Black Hole Attack in MANETs: Defending and Detecting Techniques

Jaspreet Kaur[*] , Rajneesh Talwar[**], Ashok Kumar Goel[***]

[*]Gujral Punjab Technical University, Jalandhar, Punjab, India
[**] Department of ECE, Principal, CGC Jhanjeri, India
[***]Department of ECE, GZS Campus College of Engineering and Technology, MRRSSTU, Bathinda, India
Jaspreetwphd@gmail.com, rtphdguidance@gmail.com, ashokgoel1@gmail.com
ORCID ID: 0000-0002-5874-4606, 0000-0002-1751-9584, 0000-0002-8314-0417

Research Paper Received: 17.09.2019 Revised: 22.11.2019 Accepted: 02.12.2019

Abstract: Security in the Mobile Adhoc Network is a very crucial issue that requires continuous attention for the betterment of communication and safe delivery of the data. Several researchers proposed different security mechanisms to prevent a network from breaches but still, there is a lack of security and is vulnerable to different attacks like blackhole attack, Gray-hole, DoS and many more. Blackhole redirects the traffic towards the intruder node which is not a real node and not even the part of the network like, blackhole in the universe. In this, the fake path is created from source node to destination node and then all the packets are attracted towards itself to drop it. This paper describes the blackhole attacks in mobile adhoc network in detail along with its variants. The other existing techniques for detection and prevention from blackhole attacks are also discussed and their performance is analyzed based on different security measures.

Keywords: Security, MANETs, Blackhole, Defending, Detection.

1. Introduction

With the development of the technologies, networks are also developed in different areas and the transmission of the information is increased day by day. Now-a-days wireless networks are highly on demand due to its performance. Moblie Adhoc Network (MANET) is also a wireless network where the connection of the nodes is through wireless media. In this network, nodes are act as a forwarder and help to transfer the data from one end to the other end. So, the chances of attacks are more in these networks to disturb the network and lowering its performance.

The topology of the adhoc networks are not static due to its dynamic nature and nodes can move anywhere from one place to another. The movement may be the cause of leaving one network and joining other network to continue transmissions and communication. In this each node can be a host or router. For routing, there are different methods of routing for instance, (a) Reactive Routing, (b) Proactive Routing, and (c) Hybrid Routing. One of the most popular method of routing in MANETs is Reactive routing and AODV protocol is the protocol that is mostly used under this routing mechanism. Due to its wide usage, the process phases of AODV are known by everyone and it is easy to find the vulnerabilities of this protocol. This is why the chances of attacks in AODV is much more than other protocols [22].

The classification of the attacks is done in two different types namely (i) Active Attacks, and (ii) Passive Attacks. In this, Passive attacks are difficult to detect as compare to active attacks because in this attacker node only analyses the pattern of the data or the data sent through the network whereas active attack disturb the network during its transmission with different methods. There are number of attacks in wireless networks [9]. Table 1 describes the information about some of these attacks.

There are many more attacks in wireless networks that will diminishes the network performance. Blackhole attacks is the most implemented attack from the above attacks [23] so, in the next section the details of blackhole attacks will be discussed along with some prevention and detection mechanism. The next sections also analyzed the year wise work done on this attack along with the challenges.

Table 1. Different Attacks

Name of Attack	Attack Type	Description
Grayhole Attack	Active	When malicious node theft the identity of the original node along with its route and drops all the data.
Sinkhole Attack	Active	In this attack, all nodes are attracted towards the malicious node and information about the false route is given to the nodes by attacker.
Eavesdropping	Passive	Obtain confidential information
Wormhole Attack	Active	In this, all the information is recorded by the malicious node and then it sends it to other end.
Byzantine Attack	Active	Intermediate nodes took part into the attacks and become Malicious.
Flooding attack	Active	In this attack, malicious nodes spread a huge number of packets and send it to all the nodes present in the network.
Black Hole Attack	Active	False Route information is floated by the malicious node in a way that it looks like the best route and then all data dropped by the malicious nodes.
Spoofing Attack	Active	In this type of attack, malicious node receives data of the nodes by admitting its characteristic into it.

2. Black Hole Attack in MANETs

In Reactive Protocols, blackhole attack is found too frequently [25]. It is defined as a special type of attack that falsely claims for the shortest path from the source node to its destination and then get packets all the packets and drop it. Some of the actions performed by blackhole attacks on the network are [21]:

- Act as a Source node by falsifying the RREQ-Packet

- Act as a Destination node by falsifying the RREP-Packet.
- Decrease the number of hop count, when forwarding Route Request packet

Blackhole attacks is broadly classified into two categories as shown in fig 1:

(a) Single Blackhole Attack: in this blackhole attack, attacker/ blackhole node individually attack between source and destination and absorb its packets [6].

(b) Cooperative Blackhole Attack: in this, attacker attacks with a group of forged nodes and absorb multiple packets transmit from one end to other-end [10].

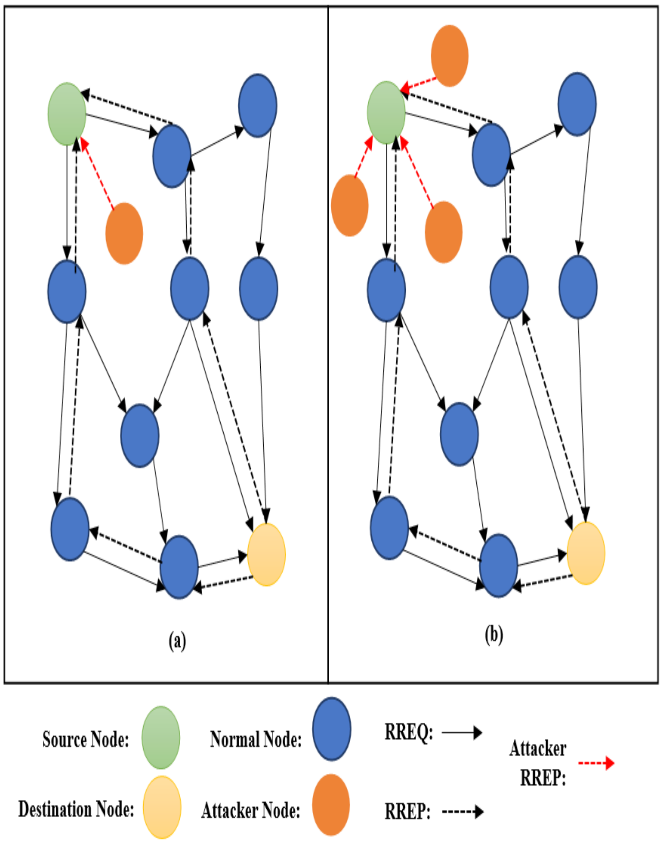

Fig 1: Blackhole Attack: (a) Single Blackhole Attack, (b) Cooperative Blackhole Attack

Fig 1 depicts the behaviour of both single and cooperative blackhole attack. In reactive protocol like AODV, RREQ packets are send by the source node to all its neighbour nodes till the packets reaches to its destination. Then after receiving RREQ packets destination originates RREP packet for the selection of the path to be followed for the transmission of the data. In the above fig 1 (a) False RREP packets is sent by the attacker node to the source with 1 hop count to show the shortest path. When source sends data packet through this shortest path, it drops all the packets whereas in cooperative blackhole, RREP is send by multiple attacker nodes to one source node and increase the confusion between the real and fake paths as shown in fig 1 (b) and then drop all the packets.

To deal with this problem of fake/imaginary path, various researches proposed different approaches as explained in the next sections. This paper divided the approaches into prevention and detection strategies. Section 3 illustrates the prevention methods and Section 4 interprets all the detection methods.

3. Existing Techniques to Prevent MANETs From Blackhole Attack

Preventive strategies are an important step for protecting the network from attacks because with this the information/data loss will be reduced. This section gives details about some of the preventive measures/ techniques used in Mobile Adhoc Network.

3.1 Light-Weight Trust-Based Routing (LWTBR) Protocol

Marchang and Datta [2] proposed a LWTBR protocol for MANETs. In this, a trust value is maintained by each neighbor and it will help to improve scalability. This model works on binary output where 1 represents full trust whereas 0 represents no trust. A new data structure has been added to the protocol for the estimation of packets that will be going to deliver. Trust of the node is evaluated using the observations of the nodes to their neighbors. In this trust model, routes which are obtained also have their own trust values so in case of any alteration in the routes can be verified. This trust model was integrated with AODV protocol and its performance was improved in adhoc network. Here if two routes have the same trust value then AODV selects the route that has the shortest path. For the analysis of this proposed protocol, authors simulated it using NS-2 Simulator and on the basis of six different performance factors where on an average 95% Packet Delivery Ratio was achieved.

3.2 Trust-Based Fuzzy Implicit Cross-Layer Protocol (TruFiX)

A new cross-layer framework was proposed T-XLM by Umar et al. [4] where a fuzzy-based trust evaluation approach was owned by the authours. Fuzzy evaluated the nodes as Trusted, Uncertain and Distrusted categories on the basis of packets forward and dropped by the nodes. In this approach, the sender broadcasts the RTS packet for channel reservation and whenever the receiver will be ready it sends CTS signal by piggybacking. In this modification of the 802.11 DCF MAC protocol was done by using two fuzzy logic systems that were created for both reservation and packet exchange phase. Simulation of this proposed protocol was done using MATLAB with 196 nodes and 20 maximum attackers. The performance of this proposed mechanism was evaluated on different performance factors and it has been noticed that on an average 83% PDR was achieved by this protocol.

3.3 ENADAIR-Based Routing Protocol

Djenouri et al. [8] proposed a technique that worked on the basis of directed and broadcast control packets and considering it as a hybrid solution. Two-hop-ACK and the watchdog methods were combined in this to deal with both type of control packets. This proposed work uses the most secured protocol named as enforce ENDAIRA that enhances the security in terms of the reduction of the drop rate.

3.4 Blackhole Attack Avoidance Protocol (BAAP)

There is a requirement of techniques that are independent of any kind of hardware or physical medium for blackhole avoidance so, a new Blackhole Attack Avoidance protocol (BAAP) was proposed by Gupta et al. [13]. In this, they used the legitimacy table-based mechanism which was obtained by each node of the network to help in avoidance from the malicious nodes from its path.

AOMDV was the base protocol for this proposed protocol. In this threshold-based checking was done and selects the path only if it doesn't cross the lower threshold level of legitimacy ratio. To analyze the performance of BAAP its implementation was done using NS2 with 60 nodes distributed in the area of 1000x1000m2 with CBR traffic. Its performance analysis was done on the basis of different performance factors.

3.5 Secure Route Discovery for the AODV Protocol

Tan and Kim [16] proposed aroute discovery approach for AODV protocol that enhances its performance by using security mechanism which works on the basis of the verification of sequence number provided by the source node and destination node during its control transfer means the transmission of the RREQ and RREP packets using thresholds. In this, the minimum value for a sequence number is 0 and the maximum is 232. The threshold value in this work depends on the environment and environment was divided into three different types named as: (a) Small Environment, (b) Medium Environment, and (c) Large Environment. For analysis of the performance, NS2 Simulator was used and a network is generated by varying number of nodes and performance is calculated on the basis of the PDR. The proposed protocol achieved better performance than AODV as analyzed in this paper.

3.6 Trust-Based Approach in AODV Protocol

Thachil and Shet [17] proposed a trust-based collaborative approach in AODV protocol to prevent a network from blackhole nodes. In this the trust value is calculated by the node for its each neighbour and if the trust value is lesser than threshold then the node is declared as a forged node and then that node was not able to take part in any communication of the network. This value of trust was computed on the basis of the packet forwarded and dropped by a node. The performance of this proposed technique was analyzed using NS2 simulator and calculating packet delivery ratio.

3.7 A Trusted On-Demand Routing Approach

A new trusted on-demand routing approach where trust computation is done at different levels was proposed by Hazra and Setua [20]. This trust-based technique works on four different modules: (a) Node Manager, (b) Trust Manager, (c) Decision Manager, and (d) On-Demand Routing Protocol and final trust were calculated using a direct and indirect trust. For simulation, the nodes were distributed in the area of 1000mx1000m using NS2 simulator and analysis was done on the basis of Packet Loss.

3.8 EMAODV Protocol

Rana et al. [24] proposed Enhanced Modified AODV using control packets and the threshold value. In this method protocol sends control packets along with sequence number on regular intervals and response can be formed only if matched with the ID. Routing tables in this were modified and two new fields were added called RL-Reliability List and TV-threshold value. RL field has a list of trustworthy nodes and TV is calculated by averaging of all Destination Sequence numbers of reliable nodes. For testing the performance, a simulation was done for 90sec using 23 nodes and 3 blackhole nodes and calculated various performance factors.

4. Existing Techniques for Blackhole Detection

With the increasing demand for network increases the risks of attacks so the requirement is to detect attackers and prevent a network from attackers. In this section of paper different protocols/methods will be discussed which were proposed by different researchers to detect the malicious/blackhole nodes.

4.1 A Cooperative Bait Detection Scheme (CBDS)

A dynamic source routing (DSR)-based routing technique was proposed by Chang et al. [1] and they named it as CBDS where the reverse tracing technique was implemented to detect all the forged nodes. This scheme was divided into two phases where three different steps involved. In the first phase, first two steps namely Initial bait step and Initial reverse tracing step was implemented and is known as proactive defense step whereas in the second phase, route discovery will be started, this step is known as reactive defense step. To implement this proposed scheme QualNet simulator was used and analysis of the performance was done based on different performance factors.

4.2 Statistical-Based Detection of Blackhole and Greyhole Attackers (SDBG)

Pham and Yeo [3] worked on Delay Tolerant Networks to take advantage of less delay in wireless networks. As its connectivity is intermittent, so it is vulnerable to both blackhole and greyhole attack and to detect these attackers, a new statistical-based Detection mechanism was proposed. This mechanism evaluates the behaviour of the nodes for forwarding based on their history means past exchanges. Here, forwarding ratio metrics were defined for the detection of any intruder activity. The other parameter was the identification of the abnormal patterns of the traffic and uneven frequency appearance that detects fake messages sent by an intruder. ONE simulator was used by the authors for experimentation and analysis of the results using parameters like Detection Accuracy, FPR, Delivery Ratio and many more.

4.3 Proactive Alleviation Procedure

An alleviation procedure that consists of timely mandate procedure, hole detection algorithm, and sensitive guard procedure was proposed by Babu et al. [5] to detect the forged nodes. In this scheme, the node status was updated timely from the monitoring units and then hole detection algorithm was used to record the status of the data transmits and acknowledgement by generating a message and broadcast it to the next hop randomly. The other protective layer is added by encrypting data using RSA algorithm in this work. This work was based on the datasets where data from I-LENSE software was collected and then attack conditions were applied on the dataset and implement proposed methodology. The performance of this proposed process was analyzed using PDR, Throughput and QoS guarantee.

4.4 Intrusion Detection Technique

Kumar and Dutta [7] proposed an IDS for the detection of blackhole nodes. In this, Sequence number of the destination, queueing delay, packet processing delay and hop count were used and verified by source node while transferring information. To analyze the performance of this proposed technique, 50 nodes were distributed over the area of 1500m x 1500m using NS2 simulator and performance was analyzed based on PDR, AED, Throughput, Detection Rate, and FPR.

4.5 Routing Information Based Detection Technique

The enhancement of the AODV protocol by adding the detection of malicious node by intermediate nodes was proposed by Jhaveri et al. [14].In this, the RREP packet was accepted by the nodes only if its sequence number is one higher than the sequence number in the RREP packet. Here the calculation of the PEAK value is done after every interval of time and this includes Sequence number of Routing Tables, RREP Sequence number, and count of the received replies. If RREP packet was sent by the intruder and identified by this proposed mechanism then it was marked by DO_NOT_CONSIDER. The performance analysis of this proposed method is done theoretically and it declares that the improvement in the PDR is more enough to achieve QoS.

4.6 Triangular Encryption Based AODV

A triangular encryption-based technique was proposed by Chatterjee and Mandal [15] identify the blackhole nodes. This proposed mechanism worked on the principle of agreement between sender and receiver before any transmission. They also shared partition and the key information for encryption and decryption. To analyze its performance implementation was done using TC1 with 5 different simulation where number of nodes are varied in every simulation and PDR is calculated.

4.7 CBHDAP Protocol

A novel technique to detect black hole attack was proposed by Kuamr and Somasundaram [28] that work on the basis of efficient crypto-key mechanism. In this Diffie-Hellman that is a group key-based technique used for key agreement purpose and is forward to only authenticated members which validate the nodes before transmission of data packets. Different parameters like. The calculation of the time taken by the different process like, Route Reply (RREP), hop count, and Packet Delivery Ratio (PDR) were used here to detect and avoid blackhole nodes. Different parameters were calculated for the analysis of the performance of this proposed technique using NS2 simulator.

5. Research Challenges in Existing Techniques

This section describes the year wise distribution of the work done on blackhole attack in different network environment. The existing techniques focussed on either prevention or detection of the attacker as shown in Figure 2 and analyzed the performance based on different performance metrics as given in Table 2. All these techniques help to detect/prevent blackhole to some extent but still a lot of challenges are there in these existing approaches. It may be overhead, threshold selection, more computation, and many more as discussed in Table 2.

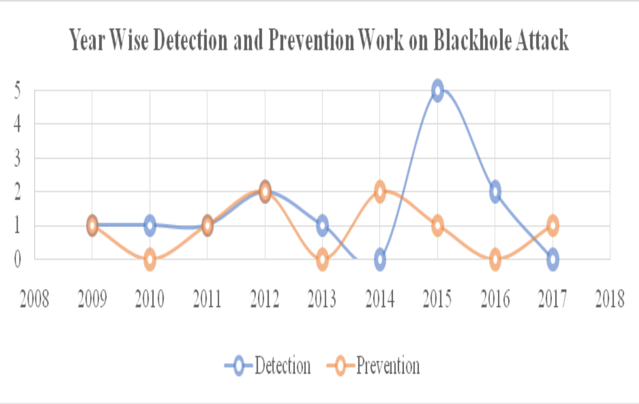

Fig 2. Work done on Detection and Prevention (Year Wise)

6. Conclusion and Future Scope

This paper concludes that a number of approaches were proposed by different authors for the detection and prevention of blackhole attacks using different protocols, approaches, simulation tools and parameters as given in Table 3 and they have used different parameters for the analysis of the performance of their proposed approach. Some of the technique had a very high performance and they were successful to detect attacker or to prevent network from attacks but still there are some problems that were not resolved by the existing approaches like, overhead, delay, selection of threshold and many more. The year wise findings help to analyze that very less work was done on the blackhole attack in past few years so, there is a need to focus on this attack and also need to propose an approach that will help to resolve the issues rose.

Table 2. Research Challenges in Existing Techniques

Sr. No	**Ref No.**	**Year**	**Detection/ Prevention**	**Performance Metrics**				**Research Challenges**
				PDR	DELAY	PLR	OVERHEAD	
1	[8]	2009	Prevention	✗	✗	✓	✗	computational capabilities are required
2	[18]	2009	Detection	✗	✓	✗	✓	packet overhead is more
3	[12]	2010	Detection	✗	✗	✓	✗	tested only on two threshold values
4	[10]	2011	Detection	✗	✗	✓	✗	work efficiently only if threshold is properly set.
5	[13]	2011	Prevention	✗	✗	✓	✗	tested only by using 2-3 blackhole nodes
6	[2]	2012	Prevention	✓	✓	✗	✓	Delay increases
7	[14]	2012	Detection	✓	✗	✗	✗	only theoretical analysis done
8	[17]	2012	Prevention	✓	✗	✗	✗	Computational Overhead
9	[19]	2012	Detection	✗	✗	✗	✓	Sometimes false responses create problem
10	[15]	2013	Detection	✓	✗	✗	✗	Unable to eliminate the blackhole nodes
11	[16]	2014	Prevention	✓	✗	✗	✗	No check for attacks during data transmission
12	[20]	2014	Prevention	✗	✗	✓	✗	computations are more
13	[1]	2015	Detection	✓	✓	✗	✓	Overhead is more
14	[3]	2015	Detection	✓	✗	✗	✓	Low Detection Accuracy
15	[5]	2015	Detection	✓	✗	✗	✗	work efficiently only if threshold is properly set.
16	[7]	2015	Detection	✓	✓	✗	✗	Queuing delay is more
17	[24]	2015	Prevention	✓	✓	✗	✓	overhead increases
18	[26]	2015	Detection	✓	✓	✗	✗	Testing with low traffic
19	[27]	2016	Detection	✓	✗	✗	✓	FPR increases
20	[28]	2016	Detection	✓	✓	✗	✓	Extra DS required
21	[4]	2017	Prevention	✓	✗	✗	✗	Delay increases

Table 3. Detection and Prevention Methods

Protocol Name	**Network Type**	**Approach used**	**Simulation Tool**	**Area of Network**	**Maximum Number of malicious Nodes**	**Number of Nodes**	**Simulation Time**	**Overall Performance Measure (Average Packet Delivery Ratio)**
LTB-AODV [2]	MANETs	Trust Based	NS-2	700m x 300 m	15	Not Defined	9600sec	95%
TruFix [4]	WSN	Fuzzy based Trust Evaluation	MATLAB	150x150 m^2	20	196	Not Defined	83%
ENDAIR [8]	MANETs	two-hop-ACK and the watchdog	NS2	Not Defined	Not Defined	Not Defined	Not Defined	Reduces Packet Drop Ratio
BAAP [13]	Wireless Network	legitimacy table	NS2	1000x1000 m^2	2-3	60	Not defined	84% and 78.7%
SRD-AODV [16]	MANETs	Sequence Number and Threshold	NS2	1000x1000 m^2	Not Defined	50,100, and 200	10 min	91-97% in small, 88-97% in medium and 86-97% in large environments
T-AODV [17]	MANETs	Trust Based	NS2	750m x 750m	25	50	500ms and 1000ms	72% and 87%
CST-AODV [20]	MANETs	Trust Based	NS2	1000x1000 m^2	10	10, 20, 30, 40, 50, 60, 70	100sec	100%
EMAODV [24]	MANETs	Control Packets and Threshold based	NS2	Not Defined	3	23	90sec	98%
CBDS [1]	MANETs	Bait detection Approach	QualNet	700m x 700m	0% and 40%	50	800sec	98%
SDBG [3]	DTN	Behavior of Nodes	ONE	4500m x 3400m	6 and 12	40	43200sec	98%
PAP [5]	WSN	Status Monitoring and Encryption Based	I-LENSE	Dataset Based	-	-	-	85%
IDSAODV [7]	MANETs	IDS on AODV-based	NS2	1500m x 1500m	5	50	500 sec	90%
AODV [14]	MANETs	False routing information based	No Simulator	Theoretical Analysis	-	-	-	Increased
AODV [15]	MANETS	Triangular Encryption	TC1	-	-	40	-	95%

CBHDAP [28]	MANETs	Crypto key based	NS2	-	-	50	100ms	90%

References

[1] Chang, J., Tsou, P., Woungang, I., Chao, H., & Lai, C. (2015). Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach. IEEE Systems Journal, 9(1), 65-75.

[2] Marchang, N., & Datta, R. (2012). Light-weight trust-based routing protocol for mobile ad hoc networks. IET Information Security, 6(2), 77.

[3] Pham, T. N., & Yeo, C. K. (2016). Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks. IEEE Transactions on Mobile Computing, 15(5), 1116-1129.

[4] Umar, I. A., Hanapi, Z. M., Sali, A., &Zulkarnain, Z. A. (2017). TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks. IEEE Access, 5, 2550-2562.

[5] Babu, M. R., Dian, S. M., Chelladurai, S., &Palaniappan, M. (2015). Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version. The Scientific World Journal, 2015, 1-11.

[6] Su, M. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications, 34(1), 107-117.

[7] Kumar, S., & Dutta, K. (2015). Intrusion detection technique for black hole attack in mobile ad hoc networks. International Journal of Information Privacy, Security and Integrity, 2(2), 81.

[8] Djenouri, D., Bouamama, M., &Mahmoudi, O. (2009). Black-hole-resistant ENADAIR-based routing protocol for Mobile Ad hoc Networks. International Journal of Security and Networks,4(4), 246.

[9] Francois, J., Aib, I., &Boutaba, R. (2012). FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks. IEEE/ACM Transactions on Networking, 20(6), 1828-1841.

[10] Weerasinghe, H., & Fu, H. (2007). Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. Future Generation Communication and Networking (FGCN 2007), 2.

[11] Ramaswamy, Sanjay & Fu, Huirong&Sreekantaradhya, Manohar & Dixon, John & Nygard, Kendall. (2003). Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks.. 570-575.

[12] Su, M., Chiang, K., & Liao, W. (2010). Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks. International Symposium on Parallel and Distributed Processing with Applications.

[13] Gupta, S., Kar, S., & Dharmaraja, S. (2011). BAAP: Blackhole attack avoidance protocol for wireless network. 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011).

[14] Jhaveri, R. H., Patel, S. J., &Jinwala, D. C. (2012). A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad Hoc Networks. 2012 Second International Conference on Advanced Computing & Communication Technologies.

[15] Chatterjee, N., & Mandal, J. K. (2013). Detection of Blackhole Behaviour Using Triangular Encryption in NS2. Procedia Technology, 10, 524-529.

[16] Tan, S., & Kim, K. (2013). Secure Route Discovery for Preventing Black Hole Attacks on AODV-Based MANETs. 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing.

[17] Thachil, F., &Shet, K. (2012). A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET. 2012 International Conference on Computing Sciences.

[18] Zhang, X., Sekiya, Y., &Wakahara, Y. (2009). Proposal of a method to detect black hole attack in MANET. 2009 International Symposium on Autonomous Decentralized Systems, 1-7.

[19] Sarkar, P., &Chaki, R. (2012). A Cryptographic Approach towards Black Hole Attack Detection. Advances in Computing and Information Technology Advances in Intelligent Systems and Computing, 273-278.

[20] Hazra, S., &Setua, S. K. (2014). Blackhole Attack Defending Trusted On-Demand Routing in Ad-Hoc Network. Advanced Computing, Networking and Informatics- Volume 2 Smart Innovation, Systems and Technologies, 59-66.

[21] Kim, Y., & Kim, D. (2013). IDS Scheme for Blackhole Attack on MANETs. Lecture Notes in Electrical Engineering Future Information Communication Technology and Applications, 863-870.

[22] Banerjee, S., Sardar, M., & Majumder, K. (2014). AODV Based Black-Hole Attack Mitigation in MANET. Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013 Advances in Intelligent Systems and Computing, 345-352.

[23] Ahmad, S. J., Reddy, V. S., Damodaram, A., & Krishna, P. R. (2015). Detection of Black Hole Attack Using Code Division Security Method. Advances in Intelligent Systems and Computing Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2, 307-314.

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

[25] Kumar, V., & Kumar, R. (2015). An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. Procedia Computer Science, 48, 472-479.

[26] Dhaka, A., Nandal, A., & Dhaka, R. S. (2015). Gray and Black Hole Attack Identification Using Control Packets in MANETs. Procedia Computer Science, 54, 83-91.

[27] Subba, B., Biswas, S., &Karmakar, S. (2016). Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation. Engineering Science and Technology, an International Journal, 19(2), 782-799.

[28] Kumar, K. V., & Somasundaram, K. (2016). An Effective CBHDAP Protocol for Black Hole Attack Detection in Manet. Indian Journal of Science and Technology, 9(36).