Enhanced Detection and Elimination Mechanism from Cooperative Black Hole Threats in MANETs

Samiullah Khan*, Faqir Usman†, Matiullah‡, and Fahim Khan Khalil§,
*§Institute of Business Management Sciences, The University of Agriculture Peshawar-Pakistan
†Department of Computer Science , Qurtuba University of Science and Information Technology-Pakistan
‡Department of Basic Sciences and Islamiat, University of Engineering and Technology,Peshawar-Pakistan

***Abstract*—Malicious node invasion as black hole attack is a burning issue in MANETs. Black hole attacks with a single malicious node is easy to detect and prevent. The collaborative attacks with multiple cooperative malicious node is a challenging issue in security of MANETs as it is difficult to figure out due to its complex and sophisticated mechanism. This study proposed a novel signature-based technique to detect and handle the cooperative black hole attack in MANETs. For this purpose, diverse type of simulation scenarios are used with increasing number of nodes. The parameters such as average throughput, average packet drop, average end to end delay, average processing time and malicious node detection rate are used to measure the impact of signature-based malicious node detection scheme. AODV is used as routing protocol in this study. This study revealed that the performance of MANETs degrades with an increase in a number of malicious nodes. The average throughput of MANETs decreases with increase in average end to end delay and average packet drop. Signature-based malicious nodes detection mechanism is used to counter the cooperative black hole attack. The signature-based technique has enhanced the detection and elimination of cooperative black hole attack in MANETs. This helps in comparatively an increase in average throughput and decrease in packet delay and packet drop.**

***Keywords*—Mobile Ad-hoc Networks (MANETs); black hole attack; AODV; malicious node; cooperative attack**

I. Introduction

In the recent years, wireless network gained much attention from the researchers due to its diverse application in various fields. Mobile Ad-hoc Networks (MANETs) are specific types of wireless network that have autonomous and decentralised structure [1]. MANETs are easy to be deployed and are dynamic. These features of MANETs enable its usage in a situation which has strict geographical constraints, such as in battlefields and disaster management. In MANET, nodes are free to move and connect with all other nodes in an ad-hoc way. A node in MANETs can act as a source or destination as well as forwarder (router) node to relay the packets to another destination node as shown in Fig. 1. Routing in MANETs is performed in three different ways that are: Proactive, Reactive and Hybrid [2].

MANETs are susceptible to security threats due to a number of reasons like; open communication environment, dynamic topology requirements, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism [1]. These security threats in MANETs have also changed the battlefield situation. The challengeable task is to ensure the security of routing protocols in MANETs against the misbehaviour of malicious nodes. A MANETs is more prone to security attacks due to communication based on mutual trust between the nodes.

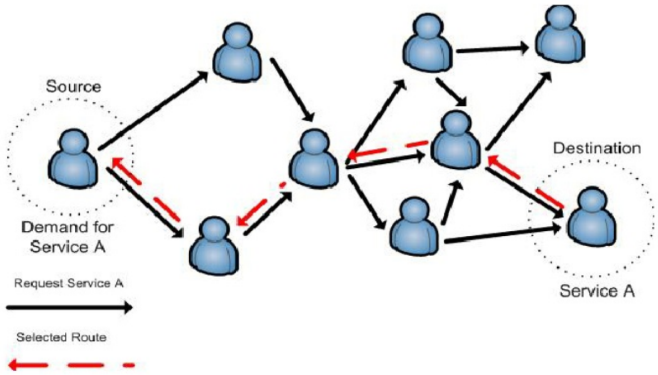

Fig. 1. Routing in MANETs [24].

Some routing protocols such as Ad hoc On-Demand Distance Vector (AODV) [3], Dynamic Source Routing (DSR) Protocol [4], [27] and Destination-Sequenced Distance-Vector Routing (DSDV) [5] are developed to cope with routing in MANETs. AODV protocol is most widely used routing protocol for MANETs. Routing path selection in AODV routing protocol makes use of a sequence number to select most recent path to the destination [2]. In most of the discussed protocols, the routing decision relies on the cooperation and coordination between the nodes due to the lack of a centralised administration. Also, all of the nodes need to believe that each of them is trustworthy and well-behaved. Malicious nodes exploit these attributes of MANETs to launch attacks on the network. The wormhole attack, black hole attack, sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving and impersonation are possible active attacks on the routing protocols of MANETs [6]–[11].

In Black hole attack, the intermediate malicious nodes pretend to be the best forwarding nodes to the destination and ultimately drop the packets upon reception. Black hole attack can be categorised into two different attacks, based on the number of malicious nodes. The first one is termed as single Black hole attack where an individual node is acting as malicious nodes to perform the attack. Secondly, the multiple attackers synchronise their efforts to harm the network. This causes intense damage to the network and is called cooperative black hole attack [12], [13].

Black hole attacks that involve a single node are easy to figure out [14]. However, collaborative attacks are very complex, powerful and sophisticated in the mechanism. Thus, dealing with these types of attacks is comparatively more challenging. Some researchers have worked on techniques and protocols for detection and mitigation of the effects caused due to black hole attack [15], [16]. Most of them catered the problems in a very efficient way. However, in most of the presented solutions, there is a possibility of an increase in overhead and average end-to-end delay. The increase in overhead can lead to degradation in the overall performance of MANETs. This study intends to introduce a novel approach that will try to detect and eliminate cooperative malicious nodes in a path with minimum overhead and average end-to-end delay. The proposed approach will make use of the signature based mechanism for malicious node detection.

The rest of the research article is organised as follows: The background study of MANETs routing protocols and related work about the different types of attacks is presented in Section I. Literature survey of different approaches and protocols used for the detection of black hole (i.e.single and cooperative) attacks are presented in Section II. Section III discussed the proposed solution approach along with the working details. Result and discussion with detail of simulation scenarios and parameters are presented in Section IV. Finally, conclusion and future work are discussed in Section V.

A. Background of Study

In the last few years, wireless networks gained attention of industry as well as from the researchers due to its application in various fields. Example of currently used wireless networks includes Mobile Ad hoc Networks (MANETs), Vehicular Ad-hoc Networks (VANETs), Urban Mesh Networks (UMNs), and Wireless Sensor Networks (WSNs) [17], [18]. MANETs are self-organised wireless networks where nodes move freely around and interact with other nodes. Topology in MANETs is dynamic due to continuous movement of nodes in the vicinity. A node in the MANETs act as a source or destination or as a router at a time. Different routing schemes such as reactive, proactive and hybrid are employed to perform routing across the network as shown in Fig. 2. In reactive routing protocols, the source node initiates a request for the path towards the destination at a time when it has to send data to the destination [19]. Reactive routing protocols consume fewer resources and thus are efficient regarding memory as it does not need to maintain a routing table for all the routes. However, selection of the best path to the destination is a tough task in reactive protocols. Proactive routing protocols maintain a routing table and contain information about paths that lead to the destination [20]. Nodes that have a packet to send to any node can forward packet instantly, as routes to all nodes in the vicinity are listed in the routing. Even though proactive routing protocols can achieve good packet throughput, they have several disadvantages [47]:

- *Overhead of maintaining routing table .*
- *Slow convergence due to frequent path failures in MANETs due to having a dynamic topology.*

Hybrid protocols were introduced to combine the features of proactive and reactive routing protocols intelligently. Routing is performed in two different ways; use reactive approach for communication among neighbour nodes and use proactive routing strategy for communication among nodes that are located a distance of two or more hops from each other [21].

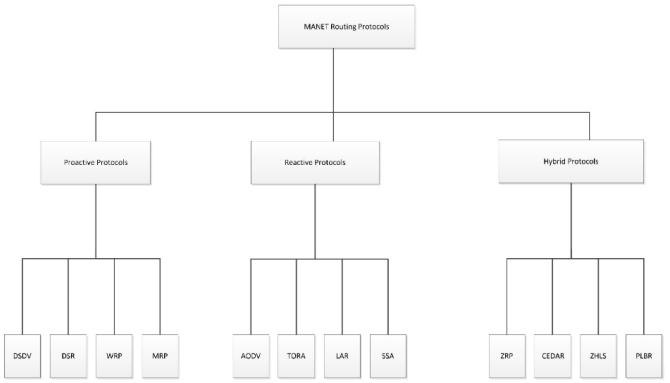

Fig. 2. Classification of routing protocols in MANETs.

1) Ad hoc On-Demand Distance Vector (AODV): AODV routing protocol is one of the important reactive routing protocols in MANETs that make use of sequence number to select a new path for the communication between the sender and destination nodes as shown in Fig. 3 [22]. To perform communication among nodes, AODV uses two different packets that are: Route request (RREQ) and Route Reply (RREP). RREQ contain information about the sending node whereas RREP is the response packet sent in a reply from intermediate nodes that have a new route to the destination node. A new route is a route whose sequence number is higher than the sequence number contained in the RREQ received at the intermediate nodes [23]. Since nodes in the MANETs communicate over the wireless medium, message security is indeed a major concern. The security of routing protocol in MANETs is vulnerable to jamming attack [24], worm hole attack [4], black hole attack and gray hole attack.

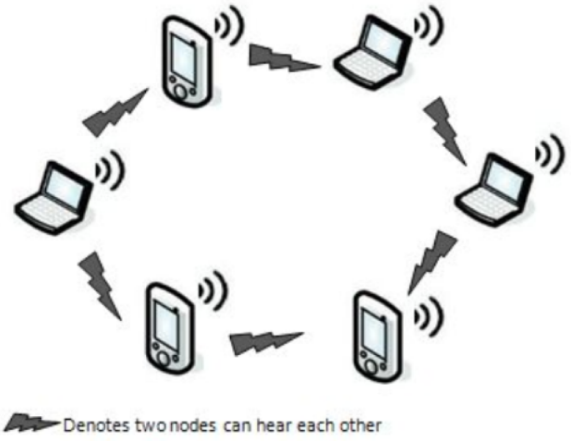

Fig. 3. Data communication among the nodes in MANETs.

2) Black hole attacks in MANETs: Blackhole attack is a type of attack which is launched by one or more of the intermediates nodes (called black hole nodes). These malicious nodes send a false RREP message to the source, claiming that it has the shortest path to the intended destination node [2], [25].

Black hole attack is considered as one of the most devastating attacks on the MANETs. The black hole node intercepts the packets, coming from the source nodes and silently drop. This will lead to immense loss of packets and cause an end-to-end delay to transfer the data packets through the network. Fig. 4 shows the example network topology where AODV protocol is used as a routing protocol. Suppose one of the nodes "S" has data that is to be sent to destination node "D". The source node initiate route request by broadcasting RREQ packet to all the nodes in the neighbours. The malicious node "M" send a forge RREP reply message containing a spoofed destination address, less number of hops and smallest sequence number to deceive the source node. The source node selects the route contained in the forged RREP message for packet sending to the destination nodes. Packets that are received by the malicious nodes are dropped thereby not allowing communication between the sender and original destination.

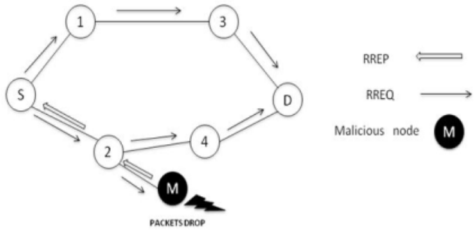

Fig. 4. Single black hole attack.

Another type of black hole attack is called Collaborative black hole attack that involves more than one node in launching the attack. The core idea behind this type of attack is to fabricate the RREP packet by all the malicious nodes with mutual understanding and cooperation [26]. Fig. 5 depicts the collaborative attack launched by malicious nodes "M1" and "M2". The malicious nodes "M1" and "M2" intercept the RREQ message and reply back to the source node after a mutual consensus between "M1" and "M2". Collaborative black hole attacks are more severe than single black hole attacks and can lead to huge packet loss.

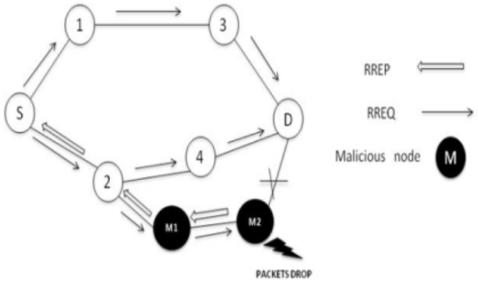

Fig. 5. Collaborative black hole attack.

B. Motivation

Collaborative attacks can lead to devastating impacts on a network causing huge packet loss in the MANETs. Securing routing against such destructive attacks in MANETs is a big challenge that has attracted many researchers. In [2], author proposed an approach which allows the source node to checks the Next-Hop-Node (NHN) and Previous-Hop-Node (PHN) of the Route Reply (RREP) of the intermediate nodes to ensure the authenticity of the route. In this research work, an enhanced attack detection and elimination technique are proposed that make used filtered based algorithm. The idea is to cope with collaborative black hole attack in a way that can lead to minimising overhead and average end-to-end delay.

C. Research Questions

This research work is going to answer the following research questions:

- *Does the proposed filtered based approach is more accurate and less resource intensive as compared to the technique discussed in [2]*?
- *Does signature based malicious node detection technique is more efficient than the currently available approaches*?

D. Research Objectives

The significant contributions of this research work are as follows:

- *To analyse the effects of the single black hole and cooperative black hole attacks on AODV based MANETs.*
- *To mitigate the cooperative black hole attack on AODV routing protocol efficiently, while keeping packet overhead and network overhead as low as possible.*
- *To reduce the number of false positive nodes from being considered as malicious.*
- *Comparison of the proposed approach with the state of the art techniques.*

E. Research Significance

Recently, wireless networks gained much attention from the researchers due to its diverse application in different fields. One of the most famous wireless networks is MANETs that has self-organised structure. Assuring data Integrity, confidentiality, and availability of wireless networks require all security concerns to be addressed. MANETs security is considered as essential concerns to assure normal functionality of the network. The lack of a centralised monitoring system and easy to access open wireless medium make MANETs more vulnerable to several attacks. Black hole attack is considered as one of the most disastrous attacks on the MANETs routing protocols. Malicious node deceives the source nodes convincing it to consider their route for sending a packet to the destination. Once the source node chooses the path containing the malicious nodes, the malicious nodes drop all the data packets received in the network [48].

The multiple attackers synchronise their efforts to harm the network cause intense damage to the network. Collaborative black hole attacks are very complex, powerful and sophisticated. Thus, dealing with these types of attacks is more challenging and exciting. Keeping in view the importance of security provisioning in MANETs, this research work introduces an enhanced approach to detect and mitigate collaborative black hole attack in an efficient way.

II. Literature Review

Wireless networks growth is observed in the last few years due to its applications in many fields. MANETs are one of the most famous wireless networks that attracted research community due to their versatile nature. MANETs have a high dynamic topology and self-organised. Their decentralised nature has lead to the number of security concerns in their deployment. One of the most severe threat is the black hole attack. Some solutions are proposed by the researchers, which cope with the black hole attacks in the context of MANETs routing protocols (i.e. proactive, reactive and hybrid routing protocol). Few of the proposed approaches are discussed below.

Author in [29] introduced an approach that instructs all of the intermediate nodes to provide the information about next hope of its path that leads to the destination. Intermediate nodes incorporate the required information in its route reply (RREP) packet at the time of sending replies to the route request (RREQ) packet of the sender. The source nodes do not send packets immediately on the route specified by the intermediate. The source will try to send a special message FRq to the next hop node to ensure whether this node has a valid route to the destination [29]. The next hope node will reply with a special message FRp that contain the resultant information. At the sender side, if the next hope response regarding valid host is acknowledged with a positive reply, then route is constructed and chosen as the best path for transmission of data. However, if the response in FRp message contains negative acknowledgment then sender broadcast an alarm packet all other nodes to cope with this situation at their end. The proposed mechanism has good results regarding malicious node detection. However, extra overhead cost associated with the additional message sent to the next hop nodes for ensuring valid route. Secondly, the proposed solution is only feasible for single black hole detection and has no way to mitigate the cooperative black hole attacks [49].

Author in [30] has introduced a new approach to mitigating the issues related to cooperative black hole attacks in MANETs. The proposed mechanism makes use of an additional Data Routing Information (DRI) table that is used to detect the malicious nodes placed in the MANETs [30]. The idea is to get information about the next hop of all the neighbour nodes who claim to have a valid route to the destination. The neighbour nodes provide the required information in the RREP packet to the source that is placed in the source DRI table. Also, the source node requests the next hop node whether it has a valid route to the destination. Moreover, the next hop node is also required to provide information about its next hop node to the source node. The resulted information is helpful regarding cross-checking the validity of the node. However, this will lead to increase the average end-to-end delay. Author in [2] proposed an approach that allows the source node to checks the Next Hop Nodes (NHN) and Previous Hop Nodes (PHN) of the Route Reply (RREP).

The packet is forwarded from the intermediate nodes to ensure the authenticity of the route [2]. The information regarding PHN and NHN is stored in a particular table called DRI. The proposed approach works in three different phases. In the first phase, the new path is to find out. Next step is to check the trustworthiness of the selected path, and lastly, the malicious nodes are eliminated. The path that has the highest sequence number is selected as the best path for sending packets towards the destination. The algorithm detects all the attacking nodes that generate the false packets. One of the problems with the proposed technique is the overhead involved in processing the information regarding checking and storing NHN and PHN information in the DRI table.

Author in [31] proposed a table based approach to mitigate the cooperative black hole attack in the context of MANETs. The idea is to use data control packet to ensure the authenticity of all the nodes in the selected path. The concept of extended DRI table is used to detect and eliminate the malicious black hole nodes. The simulation result reveals improved overhead with no false positive records during the malicious nodes detection and elimination.

Enhanced Secure Trusted AODV (ESTA) protocol is proposed to mitigate the security issues related to the black hole attacks in MANETs [32]. The proposed approach makes use of an asymmetric key to assure security across the network. Also, a trust-based mechanism is used to select multiple paths for the delivery of packets across the network. The route selection involves two different tables namely "LINK-Table" to store information about the RREQ received from several neighbour nodes, and "Link-info" is a special control packet used by an intermediate node that is part of the selected path. The main drawback of the proposed approach is the overhead involved in storing information in two different tables [50].

Author in [33] introduced an approach to mitigate the black hole attacks in context of MANETs protocol. The proposed solution maintains a special table namely Collect Route Reply Table (CRRT) to prevent black hole attacks from occurring the MANETs. The main idea is to keep information about the sequence number and arrival time of the RREP packet from its neighbour nodes. The obtained information is used to calculate the timeout value about the RREP by first RREP arrival. Moreover, the source node looks for the repeated next hop nodes to ensure whether the route is safe or not. Repeated entry found the route and will be considered as safe. However, if no repeated next hop node found in the CRRT, any random path is chosen for the data delivery to the destination. One of the problems with this technique is that if no repeated next hop nodes are found in the CRRT. Then there is a fair chance of black hole attack at a time when the algorithm chooses a random path.

The concept of Fidelity Table is proposed to extend the approach to cope with the black hole (cooperative) attacks [34]. The table keeps information about all of the nodes of MANETs, by assigning every node a fidelity level. The fidelity level is used to find out the reliability of the intended nodes. The value of fidelity is calculated based on each nodes participation in routing convergence. The nodes fidelity status is checked after a certain interval of time and thus considered as malicious if its value dropped down to zero.

Author in [35] introduced Baited-Black hole DSR (BDSR) secure routing protocol that has the potential to mitigate the collaborative (black hole) attacks in the context of MANETs. The basic idea of the proposed approach is to allow the sending node to select one of the neighbour nodes to detect malicious nodes. The sender node makes use of that neighbour nodes

address for replying to the RREP message. Thus, black hole nodes can be detected and prevented by applying the concept of reverse tracing.

The idea of watchdog was proposed by [36] to tackle the problems related to black hole malicious in the context of MANETs. The basic idea is to use eavesdropping during the communication of the next hop node, to find out malicious activities, performed by the black hole nodes. The packet sent by the sending node is placed in the buffer and is compared with the overhead packet by the watchdog. If both of the packets found to be matching, the node is considered as legitimate, and thus packet is removed from the buffer. However, if there is a mismatch between the two packets, then the failure tally is incremented for the adjacent node. It may be the possibility that packet remained in the buffer for a certain period, which crosses the threshold value. Thus, a node will be considered as malicious if the value of tally crosses a certain threshold and the sending node is notified about the black hole node. Pathrater helps in finding the malicious free routes. Moreover, all the nodes keep track of the trustworthiness rating of every known node [36]. The shortest path is selected by the Pathrater in case if there are some routes leading to the intended destination node. One of the issue with the proposed technique is that it may not be possible to figure out malicious node if the transmission power is limited, partial packet drops or false behaviour [50]–[55].

Author in [37] proposed a novel technique namely REAct system to detect malicious black hole nodes in MANETs. The proposed approach is consist of three phases and are mentioned below:

1) Audit,
2) Search, and
3) Identification.

In the audit, each packet is verified before forwarded to the intended destination from the audit node. An audit node is selected by the sending node that makes use of bloom filter to generate a behavioural proof. Also, the sending node also makes use of bloom filter to generate a behavioural proof which is then compared with the proof produced by the audit node. The result of this comparison is used to identify the segment that has the black hole node. However, the proposed method can detect the malicious node only after an attack has already been launched by the malicious node.

Author in [38] introduced an approach for the detection of malicious (black hole) nodes in the context of MANETs that make use of the concept related to Merkle tree. The proposed solution can detect most of the malicious nodes at the cost of excessive computation overhead involved in the routing phase. Th proposed solution can detect and remove malicious black hole attacks in the context of MANETs. The basic theme of the research work is to make use of equal and small sized blocks of data and to observe the data packets during the transmission to detect cooperative malicious nodes. If the packets do not arrive at the intended destination, passing through a certain intermediate nodes, those nodes will be considered as malicious nodes. A major issue with the proposed solution is that it can lead to the increase in false positive records, which can consider some of the legitimate nodes as a malicious.

Author in [39] introduced an approach to mitigate the black hole attacks in MANETs routing protocols by making use of a certificate-based authentication method. Each node needs to have a certificate for authentication before they can start transmission over the network. The proposed solution performs the authentication of nodes in two distinct phases. First phase is related to the issuance of certificate whereas the second phase starts with the authentication of nodes over the MANETs. At the moment when the route is established between the source and destination, the nodes that are involved in the routing path enter into certification phase. The sending nodes send an authentication message to the destination node upon the reply of authentication and then the source node transmits the data to the destination. However, if the node is found to have incorrect information then this will lead to the revoking of the certificate, thereby considering the node as malicious.

Author in [40] came up with a novel approach namely Secure AODV (SAODV) to mitigate the problem of black hole attack in the context of MANETs. The proposed approach has led to cope with the security concerns inherent in the AODV and do avoid the black hole attacks. SAODV uses extra packets (i.e., for exchanging random numbers) to ensure the legitimacy of the destination node. Verification phase starts at a time when the RREP message is received by the sending node. The sender node then transmits verification (secure RREQ Packet) packets to the destination node that contains a random number generated at the sender side. The destination node then replies with a secure RREP packet that contains the random number generated. To obtain the best route, the source node waits until it gets two or more RREP (i.e., secure packets) along two different paths that have the same random number. Proposed algorithm will be unable to identify the black hole nodes in case of receiving only a single secure RREP packet. The overhead of maintaining information about the nodes and extra packets can lead to the processing overhead involved in the routing process. Moreover, the end-to-end delay is also increased because source node has to wait for the RREP packets from the receiver nodes that will be arriving through different paths towards the source.

Author in [41] extended the approach proposed in that make use of password-based approach during the routing process. All the nodes need to have a password at time of route selection process. Author in [42] introduced an approach namely DPRAODV, for the detection and isolation of black hole attacks in the context of MANETs. The basic theme behind the working of the proposed technique is that upon reception of RREP packet from the destination node, the sender node looks for the sequence number in its routing table and also try to find whether the sequence number is higher than a specified threshold value and is updated instantly. A node is considered as malicious RREP sequence has a higher value than the maximum threshold. The detected malicious node is blacklisted, and all of the nodes are sent an ALARM packet. The ALARM packet contains the black hole malicious node's address to alert the neighbour nodes. In this way, the nodes discard the RREP packet initiated from the black hole. However, one of the drawbacks of the proposed approach is the excessive overhead involved in maintaining the threshold value after a constant period.

Author in [43] proposed a novel security-based approach

for the detection of malicious black hole attacks in MANETs. The proposed approach is comprised of two parts that are detection and reaction. All the intermediate nodes maintain a special table called Black Identification Table (BIT) that contains the information about sending and receiving packets originating from the source node. A node is identified as malicious if there is a difference between the number of send and received packets. After malicious node identification, the next task is to isolate the black hole node and information is updated in a special table called Isolation Table (IT). Moreover, the ID of the black hole node is broadcasted across the whole network to prevent the malicious node from further participation in the routing operation. Higher packet delivery ratio is achieved, at the cost of small additional delay in the overall communication in the network.

The cluster-based technique is proposed in to cope with the issues related to black hole attacks in MANETs. The technique is also known as Black hole Attack Prevention System in Clustered MANETs (BHAPSC) that try to find out malicious nodes existence and its location at a specific time. The idea behind the proposed solution is to maintain a special table called Friendship (Table) that maintain the information about the cluster head and its neighbours within a certain cluster [44]. Based on the information of Friendship table, the conclusion are drawn about the node trustworthiness. The next hop node is said to be stranger if the table does not contain the record of the next hop. A special parameter called trust estimator is used to calculate the trust level, and thus table is updated with the value calculated at the trust level of a given next hop node. In the situation, where the node trust level (value) crosses the threshold value, that node's ID will be broadcasted as black hole node, to all the nodes in the network. The approach is costly regarding overhead in maintaining the trust information about all the nodes and processing involved in broadcasting information across the whole network for trust convergence.

Most of the proposed techniques were suffered from two different limitations. Firstly, the overhead required was too costly due to which the achieved throughput was very low. Second, the problem was the increase of end-to-end delay which causes performance degradation in most of the cases. Moreover, a significant problem with some of the proposed solution is the false positive records identification that leads to the performance degradation of the network. The resource constraints in MANETs require a malicious detection solution that is less costly regarding resources as well as efficient regarding the end-to-end delay. This work presents the solution that makes use of the signature-based scheme. The basic idea behind the proposed algorithm is to make use of the sequence number assigned to the nodes. In MANETs based networks, all the nodes are assigned a sequence number in a range of minimum to maximum.

Let Min-Seq-No be the minimum sequence number, Max-Seq-No be the maximum sequence number and Source-Seq-No is the sequence number of the node that can be either source or destination node. If the packet sends is an RREQ packet the Source-Seq-No represents the source sequence number. However, if the packet received is RREP, then the Source-Seq-No represents the sequence number of the destination node. Any node that sends or forwards an RREQ is accepted if the value of the sequence number of that node is in between the minimum and maximum sequence number allowed in the MANETs (minimum and maximum are controlled in the proposed algorithm). However, if the sequence number is greater or less than the specified sequence numbers then the RREQ is rejected, and the node is considered as a malicious node. Similarly, the node that responds with an RREP packet is considered as a malicious node if its sequence number does not lie between the minimum and maximum sequence numbers specified. The collaborative attacks are handled in a way if all the nodes whose sequence numbers are higher than the specified maximum allowed sequence numbers and smaller than that of the sequence number allowed in the MANETs routing protocol. Table I presents the details about different approaches along with their limitations.

III. Proposed Signature Based Black hole Detection Mechanism

This work extends the work carried by [2] towards the mitigation of cooperative black hole attacks in AODV based MANETs routing protocol. The proposed algorithm makes use of the sequence number to identify the black hole nodes during the communication over the network. The pseudo-code of the algorithm is given as below:

Algorithm 1 Signature Based Black Hole Detection

Input: [Route Request (RREQ), Route Reply (RREP), Min_Seq_No, Max_Seq_No, Destination (D)]
Output: [Accept RREQ/RREP, Reject RREQ/RREP]

A: Route Discovery Phase
Let route discovery phase is used by each node to search for ultimate destination D among all the neighbor nodes.
if next-hop != D && Loop free **then**
  Source S broadcast the RREQ packet to all the neighboring nodes and continues till destination is not explored.
else
  if Min_Seq_No $\leq$ Node_Seq_No $\leq$ Max_Seq_No **then**
    Accept the RREQ
    Destination D is reached
  else
    Reject the RREQ
  end if
end if

B: Route Reply Phase
In the cache of the direct/intermediate nodes retrieve the routes from route caches.
Add these routes in the route record and then generate the route reply packets in that order.
if the route/s is/are found **then**
  Maintain a list of all discovered routes as List of Routes (LR).
else
  Destination node D is not reachable due to high mobility of nodes and network partitioning;
end if

The basic idea behind the proposed algorithm is to make use of the sequence number assigned to the nodes. In MANETs based networks, all the nodes are assigned a sequence number

TABLE I. SUMMARY OF PROPOSED APPROACHES FOR BLACK HOLE ATTACKS DETECTION

Authors	Summary	Single Black hole Detection	Cooperative Black hole Detection	Limitations
(Deng, Agrawal, 2002)	Use of intermediate node information about the next hope of its path that leads to the destination	Yes	No	Unable to detect cooperative black hole attacks [28]
(Ramaswamy et al., 2003)	Use DRI table detect the malicious nodes [29].	Yes	Yes	Overhead in maintain extra table
(Tamilselvan and Sankaranarayanan, 2007)	Use CRRT table to prevent black hole attacks from occurring the MANETs.	Yes	No	Overhead in maintain extra table
(Tamilselvan and Sankaranarayanan, 2008)	The fidelity level is used to find out the reliability of the intermediate nodes.	Yes	No	Overhead in maintain extra table
(Tsou etl al., 2011)	Baited-Blackhole DSR secure routing protocol is proposed to mitigate the collaborative (black hole) attacks.	Yes	Yes	False negative records lead to detection of legitimate nodes as a black hole node
(Marti et al., 2000)	Use eavesdropping during the communication of the next hop node.	Yes	Yes	Overhead in maintain extra information and involve end-to-end delay
(Kozma and Lazos, 2009)	Comprised of three phases that are: 1) audit; 2) search 3) identification; that are used to detect black hole attacks	Yes	No	Can detect the malicious node only after an attack has already been launched by the malicious node.
(Anita and Vasudevan, 2010)	Use certificate based authentication method to mitigate black hole attacks	Yes	No	Lead to an increase in end-to-end delay.
(Nikdel, 2015)	Source node to checks the next hop nodes and previous hop nodes of the Route Reply packet forwarded from the intermediate nodes	Yes	Yes	An increase in overhead and end-to-end delay
(Ali, 2017)	Use data control packet to ensure the authenticity of the all the nodes in the selected path	Yes	Yes	Packet drop due to high end-to-end delay.

in a range of minimum to maximum. Let Min-Seq-No be the minimum sequence number, Max-Seq-No be the maximum sequence number and Source-Seq-No is the sequence number of the node that can be either source or destination node. If the packet sends are an RREQ packet the Source-Seq-No represents the source sequence number. However, if the packet received is RREP, then the Source-Seq-No represents the sequence number of the destination node. Any node that sends/forwards an RREQ is accepted if the value of the sequence number of that node is in between the minimum and maximum sequence number allowed in the MANETs (minimum and maximum are controlled in the proposed algorithm). However, if the sequence number is higher or less than the specified sequence numbers then the RREQ is rejected, and the node is considered as a malicious node. Similarly, the node that responds with an RREP packet is considered as a malicious node if its sequence number does not lie between the minimum and maximum sequence numbers specified. The collaborative attacks are handled in a way if all the nodes whose sequence numbers are higher than the specified maximum allowed sequence numbers and smaller than that of the sequence number allowed in the MANETs routing protocol.

A. Research Nature

The design of research methodology depends on the type of research, i.e., quantitative, qualitative and mixed approach. The qualitative approach is mostly used in research about social interaction, social settings, and social process [1]. On the other hand, quantitative-based research is used to find a numerical evaluation of the underlying research. The work in this study is evaluated using quantitative approach (i.e., simulation) in comparing the performance of the proposed algorithm with the work done in [2]. The simulation technique is a most common way of evaluating the performance of the developed systems. Some simulation tools (i.e., NS-2 [3], NS-3 [4], OMNeT++ [5], OPNET [6] and QualNet [7].) based on sequential/parallel Discrete Event Simulation (DES) kernel are being employed by network researchers to verify their protocol designs. However, the selection of a network simulator depends on several important factors such as ease of configuration, learning curve of the programming language involved, type of scenario one may intend to simulate, provisioning of GUI environment, and support for scalability. This study considers OPNET modeler [6] as simulation tool.

B. Simulation Tool

Selection of relevant simulation tool is an important part of the performance evaluation. The selection of a network simulator depends on several important factors such as ease of configuration, learning curve of the programming language involved, type of scenario one may intend to simulate, provisioning of GUI environment, and support for scalability. OPNET modeler is selected to quantify the performance of the proposed algorithm. OPNET require the configuration of Visual C++ environment for the successful compilation and execution of the simulation. The implementation of simulation in OPNET required C language as a development platform to build the simulation application. The platform specification for simulation experiment about the proposed algorithm is shown in Table II:

TABLE II. PLATFORM SPECIFICATION

Simulation Tool	OPNET Modeler 14.5
Operating System	Windows
Memory	8 GB
Hardware	4
Number of Cores	Laptop core I-7

The simulation is sometimes conducted, to ensure the accuracy of the presented results. The same simulation is performed for the technique proposed in [2] and compared with the simulation of the proposed technique. The simulation is executed for 1000 seconds during each simulation run. The number of nodes chosen for the simulation is 45, and the number of malicious nodes is in the range of 1-18 nodes during different simulation execution. Random Way Point

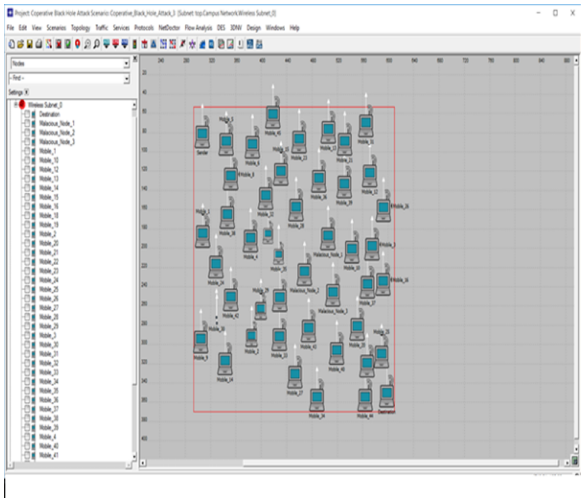

Fig. 6. Simulation environment of OPNET.

(RWP) mobility model is considered in this study [8] for nodes movement in the MANETs. All the nodes moved at the speed of 10 meters per second during the simulation execution. Fig. 6 shows the OPNET graphical view of the nodes used for the simulation experiments.

IV. Results and Discussion

Four parameters, i.e. Average Throughput, Average Packet drop, Average Delay and Malicious Detection Rate are used to quantify the performance of the proposed signature-based approach. The overhead involved in malicious node detection may lead to the decrease in throughput. The packets will drop if the malicious node is not detected in due time. Packet Drop rate is used to compare the effectiveness of the proposed approach as compared to that of the existing techniques. End to end delay is defined as the time required for a packet to reach the intended destination. Malicious Detection Rate represents the success rate of detecting black hole attacking nodes, during the routing process in AODV. The proposed algorithm is implemented using OPNET and compared with the technique proposed in the base paper. The same simulation is run with four different combinations where a various number of malicious nodes (i.e., 1, 3, 6, 9, 12 and 18) are used. The results obtained from the simulation are discussed as below.

A. Average Throughput

Fig. 7 shows the average throughput of the signature-based scheme with a different number of nodes. Signature-based scheme achieves the high throughput of 40.4 Packets/Second. For single black hole attack, the average throughput is 39.2 Packets/Second. The minimum throughput value is observed when the cooperative black hole attack has three number of nodes. Results show an improved throughput by employing signature-based scheme as compared to the scenarios of cooperative black hole attack.

Average throughput is defined as average data packets received per unit time at the destination from a sender [45]. Fig. 7 presents the results regarding the achieved throughput for signature-based black hole detection technique and cooperative black hole attack with a various number of malicious

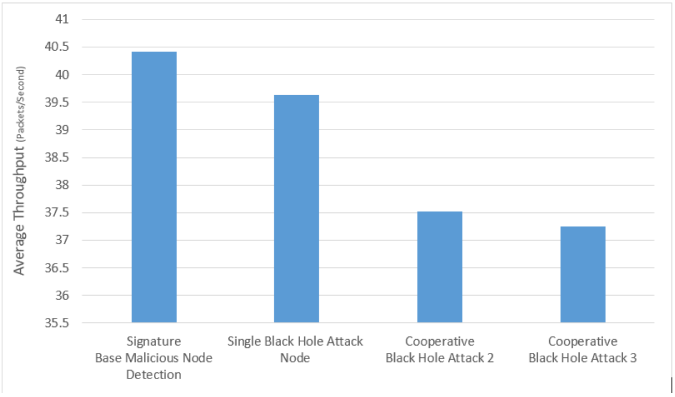

Fig. 7. Average throughput of signature-based malicious node detection.

nodes. A slight improvement (i.e., 2-5 %) in throughout is observed, when the number of black hole nodes was 1 and 3, during the first two simulations run. The proposed algorithm achieves better throughput (7-16%) with the increase in a number of malicious nodes as compared to that of state of the art technique. The presented results lead to the conclusion that with the increase in a number of a black hole, the proposed algorithm still able to achieve higher average throughput as compared to that of the technique used in [2] for cooperative black hole node detection. Moreover, both techniques reveal almost similar results with single black hole attack or when the number of black hole nodes is less than or equal to 3.

B. Average Packet Drop

Fig. 8 shows the results regarding some packets dropped when employing signature-based scheme with an increasing number of malicious nodes (i.e., 1, 2, and 3). Packets drop is reduced to zero with the implementation of the signature-based scheme for AODV based MANETs. The highest number of packets drops is observed when the number of cooperative-based malicious nodes are increased up to 3.

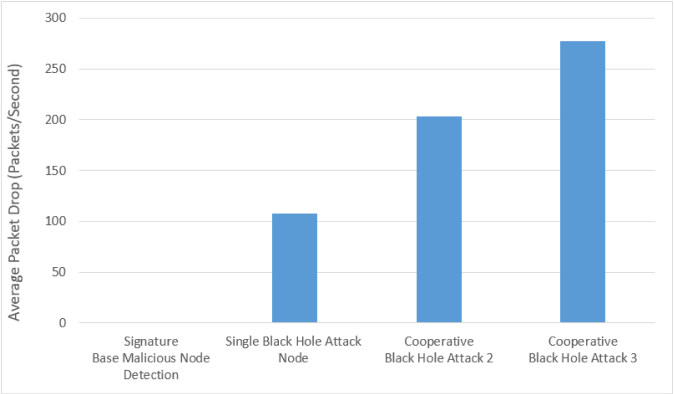

Fig. 8. Average packet drop (packets/second) of signature-based malicious node detections.

The results lead to the conclusion that signature base malicious node detection technique is efficient by having minimum average packet drop.

C. Average Delay

The average delay is defined as the average delay experienced by a packet to reach the intended destination [46]. The average delay is obtained by dividing the total delay by the total number of packets sent during the whole communication. The results presented in Fig. 9 corresponds to the average E2E delay, experienced by the network, for the signature-based algorithm. Results reveal better performance (regarding average end-to-end delay) for the proposed algorithm.

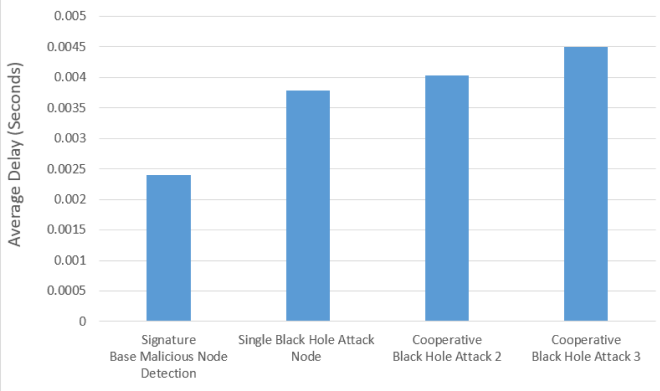

Fig. 9. Average delay of signature-based malicious node detection technique.

D. Average Processing Time

Fig. 10 shows the results of processing time taken on each of the techniques (i.e., proposed signature-based algorithm, and existing technique) for trusted route selection with varying number of malicious (cooperative black hole) nodes. The horizontal axis represent the number of black hole nodes, whereas the vertical axis represent the processing time (seconds) required to select the best suited route from source to the destination. The processing time for 1 and 3 number of black hole nodes on the proposed technique is almost equal to that of the base paper. Results shows an improvement of 10-22 % in processing time, for the route selection on our proposed algorithm as compared to that of the technique proposed in base paper. From the given results it can be concluded that the proposed algorithm can provide better connection rate as compared to that of the existing techniques. The proposed technique provides more scalable solution with a reasonable amount of processing time required for stable and trusted route selection from the sender to the destination nodes.

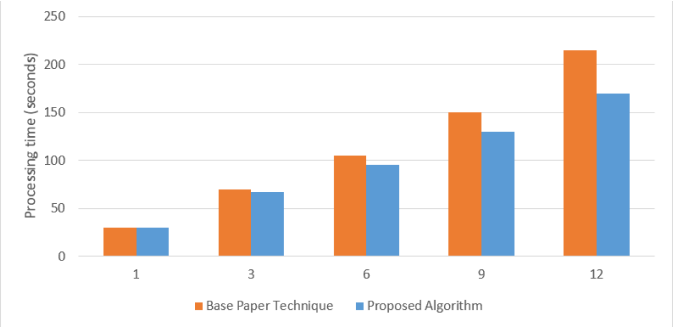

Fig. 10. Average processing time of signature-based malicious node detection technique.

E. Malicious Detection Rate

Fig. 11 presents the results of the black hole nodes detection rate on both the techniques (i.e., base paper and proposed technique). The simulation is configured for 45 mobiles nodes and varying number (i.e. 6, 9, 12, 15 and 18) of black hole nodes. An equal detection rate is observed in both the techniques, i.e., proposed signature-based algorithm and base paper [2]. The results show an improvement of 11-17 %, as the number of black hole nodes is increased up to 6,9,12,15 and 18. The simulation results conclude that the proposed algorithm achieves better performance regarding malicious detection.

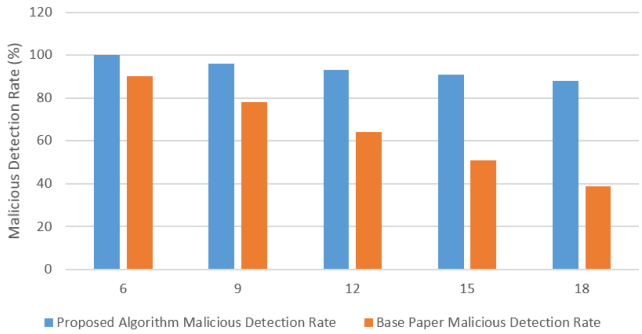

Fig. 11. Malicious detection rate of signature-based malicious node detection.

V. Conclusion and Future Work

This research work presents an essential step towards an efficient detection of cooperative black hole attacks. The concept of signature-based detection in combination with the use of sequence number, lead to the implementation of an efficient approach for the detection of malicious attacks in AODV-based MANETs. The results obtained through simulation shows significant improvements regarding collaborative black hole detection. Results lead to the conclusion that with the increase in a number of malicious node in cooperative black hole attack, the proposed algorithm still able to achieve good throughput as compared to state of art techniques. Moreover, the proposed algorithm is efficient regarding detecting collaborative black hole attacks and can lead to efficient results regarding increased malicious attacks. Even though some techniques have been introduced to mitigate the black hole attacks in MANETs, many of the proposed solutions were capable of detecting single black hole attack and are unable to detect and avoid collaborative-based black hole attacks in the context of AODV based MANETs. The benefits of the proposed algorithm are mentioned below:

1) Better malicious detection rate for higher number of black hole nodes in the context of the cooperative black hole attacks.
2) Achieved less processing time regarding trusted path selection.
3) Good throughput and average delay.

In future, this research work will be extended by analysis of the proposed algorithm for Proactive routing (DSDV and DSR) protocols in MANETs. It is also recommended to increase the number of malicious nodes up to 100-150 and to the check the behavior of these routing protocols with the proposed technique.

REFERENCES

[1] A.K. Jain, V. Tokekar, & S. Shrivastava. Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks. In Information and Communication Technology, Springer, Singapore, pp. 39-47, 2018.

[2] A. Dorri & H. Nikdel. A new approach for detecting and eliminating cooperative black hole nodes in MANET. In IEEE 7th Conference on Information and Knowledge Technology (IKT),Urmia, Iran, pp. 1-6, 2015.

[3] C. Perkins, E. Belding-Royer, & S. Das. Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561), 2003.

[4] Johnson, B. David, A. David, Maltz, and J,Broch. DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." Ad hoc networking Vol.5, pp. 139-172, 2001.

[5] G. He. Destination-sequenced distance vector (DSDV) protocol. Networking Laboratory, Helsinki University of Technology, pp. 1-9, 2002.

[6] N. Gupta, & S.N. Singh. Wormhole attacks in MANET. In Cloud System and Big Data Engineering (Confluence), Noida, India,pp. 236-239, 2016.

[7] M.M. Singh, & J.K. Mandal. Effect of Black Hole Attack on MANET Reliability in DSR Routing Protocol. In Advanced Computing and Communication Technologies (pp. 275-283). Springer, Singapore. 2018.

[8] A.K. Jain, V. Tokekar & S. Shrivastava. Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks. In Information and Communication Technology (pp. 39-47). Springer, Singapore, 2018.

[9] P.R. Muchintala, & L. Hash. Routing Protocols for MANETs, 2016.

[10] R.H. Khokhar, M.A Ngadi & S. Mandala. A review of current routing attacks in mobile ad hoc networks. International Journal of Computer Science and Security, Vol. 2, No. 3, pp. 18-29, 2008.

[11] Y.C. Hu, A. Perrig & D.B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2nd ACM workshop on Wireless security. pp. 30-40, 2003.

[12] Routing in MANET, https://goo.gl/LdjeVk

[13] D. Dave & P. Dave. An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET. In Advances in Computing, Communications and Informatics, pp. 1690-1696, 2014.

[14] S. Sinha & A. Paul. FuNN-an Interactive Tool to Detect Sybil Attack in MANET. International Journal of Applied Research on Information Technology and Computing, Vol. 7, No.1, pp. 15-31, 2016.

[15] A. Kalia & H. Bajaj. EDRI based approach with BERP for Detection & Elimination of Co-operative Black Hole in MANET. International Journal for Science, Management and Technology (IJSMT), Vol. 15, 2018.

[16] A.K. Jain & V. Tokekar. Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks. In Pervasive computing (ICPC), pp. 1-6, 2015.

[17] K. Wehrle, M. Gnes & J. Gross. (Eds.). Modeling and tools for network simulation. Springer Science & Business Media, 2010.

[18] M. Sharif & A. Sadeghi-Niaraki. Ubiquitous sensor network simulation and emulation environments: A survey. Journal of Network and Computer Applications, Vol. 93, pp.150-181, 2017.

[19] K. G. R. Narayan, T.S. Rao, P.P. Raju & P. Sudhakar. A Study on Certificate-Based Trust in MANETs. In Proceedings of International Conference on Computational Intelligence and Data Engineering (pp. 41-54). Springer, Singapore, 2018.

[20] Mbarushimana, C., & Shahrabi, A. Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In Advanced Information Networking and Applications Workshops, AINAW'07. Vol. 2, pp. 679-684, 2007

[21] P. Nayak, & B. Vathasavai. Impact of Random Mobility Models for Reactive Routing Protocols over MANET. International Journal of Simulation–Systems, Science & Technology, Vol. 17, No. 34, 2016.

[22] N. Marchang & R. Datta. Light-weight trust-based routing protocol for mobile ad hoc networks. IET information security, Vol. 6, No. 2, pp.77-83, 2012.

[23] S. Kalwar. Introduction to reactive protocol. IEEE Potentials, Vol. 29, No. 2, pp. 34-35, 2010.

[24] Routing in MANET, https://goo.gl/LdjeVk

[25] A. S. K. Pathan. Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2016.

[26] [26] A. Rana, V. Rana & S. Gupta. EMAODV: Technique to Prevent Collaborative Attacks in MANETs. Procedia Computer Science, Vol. 70, pp. 137-145, 2015.

[27] I. Woungang, S.K. Dhurandher, R.D. Peddi & I. Traore (2012, October). Mitigating collaborative blackhole attacks on dsr-based mobile ad hoc networks. In International Symposium on Foundations and Practice of Security. Springer, Berlin, Heidelberg, pp. 308-323, 2012.

[28] H. Deng, W. Li & D.P. Agrawal. Routing security in wireless ad hoc networks. IEEE Communications magazine, Vol. 40, No.10, pp.70-75, 2002.

[29] [29] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon & K.E. Nygard. Prevention of cooperative black hole attack in wireless ad hoc networks. In International conference on wireless networks, Vol. 2003, pp. 570-575, 2003.

[30] L. Tamilselvan & V. Sankaranarayanan. Prevention of blackhole attack in MANET. In Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on, pp. 21-21, 2007.

[31] A. Dorri. An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. Wireless Networks, Vol. 23, No.6, pp. 1767-1778, 2017.

[32] D. Singh & A. Singh. Enhanced Secure Trusted AODV (ESTA) Protocol to Mitigate Blackhole Attack in Mobile Ad Hoc Networks. future internet, Vol. 7, No.3, pp. 342-362, 2015.

[33] L. Ta Tamilselvan & V. Sankaranarayanan. Prevention of co-operative black hole attack in MANET. JNW, Vol. 3, No. 5, pp.13-20, 2008.

[34] P.C. Tsou, J.M. Chang, Y.H. Lin, H.C. Chao & J.L. Chen. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. In Advanced Communication Technology (ICACT), pp. 755-760, 2011.

[35] S. Marti, T.J. Giuli, K. Lai & M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265, 2000.

[36] W. Kozma, & L. Lazos. REAct: resource-efficient accountability for nodemisbehavior in ad hoc networks based on random audits. In Proceedings of the second ACM conference on Wireless network security, pp. 103-110, 2009.

[37] A. Baadache & A. Belmehdi. Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks. arXiv preprint arXiv:1002.1681, 2002.

[38] S. Jain, M. Jain & H. Kandwal. Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. International journal of computer Applications, Vol.1, No.7, pp.172-175, 2010.

[39] D. Sathiya & B. Gomathy. Improved security and routing path learning in MANETs using BeerQuiche game theoritical model in cloud computing. Cluster Computing, pp.1-11, 2018.

[40] S. Lu, L. Li, K.Y. Lam, & L. Jia . SAODV: a MANET routing protocol that can withstand black hole attack. In Computational Intelligence and Security, Vol. 2, pp. 421-425, 2009.

[41] S. Deswal, & S. Singh. Implementation of routing security aspects in AODV. International Journal of Computer Theory and Engineering, Vol. 2, No. 1, pp. 135, 2010.

[42] P.N. Raj & P.B. Swadas. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. arXiv preprint arXiv:0909.2371, 2009.

[43] N. Jaisankar, R. Saravanan & K.D. Swamy. A novel security approach for detecting black hole attack in MANET. In Information processing and management, Springer, Berlin, Heidelberg, pp. 217-223, 2010.

[44] D.B. Johnson & D.A. Maltz. Truly seamless wireless and mobile host networking. Protocols for adaptive wireless and mobile networking. IEEE Personal Communications, Vol. 3, No. 1, pp.34-42, 1996.

[45] P. Manickam, T.G. Baskar, M. Girija & D.D. Manimegalai. Performance comparisons of routing protocols in mobile ad hoc networks. arXiv preprint arXiv:1103.0658, 2011.

[46] S. Mylsamy & J. Premalatha. Performance amelioration of MANETs using cooperative routing with cross-layer design. International Journal of Business Intelligence and Data Mining, Vol. 13, No.3, pp. 15-25, 2018

[47] S. Khan, M. A. Qadir, . Inter-path OOS packets differentiation based congestion control for simultaneous multipath transmission. Int. Arab J. Inf. Technol. Vol. 4, No. 6, pp.907-913, 2015.

[48] S. Khan, M.A. Qadir, F.A. Khan and E. Rehman. Adaptive fast retransmission (AFR) with respect to receiver buffer (Rbuf) space in simultaneous multipath transmission (SMT) , Malaysian Journal of Computer Science, 2017.

[49] S. Khan and M.A. Qadir. Deterministic Time Markov Chain Modelling of Simultaneous Multipath Transmission Schemes. IEEE Access, Vol. 5, pp.8536-8544, 2017

[50] H. Ali, S. Khan and M. Quaid. Comparative analysis of controlled delay (CoDel) with Deficit Round Robin (DRR) to overcome bufferbloat problem in wired network. International Journal of Current Engineering and Technology, Vol. 5, No. 5, pp. 3378-3386, 2015.

[51] F. Khan, S. Abbas and S. Khan. An Efficient and Reliable Core-Assisted Multicast Routing Protocol in Mobile Ad-Hoc Network. International journal of advanced computer science and applications, Vol. 7, No. 5, pp. 231-242, 2016.

[52] S. Shakir, S. Khan, L. Hassain, Matiullah, QoS Based Evaluation of Multipath Routing Protocols in Manets, Advances in Networks. Vol. 5, No. 2, 2017, pp. 47-53. doi: 10.11648/j.net.20170502.13, 2017.

[53] S. Khan, F. Faisal, M. Nawaz, F.Javed, F.A. Khan, R.M. Noor, Matiullah, Z. ullah, M. Shoaib and F.U. Masood, Effect of Increasing Number of Nodes on Performance of SMAC, CSMA/CA and TDMA in MANETs International Journal of Advanced Computer Science and Applications (IJACSA), Vol.9 , No. 2, 2018. http://dx.doi.org/10.14569/IJACSA.2018.090241.

[54] F.K. Khalil, S. Khan, F. Faisal, M. Nawaz, F. Javed, F.A. Khan, R.M. Noor, Matiullah, Z. ullah, M. Shoaib and F.U. Masood, Quality of Service Impact on Deficit Round Robin and Stochastic Fair Queuing Mechanism in Wired-cum-Wireless Network International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 9, No. 2, 2018. http://dx.doi.org/10.14569/IJACSA.2018.090240 .

[55] A. Rashid, F. Khan, T. Gul, Fakhr-e-Alam, S. Ali, S. Khan and F.K. Khalil, Improving Energy Conservation in Wireless Sensor Network Using Energy Harvesting System International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 9, No.1, 2018. http://dx.doi.org/10.14569/IJACSA.2018.090149 .