© 2017 IJSRST | Volume 3 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

SCMR : Secure Cognizant Multipath Routing for MANET

Madgula Vijaya Bhaskar*[1], Prof. G. A. Ramachandra[2], Y. Deepika[3]
*[1]Research Scholar, Computer Science & Engineering, Rayalaseema University, Kurnool, Andhra Pradesh, India
[2]Computer Science, Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India
[3]Computer Engineering, Government Polytechnic, Dharmavaram, Andhar Pradesh, India

ABSTRACT

A MANETs is a multihop system that comprises of multiple mobiles over wireless nodes. We propose cognizant multipath routing for security by establishing multiple paths under routing metrics over source destination in MANET (Mobile Ad hoc Network). Two paths are considered in this paper for transmission between source and destination. Use of AOMDV protocol helps to determine the optimal route for transmission of data for the reducing energy consumption. So, to overcome these issues security analysis algorithm is provided which provides key authentication for threats. Also, security algorithm is used to provide a safe path between source and destination during transmission of data packets. The aim of this paper is to develop a security over multipath routing protocol for MANET. Also, to improve the performance parameter such as throughput and packet delivery ratio by detecting anonymous activity in a network and hence avoid the attackers in routing. A black hole attack type of DoS (Denial of Service) is considered in this paper, constitutes a severe threat against multipath routing. Also, it makes the destination node as unreachable or downgrades its communication over an entire network. Finally, the performance parameters of throughput, packet delivery ratio, an end to end delay, and energy consumption are calculated for SCMR and compared with the existing protocol. On the other hand, the node failure is analyzed by the collection of information about the node respectively.

Keywords: MANET, multipath routing, AOMDV, MAC layer, DOS attack.

I. INTRODUCTION

Mobile ad hoc network (MANET) is one of the self-organized multi-hop system that includes multiple mobile wireless nodes[1] MANETs is said to be a wireless ad-hoc network that consists of network routing environment at the top of the link layer. Multiple routes are determined by AOMDV protocol between source and destination. Because in case any route failure occurs during transmission in multipath routing then that can be recovered by the use of AOMDV protocol respectively. AODV has an ability to balance the load and to avoid the occurrence of traffic. Furthermore, there will be an increase in reliability. Also, loop free nodes are created and maintain its connectivity. AOMDV protocol establishes many routes over demand. Since it is one of the efficient and fast recovery protocol from failure [2]. Nodes that are connected to network exploited as routers for rapid delivery of data packets. Routes consist of link connection between two intermediate nodes. Typical change in link connection may influence the route quality. [3]. Mobile Ad-hoc network is shown in figure 1.

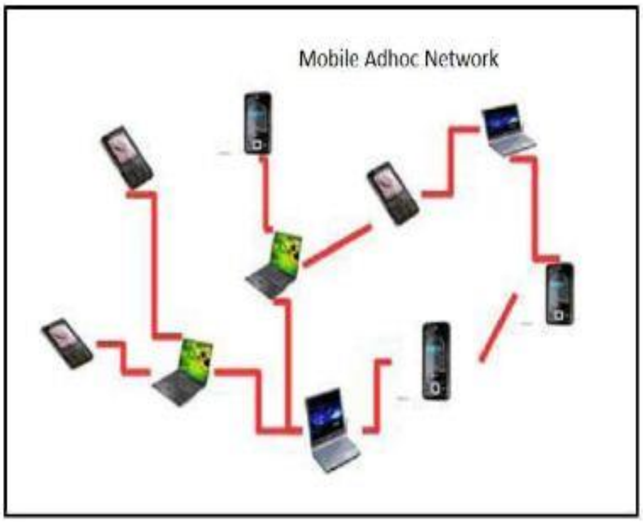

Figure 1. Mobile Ad-hoc Network

Routing protocol over MANET can be classified according to the nodes and number of paths available in the network. They are single path and multipath routing. In a single path routing the data packets can be able to send the data as well as receive an acknowledgment from destination via a single path. This type of routing causes heavy traffic, delay, energy consumption, loss of packet delivery etc. So, a multipath routing is considered in this paper which provides an alternative path for sending the data from source to destination with less delay. The load balanced and fault tolerance can be achieved by the multipath routing protocol [4]. AOMDV protocol used in this paper organize multiple paths between source and destination. At the time of discovery process, best route is selected among the availability of different routes by the source node. Suppose, there is a failure during transmission of data then there will be an increase in energy consumption, life time of a network, and end to end delay [5]. Additionally, many multipath routing protocols have been proposed in MANET.

Various type of attack may harm each layer of the network protocol. Generally, a black hole attack is a type of DOS attack that comprises severe threat against routing protocol and capable of dropping packets. The DOS attacks are easily retained against the routing in a MANET. By examining the lost traffic the invisible action of black hole nodes are detected easily. The main objective of the multipath routing presented in this paper is to develop secure multipath routing protocol for MANET not only to improve the performance parameters like packet delivery ratio and throughput by detecting anonymous activity in a network but also to avoid the attackers in routing. Hence, a novel routing protocol is introduced to establish a multiple paths based on routing metrics between source and destination pair.
The rest of the paper is organized as follows: Section II discuss the related work of AOMDV, various types of security attacks and relative studies; Section III represents the proposed methodology; Section IV presents performance and comparisons, Section V gives conclusion and presents its future work.

II. RELATED WORK

There are various types of attacks such as wormhole, relay, flooding, black hole etc. that occur in the multipath routing during transmission of data from source to destination. The theoretical analysis provides security over routing attacks in Mobile Ad-hoc Network. Sanaei, et al. [6]Sanaei, et al. [7] An efficient routing protocol was introduced for MANET. The data packets communicated and exchanged by the set of mobile nodes to each other is known as Mobile Adhoc Network (MANET). MANET is also known as an emerging technology because this type of network deployed immediately by distrusting on predefined infrastructure. This could be used in various situations that ranges from disaster relief. But providing security for emergency operations in military services was critical. Additionally, a current state of routing attacks and countermeasures were examined in the corresponding article. Many solutions like spoofing, black hole attack, wormhole attack, flooding attack, rushing attack, a message with holding attack, node isolation attack, replay attack, colluding MISRELAY attack, trust based security, and SNARE attack were proposed. The proposed analysis showed that through various solutions had been introduced, they were not perfect in terms of tradeoffs between efficiency and effectiveness. In addition to that, each and every solution proposed here consists of some specific attack and those solutions may be vulnerable to unexpected attacks.

Mishra [8] Proposed that MANET was a special group of nodes that worked without any fixed infrastructure. The reputation management systems and security features, challenges, and several attacks were discussed over MANET. Further, different security attacks on MANET that occurs due to the different network layers were also been discussed elaborately. The main aim of the security solutions for MANET that had been introduced was to provide security services like integrity, availability, authentication, also to provide security to mobile users, confidentiality, and anonymity. Thus, a systematic literature survey was showed in this method helps to understand the issues that were related to the security model and attacks on MANET. The movability of nodes on MANET presented here, proved that there were higher security needs than the traditional wired network. Rather, the security of mobile ad-hoc network was a challenging task and complicated.

Singh, et al. [9] Undergone a study around security attacks found against mobile ad-hoc network. Various attacks were found against mobile nodes such as warm hole, Byzantine attack, black hole, collaborative attack, flooding, and packet dropping. Hence, different types of attacks against MANETs were addressed and the vulnerabilities of MANET was studied successfully. Moreover, the defense and detection mechanism were to be developed for the management of messages in secure manner.

Bhatia and Verma [10] Proposed that the inherent features of MANETs such as limited network resources like battery power, bandwidth, and memory; lack of centralized trusted authority, and dynamic topology were made vulnerable to attacks than the wired network. Complete security issues was focused through which both proactive and reactive mechanisms were involved. The drawback of this analysis states that the security solution should incorporate wider perspective that consists of both known and unknown attacks. Therefore, multifence security solution must be developed for further studies.

Pandikumar, et al. [11] Reveals that MANET suffers from several attacks because of lack of centralized governing system. Though there were various types of attacks, black hole attack was known to be a difficult attack against network integrity through the absorption of all data packets on the network. A measurable technique named IDS had been adopted for the mitigation of black-hole nodes over MANET. IDS was implemented through the modification of AOMDV protocol. As well as the intrusion detection system was verified by NS2 simulations with and without black hole attack on mobile nodes through AOMDV routing protocol. The results proved that the throughput and packet delivery ratio increased different mobility. Thus, the proposed IDSAOMDV showed that it consists of highest performance through the improvement of average throughput value. Though there occurs a better performance on throughput, eradication of black hole attack the energy consumption, end to end delay, and jitter in MANET can also be increased. Furthermore, multiple black-hole and external black-hole attack can also be organized with different routing protocol.

Sharma, et al. [12] Proposed to detect multiple attacks by the use two combined methods either in DSR or AODV routing protocol. A review of black hole attack had been represented over AODV routing protocol. Where the AODV routing protocol acted as an adaptation for DSDV protocol on dynamic link conditions. The black hole attack besides a network layer paid attention towards AODV routing protocol when compared to the other protocol. The black hole attack was divided into two basic types in an existed AODV routing protocol named as internal and external black hole attack respectively. The internal black hole attack consists of inherent malicious node between source and destination. Whereas, external node stayed outside the network and refused to access the network. The proactive based method gave highest packet delivery ratio, rather overhead had been created mostly. On the other hand, a reactive based method provided lower overhead where there exist high packet loss respectively. Hence, the hybrid method provides a solution to the problem. Similarly, the combination of reactive and proactive method provides better results Bhalodiya and Vaghela [13].

Patel and Thoke [14] Investigated on Blackhole and DoS attack over MANET. In a black hole attack, malicious nodes promote itself through the transmission of false route reply packet to a source node through which a route discovery process and every packet drops had been initiated. While DoS attacks targeted the resources of services that lower the ability to provide optimum utilization of network infrastructure. The DoS flooding and black hole attack can be deployed easily to pretend to be another node on MANET. Since mobile ad hoc network consists of no clear line of defense, both malicious nodes and legitimate network users could be approached easily. Key defense threat in MANET was initiated successfully. Further, various DoS attack flooding and black hole attack prevention and detection technique were explored. Hence these solutions proved that it provides safe and security to the network. Therefore, through the evaluation of cons and pros of obtained techniques the open research challenges over mobile ad hoc network were studied.

Salem and Hamamreh [15]Jamali [16] Proposed an enhanced RID-AODV mechanism to detect and mitigate the effects of multiple black hole attacks over MANET. The effects were detected by the growth of throughput and packet delivery ratio (PDR) as well as an end to end delay was reduced than the predecessors. The enhanced RID-AODV method was achieved by the ns-2 simulator and hence compared to the existing solutions for the mitigation of multiple black hole attacks through the performance metrics such as throughput, packet delivery ratio, and an end to end delay. The simulated results of enhanced RID-AODV protocol proved that greater packet delivery ratio and throughput compared to that of the existing report.

Jain and Buksh [17] Reviewed about different solutions to perform secure routing over MANET and provides concept of MANET. From the survey, it have been analyzed that the popularity of MANET was increased due to the wide range of multimedia applications functioned over an infrastructure less environment. Owing to the infrastructure less environment, dynamic topology and less power became very difficult to provide secure routing environment o MANET. Though various solutions were provided to secure routing over MANET, still there exist challenging task for the prevention of various attacks.

Shah, et al. [18] Developed a trust over routing strategy named as secure-before routing knows as best forwarding path estimation. The trust was developed to protect the estimation of an optimal path through hop counts and expected value by the use of dummy packets at an inner side of the network at 1-hop level. The proposed methodology not only helps to alleviate the various malicious attack over MANET, also to improve the overall performance of a network by the utilization of optimum resources. The efficient security mechanisms provided to alleviate the malicious attacks were highly essential to improve the performance of a network. The authenticity of intermediate nodes was checked by using private key between source and destination. Since there was lack of knowledge of secret key among the nodes, intermediate nodes cannot be analyzed. Therefore, rather using dummy packets secure-Before routing packets can be used with enhanced security technique by the complexity level.

Brar and Angurala [19] Reviewed on Grey-Hole attack detection and prevention. Where the gray-hole attack acts as a severe threat to the routing services by the attack over reactive protocols that results on drastic drop of data packets. The survey provides a detailed information about all the work done process. Likewise, the security issues also provided a brief description for layered architecture and applications of MANET. A clear concise was also provided to secure the network from gray hole attacks. A gray hole attack under AODV protocol proved the effects of network layer. The malicious behavior of AODV protocol was also been tested under different attacks by the utilization of various performance parameters such as normalized network load, packet delivery ratio, throughput, and end to end delay respectively. As a result, gray hole attack successfully degraded the network performance in terms of packet efficiency and throughput. Anyway, the behavior of gray hole attack was very difficult to evaluate because in some cases they acted as normal node and dropped selective packets.

Sarkar and Datta [20]Sunitha, et al. [21] Suggested to provide security and energy efficiency that were stochastic to the multipath routing by the utilization of Markov-chain process for MANET (Mobile Ad-hoc Network). The recommended routing protocol is computed between source and destination. Those paths were selected as an energy efficient from the provided route in order to lead those data packets respectively. Further, the routing protocol provided a secured data transmission over network. So that the packets delivered by the random paths might be started from source to destination. Because the random data flow demand the attackers to listen each and every paths from source to destination. Hence, the numerical results and performance analysis proved that the proposed routing protocol achieved a significant performance gain by means of security for routing protocols, throughput, delay, and energy consumption respectively.

Chaubey, et al. [22] Proposed a conviction to provide security to black hole attack for demand routing protocol named as AODV and TSDRP respectively. The performance metrics considered in the proposed method was demonstrated under different environment scenarios such as packet delivery ratio, normalized routing load, throughput, and end to end delay. A complete evaluation method was also been explained briefly with the network scenario and simulation environment. Where the simulation method was performed using NS-2 (Network Simulator). The proposed routing protocols such as TSDRP and AODV were tested regarding the different performance metrics. Also, the results were made more accurate. Finally, concluded that black hole attack TSDRP demonstrated better performance over the parameters such as AT, AODV, PDF, NRL, and AED respectively.

Joseph, et al. [23] Suggested performance measurement for MANETs using black hole attack in different network scenarios. These networks were simulated by NS-2 in combination with AODV protocol. Also the performance was studied for accompanying and not accompanying the black hole attack. In addition to that, the performance were also evaluated for packet drop, PDR, control overhead, and delay. The overall PDR and throughput increased the number of flows. Meanwhile, the attacks were also been reduced. The overall delay varied based on the attack position. Hence, the simulation results proved that it provided a very good performance in MANET for accompanying and not accompanying the black hole attack in various network scenarios.

Ponsam and Srinivasan [24]Dorri, et al. [25] Undergone a survey over MANET security challenges, its countermeasures, and attacks. Various attacks were surveyed to the ad-hoc network also discussed and studied the available solutions. Different layers such as network layer, application layer, physical layer, transport layer, and data link layer of attacks were discussed briefly in the mobile ad-hoc network. These layers provides different solutions for the attacks. The major issue to provide security to the network was ad hoc network which became vulnerable to many types of attacks. Those attacks were prevented by some researchers was discussed briefly. Hence, the challenges and solutions of the security threats in a mobile ad hoc network were overviewed. Still, more researches should be done on MANET to provide better security solutions respectively.

III. PROPOSED SYSTEM

This section illustrates a novel routing protocol which authorizes multiple paths based on routing metrics between source destination pair and provides security for node authentication respectively. The proposed multipath routing protocol set up two-way paths between the source and destination. There are different layers in the network suffering from various types of attacks such as flooding, wormhole etc., Blackhole attack is mainly focused in this paper. In networking, a black hole or a packet drop attack is said to be a type of DoS attack (Denial of Service) through which router can be assumed as relay packets instead of neglecting them. This type of attack usually occurs from a router becoming compromise through different causes. A black hole attack constitutes a severe threat against routing protocol accomplished by dropping packets. Hence, these attacks are easily occupied over routing in MANET. The invisible action of black hole node is detected by monitoring the lost traffic. Here, a routing problem is designed as a zero-sum stochastic multipath discrete time, among the source and attackers in MANET. The path variation and time variation at different stages of the proposed routing game are used to counter the attacks for ensuring reliable data flow in MANETs. The proposed flow diagram is shown below in figure 3.

From the flow diagram, it has been analyzed that the network deployment is the process of determining the new routing path for effective work in an environment. Neighbor discovery is one of the important steps for self-configured networks since it is helpful to identify the active nodes from the available nodes. Once the nodes are identified, the source and send route request (RREQ) to the neighbor from the destination node. Suppose multiple n data are being sent continuously then broadcast reply request should also be sent until it reaches the destination. The destinations receive only nearby route requests being sent by the source. When multiple requests have been sending, then source finds the other available path i.e. acknowledgment path and sends its request. By the way, destination receives RREQ source from the neighbor and the process is continued. During this process, if there exist any delay in sending the requests then the destination calculates Airtime Traffic in a path. The mathematical model of Airtime Traffic can be given as follows

$$ATT(i) \rightarrow Air\ Time\ Traffic = \alpha\left\{\sum_{link\ i\in p}\left(\frac{1}{\alpha}-1\right)lc(i)+RTT(i)\right\} \qquad (1)$$

$lc(i) \rightarrow link\ cost\ of\ i-th\ node$,
$RTT(i) \rightarrow Round\ trim\ time\ of\ i-th\ node$,
$\alpha \rightarrow tunable\ factor\ fixed\ as\ 0.425$

Destination sends Route reply RREP from source to its neighbors based on queuing method. Then source receives RREP from its neighbor sent by its destination. Once source receives RREP then ATT is calculated to check the traffic condition. Suppose, ATT of ith path is greater than (i+1)th path then it switches to the current path which is equal to (i+1)th path and the RREP of ith path will be dropped. In case, ATT of ith path is lesser than (i+1)th then keep the current path ith until it balances the traffic. Once the traffic is balanced then check the Q utilization that is greater than the threshold.

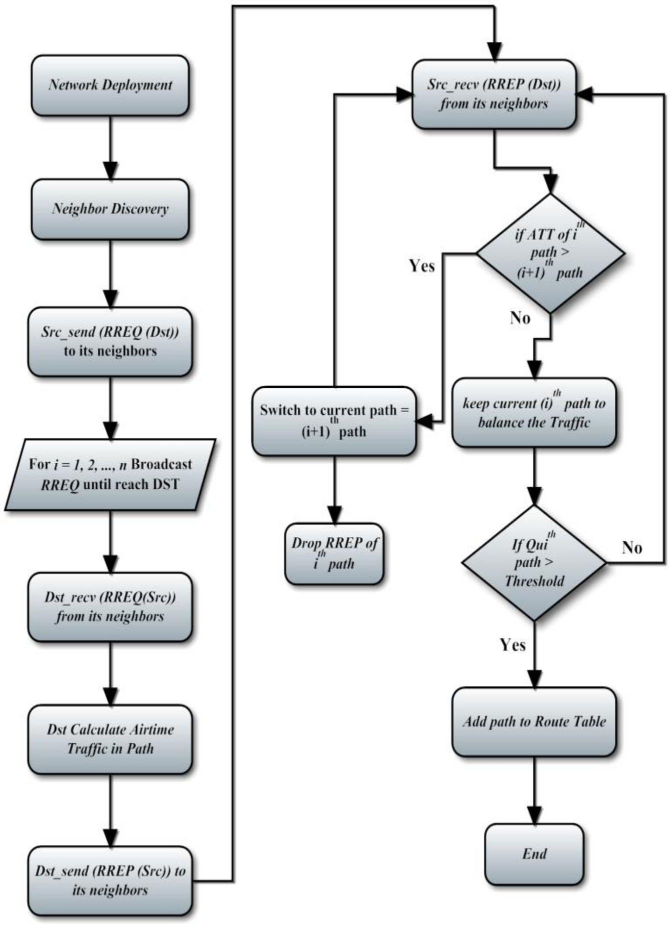
Network Deployment
Neighbor Discovery
Src_send (RREQ (Dst)) to its neighbors
For i = 1, 2, ..., n Broadcast RREQ until reach DST
Dst_recv (RREQ(Src)) from its neighbors
Dst Calculate Airtime Traffic in Path
Dst_send (RREP (Src)) to its neighbors
Src_recv (RREP (Dst)) from its neighbors
if ATT of i th path > (i+1) th path
Yes
No
Switch to current path = (i+1) th path
keep current (i) th path to balance the Traffic
Drop RREP of i th path
If Qui th path > Threshold
No
Yes
Add path to Route Table
End

Figure 2. Flow diagram of the proposed method

The mathematical expression for Q utilization is given as follows

$$Qui = \frac{\sum_{i=1}^{n} A_{qi} - O_{qi}}{n} \rightarrow utilization\ of\ i-th\ node\ Queue \quad (2)$$

$$A_{qi} \rightarrow Available\ Queue\ in\ i-th\ node$$

$$O_{qi} \rightarrow Occupied\ Queue\ in\ i-th\ nodes$$

Q utilization refers to storage of memory based on FIFO model. If there is no free space then RREP of i^{th}path will be dropped. Also, if Q utilization is less than the threshold then there occurs an error then again source receives RREP from its neighbor and the process is continued. If it is greater than the threshold then there will be no error, hence another path will be added to route table and the process ends. In the proposed method of routing protocol, RH (Region Header) will generate the key randomly. RH is selected from maximum number of persons present in the region respectively.

A. Security Algorithm

A node authentication is done by providing security algorithm during transmission of data by the use of multiple nodes disjoint paths between source and destination.

Step 1: Initialization

The RH choose a random secret SK_l for every member $U_l, l = 1, 2, \cdots, n$. Here, the pairwise key UK_l is$\{SK_l\}$. The Region Header (RH) generates security at an initialization step.

Step 2: Broadcast

In session i, RH generated an access polynomial

$$\emptyset_i(x) = \beta_i\big(1 + (\theta_i x - 1)\prod_{l:U_l \epsilon G_l}(x - UK_l)\big) \qquad (3)$$

Where θ_i is random and makes each access polynomial different for every session. Here, RH encrypts GK_l using β_i and received $E_{\beta_i}(GK_v), V = 1, 2, \cdots, i$. At that moment, the message β_i gets broadcasted into the group.

$$B_i = \left\{\emptyset_i(x) | \{E_{\beta_i}(GK_v)\}_{v=1,2,\cdots,i}\right\} \qquad (4)$$

Here, when a new user joins the RH, ID and broadcast are created and that cannot be shared by the other group. The key authentication is based on the above equation (4) which forwards the node only after verification.

Step 3: Group Key Recovery

At the time of receiving B_i , a valid note $U_l \epsilon G_i$computes $\beta_i = \emptyset_i(UK_l)$. While revoked nodes get only random numbers. Then U_l can recover group session key GK_l , belonging to itself by decrypting $E_{\beta_i}(GK_v)$.

Step 4: Node addition and revocation

$$\emptyset_{i+1}(x) = \beta_{i+1}\big(1 + (\theta_{i+1}x - 1)\prod_{l:U_l \epsilon G_i}(x - UK_l)(x - UK_w)\big) \qquad (5)$$

When a new node $\mathrm{U_w}$ joins the group, it should be preloaded with a secret$\mathrm{UK_w}$. RH generates a new access polynomial shown in above equation (5).

Similarly, when a node $\mathrm{U_r}$ is revoked in session $\mathrm{i+1}$. RH generates new$\emptyset_{\mathrm{i+1}}(\mathrm{x})$,

$$\emptyset_{i+1}(x) = \beta_{i+1}\big(1 + (\theta_{i+1}x - 1)\prod_{l:U_l\epsilon G_i}(x - UK_l)/(x - UK_r)\big) \tag{6}$$

Node adding and recovery in the sense, a new user gets entry and any of the user gets exist from the node. When any of the existing user is exit then user ID will be removed and rekeying. The removed ID gets stored in the broadcast. Meantime, when a new user gets entry, new user ID will be provided. But both the node entry and exit consists of broadcasting.

B. Lack in forwarding security

Assuming the node $\mathrm{U_w} \in \mathrm{G_i}$ will be revoked in $\mathrm{i+1}$, gets information $\beta_\mathrm{i} = \emptyset_\mathrm{i}(\mathrm{UK_w})$ with

$$(\emptyset_i x - 1)\prod_{l:U_l\in G_i}(x - UK_l) = \frac{\emptyset_i(x)}{\beta_i} - 1 = \frac{\emptyset_i(x)}{\emptyset_i(UK_w)} - 1 \tag{7}$$

Thus, θ_i is derived from the above equation (7). A core information is received after the derivation.

$$\prod_{l:U_l\in G_i\backslash U_w}(x - UK_l) = \frac{\left(\frac{\emptyset(x)}{\emptyset_i(UK_w)}-1\right)}{(\emptyset_i x-1)(x-UK_w)} \tag{8}$$

$$\emptyset_{i+1}(x) = \beta_{i+1}\big(1 + (\emptyset_{i+1}x - 1)\prod_{l:U_l\epsilon G_{i+1}}(x - UK_l)\big) \tag{9}$$

Then, no other changes will be made in the group and holds $\mathrm{G_{i+1} = G_i \backslash U_w}$. But $\mathrm{U_w}$ can obtain $\beta_{\mathrm{i+1}}$ using $\prod_{\mathrm{l:U_l\epsilon G_{i+1}}}(\mathrm{x - UK_l})$ and constant term $\beta_{\mathrm{i+1}}(1 - \mathrm{C_{i+1}})$ in above equation (9).

The above algorithm helps to provide an alert in case of failure in key verification process.

C. Secondary Path Routing

In an alternate path routing, first a path is determined from the source node. In order to identify an alternate route for transmission, first initialized a path by real time clock T to 0; then broadcast RREQ message with its SA and DA and check the time out period with the condition $(\mathrm{T < T_{Max}})$. If suppose RREP message is received then collect the RREP messages and create a path list with $\mathrm{P_i}$ and $\mathrm{T_i}$. Once the path list is created, then calculate least common multiple of all $\mathrm{T_i}$. Then data packets are transmitted and waits for receiving the acknowledgement. Once the acknowledgement is received within the time then send the next data packet else resend the packet respectively. Secondly, route_intermediate_node is determined based on the transmitting and receiving the message routes. Here, if both SA and DA are not equal to its own id, then receive RREQ. Suppose RREQ is received then send RREQ message with its own id; In case, instead of RREQ, RREP is received then send the RREP message with its own id. In some cases, data packets or ACK or NACK will be received. In such cases, forward the data packets or ACK or NACK packets respectively. Finally, find the destination node. This is an important step because the alternate path is chosen mainly to attain the destination node by the packets. The path initialization is made providing own id to DA. If RREQ is received then send RREP message from the received RREQ. During data transmission if data packets have been received correctly then the acknowledgement will be send, else NACK will be send respectively. After receiving the acknowledgement send the next packet. Hence, through security analysis and multipath routing data packets reaches the destination successfully.

IV. PERFORMANCE ANALYSIS

This sections illustrates the performance analysis of proposed method. The performance is calculated for various parameters such as packet delivery ratio, end to end delay, energy consumption, and throughput.

A. Packet Delivery Ratio

Figure 3 (a) shows the comparison of packet delivery ratio for SCMR, AOMDV, AOMR-LM, and CA-AOMDV. The graph shows that SCMR performs higher than AOMR-LM, AOMDV, and CA-AOMDV protocol. The packet delivery ratio can be defined as a ratio of a number of received packets by the destination node to the number of transmitted packets from the source node.

$$PDR = \frac{number\ of\ packets\ received}{number\ of\ packets\ send} X100 \quad (10)$$

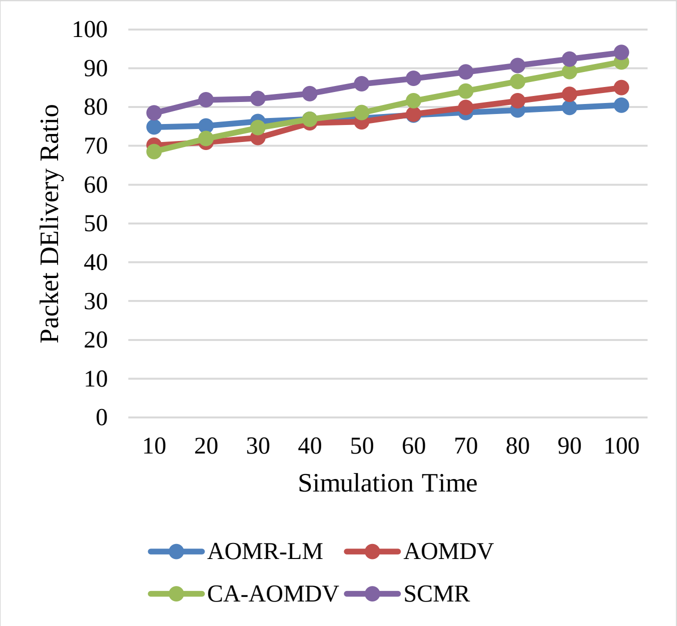

Figure 3 (a). Packet delivery ratio

From the graphical results, we analyzed that proposed methodology SCMR consists of high delivery ratio of 78.32% compared to CA-AOMDV, AOMR-LM, and AOMDV. The packet delivery ratio is calculated based on the reception of packets between source and destination. Higher the delivery ratio higher the performance. Thus, the proposed routing protocol of SCMR provides better performance than the other.

Figure 3 (b) shows the packet delivery fraction of AOMR-LM, AOMDV, CA-AOMDV, and SCMR for various attacks. The packet delivery fraction is similar to that of the packet delivery ratio. The only difference is that % of attacks is calculated for different routing protocol and compared with the proposed routing protocol which proves to be faster than the AOMR-LM, AOMDV, and CA-AOMDV respectively. Thus, from the shown figure it is seen that proposed routing protocol of SCMR consists of higher packet delivery fraction compared to other.

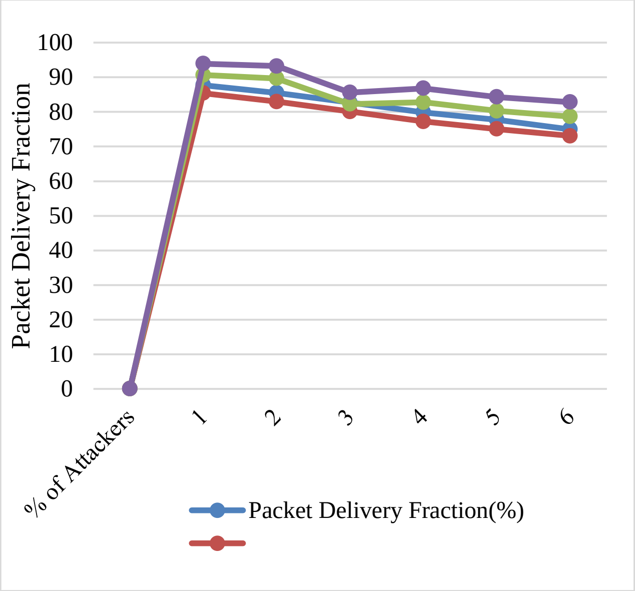

Figure 3 (b) Packet Delivery Fraction

B. End to End Delay

Figure 4 (a) shows the different delay values for SCMR, CA-AOMDV, AOMR-LM, and AOMDV. When there is an increase in speed of the node then automatically there will be an increase in an end to end delay. The average value of data packets determined during successful transmission in message across the network from source to destination is referred to as an end to end delay. The end to end delay stated as follows

$$End\ to\ End\ delay = \frac{\sum_{i=1}^{n}(Ri-Si)}{n} \quad (11)$$

An end to end delay is also calculated based on the time taken for a packet to deliver from source to destination in a network. Figure 4(a) shows that the proposed routing protocol consists of less delay than the other protocol. If delay is reduced then transmission of packets will be faster. Hence the proposed routing protocol SCMR consists of average delay about 27.06ms. While AOMR-LM consists of 28.44ms, AOMDV consists of 36.12ms, and CA-AOMDV consists of 32.09ms respectively. Hence, from the above results, it is proved that SCMR outperforms AOMR-LM, AOMDV, and CA-AOMDV protocol respectively.

Figure 4(b) shows end to delay for attacks. The percentage of attackers for different routing protocols is calculated. Similar to the above mentioned definition, % of attackers in end to end delay also proves that the proposed SCMR is lower when compared to the other three routing protocol. AOMR-LM, AOMDV, and CA-AOMDV consists of delay average about 10.571, 9.151, and 4.661 in milli seconds. Whereas, SCMR delay average is about 3.975 respectively.

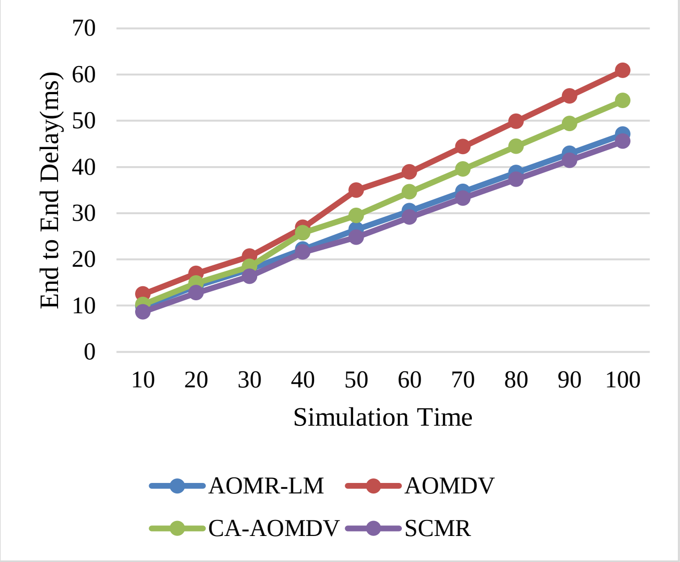

Figure 4 (a). End to End Delay

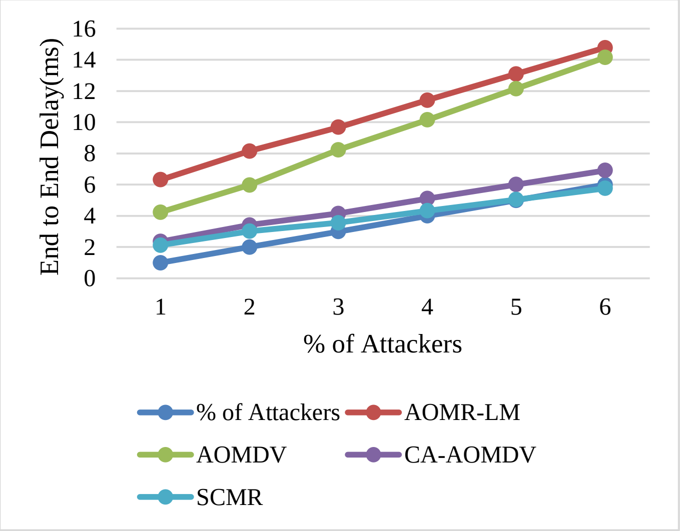

Figure 4 (b) End to end delay (ms)

C. Energy Consumption

Figure 5 shows the energy consumption for SCMR, AOMR-LM, CA-AOMDV, and AOMDV measured in joules. Amount of energy spent by the network nodes is said to be energy consumption. The energy consumption is estimated through energy level produced at each node during an end of the simulation. When there is an increase in node speed then more energy will be consumed. The energy consumption formula is given as

$$Energy\ Consumption = \sum_{i=1}^{n}\left(ini(i) - ene(i)\right) \quad (12)$$

The energy consumed by the proposed method is less due to the fact that the packet delivery is fast when compared to the other routing protocol. Thus, the energy consumed by the proposed routing method SCMR average is 63.46 (joules). While AOMR-LM, AOMDV, and CA-AOMDV energy consumption average is 83.732, 111.337, and 88.932 joules. Therefore based on the above values it is analyzed that the energy consumed by SCMR is less due to fast transmission of data with less delay.

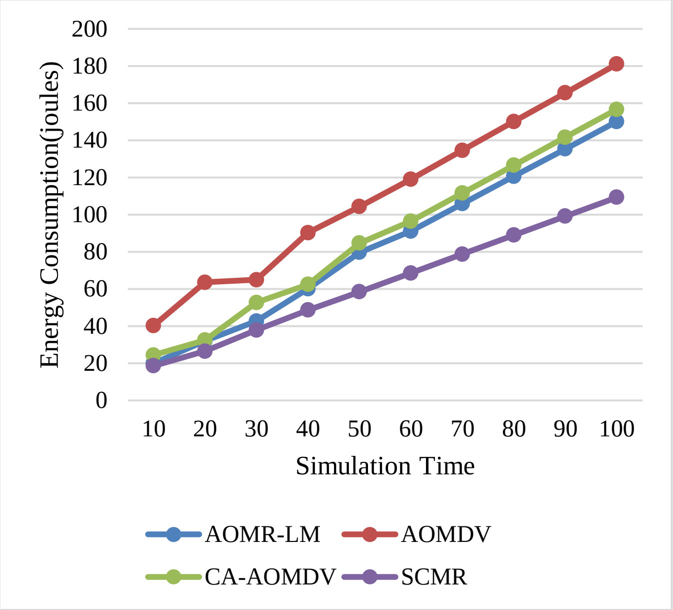

Figure 5. Energy consumption

D. Throughput

Throughput is said to be number of bits through which the destination receives it successfully. Here, a routing protocol is measured by the throughput through destination in receiving the data packets.

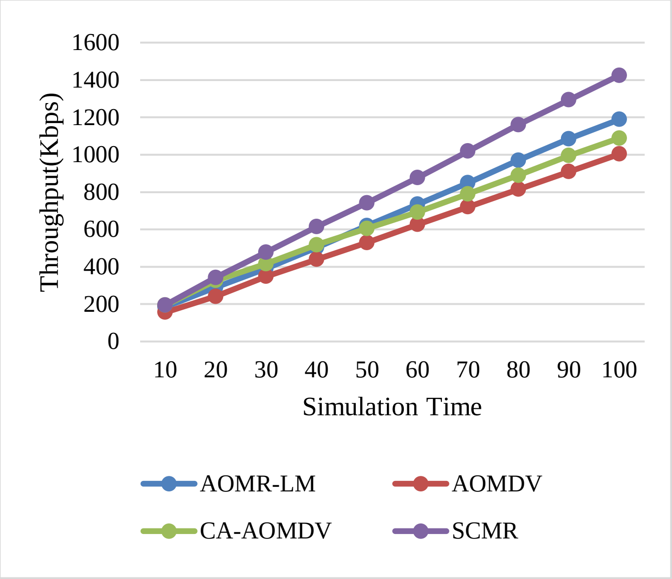

Figure 6 (a). Throughput

Figure 6(a) shows the throughput performance for various routing protocol such as AOMR-LM, AOMDV, CA-AOMDV, and SCMR. From the figure it is seen that proposed SCMR provides higher throughput compared to other three protocols. Throughput is calculated based on the formula

$$Throughput = \frac{(number\ of\ bytes\ received\ X\ 8)}{Simulation\ time} X1000Kbps \qquad (13)$$

Based on this formula the SCMR provides higher throughput with the average of 814.7 Kbps, while AOMR-LM consists of 681.6 Kbps, AOMDV consists of 578.6 Kbps, and CA-AOMDV consists of 651.4 Kbps. Higher the throughput, higher the performance. Hence, from these results it proves that SCMR consists of higher throughput and better performance between source and destination. Figure 6(b) shows the throughput performance measures in bytes per second. Similar to the previous figure 6(a), the above shown figure also provides higher throughput when compared to the other.

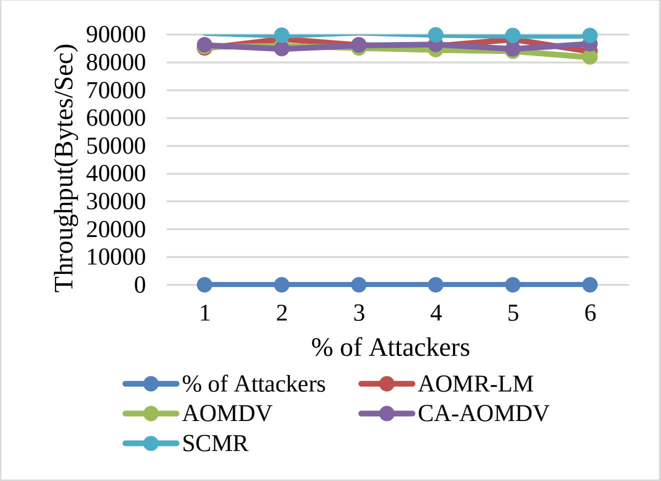

Figure 6 (b) Throughput (Bytes/Sec)

The only difference is that figure 6(a) is measured in kbps and figure 6(b) in bytes/sec respectively. From the above figure we analyzed that the SCMR provides higher throughput average of about 90011.66 bytes/sec, Other routing protocol such as AOMR-LM, AOMDV, and CA-AOMDV provides 86345, 84534.33, 85870.16 bytes/sec.

V. CONCLUSION & FUTURE WORK

In this paper, the multi routing protocol is considered for MANET to transmit the data from source to destination. The multipath routing proposed in this work provides more than one path with less delay between source and destination. Various attacks like a wormhole, flooding, black hole, and relay attacks may occur during the transmission of data. So, in order to safeguard the data packets from those attacks, a security mechanism is provided to transfer the data from source to destination without any threats and delay. A black hole says DoS attack is considered in this paper which constitutes a severe attack against routing protocol. This type of attack is easily engaged against routing in MANET. Hence, a secure multi routing protocol is developed for MANET and provides better performance. The performance is calculated based on the ratio of packet delivery, energy consumption, end to end delay, and throughput respectively. As a result, the end to end delay is reduced during transmission, throughput is increased and provides a superior performance. Also, there is a fast transmission of packet delivery from source to destination. Consequently, the energy consumption is reduced by SCMR. Based on the above results it is concluded that the SCMR provides high security by detecting anonymous activity in a network. The attackers are also avoided in routing path successfully. Several scenarios can be implemented in future work, to enhance packet delivery ratio (PDR) via splitting the multipath data transmission. The bio-inspired algorithm can be proposed not only to detect the malicious behavior but also to improve its accuracy over intermediate multiple paths respectively.

IV. REFERENCES

[1]. A. Bhattacharya and K. Sinha, "An Efficient Protocol for Load-Balanced Multipath Routing in Mobile Ad Hoc Networks," Ad Hoc Networks, 2017.

[2]. I. Aggarwal and E. P. Garg, "AOMDV Protocols in MANETS: A Review," International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016), vol. 32, 2013.

[3]. E. S. A. Ganie and M. N. Sharma, "Interference-Aware and Fault Tolerant Multipath Routing Protocols for Mobile Ad Hoc Networks," International Journal of Engineering Science, vol. 2524, 2016.

[4]. P. Purniemaa, K. Manikandan, and M. S. Durai, "A Review on Security Issues in Multipath Routing Protocol in MANET," International Journal of Advanced Research in Computer Science, vol. 2, 2011.

[5]. A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, "Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function," IEEE Access, vol. 5, pp. 10369-10381, 2017.

[6]. P. Sanaei, M. Ghanaat, I. Ghani, A. Hakemi, and S. R. Jeong, "ROUTING ATTACKS IN MOBILE AD HOC NETWORKS: AN OVERVIEW," Science International, vol. 25, 2013.

[7]. M. G. Sanaei, B. E. Abarghouei, H. Zamani, and M. Dabiranzohouri, "AN OVERVIEW ON WORMHOLE ATTACK DETECTION IN AD-HOC NETWORKS," Journal of Theoretical & Applied Information Technology, vol. 52, 2013.

[8]. P. Mishra, "SECURITY ISSUES AND ATTACKS IN MOBILE AD HOC NETWORKS," 2017.

[9]. U. K. Singh, D. N. Goswami, K. C. Phuleria, and S. Sharma, "An analysis of Security Attacks found in Mobile Ad-hoc Network," International Journal of Advanced Research in Computer Science, vol. 5, 2014.

[10]. T. Bhatia and A. Verma, "Security issues in MANET: a survey on attacks and defense mechanisms," International Journal, vol. 3, 2013.

[11]. T. Pandikumar, B. Zewdie, and C. Z. Haile, "Mitigating Black Hole Attack on MANET with AOMDV Protocol," International Journal of Engineering Science, vol. 12666, 2017.

[12]. G. Sharma, A. Mittal, and R. Aggarwal, "Attacks on Ad hoc On-Demand Distance Vector Routingin MANET," 2016.

[13]. S. Bhalodiya and K. Vaghela, "Study of Detection and Prevention Techniques for Flooding attack on AODV in MANET," International Journal of Science and Research (IJSR), vol. 4, pp. 433-436, 2015.

[14]. K. Patel and A. Thoke, "A Details Survey on Black-hole and Denial of Service Attack over MANET Environment," 2016.

[15]. A.-R. Salem and R. Hamamreh, "Efficient Mechanism For Mitigating Multiple Black Hole Attacks In Manets," Journal of Theoretical and Applied Information Technology, vol. 83, p. 156, 2016.

[16]. S. B. S. Jamali, "A survey over black hole attack detection in mobile ad hoc network," International Journal of Computer Science and Network Security (IJCSNS), vol. 15, p. 44, 2015.

[17]. A. Jain and B. Buksh, "Solutions for Secure Routing in Mobile Ad Hoc Network (MANET): A Survey," Imperial Journal of Interdisciplinary Research, vol. 2, 2016.

[18]. R. Shah, S. Subramaniam, L. Dasarathan, and D. Babu, "Mitigating Malicious Attacks Using Trust Based Secure-BEFORE Routing Strategy in Mobile Ad Hoc Networks," CIT. Journal of Computing and Information Technology, vol. 24, pp. 237-252, 2016.

[19]. S. Brar and M. Angurala, "Review on Grey-Hole Attack Detection and Prevention," 2016.

[20]. S. Sarkar and R. Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks," Ad Hoc Networks, vol. 37, pp. 209-227, 2016.

[21]. Sunitha, P. V. Srinivas, and T. Venugopal, "An Energy Efficient Routing Based on Route Segmentation in Mobile Ad Hoc Network,"

Global Journal of Computer Science and Technology, 2017.

[22]. N. Chaubey, A. Aggarwal, S. Gandhi, and K. A. Jani, "Performance analysis of TSDRP and AODV routing protocol under black hole attacks in manets by varying network size," in Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on, 2015, pp. 320-324.

[23]. C. Joseph, P. Kishoreraja, R. Baskar, and M. Reji, "Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios," Indian Journal of Science and Technology, vol. 8, 2015.

[24]. J. G. Ponsam and D. R. Srinivasan, "A survey on MANET security challenges, attacks and its countermeasures," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3, 2014.

[25]. A. Dorri, S. R. Kamel, and E. Kheirkhah, "Security challenges in mobile ad hoc networks: A survey," arXiv preprint arXiv:1503.03233, 2015.