is reduced in such a way that both connection and set up time is done at a time. An example of such protocol includes:

- Dynamic Source Routing (DSR) Protocol ,
- Ad hoc On-Demand Distance Vector (AODV) ,
- Cluster-Based Routing Protocol (CBRP) and
- Temporally Ordered Routing Algorithm (TORA).

In reactive MANET packet can send after connection is established based on, on demand request as AODV protocol with three information, RREQ, RREP and RERR, as star topology,

3) Hybrid Routing Protocol: The combination of both proactive and reactive routing protocols are called hybrid routing protocols. Normally, the hybrid routing protocols for mobile ad hoc networks utilize hierarchical network architectures [14]. Examples are –

- Zone Routing Protocol (ZRP)
- Distributed Dynamic Routing (DDR) Protocol
- Zone-Based Hierarchical Link State (ZHLS)

- Distributed Spanning Trees Based Routing Protocol (DST)

The classification of MANET routing protocols based on data transmission mode: [17].

- Unicast, when there is one sender and one receiver.(it has delay problems in QoS)
- Multicast,(ie tree, mesh and hybrid), when there are multiple sender and multiple receiver (it has mobility, security and node selection problems)and,
- Broadcast. When there is one sender and multiple receivers.

There are different protocols where performance is analyzed, and it is very difficult to develop good performance of MANET protocol. OLRS, AODV, and DSDV are among the most studied protocols and they are used as the cooperation as bench marks [4]. However, analyzing protocols performances in MANETs is a complex task. For each scenario, several critical parameters (e.g., number of nodes, number of connections, data rate, node velocity, security and attack, mobility, resource optimization, quality of service(QoS), and pause time) must be accurately controlled to satisfy the required characteristics of the performance analysis. Securing routing protocols against misbehavior and malicious nodes is highly challengeable in MANET security. In ad hoc networks one of the most challenging attacks to defend against is the black-hole attack and grey hole attack.[6].

In the previews research work of journals, it was tried to solve the different types of protocol design in MANET, with the consideration of both QoS and security, once independently and in another research as a hybrid task but stile it is impossible to achieve both requirement at a time. Let us consider some of the attacks in MANET which affect QoS as a major issue. Even this is another active area in Ad Hoc Network researchers, it is also considered as provisioning of QoS in Ad Hoc Network as follow:

B. Some common attacks in MANET

- Routing Attacks: The traffic of the network can be routed to other nodes when routing attack is trigger. The destination node is free here.
- Eavesdropping Attack: The attacker collects the secret information such as the passwords or private keys from the network
- Black hole Attack: Fresh path to reach destination. But not forward packets to destination. In cooperative black hole attack malicious nodes work together in a team.
- Wormhole attack: In wormhole attack packets are received from the one end of the network and the rest of the traffic is sent to another side, then traffic delay of other node happens.
- Jamming Attack: Abundant packets are sent to specific node by the malicious nodes and packets are not capable to be handled by the node. The network will be blocked in such type of condition
- Man-in-the-Middle Attack: When the two parties that is exchanging information between each other, and the third party (attacker) lies between any information being exchanged amongst them can be detected by the attacker. There is a need to get hold on the information being transferred between two parties.
- Denial-of-Service Attack: The Large no. of burst packets is sent with respect to the legal nodes in this scenario by showing illegal sources as legal ones.
- Replay:An attacker in replay attack misuses the mobility feature in MANETs by resending previously recorded packet and causing other nodes in the network to store stale route in their routing tables.

C. Network Quality of Service

As a conclusion, When multiple data types are involved there is a need to address the issue of Quality of Service (QoS). QoS is the process of differentiating traffic types so that a certain set of requirements can be satisfied in terms of a set of constraints. In other words, QoS is a process of discriminating deferent packet types to provides them with an appropriate level of service. Data within a MANET may have different priority requirements, just as they do in traditional fixed networks. These requirements are typically satisfied by servicing higher-priority traffic before lower-priority traffic.

As a MANET can be used to extend the Internet, it should therefore aim to provide a comparable level of QoS. However, the characteristics of a MANET may present a challenge to the way in which QoS can be provided. In traditional networks QoS is supported by the presence of infrastructure, which includes routers. The position of a router is fixed in such networks. In infrastructure-less MANETs, routers, which are peer communication nodes, are also mobile. The dynamic nature of MANETs therefore presents a significant challenge to QoS provisioning. In addition, the issue of QoS provisioning is further complicated by the fact that not all communication nodes may be able or willing to participate in the routing (packetforwarding) process.

II. Related Works

Mahmoud Abu-Zant and Dr. Mohammad Hamarsheh [3], presented a performance comparison between TCP variants with a different reactive routing protocol. The comparison is held by running a simulation scenario many times using NS2.Three performance metrics were used to compare the performance of TCP variants Throughput, Jitter, and Packet drop. TCP variants perform in a similar way in both DSR and AODV routing protocol. There is no much effect on the routing protocol on the TCP variants. TCP-Vegas outperform the other two variants in all parameters, packet drop, throughput, and jitter. The results show that DSR has better performance compared with AODV, because DSR routing protocol mechanism outperforms AODV at low traffic, nodes and mobility. It generates less routing load and depends more on caching. But there is not any consideration of QoS such as, number of nodes, number of connections, data rate, node velocity, security and attack, mobility , resource optimization, quality of service(QoS), and pause time.

Mohamed Skander Daas and Salim Chikhi [4], In this paper the Response Surface Methodology (RSM) For Performance Analysis and Modeling of MANET Routing Protocols is designed based on Box–Behnken design and NS- 3 simulations with the consideration of the following six metrics. T First Rx Packet and t Last Rx Packet ,delay Sum and jitter Sum , tx Packets , rx Bytes and rx Packets ,times Forwarded and tx Routing Packets. Eighteen empirical quadratic mathematical models are developed using the Box–Behnken design. The models can be effectively employed to analyze, optimize, and accurately predict the six performance metrics under a given configuration of five parameters. The presented response surface plots provide an extensive exploratory analysis and comparison of these metrics, and give insight into the effects of various parameters. Developing models rather than conducting traditional experimental analysis is important; various models can be exploited by a third party to extract, analyze, or compare performances without performing additional specific experiments. The matimatical modeling of performance in such metrics are new and appreciated, but some metrics like MAC protocol, node mobility and security are not considered and also difficult to achieve both security and performance at a time in MANET. M. Jeevamaheswari. The MAODV protocol has been detect the way of packet dropping nodes in MANET and thus forwarding a secure route from source to destination nodes and then avoiding the malicious nodes due-to black and gray-hole attack. The studied experimental results have been verified using with ns-2 and compared with the AODV and (Association based –Data Routing Information) AB-DRI security approach. In this proposed work each node should be maintain additional AB-DRI table, in bit “ 1” is denoted by true at the same time bit “0” denoted by false. This work is not tested to other protocol with packet dropping and should test for the future. [1][6]. Neelam Janak Kumar Patel, Dr. Khushboo Tripathi: There is two kinds of attack in MANET: Packet dropping and modification. In this paper the author proposed a trust value algorithm using IDS AODV that secure the network routing activity from the attacker using clustering approach based on energy i.e nodes with higher energy should selected as cluster head which is trusted to all nodes. If the particular node is properly transmitted data packets from one node to another node, then each time the trust value of reliable node will increase by 1.When a trust value of a specific node is equal or more than the threshold value then it node will be considered as a genuine node for further communication. When a trust value of the specified node is less than the threshold value then it will be treated as the packet dropper or modifier node and it will be called as a malicious node for more communication and re-updates the table to be trusted in all communication. The proposed technique will be based on to analyze the route reply packets in which the nodes reply with the exceptional high sequence number is add into blacklist. But the technique is not tested for other attaches like Worm-Hock attack [2][8][10].

Salem Sati, Ahmed El-bareg [11], tried to compare performance of the two proactive routing protocols Babel and Optimized Link State Routing Protocol(OLSRP) in MANET. Their evaluation and experiments are based on a testbed with various node mobility conditions at different traffic loads. Regarding the throughput metric OLSR protocol considered as better than Babel especially in the large scale and dense networks. In these networks as the number of hops increases in the path the throughput decreases with about 15 percentages. But they are not considered more MANET routing protocols, Furthermore, deep investigation of the comparison between proactive, reactive and hybrid routing protocols is needed to conclude as which protocol has best performance. Faisal Ahmed and Fakir Mashuque Alamgir: This is another compression study of AODN and OLSR routing protocols based on the End-to-end dela, Throughput, Packet loss, Packet delivery ratio and Routing overhead.

AODV is a reactive protocol and creates a very low routing overhead due to discovering routes only when needed, OLSR is proactive in nature. But the authors cannot consider node mobility and security as compares ion. [12]. Ad-hoc Multichannel Negotiation Protocol (AMNP) and Reliable Broadcast Algorithm (RBA) are proposed to the multi-hop MANET transmission capacity to be improved by adopting parallel multichannel access schemes. Protocol addresses the problems like multichannel hidden terminal problem and the multichannel broadcast problem. This is due to those mobile nodes that cannot listen to all channels simultaneously. The protocol is working based on In IEEE 802.11 the sender and the receiver should perform a four way handshaking mechanism: Request-to-send/clear-to-send (RTS/CTS), data, and acknowledgment (ACK) when they have data to transmit in the same channel. [13]. This protocol is not compared with directional antenna as collision avoidance.

Kavitha Balamurugan [14], in this paper the authors tried to develop Hierarchical protocol using Free-Space-Optical(FSO) communication of IR and optical communication in unidirectional way by clustering method. The clustering process mainly depends on the neighbor discovery algorithm (NDA). The performance of the Hierarchical Routing protocol with Optical Sphere for Smooth Routing (HROS) is evaluated through NS-2 simulation.

In this work [15], the authors considered the four performance measures in an ad-hoc network by varying parameters i.e. message delivery ratio, loss of packets, average end-to-end delay and throughput with different number of nodes (100 nodes), different speed of nodes. Consider the simulation results in the table below.

From results reported in the table above concluded that FAODV protocol is the best in terms of average MDR. Large numbers of packets are loss as well as large number of packets dropped when a DSDV routing protocol apply for this networks. Message packets loss and dropping the packets when a transmission occurs are based on variety of nodes, with in their region. FAODV works with less packet losses than other routing techniques. The NS-2 based simulation has confirmed that the advantages of FAODV and demonstrated for the improvement of packet delivery, reduction of delay in end-to-end, throughput are compared with DSR, DSDV. In future, energy metrics to be considered with these performance measures for design such a protocol that can be provide best data delivery in high random mobility network. Analyses the energy metrics for QoS applications for better routing and broadcasting the message.

TABLE 1. METRICS

Metrics	100 node		
	FAODV	**DSR**	**DSDV**
Generated Packets	5679	16254	3736
Received Packets	5619	15831	1503
Message Delivery Ratio	98.9%	97.4%	40.3%
Total Dropped Packets	25	15	37
Average End-to-End	346.37	193.40	262.48
Delay[ms] Average	165.42	465.99	243.39
Start time	10.0	10.3	103.0
Stop time	1499.9	150.0	128.7
Send line	5679	15902	1569
Receive line	5619	15831	1503
Forward line	11061	6133	1526
Ratio	0.98	0.99	0.95

III. ISSUES TO QOS IN MANET

The goal of QoS provisioning is to get more deterministic network behavior, so that information carried by the network can be better delivered and network resources can be better utilized [16]. There are significant issues related to QoS solutions in MANET which have been discussed below.

Mobility of the node: here the nodes are mobile and they move independently and randomly to any direction by any speed, the topology information has to be updated frequently so as to provide routing to reach the final destination which result in again less packet delivery ratio and bound to affect the QoS.

Unreliable channel: The bit errors are the main problem which arises because of the unreliable wireless channels. These channels cause high bit error rate and this is due to high interference, multipath fading effects and so on. This leads to low packet delivery ratio. Since the medium is wireless in the case of MANETs, it may also lead to leakage of information into the surroundings, a serious threat to QoS in network Scalability: Although, the heterogeneous networks (MANET) consist of different nodes with different resource but still has better scalability as compared to homogenous networks. Maintenance of route: the nat5ure of MANET is dynamic and the path may be Brocken even if during the transmission stage of packets. That 'why the need for maintenance and developing of paths in MANET with minimum routing overhead and delay causes the QoS which needs more investigation still now.

Limited power supply: In MANET, Offering QoS to the network absorb more power because of overhead from node which may drain the node's power quickly and it is another researcher area.

Lack of centralized control: The node in MANET can join or leave dynamically and the network is set up unexpectedly. So, there is not an any provision of centralized control on the nodes which leads to increased algorithm's overhead and complexity, as QoS state information must be disseminated efficiently. .

Security: although considering security Leeds another QoS problems and vice versa, Security provision must be considered as an important QoS attribute in MANET. Hence, we need to design more security-aware routing algorithms for this kind of network.

IV. EVALUATION METRICS FOR QOS ROUTING PROTOCOLS

In MANET each application has its own different requirements and the services. The related QoS parameters in the network differ from application to application. For instance, in the multimedia applications, packet loss, delay, bandwidth and jitter (delay variation) are the main QoS parameters, whereas in the military type applications strict and reliable security requirements are demanded. [16].

To develop MANET with QoS, the value of a metric over the entire path can be one of the following compositions: Additive metrics- This is an examples of delay in MANET and can be represented mathematically as follows

$$m(p) = \sum_{i=1}^{LK} m(lki) \tag{1}$$

where m (p) is the total of metric m of path (p), lki is a link in the path (p), LK is the number of links in path (p), and i= 1, LK delay, delay variation (jitter) are examples of this type of composition.

Concave metrics: This is an example of residual Bandwidth and can be represented mathematically as follows:

$$min\ (m(lki)). \tag{2}$$

Multiplicative metrics. This is an example of packet loss probability and can be represented mathematically as follows:

$$m(p) = \prod_{i=1}^{LK} m(LKi) \tag{3}$$

Convex metrics: This can be represented as the maximum of all metric along the path m(p)=max(m(lki)) (4)

Here, vulnerability (in context of security) and throughput use the convex rule. Whatever the metrics used in determining the path, these metrics must represent the basic network properties of interest. These metrics include residual bandwidth, delay, and jitter. Therefore, the flow of QoS requirements has to be mapped onto path metrics in MANET. Hence the metrics illustrate the types of QoS guarantees, a network can support [16].

V. Performance Metrics used for MANET with QoS

The set of constraints in the network which tend to regulate for a specific link to satisfy the requirements for a specific application is known as QoS metrics. The following are sample of the metrics commonly used by applications to specify QoS requirement in must literatures.

A. Throughput

In MANETs throughput is a measure as a rate of successful packets delivery over a wireless channel. This data can be forwarded over logical link, or pass through a neighbor nodes. The throughput is generally measured in bits per second (bps), or sometimes in data packets per second, or data packets per time slot.

Throughput= Total packet received/ amount of forwarded packet over certain time interval

B. Dropped Packets

These are the number of packets that sent from the source node and fail to reach the destination node.

Dropped packets = sent packets from source minus received packets at destination

C. Mean inter arrival time

Mean inter-arrival time is the summation of inter-arrival times by the number of received packets and can be computed by the following equation:-

$$av = (\sum ai/n) \qquad (5)$$

where av = mean inter arrival time, ai = arrival time of the packet and n = number of received packets.

D. Average end to end delay

It represents the time required to move a packet from source node to destination node. The average end to end delay can be calculated by summing the times taken by all received packets divided by its total number

$$\sum(received\ time - sent\ time)/\sum(number\ of\ packet) = (\text{E-2-E delay})$$

It is the accumulation of queuing delay, transmission delay and end system processing delay in mobile node; propagation delay in the links. Lesser End to End delay (E-2-E)) implies better performance in network.

E. Jitter

In MANET, Packet jitter is measured as an average of the variation in latency from the network mean latency. However, the standard based term is "packet delay variation" (PDV) which is an important quality of service (QoS) factor in assessment of network performance. A network with constant latency has no jitter.

$$Jitter(J) = Di + 1 - Di \qquad (6)$$

Where Di+1 is the delay of ith+1 packet and Di is the delay of ith packet.

F. Packet delivery fraction (PDF)

It can be expressed as the ratio of the delivered packets at destination to the packets sent from the source node. [16]. PDF= 100*(Number of received packets / Number of sent packets)

G. Normalized Routing Load metric

The routing load metric evaluates the efficiency of the routing protocol. Note, however, that these metrics are not completely independent. For example, lower packet delivery fraction means that the delay metric is evaluated with fewer samples. In the conventional wisdom, the longer the path lengths, the higher the probability of a packet drops. Thus, with a lower delivery fraction, samples are usually biased in favors of smaller path lengths and thus have less delay.

VI. Conclusion

At the start of this survey, the related literature was read critically and analyzed. MANET characteristics, performance metrics and security threats were investigated to understand their implications on QoS provisioning. It was observed that there is plenty of literature covering performance metrics and security or QoS, but there is little which addresses both issues together. The aim of this study was to analyze critically the existing approaches (1) To provide evidence that security and QoS should be integrated to achieve QoS, but still there is a gap where both security and performance of QoS are not achieve at the same time easily based on current research results, (2) To identify the areas where provisioning of QoS will be covered with their current and feature works and (3) To use the insights gained from the study to inform the designs of the novel solutions presented in this survey as basics of metrics and requirements as provisioning of QoS in MANET where we have discussed several issues and challenges involved in providing QoS. A basic overview of QoS metrics and design considerations is also provided with the summarized QoS routing metrics and performance measurements for MANET.

REFERENCES

[1] M. Jeevamaheswari, R. Anandha Jothi, V. Palanisamy "AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack In MANET", IJSRST, vol. 4, no. 2, 2018.

[2] Neelam Janak Kumar Patel, Khushboo Tripathi, "Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method," IJSRSET, vol. 4, no. 4, pp. 281-287, 2018.

[3] Mahmoud Abu-Zant and Mohammad Hamarsheh, "A Comparison of Congestion Control Variants of TCP in Reactive Routing Protocols MANET," International Journal of Computer Science & Information Technology, vol. 9, no 6, pp. 25-33, 2017.

[4] R. Ganesh Babu and V. Amudha, "Comparative Analysis of Distributive Firefly Optimized Spectrum Sensing Clustering Techniques in Cognitive Radio Networks", Journal of Advanced Research in Dynamical and Control Systems, vol.10, no.9, pp.1364-1373, 2018.

[5] Mohamed Skander Daas and Salim Chikhi, "Response Surface Methodology for Performance Analysis and Modeling of MANET routing Protocols," International Journal of Computer Networks & Communications, vol.10, no.1, pp. 45-61, 2018.

[6] Karthika, Vidhya Saraswathi, "A Survey of Content based Video Copy Detection using Big Data", International Journal of Scientific Research in Science and Technology, vol. 3, no. 5, pp. 114-118, 2017.

[7] R. Ganesh Babu and V. Amudha,"Allow an Useful Interference of Authenticated Secondary User in Cognitive Radio Networks", International Journal of Pure and Applied Mathematics, vol. 119, no. 16, pp.3341-3354, 2018.

[8] K. Rama Krishna Reddy, "Improved Protocol Design with Security and QoS over MANET," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, no. 1, pp. 735-739, 2018.

[9] Dimpal Joshi, Nisha Velani, "A Study of Modified Routing Protocols in MANET," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, no. 1, pp. 1621-1624, 2018.

[10] Nitika Singhi, "Analysis of Key Management Schemes in MANET," International Journal of Applied Environmental Sciences, vol. 13, no. 2, pp. 161-169, 2018

[11] Veerpal Kaur, "A Hybrid and Secure Clustering Technique for Isolation of Black hole Attack in MANET," International Journal of Advanced Research in Computer Engineering & Technology, vol. 7, no. 3, pp. 230-237, 2018.

[12] Mahesh Dandugudum, Nagendar Yamsani, "Difficulties of MANET for Mobile Social Networks," International Journal on Computer Science and Engineering, vol. 10, no. 1, pp. 1-6, 2018.

[13] Karthika, Vidhya Saraswathi, "Digital Video Copy Detection Using Steganography Frame Based Fusion Techniques," In: Pandian D., Fernando X., Baig Z., Shi F. (eds) Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering, Lecture Notes in Computational Vision and Biomechanics, vol. 30. Springer, 2017.

[14] Hardik N. Talsania, Zishan Noorani, "A Survey on Techniques to Handle Black Hole Attack for AODV in MANET," International Journal for Innovative Research in Science & Technology, vol. 4, no. 10, pp. 33-37, 2018.

[15] Salem Sati, Ahmed El-Bareg, "MANET Testbed using Raspberry PIs," I.J. Wireless and Microwave Technologies, vol. 2, pp. 52-63, 2018.

[16] Karthika, Vidhya Saraswathi, "Content based Video Copy detection using Frame based Fusion Technique," Journal of Advanced Research in Dynamical and Control Systems, vol. 9, vo. sp. 17, pp. 885-894, 2017.

[17] Faisal Ahmed, Fakir Mashuque Alamgir, "Simulation-based Proportional Study of Routing Protocols for MANET," International Journal of Computer Networks and Communications Security, vol. 5, no. 12, pp. 271-276, 2017.