I. J. Computer Network and Information Security, **2018, 6, 40-51**
Published Online June 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.06.04

Alleviating Malicious Insider Attacks in MANET using a Multipath On-demand Security Mechanism

Mir Shahnawaz Ahmad
Shri Mata Vaishno Devi University, Katra, J&K, India.
E-mail: mirshahnawaz888@gmail.com

Received: 20 January 2018; Accepted: 23 April 2018; Published: 08 June 2018

Abstract—MANET is a family of ad hoc networks that spans a huge spectrum of other networking paradigms such as WMN, WSN, and VANET etc. There is a dire need for strengthening the base of all these networks from the security point of view. The vulnerability of MANET towards the attacks is huge as compared to its wired counterparts. MANETs are vulnerable to attacks because of the unique characteristics which they exhibit like the absence of central authority, usage of wireless links, dynamism in topology, shared media, constrained resources, etc. The ramification being that the security needs of MANETs become absolutely different than the ones which exist in the customary networks. One of the basal vulnerabilities of MANETs comes from their peer to peer architecture which is completely open wherein the mobile nodes act as routers, the medium of communication is open making it reachable to both the legitimate users of the network as well as the malicious nodes. Consequently, there is a bankruptcy of clear line of defense from the perspective of security design. This in turn implies that any node which may even be authentic can enter the network and affect its performance by dropping the packets instead of forwarding them. The occurrences of the attacks of this type in ad hoc networks result in the situation where even the standard routing protocols do not provide the required security. The proposed solutions in literature such as SAODV, ARAN, and SEAODV all provide authentication and encryption based solutions to these attacks. But, the attack on availability which is the most common and easiest of them all cannot be avoided by the authentication and encryption because even the authentic user can be the attacker. Also, the encryption cannot be helpful to prevent such attacks. Therefore, in such a situation if a proper solution is not provided the entire MANET operation will get crippled. The main aim of this paper is to guarantee a security solution which provides defense against these attacks. To achieve this, a Multipath On-demand security Mechanism, called Secure Multipath Ad hoc On-demand Distance vector routing protocol (SMAODV), is presented which eliminates the malicious nodes from the network thereby preventing MANETs from the effects of such malicious nodes.

Index Terms—MANET, authentication, encryption, SAODV, ARAN, SEAODV, SMAODV, Malicious Nodes.

I. INTRODUCTION

Over the past few decades, there has been a progressive of the shift from wired networks to wireless networks. Wireless networks came as a blessing for the applications that required scalability and mobility which could not be provided by their wired counterparts. Among the wireless networks that exist today, the most unique and important application is that of MANET [1]. MANETs are the category of the wireless networks which do not require a fixed infrastructure to function I.e. in MANETs there is no central authority and therefore for the purpose of communication all the nodes act both as transmitters as well as the receivers. The communication is achieved as follows: When the destination is easily reachable from the source, i.e. the destination lies within the transmission range of the source, they communicate directly and when they are far apart, they take the help of neighbor nodes. This blatantly implies that every node behaves like a router in MANETs. All the links in MANETs are bidirectional. The biggest advantage of the wireless networks is their tendency to allow different nodes to communicate while maintaining their mobility at the same time. Since MANETs does not rely on any infrastructure, all the nodes are independent and can move freely [2, 3]. The transmission range of MANET nodes is limited, which means that the direct communication between source and destination is not possible when they are outside their zones of transmission. For that intermediate nodes take part in communication and hence communication in MANETs is divided among 2 types: “Single-hop communication” and “multi-hop communication”. In the former, the nodes which lie in the radio range of each other communicate directly while as in multi-hop communication when the destination node is beyond the source node’s radio range, intermediate nodes help to relay the messages to their destinations.

A. Characteristics of MANETs

MANETs are the systems which are known for their dynamism, the medium of communication in MANET is air, and therefore the entire communication is vulnerable to interference and attacks [4]. The dynamism is brought by the nodes which are mobile-they give rise to frequent changes in the topology. Owing to these frequent topology changes and absence of centralized authority (infrastructure), MANET operation calls for two fundamental requirements:

1. Similar management capabilities for all nodes in MANET
2. Every operation of network as data flow, routing, locating etc. needs to be infrastructure less (decentralized) [5].

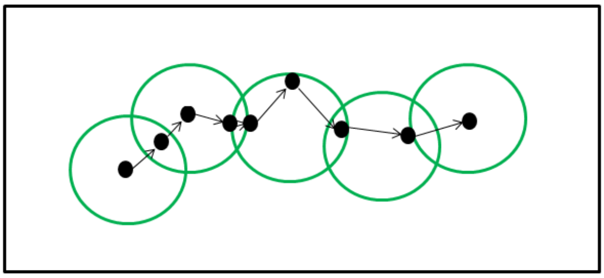

Fig.1. MANET Single Hop and Multi Hop Communication

B. Opportunities and limitations of MANETs

Self-configuring networks: MANETs have the ability to form self-configuring and self-maintaining networks. They tend to be “self-configuring” and “self-maintaining” since no central administration is present to do this job for them. This means, MANETs does not need any static infrastructure to perform a particular job well (applications where infrastructure based networks are hard to be deployed).

Nominal configuration is needed to install MANETs. Their quick implementation makes them one of the best network choices to be used in the situations of emergency, such as natural disasters, medical emergencies, etc. In such situations having the infrastructure based network communication is not possible.

Costly routing: since there are no access points, no fixed infrastructure, and every node in MANETs need to perform the function of routing-which becomes expensive. Furthermore, when the destination is far away, the routing cost increases even more. Therefore, in MANETs, neighbor communication is favored.

Unreliable links: The links established in MANETs are unreliable because the topology changes rapidly owing to mobility, plus there are environmental factors and interference of other elements. Also, collisions cannot be detected in wireless networks like their wired counterparts. As a result the percentage of message losses are high in MANETs.

Limited resources: the nodes in MANETs are relatively small in size - hence they have limited power, processing ability and memory.

Broadcast communication: The communication in MANETs is mostly broadcast based. So if 10 nodes lie within the range of source, all of them receive the information. These nodes, then further move the message forward by relaying it on to their transmission ranges. Therefore, every time source node talks to its neighbors, the gossip reaches to all the other notes in vicinity at no extra cost.

Mobility: Nodes in MANET move freely while carrying information. This feature may help in dispersion, mixture and aggregation of information.

Data-centric routing: Unlike traditional MANETs that use point to point addressing centric model, some MANETs use data centric communication model in routing. In data centric communication model, the priority is given to type of data rather than the source’s identity. This model supports data aggregation, which is performed in-network. It also puts restrictions on the way in which storage and routing tasks are executed in the network [4].

C. Architecture of MANETs

Three types of architectures are possible in MANETs namely, centralized, distributed and Peer to peer (P2P) [6].

Centralized architecture based MANET: This architecture consists of the following entities:

Service Publisher: A MANET node that has some service to offer is called a service publisher. A service publisher publishes its service to the network.

Service Broker: MANET node which acts as the mediator between publisher and consumer nodes.

Service Subscriber/ Consumer: A MANET node that consumes the service published by the service publisher.

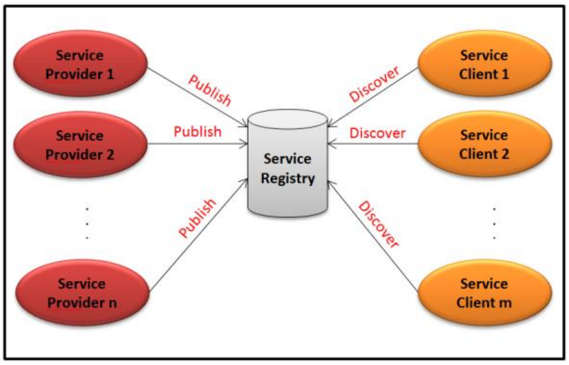

Fig.2. Centralized Architecture

In Centralized MANET architecture a central service publishing node is always available. This architecture maintains a centralized registry for publishing the services. The consumer may avail the services by joining with the service's publisher and simultaneously accessing the centralized registry. Today MANETs are used for critical applications like military missions, battlefield communications, et cetera. They are also proving to be extremely useful in the areas of intelligent commerce, prompt messaging, CRM, online multimedia content of business organizations etc. [7]. Consequently, there is the need of having service oriented architecture of MANETs to ensure easy access and benefits of using MANETs. Using centralized MANET architecture is not an option in the case when MANET is specifically used for critical applications [8] because of the following reasons:

Fault Tolerance: There is a central service publishing Node whose job is to retain the focal service registry, so if this node becomes unreachable or goes down, the entire system fails.

Quality of Service: Providing service specific quality of service parameters such as reliability (an assurance that the service will be available for certain duration), security mechanism etc. used by the service is a challenge [9].

Other problems: These include trust on registry node (what if it gets corrupt), breakdown of centralized broker like UDDI [10, 11] wherein UDDI becomes inaccessible because of nodes mobility et cetera. Therefore, this architecture is most suitable for small or average sized MANETs and cannot be used as the underlying architecture for service oriented architecture (SOA).

Distributed architecture based MANETs: The central Service publishing node is unavailable, therefore, any Service publisher node can publish a service and any service consumer node may discover the published service and consume it.

Peer to Peer architecture based MANETs: In this type of architecture, every node has equal status and hence can both produce services for other nodes as well as consume services provided by others.

Both Peer to Peer and distributed architectures do not depend on the central register. These Architectures are well suited for large-scale services. The issues faced by a centralized architecture-based MANETs namely, fault tolerance, network resilience are removed here. [12, 13] proposed methods to install SOA on underlying Peer to Peer and distributed architectures.

D. *MANET Standards*

The unique characteristics such as infrastructure independent operation, dynamism in the topology, mobility, constrained resources exhibited by MANETs chase numerous challenges from security, trust and performance points of view. What protocols or standards do nodes in MANET follow when they need to communicate with their neighbors? Standardization and normalization of information technology and communication strategies is important for the quick implementation of any new technology. They not only provide interoperability, but also reduce the costs of implementation and give way to easy installation.

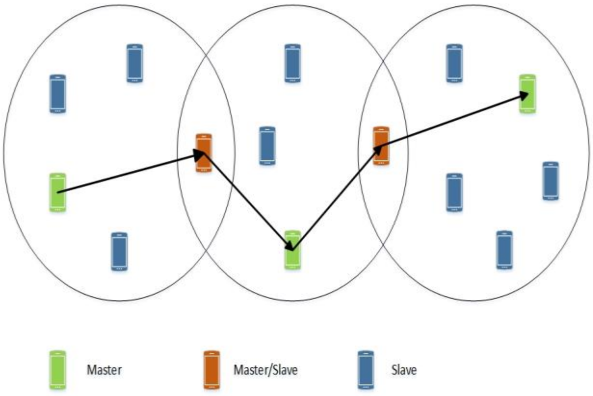

Fig.3. Bluetooth Piconet Master/Slave Configuration

A set of IEEE WLAN standards used for MANETs are: “IEEE 802.11 [14 – 16], IEEE 802.15 [17], IEEE 802.15.4, IEEE 802.16 [18, 19], IEEE 802.20 [20]”.

E. *MANET Challenges*

Today MANET is considered to be one of the best emerging technologies for mobile computing. MANET is the fastest growing of networks because of the increase in affordable, powerful and portable devices. Unlike their wired counterparts, MANET displays some unique characteristics which ultimately pose numerous challenges related to security and routing. Also, the medium of communication is shared which means that not only the legitimate user gets the access, illegitimate users also can access the medium easily therefore breach of security. This clearly implies that in MANETs there is no clear line of defense as we have in wired networks. In wired networks, there are fixed routes, but in MANETs, every node can be treated as a router. Thus, securing such a network is in itself a challenge because the attacker field/range is vast. Other non-trivial challenges are the server resource bondage, hugely dynamic topology of network, etc. MANETs offer alluring applications because of their features discussed in preceding sections, but before they can be expected to be deployed on a commercial scale, some of the typical challenges and thought provoking problems require to be solved. These include [21, 22]:

Changing Topologies: MANET nodes are highly dynamic, independent in motion, frequently fuse with or dispense the network, stray around the network at their own drive [23]. Bringing security along with such dynamism is in itself a challenge because, no doubt, that nodes roam easily in the network, they request for security at anywhere and anytime.

Routing: Owing to the dynamism of the topology, problems stack up in routing also. Since the nodes are straying continuously, table driven routing protocols cannot be used, therefore only the reactive routing protocols can be used. Again Multicast routing becomes a challenge here because the nodes move freely and multicast tree is no more static. Also, it is not necessary that the source and destination lie within each other's radio range, therefore multi-hop communication is needed which is more complex than single hop.

Device discovery: Recognizing the honest nodes, which enter into the network and informing about their entries require dynamic updates to ensure optimal automatic route selection. This requires authenticating the nodes [24].

Constraint Resources: The capacity of wireless links is limited and variable which pose numerous challenges. Moreover, almost all the MANET nodes run on exhaustible energy sources to gain energy. Therefore the design of mobile nodes requires considering energy conservation seriously. The consumption of power should be lean, energy conserving routing protocols need to be proposed which are also secure.

Reliability Challenge: Numerous reliability issues creep in among MANETs, like constrained wireless transmission range, hidden terminal problem, packet losses because of mobility and data transmission errors etc.

Quality of Service: To arrange distant QOS levels for devices in an environment which is hugely dynamic as in MANET is a challenge and that too not a trivial one. The communication in MANET is stochastic in nature and therefore stable QOS cannot be guaranteed. There is a dire need for adaptive QOS to be implemented.

Inter-Networking: Sometimes MANETs need to interact with fixed networks. In that case, mobile devices should have the co-existing routing protocols. This coexistence is a challenge for management of mobility.

Diffusion Hole Problem: The protocols based on geographic routing tend to deliver the packets to nodes which are positioned on the perimeter of the network, which can cost them huge consumption of resources such as energy. This enlarges the hole because the other nodes on the boundaries get drained of energy.

F. MANET Security Challenges

In order to have a sealed communication between two nodes in a hostile environment as in MANETs, security becomes a fundamental concern. The preceding section discussed the challenges which are fought in MANET environments. These challenges clearly give a hint towards the development of multi-fence security solutions [23] in order to acquire two things via: Better performance of network and vast protection. Various vulnerabilities of MANET from security point of view are:

Boundary: Nodes can move freely like nomads anytime and anywhere with varying speeds. The attacker just needs to come closer to the target node and communicate with it. This adversary can launch a number of attacks from this prospect: Eavesdropping, tampering, DOS (Denial of Services), replay etc. [24].

Attacker inside the network: In the wired networks the attacker cannot come inside the network because all the links are fixed, only the authorized nodes form the network. But in MANETs, since the nodes can leave and connect the network at their will, the attacker may join the network and behave abnormally, damaging the network. Finding the malicious node is a hard task here.

Lack of Centralized Authority: Since the traffic is not monitored by a central agency but, each and every node controls the network, detecting an attacker is very difficult. Moreover, detection of attack becomes further difficult when the adversary changes the type of attack and attacks target. Classifying the nodes as trusted ones or otherwise is an issue [25].

Limited Battery: Since MANET nodes have scarce battery lives, an attacker can overwhelm a node with packets (containing control information). The node's battery gets drained by handling these packets and hence it won't be able to deliver services to other nodes (honest ones). Moreover the attacker may direct its target to perform some useless computation, making it lose its battery as well as waste its time. The attacker may also be one which acts in a selfish manner. A selfish node is the one which does not work accordingly as per other nodes to run a common algorithm. Consider the example of cluster based intrusion detection technique [26]. In this technique, a group of nodes joins hands to find the intruder. If a node wishes to become a monitor, it is allowed to do so. A malicious node simply denies being one. If a majority of MANET nodes become selfish, entire system breaks down.

Scalability: There is a difficulty in forecasting the node count in MANET at different times. The protocols need to be built keeping in view this changing scale.

G. Criteria for Security in MANET

The main requirements which must be respected by the system to allow the proper operation of the network include: availability, authorization, privacy protection and access control [27, 28].

Availability: It refers to the requirement that even when the network is under the influence of intruder/adversaries, it should remain in operational mode. To ensure operability of networks and applications under attacks, a design which is not only secure, but also tolerant to faults, resilient to attacks and survivable protocol (the protocols which shoot back to their routine jobs once the malicious nodes are removed) are required [29].

Integrity: It makes sure that the message which was transmitted by one party and the message which was received by the other party are the same and nothing was added or removed from the message. Also, nothing was modified. Only then will the receiver be able to approve the identification of the sender at the time of transaction [30]. In order to actualize integrity, an attacker must be stopped from modifying the messages in any form because one should be sure that what it is reading is what the source had actually sent [31]. If there is an authentication procedure prior to the interaction, the attack will strain from injecting a message [32, 33]. A security protocol certifies that there is no compromise on data at the time they are forwarded from one node to another.

Confidentiality: It refers that the outsider cannot read the actual/original message because the message on medium is encrypted and therefore secured. It is achieved by using encryption (public/symmetric key) [27].

Authentication: To prove oneself to be a genuine node and not a corrupt one, authentication is a must.

Non-repudiation: Refers to the impossibility of the source (non-repudiation of source) or destination (non-repudiation of destination) to refuse having sent or received a message. It provides enough proof to the destination that the received message was actually sent by the source [34]. Non-repudiation relies on authentication, however, it creates enough proof against the attackers because of non-repudiation of source, the system can point out attackers who cannot escape from accepting that they committed their crimes [35].

Authorization: This gives different users different access rights, e.g., a network administrator may only execute the management of the network.

Privacy Protection and Access Control: In order to have privacy of nodes respected, every information regarding their identity must be kept secret [29].

II. Related Works

Unique characteristics of MANET include dynamism and their ability to survive in a decentralized atmosphere. Because of the typical characteristics of MANET, various challenges creep in among which typically important ones are related to routing, such as:

In case of internetworking when MANET want to communicate with a fixed network, a co-existing routing protocol must be available.

Since there is no centralized control and instead each and every node acts as a router, therefore again routing protocols should be such which work well under such conditions.

Nodes roam around the network, therefore the routing protocol must be robust.

Stable routing is a challenge in MANET because the links go down frequently. In addition to all this, the best results would be obtained only when routing protocol used is secure and energy efficient.

Till today, tremendous work was proposed for ad hoc network routing. The routing protocols currently present in ad hoc networks may be divided along the following directions, namely: “Proactive”, “Reactive” and “Position Based Routing Protocols” [36-38, 63].

A. *Proactive Routing Protocols*

They are also referred by the name: table driven, since these protocols maintain a clear vision of the entire topology of the network, every node remembers a table which has the path to reach all the other nodes present within the network. Any change bought in the topology is propagated to the network nodes. This implies that table driven protocols pay the cost of the paths, even when they are not used. This waste of important resources such as bandwidth [39], which are already limited in networks like MANET. Therefore table driven protocols are hardly used in MANETs. Most important example of pro-active routing protocol is DSDV.

B. *DSDV*

Based on Bellman Ford algorithm, “Destination Sequenced Distance Vector Routing” protocol was given in 1994 by Perkins and Bhagwat. DSDV guarantees loop freeness (loops are not formed). This is a pro-active routing protocol therefore every node maintains tables, updates are sent very frequently [40]. Every packet of data sent by a mobile node has the following fields via: number of hops needed, new sequence number, destination address to get to the destination and destination sequence number (a sequence number of most recent information caught by the destination).The primary concern in DSDV is the making and maintaining of tables, sending updates in a MANET environment wastes crucial bandwidth. Updates need to be sent even in the situations of heavy traffic, because DSDV won't work till the time updates are sent. Hence DSDV is not a choice for MANETs.

C. *Reactive Protocols*

Reactive protocols are also called: “on-demand routing protocols” for the reason that they maintain the route only for the time it is needed (source destination are communicating) and do not create tables, thereby reducing control overhead, load on the network is reduced because no updates are sent and only few routes are maintained at any time. To achieve on-demand routing, reactive protocols work in 2 States: Route discovery in which the path to the destination is found out and Route maintenance in which the path established in route discovery is maintained till it is needed.

Reactive protocol based routing is the best option for MANETs, however loss of packets may be witnessed if way to reach to destination gets modified and there is some initial delay also because the route needs to be discovered. Most important examples of such protocols are AODV [62] and its extension AOMDV [41 – 43].

D. Position Based Routing Protocols

It employs “Global Positioning System (GPS)” to get the location information about the nodes [44-48]. This is a pre-requisite to use position based routing protocols. The decision about routing is then grounded on the location of destination and location of neighbors of forwarding node. Position based routing doesn't need to create/ maintain routing tables. Important position based routing protocols for MANETs include “Location Aided Routing (LAR)” [55, 56] and “Location Aided Multipath Routing (LAMR)” and so on [49, 54].

E. Routing Protocol Comparison

We performed a comparison of performance of all these protocols to decipher which of these protocols is best to be used in MANETs and got the following result:

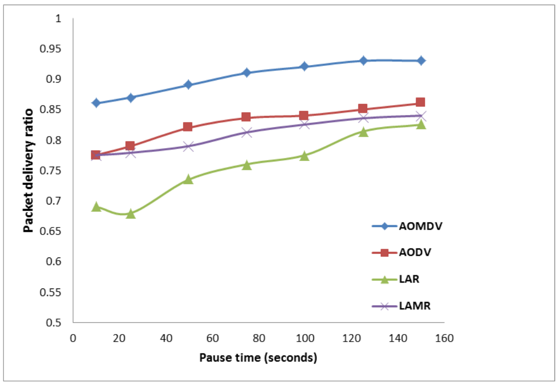

Fig.4. PDR for 10 sources with Maximum speed 20 m/sec

Figure – 4 indicates that the AOMDV has better packet delivery ratio than AODV, LAR and LAMR where we have used 10 nodes as data sources and every node travels at 20 m/Sec. In the next case, we have increased the data sources to 30, then again AOMDV has a maximum packet delivery ratio compared to other routing protocols as represented in Figure - 6. In these two cases we have configured all the nodes in such a way that all the nodes have the same speed of motion. In next case (as shown in Figure - 6) we change the speed of the nodes (i.e. Change the mobility levels of network nodes) and notice its effect on the packet delivery ratio of different nodes in the network.

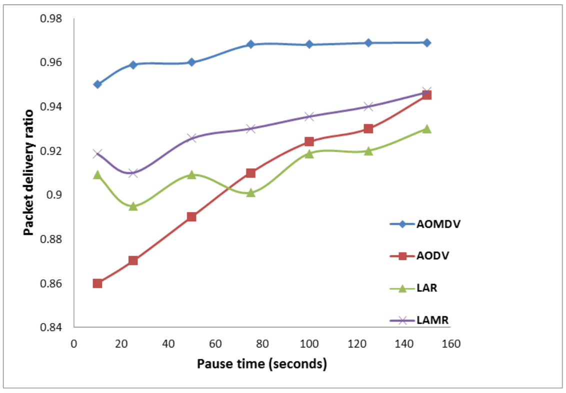

Fig.5. PDR for 30 sources with Maximum speed of 20 m/sec

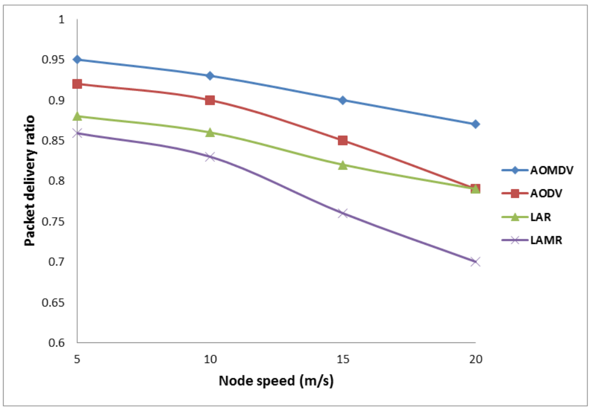

Fig.6. PDR v/s node speed

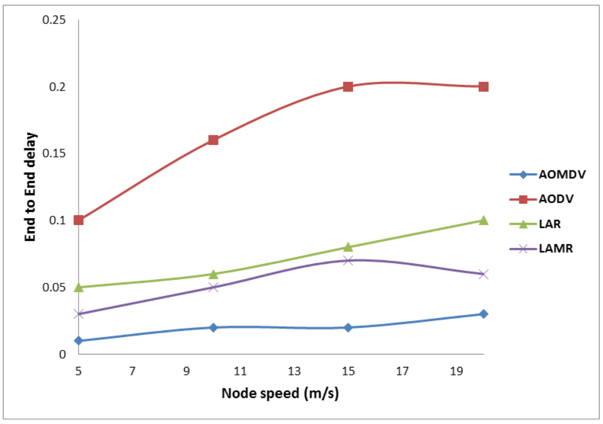

Fig.7. End to End delay v/s node speed

Here again AOMDV has maximum packet delivery ratio than other routing protocols. In the final case, shown in Figure - 8 we observed that the network node's average end to end delay with respect to varying node’s speed of motion, and the results show that escalation of node speed is directly proportional to the end to end delay, but among all the routing protocols described above AOMDV has least end to end delay.

Therefore, from these graphs it is clear that AOMDV works best for MANET from the view point of “Packet delivery ratio”, “end to end delay” many other important parameters.

Also Jan Avon Mulert [57] et al discussed AODV vulnerabilities. Here they discuss about the various attacks which can be launched in AODV environment. To secure AODV from certain vulnerabilities different protocols were proposed such as SAODV [58], ARAN [59], and SEAODV [60]. [58] proposes SAODV . However [58] can only provide solutions to attacks related to authenticity, eavesdropping and confidentiality. [59, 60] also rely on cryptographic techniques to secure AODV.

All these protocols fail to secure MANETs from the harsh DOS attacks which are launched easily in MANET environment and cause the most harm. [58-60, 64] do not have any mechanism to deal with the black hole, wormhole type of attacks, undoubtedly they carry out authentication but sometimes even the authentic nodes carries out DOS attacks.

To help MANET recover from DOS attacks, a secure Multipath Ad hoc routing protocol has been proposed which will be discussed in the upcoming sections.

III. Proposed System

In the preceding section it has been discussed that the main security issue in MANET is when a legitimate user acts as attacker of the network, causing the data packets to be dropped, thereby reducing the overall performance of the network. Also, the secure routing protocols proposed till date, are not able to overcome such problem. Thus, in-order to overcome such problem in MANET, a Secure Multipath Routing protocol (SMAODV) is presented which reduces the effect of malicious nodes to larger extend in a network.

A. Secure Multipath Ad Hoc On-Demand Distance Vector Routing Protocol (SMAODV)

SMAODV is the modification of “Ad Hoc On-demand Multipath Distance Vector (AOMDV) routing protocol” which makes use of alternate paths to eliminate the effect of malicious nodes in the network. When a node generates data packets so as to send them to some other node in a network, it initiates RREQ packet flooding process first to discover the shortest route to destination. A route is discovered and registered when the source node receives RREP packet which is sent by the destination node so as to answer the RREQ packet. The SMAODV allows each node to accept multiple RREP packets which are sent by destination in response to multiple RREQ packets (received by destination node through multiple paths available between each pair of source and destination), due to which multiple paths are constructed between each pair of nodes in a network. These multiple paths are then being used to diminish the effect of malicious nodes in a particular network. Also, the data transmitted from a particular source node to destination node are labeled with counter value, which gets incremented each time a data packet gets generated by the source node. So each packet has a unique counter value for a particular source-destination pair. This unique number (counter value) is then used to check whether the packets arrive in order or out-of-order at the destination.

SMAODV also incorporates the concept of randomization of path selection. In randomization process a random path is selected from all the multiple paths available at the source node. The malicious nodes are the first to send RREP’s to source node (if they are in between source and destination) and the source node will normally chose this route to forward packets to destination because it has less latency, but the malicious nodes present in this path will drop the packets. Due to randomization process the source node does not always selects the least cost route, but will randomly chose a route out of all the possible routes calculated during the route discovery process. This reduces the probability of selecting a path containing malicious nodes, thereby increasing the overall packet delivery ratio of nodes in a network.

The ad hoc networks are usually dynamic, i.e. the nodes of such networks are always in motion. Due to this continuous change in position of ad hoc nodes complete topology of the network gets disturbed, so it is the duty of the routing protocol which is being used in such networks to be adaptive to the changing network topology and update the routes accordingly. To do this, a continuous rebroadcasting of RREQ packets has been proposed, which is initiated at the end of re-broadcasting timer. Once an initial route discovery process comes to an end, the source node sets the re-broadcasting timer and forwards packets to the destination through a particular route selected by the source node among all the available paths. The data transmission then halts for a moment when the re-broadcasting timer gets expired (i.e. Comes to end) and rebroadcasting of RREQ packets is initiated. Due to this rebroadcasting process new alternate paths are being calculated and once the rebroadcasting process is completed, a new route is chosen in place of previous route to forward the rest of data packets between the source and destination and again the re-broadcasting timer is set. Also, if the destination node detects that some of the data packets are missing (greater than the threshold) then it informs the source node to re-transmit the missing packets through new routes. The destination node uses its counter value to check whether it has received packets in order or not. Each time the destination node receives a data packet, it compares its counter value with the counter value in the received data packet. If the value of counter of the destination is less than the counter value in data packet by a threshold, then it immediately informs source node that some of the packets are lost and requests for retransmission of those packets. But, if the counter value of the destination is equal to the counter value of a data packet, then it accepts the data packets and updates its counter value by the counter value on the last data packet. Also, when the source node gets informed about the packet loss by destination, then it removes the previously used route from its routing table (which caused packet loss). Thus, in this way all those routes are eliminated, which cause any kind of packet loss in the network. The complete process used in SMAODV has been explained by flowcharts.

When any source node chooses a particular route to transmit data to the destination node, then the source node sets the rebroadcasting timer before sending data through that route. After some particular time when the rebroadcasting timer gets expired, the rebroadcasting of RREQ packets takes place. The initial step in the rebroadcasting process is to buffer the data packets which are being generated by the source node during rebroadcasting process. After this RREQ packets are being flooded again in the network by source node and again the route discovery process is initiated, due to this process new and alternate routes will be discovered between source and destination. Once the process of finding new alternate paths between source and destination gets completed, then a new alternate route is being chosen for sending the rest of data packets to a destination node, as shown in figure 8. This rebroadcasting process helps to generate new and fresh, alternate paths between a particular source and destination nodes and also helps in the process of eliminating malicious routes (routes containing malicious nodes in them) from the network.

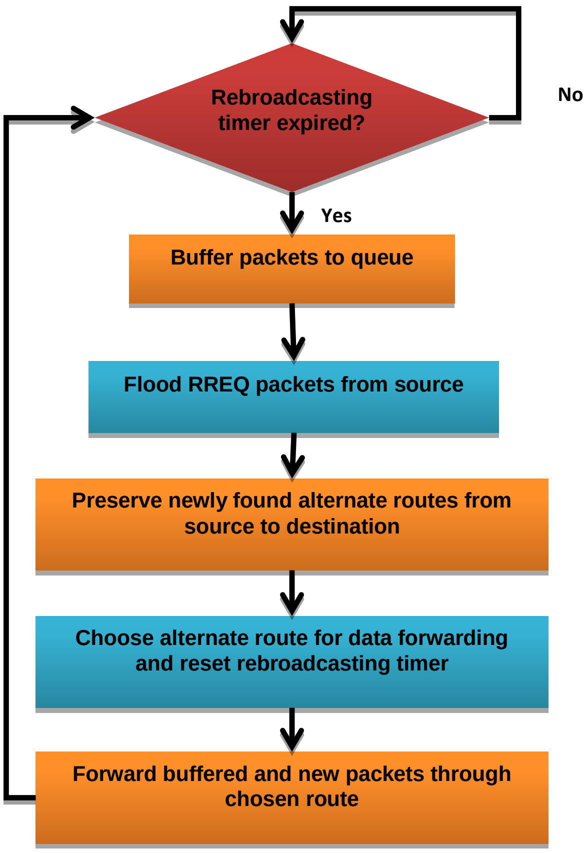
Rebroadcasting timer expired?
No
Yes
Buffer packets to queue
Flood RREQ packets from source
Preserve newly found alternate routes from source to destination
Choose alternate route for data forwarding and reset rebroadcasting timer
Forward buffered and new packets through chosen route

Fig.8. Rebroadcasting Process

Also, for each data packet received by destination node a complete process of detecting any packet loss, as shown in figure 9, takes place. Each data packet generated by any source node has a counter value, which is the "count of data packets transmitted by this source node + 1", this counter value is denoted by CP. When a packet arrives at the destination, its CP is compared with the Packets counter value at destination (Cd – the counter value of the most recently received packet by destination node). If the value of C_d is equal to or slightly less (threshold) than the value of C_P, then there is either no packet loss or least packet loss (less or equal to the threshold), for this case the destination node accepts the data packet and updates its C_d value by the value of C_P in the received packet. But if the condition is not met, i.e. Cd is less than that of CP by a larger number (greater than threshold), then there is packet loss in the network due to some malicious node, for this case the destination node discards the received packet and informs the source node about the packet loss by sending the value of C_d. When the source node receives the value of Cd and it removes the previously selected route from its routing table and retransmits the lost packets to destination through the newly selected route. So, by this way the malicious routes (routes containing malicious nodes) are not being used for data transfer, due to which the network gets secured from the effect of any malicious node.

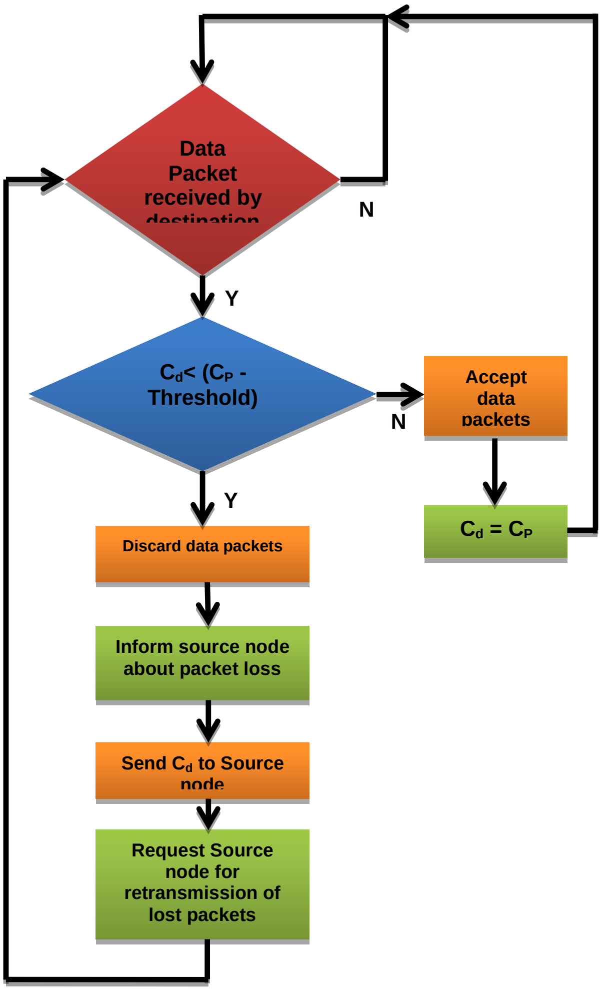
Data Packet received by destination
N
Y
C_d< (C_P - Threshold)
N
Accept data packets
C_d = C_P
Y
Discard data packets
Inform source node about packet loss
Send C_d to Source node
Request Source node for retransmission of lost packets

Fig.9. {Detection of Packet Loss at the Destination Node (C_d – Counter Value at Destination, C_P – Counter Value on Received Data Packet)

As discussed above, SMAODV make an efficient utilization of alternate paths (available between particular source and destination) for eliminating the effect of malicious nodes from a network. It continuously checks for packet loss due to some malicious node and informs source node about it. The proposed secure multipath routing protocol does not detect the malicious nodes in the network, but it eliminates their effect in the network. There is no effect on the information shared between source and destination nodes by a malicious node in the network. Thus, with SMAODV we are able to achieve robustness in the network. Also, by incorporating rebroadcasting process, one can easily deal with the ill effects of mobility in a wireless network. This feature again makes SMAODV a complete routing protocol for MANETs.

IV. Experimental Evaluation

The simulation of the proposed routing protocol has been done using NS – 2, which is an open source network simulator. We have constructed a MANET and configured the SMAODV as the routing protocol on each node. The proposed routing protocol has been implemented by modifying already existing AOMDV code. To test the performance of the proposed routing protocol, we have used "packet delivery ratio", "throughput" and "end-to-end delay" as a metric, and compared it with AODV and AOMDV routing protocols in the presence of malicious nodes (Black hole and wormhole attackers). The simulation bounds used are shown in the table – 1 and the experimental results are shown in figure 10 to 12.

Table 1. Simulation Parameters

Simulator	Network Simulator – 2 (2.35)
Number of Nodes	50
Simulation time	50 seconds
Traffic type	CRB
Routing Protocols	AODV, AOMDV and SMAODV
Packet Size	1000 bytes
Antenna type	Omni-directional
MAC type	802.11 MAC layer
Malicious Behaviors	Black hole and wormhole attacks
Mobility	Variable (5 m/s to 20 m/s)
Threshold used at the destination nodes	3 Packets
Number of Malicious Nodes	2, 4, 6, 8, 10, 12, 14, 16, 18

A. Simulation Results

The complete scenario for creating a MANET using 50 nodes has been done by using Network simulator – 2 (NS2). The type of traffic chosen between the nodes is CBR with packet size of 1000 bytes. Each node moves with a speed of 5 to 20 m/sec and each node have Omni-directional antenna for catching the signal from all the directions. At network layer we have used AODV and AOMDV as routing protocols (which are already there in NS2 – 2.35 package) for comparing the performance of the proposed routing protocol (SMAODV). SMAODV has been implemented by modifying the backend code of AOMDV using C++ language. At the data link layer we have used the 802.11 MAC layer protocol. The malicious behavior of nodes is shown by implementing black hole and wormhole attack procedures on some of the randomly chosen nodes of the network.

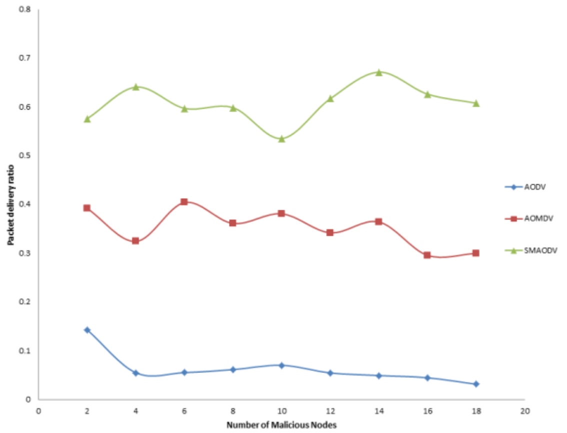

Fig.10. Average Packet Delivery Ratio of Nodes for AODV, AOMDV and SMAODV in Presence of Malicious Nodes

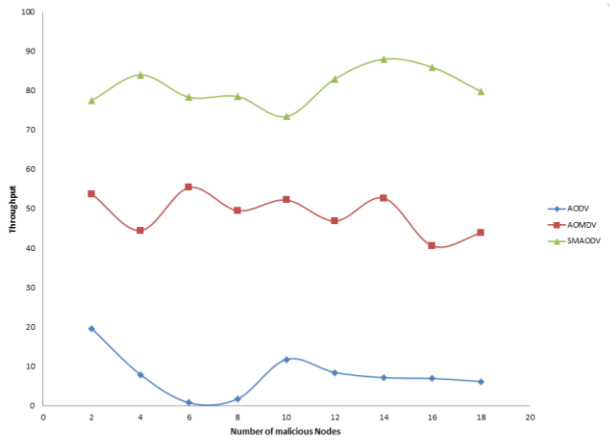

Fig.11. Average Throughput of Nodes for AODV, AOMDV and SMAODV in Presence of Malicious Nodes

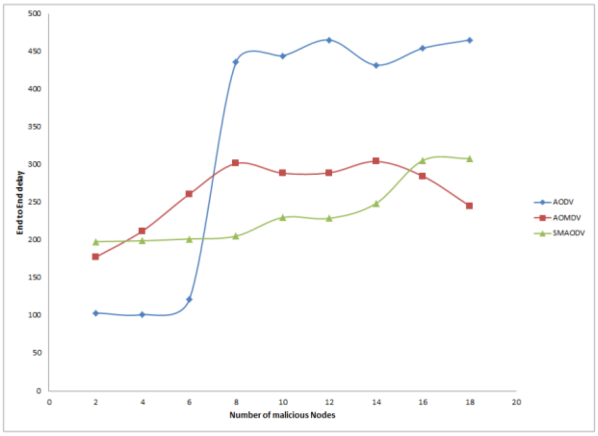

Fig.12. Average End-to-end delay of Nodes for AODV, AOMDV and SMAODV in Presence of Malicious Nodes

To find the performance of the proposed routing protocol (SMAODV), a MANET with 50 nodes has been created and some of the random nodes are configured as wormhole and black hole attacker nodes. Also to prove that the proposed routing protocol is more efficient than the other standard routing protocols, the comparison of the performance of SMAODV with the performance of AODV and AOMDV routing protocols in presence of malicious attackers has been done. As shown in figure 10, it is concluded that as the quantity of malicious nodes increase in the network the average packet delivery ratio of nodes remains almost constant, and also SMAODV routing protocol has a higher packet delivery ratio in comparison to the other mentioned routing protocol. From this result, we can say that the proposed routing protocol provides much more security than the other standard routing protocols. Also, figure 11 again shows that the average throughput of network nodes for SMAODV remains constant and is much higher than other routing protocols mentioned, again proving that SMAODV is more efficient than other routing protocols. Figure 12 shows that the "end to end delay" of network nodes for SMAODV is slightly high, which is due to the rebroadcasting and the malicious route detection procedures, which get executed continuously so as to make the data transfer more secure, but again this delay is less than that of other mentioned routing protocols.

From the above we can conclude that the proposed secure multipath routing protocol (SMAODV) outperforms than other standard routing protocols (AODV and AOMDV) which are usually used for routing in ad hoc networks. The proposed routing protocol performs better when taking "packet delivery ratio", "throughput" and "end to end delay" of network nodes into consideration (which constitute the basic metric for analyzing the performance of routing protocols for MANETs).

V. Conclusion & Future

This paper work deals with the communication of one of the dynamic networks called MANET. In today's world MANETs are getting much more attention because of their vast application in different fields. Almost all the applications of MANET in different fields are because of its support to mobility. The MANET nodes can easily enter or leave any network boundary and can easily move from one place to another without the need of any infrastructure for communication purposes. But, due to this applicative feature of MANETs there are certain dangerous security issues which can cease its use in those areas where security has major importance. One such security issue which we have discussed in detail in this paperwork is the attack on forwarded data by a legitimate user. This is the major challenge to secure a mobile network from such attacks because this type of attack cannot be tackled by using cryptographic techniques. Also, the previous work proposed to overcome this security problem does not provide a standard solution. So, in this connection a secure multipath on-demand security mechanism (SMAODV) for MANETs has been proposed, which can overcome such problem with the help of using multi paths (which are available between source – destination pairs). The proposed routing algorithm is the modification to the AOMDV routing protocol which is already being used as one of the standard routing protocol for ad hoc networks. So, the proposed secure multipath routing protocol can become a standard routing protocol which can be able to overcome all other issues of MANET also. The proposed routing protocol continuously rebroadcasts RREQ packets in the network (when the rebroadcasting timer expires), so as to gather new and alternate paths from source node to the destination node. Thus, this feature makes the protocol quite suitable for MANETs, because MANET nodes are in continuous motion thereby changing the topology of network continuously. Also the destination node continuously monitors the received packets for malicious route detection (as explained in the previous sections in detail). No other node is involved in monitoring the data packets for malicious behavior detection. This makes the proposed routing protocol secure and simple. The implementation of the proposed security mechanism (SMAODV) has been done in NS–2 for MANET and the creation of different scenarios by changing the mobility of nodes has been done. Also the comparison of the proposed routing protocol has been done with the standard routing protocols which are usually used for routing purposes in the MANET (like AODV and AOMDV). We have measured the performance of each routing protocol by using "packet delivery ratio", "average throughput" and "average end to end delay" as metric and the simulation resulted showed that the proposed routing protocol has better performance with respect to all the above mentioned performance metrics.

We have compared the proposed secure routing protocol with two commonly used standard routing protocols. Other routing protocols can be taken in future to compare the efficiency of the proposed routing protocol with them. Also, we can take some more additional parameters in the future to evaluate the proposed routing protocol in detail and check its degree of applicability to MANETs. This routing protocol can also be applied to other highly dynamic and larger networks like VANETs and evaluate its performance there. This can allow one to assign limits to this routing protocol, i.e. what is the range of mobility, where this routing protocol can perform routing efficiently. Additional techniques can be incorporated in order to find more feasible and secure routes before data transmission takes place, which can make this routing protocol even more secure and can increase the average packet delivery ratio of network nodes.

References

[1] ElhadiM.Shakshuki, Nan Kang, Tarek R. Sheltami, "EAACK – A Secure Intrusion Detection System for MANETs", in: IEEE Transactions on Industrial Electronics, vol 60,No. 3, March 2013.

[2] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput.Sci., vol. 3, no. 8, pp. 574–582,2007.

[3] B. Sun, "Intrusion detection in mobile ad hoc networks," Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[4] Roy Friedman, Daniela Gavidia, Luis Rodrigues, AlineCarneiroViana, Spyros Voulgaris, "Gossiping on MANETs: the Beauty and the Beast", in: ACM Operating Systems Review, October 2007

[5] A. C. Viana, M. D. Amorim, Y. Viniotis, S. Fdida, and J. F. Rezende, "Twins: a dual addressing space representation for self-organizing networks", in: IEEE Transactions on Parallel and Distributed Systems, 17(12):1468–1481, Dec. 2006.

[6] PrasanjitChoudhury, AnirbanSarkar, Narayan C. Debnath, "Deployment of Service Oriented Architecture in MANET: A Research Roadmap", in: IEEE 2011

[7] TommiHalonen, TimoOjala, "Cross-layer design for providing service oriented architecture in a mobile Ad Hoc network", 5th International Conference on Mobile And Ubiquitous Multimedia, 2006.

[8] Microsoft Developer Network (MSDN), "Consuming Web Services with the Microsoft.NET Compact Framework", March 2003.

[9] X. Gu and K. Nahrstedt, "Dynamic QoS-Aware Multimedia Service Configuration in Ubiquitous Computing Environments", 22nd International Conference on Distributed Computing Systems, pp 311 – 318, 2002.

[10] OASIS-Open Organization, “Introduction to UDDI: Important Features and Functional Concepts”: http://uddi.xml.org/files/uddi- tech-wp.pdf.

[11] OASIS-Open Organization, “UDDI Version 3.0.2.”, http://www.oasis open.org/committees/uddi-spec/doc/spec/v3/uddi-v3.0.2-20041019.htm

[12] TommiHalonen, TimoOjala, “Cross-layer design for providing service oriented architecture in a mobile Ad Hoc network”, 5th International Conference on Mobile And Ubiquitous Multimedia, 2006.

[13] Neema, H.; Kashyap, A.; Kereskenyi, R.; Yuan Xue; Karsai, G.;“SOAMANET: A Tool for Evaluating Service-Oriented Architectures on Mobile Ad-Hoc Networks”, 2010 IEEE/ACM 14th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), pp179 – 188, 2010.

[14] L. Miao, K. Djouani, B.J. van Wyk, Y. Hamam, “Evaluation and enhancement of IEEE 802.11 p standard: a survey”, Mob. Comput.1 (1) 2012.

[15] C.Siva Ram Murthy & B.S Manoj, “Mobile Ad Hoc Networks- Architectures & Protocols”, Pearson Education,New Delhi, 2004.

[16] An Introduction to Wi-Fi‖ 019-0170 • 090409-B USA 2007-2008.

[17] Behrouz A Forouzan, Data Communications and Networking‖, Special Indian Forth Edition, 2006.

[18] N. Srinath [CS07M035] WiMAX - An Introduction.

[19] N. Gupta and G. Kaur, WiMAX: Applications,ser. The WiMAX Handbook, S. Ahson and M. Ilyas, Eds. CRC Press (Taylor and Francis Group), ch. 3: “WiMAX Technology for Broadband Wireless Communication”, pp. 35 – 54, ISBN 9781420045474, 2008.

[20] Ajay Jangra, NitinGoel, Priyanka, Komal Kumar Bhatia, “IEEE WLANs Standards for Mobile Ad-hoc Networks (MANETs): Performance Analysis”, in: Global Journal of computer science and technology, pp 42-47, Nov 2010.

[21] Chlamtac, I., Conti, M., and Liu, J. J.-N. “Mobile ad hoc networking: imperatives and challenges Ad Hoc Networks”, 1(1), pp. 13–6, 2003.

[22] HaoYang, Haiyun & Fan Ye “Security in mobile ad-hoc networks : Challenges and solutions”, Pg. 38-47, Vol 11,issue 1, Feb 2004.

[23] Hao Yang, HaiyonLuo, Fan Ye, Songwu Lu, Lixia Zhang, “Security in Mobile Ad hoc networks: Challenges and solutions”, in : IEEE Wireless Communications, 2004.

[24] AnkurO.Bhang, PrabhakarL.Ramtake, “MANET: History, Challenges and Applications”, in: IJAIEM, pp 249-250, 2013.

[25] Rashid Sheikh, Mahakal Singh Chandel, Durgesh Kumar Mishra, “Security Issues in MANET: A Review”, in: IEEE 2010.

[26] Y. Haung and W. Lee, “A Cooperative Intrusion Detection system for Ad hoc Networks”, in Proceedings of the 1st ACM Workshop on security of Ad hoc d sensor Networks, Fairfax, Virgining, pages 135-147, 2003.

[27] V.S. Yadav, S. Misra, M. Afaque, “Security of Wireless and Self-Organising Networks: Security in Vehicular Ad Hoc Networks”, CRC Press, pp.227-250, 2010.

[28] A. Stampoulis, Z. Chai, “A survey of Security in Vehicular Networks”, Project CPSC 534, 2007.

[29] Q. Yi, N. Moayeri, “Design of secure and application-oriented VANETs”, in: Vehicular Technology Conference. VTC Spring IEEE, pp. 2794-2799, 2008.

[30] S. Biswas, J. Misic, “Proxy signature-based RSU message broadcasting in VANETs”, in: 25th Biennial Symposium on Communications (QBSC), pp. 5-9, 2010.

[31] P. Papadimitratos, L. Buttyan, T.Holczer, E.Schoch, J. Freudiger, M.Raya, et al., “Secure vehicular communication systems: design and architecture”, IEEE commun. Mag.46, 100-109, 2008.

[32] J.T.Isaac, S.Zeadally, J.S. Camara, “Security attacks and solutions for vehicular ad hoc networks”, IET commun, 4 894-903, 2010-04-30.

[33] M. Raya, P. Papadimitratos, J.P. Hubaux, “Securing vehicular communications”, IEEE Wirel. Commun,13, 8-15, 2006.

[34] F. Armknecht, A. Festag, D. Westhoff, K. Zheng, “Cross-layer privacy enhancement and non-repudiation in vehicular communication”, in: Communication in Distributed Systems (KiVS), ITG-GI Conference, pp. 1-12, 2007.

[35] B. Parno, A. Perrig, “Challenges in securing vehicular networks”, in: Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[36] D.B. Johnson, D.A. Maltz, Y. Hu, “The dynamic source routing protocol for mobile ad hoc network”, IETF Internet Draft, draft-ietf- MANET-dsr-09.txt, April 2003.

[37] X. Lin and I. Stojmenovic, “Location-based localized alternate, disjoint and multi-path routing algorithms for wireless networks”, in: Journal of Parallel and Distributed Computing, pp. 22–32, January 2003.

[38] H.D. Trung, W. Benjapolakul, “Routing protocols in mobile ad hoc networks, in: Encyclopedia of Wireless and Mobile Communications”, CRC Press, Book Chapter, in press.

[39] S.R. Das, R. Castaneda, and J. Yan, “Simulation based performance evaluation of mobile, ad hoc network routing protocols”, in: ACM/ Baltzer Mobile Networks and Applications (MONET) Journal, pp. 179–189, July 2000.

[40] C. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers”, in: Proceed- ings of the Conference on Communications Architectures, Protocols and Applications (ACM SIGCOMM ’94), London, United Kingdom, pp. 234–244, August–September 1994.

[41] C.E. Perkins, E.M. Belding-Royerand, I.D. Chakeres, “Ad Hoc On- Demand Distance Vector (AODV) Routing”, IETF Internet Draft, draft-perkins-MANET-aodvbis-01.txt, January 2004.

[42] C.E. Perkins and E. Royer, “Ad hoc on-demand distance vector (AODV) routing”, in: Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 90–100, February 1999.

[43] M.K. Marina and S.R. Das, “On-demand multipath distance vector routing in ad hoc networks”, in: Proceedings of the 9th IEEE International Conference on Network Protocols (ICNP), pp. 14–23, 2001.

[44] NAVSTAR GPS operations. Available from: <http://tycho.usno.na- vy.mil/gpsinfo.html>/.

[45] Peter H. Dana’s Page at Colorado University. Available from: http:// www.colorado.edu/geography/gcraft/notes/gps/gps.html /.

[46] G. Dommety and R. Jain, “Potential Networking Applications of Global Positioning Systems (GPS)”, Technical Report TR-24, CS Dept., The Ohio State University, April 1996.

[47] D. Niculescu and B. Nath, “Ad Hoc Positioning System

(APS)", in: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), San Antonio, vol. 5, pp. 2926–2931, November 2001.

[48] E.D. Kaplan, "Understanding GPS: Principle and Application", Artech House, Boston, MA, 1996.

[49] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position- based routing in mobile ad hoc networks", in: IEEE NetworkMagazine, vol. 15, pp. 30–39, November 2001.

[50] R. Jain, A. Puri, and R. Sengupta, "Geographical routing using partialinformation for wireless ad hoc networks", in: IEEE PersonalCommunications, vol. 8, pp. 48–57, February 2001.

[51] B. Karp and H.T. Kung, "Greedy perimeter stateless routing for wireless networks", in: Proceedings of the 6th Annual ACM/IEEE International Conference Mobile Computing Networks, pp. 243–254, August 2000.

[52] P. Bose et al., "Routing with guaranteed delivery in ad hoc wireless networks", in: Proceedings of the 3rd ACM International Workshop in Discrete Algorithms and Methods for Mobile Computer and Communications, pp. 48–55, 1999.

[53] S. Capkun, M. Hamdi, and J. Hubaux, "GPS-free positioning in mobile ad hoc networks", in: Proceedings of the International Conference in System Sciences, pp. 1–15, January 2001.

[54] H.D. Trung and W. Benjapolakul, "Location-aided multipath routing method for mobile ad hoc wireless networks", in: Proceedings of the International Conference on Communications and Electronics (ICCE'06), Hanoi, Vietnam, pp. 7–12, October 2006.

[55] Y.-B. Ko and N.H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks", in: Wireless Networks, vol. 6, pp. 307–321, July 2000.

[56] Ha DuyenTrung, WatitBenjapolakul, PhanMihnDuc, "Performance evaluation and comparison of different ad hoc routing protocols", in: Elsevier, pp. 2478-2496, 2007.

[57] Jon Von Mulert, Ian Welch, Winston K.G Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV", in: Elsevier, pp. 1249-1259, 2013.

[58] Guerrero-Zapata M. "Secure ad hoc on-demand distance vector routing", ACM SIGMOBILE Mobile Computing and Communications Review;6(3):106–7, 2002.

[59] Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM. "A secure routing protocol for ad hoc networks", In: Proceedings of the 10th IEEE international conference on network protocols (ICNP), Paris, France, p. 78–89, 2011.

[60] Mohammadizadeh M, Movaghar A, Safi SM. "SEAODV: secure efficient AODV routing protocol for MANETs networks," in: Proceedings of the 2nd international conference on interaction sciences: information technology, culture and human (ICIS), Seoul, Korea, p. 940–44, 2009.

[61] Mahmoud HashemEiza, Thomas Owens, Qiang Ni and Qi Shi, "Situation-Aware QoS Routing Algorithm for Vehicular Ad Hoc Networks", IEEE transactions on vehicular technology, vol. 64, no. 12, December 2015.

[62] Tarunpreet Bhatia and A.K. Verma, "Performance Evaluation of AODV under Blackhole Attack", in I. J. Computer Network and Information Security, 2013, 12, 35-44. DOI: 10.5815/ijcnis.2013.12.05

[63] P.Periyasamy and Dr.E.Karthikeyan, "Survey of Current Multipath Routing Protocols for Mobile AD Hoc Networks" in I. J. Computer Network and Information Security, 2013, 12, 68-79. DOI: 10.5815/ijcnis.2013.12.09

[64] J.Sathiamoorthy, B.Ramakrishnan,"CEAACK – A Reduced Acknowledgment for Better Data Transmission for MANETs", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.2, pp.64-71, 2016.DOI: 10.5815/ijcnis.2016.02.08

Authors' Profiles

Mir Shahnawaz Ahmad received the B. Tech. degree in Computer Science and Engineering from university of Kashmir, Srinagar, J&K, India, and the M.Tech. degree in Computer Science and Engineering from SMVDU, Katra, J&K, India. His main research focus lies in database management systems, Software Defined Networks, MANETs, IOT and Data Sciences.

How to cite this paper: Shahnawaz Ahmad,"Alleviating Malicious Insider Attacks in MANET using a Multipath On-demand Security Mechanism", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.6, pp.40-51, 2018.DOI: 10.5815/ijcnis.2018.06.04