Detection and Isolation of Black Hole attack in Mobile Ad Hoc Networks- A Review

Gayathri Nagasubramanian[a], Rakesh kumar Sakthivel[a], Rizwan Patan[b], Anahid Ehtemami[c], Amirhessam Tahmassebi[d], and Amir H. Gandomi[e]

[a]Research Scholar, Anna University, Chennai, India
[b]Department of Computing Science Engineering, Vijayawada, India
[c]Department of Electrical and Computer Engineering, FAMU-FSU College of Engineering, Tallahassee, Florida, USA
[d]Department of Scientific Computing, Florida State University, Tallahassee, Florida, USA
[e]Faculty of Engineering & Information Systems, University of Technology Sydney, Australia

ABSTRACT

Mobile Ad hoc Network or MANET is a wireless network that allows communication between the nodes that are in range of each other and are self-configuring. The distributed administration and dynamic nature of MANET makes it vulnerable to many kind of security attacks. One such attack is Black hole attack which is a well known security threat. A node drops all packets which it should forward, by claiming that it has the shortest path to the destination. Intrusion Detection system identifies the unauthorized users in the system. An IDS collects and analyses audit data to detect unauthorized users of computer systems. This paper aims in identifying Black-Hole attack against AODV with Intrusion Detection System, to analyze the attack and find its countermeasure.

Keywords: AODV, Black hole attack, Intrusion Detection System, MANET, OLSR

1. INTRODUCTION

MANET coordinate on their own where they are not connected to any wireless routers. Here the nodes can join and leave the network dynamically. The nodes of MANET do not have a centralized administration mechanism. Each node acts as a "router" to forward the data packets to other nodes in the network. MANET have limited energy and computing resources. Bandwidth decreases with asymptotically with hop count. Various routing goals are finding end to end paths, scaling, loop free, route maintenance. Control message consists of sequence numbers to avoid routing loops. The characteristics of MANET include dynamic topology, decentralized architecture and open medium which make it susceptible to various kinds of attacks. Various kinds of attacks in MANET include Sybil attack, snooping attack, black hole attack, rushing attack. MANET involves various challenges.[1] Lack of centralized management will impede trust management for nodes. Due to mobility of nodes, topology of ad-hoc network changes all the time. So scalability is a major issue regarding security. Security mechanism ought to be capable of handling bigger network as well as smaller ones. Now let's discuss about the black hole attack that occurs in MANET[2] and the contribution of IDS on improving the efficiency of the network.

In[3] prevention of Black Hole Problem in an efficient manner in AODV Routing Protocol is proposed. The malicious node In Black-hole attack falsely advertises the path to the destination node as the shortest path with the motive of disrupting proper communication. The proposed method is to detect the black hole node by using promiscuous node and the information is propagated throughout the network. In[4] a method is proposed which is advancement in AODV to avoid black hole attack in MANET. In,[5] proposes a trust based approach which improves the performance and scalability of MANETs. The cluster in this context refers to node groups where nodes are connected tightly based on trust relationship. The cooperation between any two nodes helps to calculate trust value. Intrusion detection is the process of monitoring the system or the network for some malicious activities, which threatens security of the system and violates computer security policies. Intrusion

Corresponding Author: Amirhessam Tahmassebi, E-mail: atahmassebi@fsu.com

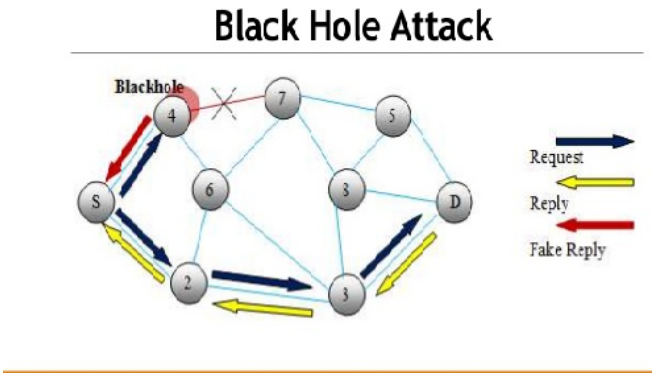

Figure 1. Black- Hole attack.

detection systems (IDS) can be classified into many ways. The major classifications are Active and passive IDS, Network Intrusion detection systems (NIDS) and host Intrusion detection systems (HIDS). An active Intrusion Detection Systems[6] is also known as (IDPS) Intrusion Detection and Prevention System. IDPS is configured to block suspected attacks without any intervention required by an operator. A passive Intrusion detection System is a technique that's configured to only monitor and analyze network traffic activity and alert an operator to potential vulnerabilities. A passive IDS is not capable of performing any protective functions on its own. NIDS examines all the traffic on the system. An effective ID should also perform protocol analysis and further detect protocols such as TCP, ICMP, UDP, FTP, SMTP, HTTP, DNS, SNMP, and Telnet. More advanced NIDS can actually display these protocol transactions in real time. HIDS monitors traffic on the specific systems only. In this case, the sensor of the Intrusion Detection System is located inside of the particular host to monitor system-level behavior. Depending on the detection techniques used, IDS can be categorized into three main categories:

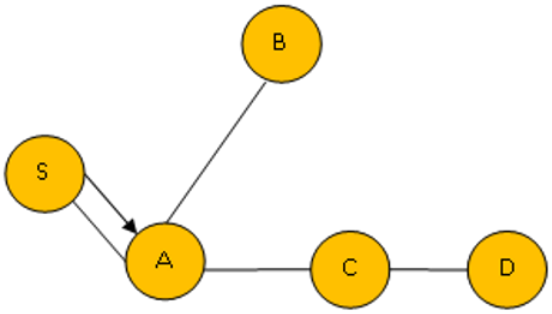

Figure 2. RREQ from S to A.

1.1 Signature-based (Misuse detection model)

It compares notable threat signatures to determined events for characterising intrusion. This is a very effective for detecting glaring notable threats but is not effective in detecting unknown threats and variations of the earlier. Signature-based detection cannot track and perceive the state of advanced communications. Hence this model cannot detect multiple events.

1.2 Anomaly-based detection

It compares normal activity against the activity which is considered malicious. This is done by characteristic monitoring for a period of time. This IDPS compares the present activity characteristics to thresholds related to the profile. Anomaly-based detection technique may generate many false positives as a slight deviation in user activity may cause an alarm but useful in detecting previously unknown threats.

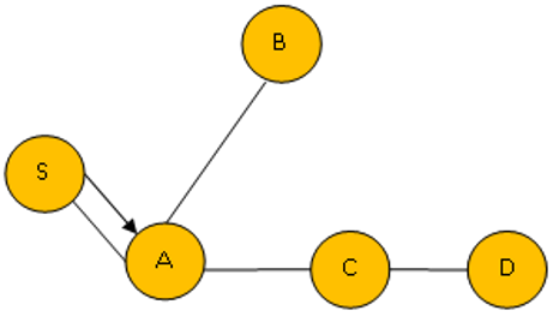

Figure 3. Broadcast of RREQ.

1.3 Specification-based detection

It defines a group of constraints that explains the proper operation of a protocol. It checks the execution of the program with respect to outlined constraints. This method has the capability of detecting previously unknown attacks with low false positive rate.

1.4 Characteristics of IDS

The characteristic of IDS includes detection method, behaviour on the detection, audit source location, detection paradigm.

- Detection Method: The characteristics of the analyzer.
- Behaviour on the detection: The response of the IDS to attacks.
- Audit source Location: Kind of input information that IDS analyses.
- Detection Paradigm: Detection mechanism.

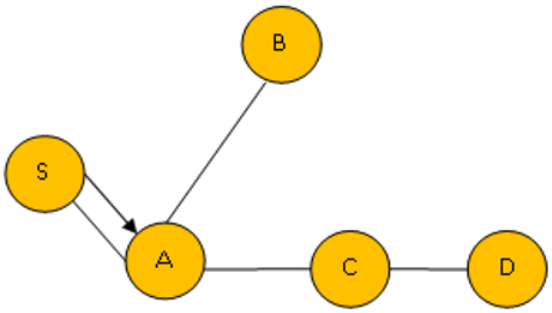

Figure 4. RREP from Node C.

1.5 Black Hole Attack

A black hole attack[7] is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. In Black hole attack, all network traffic are redirected to a specific node which does not exist in reality. Because traffic disappear into the special node as the matter disappears into Black hole in universe. Hence the specific node is named as a Black hole. Modification of the protocol leads to the control of the traffic flow through a specific node. Black hole attack may be single black hole attack or a cooperative black hole attack.[8]

A Black hole has following properties. Initially, the node has to advertise itself as having a valid route to a destination node, even though the route does not exist, with the intention of intercepting packets by exploiting the ad hoc routing protocol, such as AODV. Next, the node imbibes the intercepted packets.

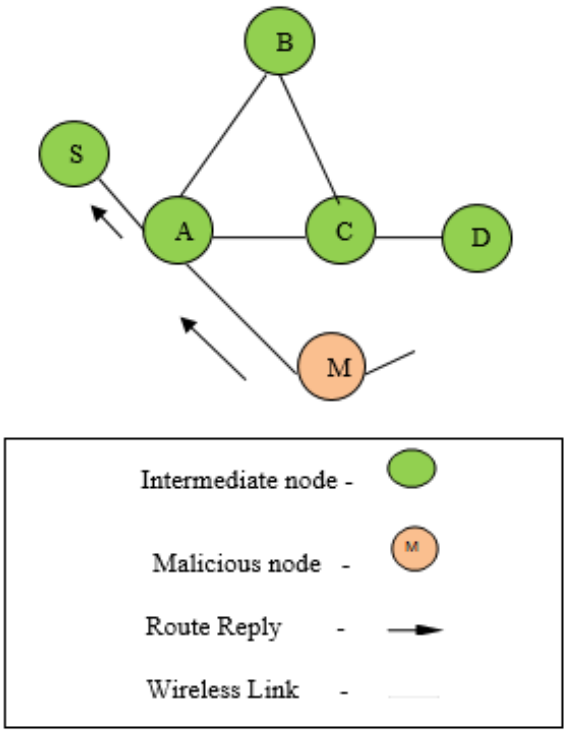

Figure 5. Malicious node's reply.

2. AODV: A BRIEF DESCRIPTION

The Ad hoc On Demand Distance Vector (AODV) is a routing protocol destined for ad hoc mobile networks. AODV has both unicast as well as multicast routing. It is an on demand algorithm, which maintains these routes as long as they are needed by the sources. AODV builds routes using a route request / route reply query cycle. AODV has three types of control messages namely:

- Route Request (RREQ) Message
- Route Reply (RREP) Message
- Route Error (RERR) Message

2.1 Route Request (RREQ) Message

When the connection between source node and destination node has to be done and if it does not have destination route entry, then a control packet; named Route Request message (RREQ); will broadcasted by the source node. The source node sends a new RREQ each time when the request ID is incremented.

RREQ format includes:

- Source Address
- Request ID
- Source Sequence No.
- Destination Address
- Destination Sequence No.
- Hop Count

2.2 Route Reply (RREP) Message

If a node has a valid route to the destination or is the destination, it unicasts a Route Reply message (RREP) back to the source. RREP format includes:

- Source Address
- Request ID
- Source Sequence No.
- Destination Sequence No.
- Hop Count

2.3 Route Error Message (RERR)

The nodes performs monitoring of their own neighborhood. A Route Error message (RERR) is developed while the route is invalid or broken, a Route Error message (RERR) is generated to notify the other nodes that use this route, that the route becomes invalid. This message is generated to avoid retransmitting by that route. Two Separate counters for Every Node:

- Sequence number.
- Broadcast-id (increments whenever the source issues a new RREQ).

The source requests using RREQ broadcasting:

- The last known number to the source is the Destination number of RREQ.

Source S sends RREQ to the neighbour node A to establish a route. Node A further broadcasts the RREQ from A to all its neighbours namely S, B, C. The destination replies using RREP (Route Reply) unicasting:

- The sequence number is first incremented when it is equal to the number within the request.
- RREP contains the current sequence number, full lifetime, hoptime = 0.

Intermediate nodes:

- Discard duplicate requests.
- Replies are done when it has an active route with S.
- If there is no such way then it broadcasts the request on all interfaces.
- The node which has route to destination replies with the RREP message. Here, in the example node C replies with the RREP message.
- Node performs recording the address of the neighbor who send RREQ.

Keep track of some information:

- Source IP address, Broadcast id, Expiration time for reverse path route entry, Source node's sequence number, Destination IP address.
- Setup forward path.
- Unicast RREP (Route reply) back to the reverse path.
- Each node on the trail sets up a forward pointer to the node from that the RREP came.
- Routing table entry is updated.
- Propagate the primary RREP or the RREP if contains a greater destination sequence number or the identical sequence number with a smaller hop count then contained in RREQ.
- Nodes that are not on the trail in which the area determined by the RREP will be timed out and can delete the reverse pointers.

Whenever a source node requires a route to a destination, it broadcasts a route request (RREQ) packet across the network where there is no route to that destination. All the nodes receiving this packet update their information for the source node and tracks back to the source node in the routing tables. In addition to the source node's IP address, broadcast ID and current sequence number the RREQ also contains the most recent sequence number for the destination, the source node is aware of. A node which receives the RREQ sends a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to the one contained in the RREQ .In that case it unicasts a RREP back to the source. Else, it rebroadcasts the RREQ. Nodes track the RREQ's source IP address and broadcast ID. If already processed RREQ is received, it is discarded and not forwarded further.

AODV deals with the route table management. The information in Route table must be kept even for short-lived routes. The routing data in AODV is collected on request, the queries present in the network helps to decide the route. The routing message has the information only about the source and the destination, not about the whole route path. Hence routing message doesn't not have increasing size. To show the freshness of the route AODV uses source sequence Number (SSN) or Destination sequence Number (DSN).

3. BLACK HOLE ATTACK IN AODV

Any intermediate node having fresh route to the destination can reply to the Route Request (RREQ) sent by the source node. Using this malicious node[9] can send the RREP packet to the source node with the claim of a promising route to the destination node. But in reality the malicious node does not have any route to the destination node but just sends false information. Source node after receiving this, send the data through this malicious node and this node drops the packets. Such nodes can crash the network. The malicious node in this network is denoted by M .The malicious node[10] falsely advertises to the source that it has route to the destination. This is done to sending RREP message to the source on seeing the RREQ request from the source. But in reality, the malicious node has no route to the destination. The source node sends data through the

advertised path of the malicious node. The packets are dropped by the malicious node without the knowledge of the source node.

Black Hole is a major security threat, for the detection of malicious node which causes black hole[11] and to terminate the malicious node a new method is propose. To block and eliminate black hole attack the proposed approach is combined with Ad hoc on demand routing protocol (AODV).[12]

4. APPROACHES TO BLACK HOLE ATTACK USING IDS

The black hole attack where a dishonest node does not forward messages to its successor. The black hole node misbehaves to preserve its resources such as its limited energy or to launch a denial of service attack aimed at the network availability. The various intrusion detection schemes[13] against black hole attack are discussed below.

A novel routing security algorithm which is called Promiscuous Listening Routing Security Algorithm (PLRSA)[14] is proposed in this paper. PLRSA does not add any overhead but only uses the characteristic of mobile ad hoc networks to examine every passing through packets. It is so-called "promiscuous listening". Another advantage of PLRSA is to easily implement the security functions in the existing ad hoc routing protocols. In addition, PLRSA can also solve the packet modifying attack. The paper[9] proposes a dynamic training method for anomaly detection, in which regular updating of training data occurs. Various modules such as feature selection and discrimination module of anomaly detection are included in the proposed technique. The average detection rate is increased and the average false positive rate is decreased.

From this result, the detection rate and false positive rate has been improved. In the proposed method, by updating the training data it can adapt to the changing environment in MANET, while using initial training data only using only the initial training data cannot adapt to the dynamically changing environment.

The Proposed authenticated end-to-end acknowledgment based approach,[5] which checks the correct forwarding of packets by intermediate nodes. This approach detects the black hole launched in simple or cooperative manner. Compared to the 2-hop ACK and the watchdog approaches, proposed approach has the best delivery ratio of packets and the highest detection ratio,[15] but it generates a communication overhead slightly more significant than that in the 2-hop ACK approach.

5. CONCLUSION

In this paper, we have analyzed various schemes for detection and removal of black hole attacks[16] in MANET. The various schemes suggest that the network parameters are affected greatly by the presence of the malicious node. So detection and removal of them would improve the network performance. This paper also discusses the diverse Intrusion Detection schemes for the detection of this black hole attack[17] and easily removing them thereby ensuring security for the network at the elementary level. The Future work will be a skilled detection and exclusion algorithm with optimization technique for minimum delay and secured data packets under Black-Hole attack.

6. CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this article.

REFERENCES

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

[2] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., and Jamalipour, A., "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless communications* **14**(5), 85–91 (2007).

[3] Singh, P. K. and Sharma, G., "An efficient prevention of black hole problem in aodv routing protocol in manet," in [*2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*], 902–906, IEEE (2012).

[4] Khare, S., Sharma, M., Dixit, N., and Agrawal, S., "Security in routing protocol to avoid threat of black hole attack in manet," *VSRD International Journal of Electrical, Electronics and Communication Engineering* **2**(6) (2012).

[5] Wang, W., Zeng, G., Yao, J., Wang, H., and Tang, D., "Towards reliable self-clustering mobile ad hoc networks," *Computers & Electrical Engineering* **38**(3), 551–562 (2012).

[6] Amiri, E., Keshavarz, H., Heidari, H., Mohamadi, E., and Moradzadeh, H., "Intrusion detection systems in manet: a review," *Procedia-Social and Behavioral Sciences* **129**(2), 453–459 (2014).

[7] Gupta, N., Das, S., and Singh, K., "A comprehensive survey and comparative analysis of black hole attack in mobile ad hoc network," *International Journal of Computer, Electrical, Automation, Control and Information Engineering* **8**(1) (2014).

[8] Agrawal, P., Ghosh, R. K., and Das, S. K., "Cooperative black and gray hole attacks in mobile ad hoc networks," in [*Proceedings of the 2nd international conference on Ubiquitous information management and communication*], 310–314 (2008).

[9] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., and Nemoto, Y., "Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method.," *IJ Network Security* **5**(3), 338–346 (2007).

[10] Raza, I. and Hussain, S. A., "Identification of malicious nodes in an aodv pure ad hoc network through guard nodes," *Computer Communications* **31**(9), 1796–1802 (2008).

[11] Gautham, P. S. and Shanmughasundaram, R., "Detection and isolation of black hole in vanet," in [*2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*], 1534–1539, IEEE (2017).

[12] Wakode, N. G., "Defending blackhole attack by using acknowledge based approach in manets," in [*2017 International Conference on IoT and Application (ICIOT)*], 1–6, IEEE (2017).

[13] Tamilselvan, L. and Sankaranarayanan, V., "Prevention of co-operative black hole attack in manet.," *JNW* **3**(5), 13–20 (2008).

[14] Li, J.-S. and Lee, C.-T., "Improve routing trust with promiscuous listening routing security algorithm in mobile ad hoc networks," *Computer communications* **29**(8), 1121–1132 (2006).

[15] Ananthi, J. V. and Vengatesan, S., "Detection of various attacks in wireless adhoc networks and its performance analysis," in [*2017 International Conference on Inventive Computing and Informatics (ICICI)*], 754–757, IEEE (2017).

[16] Elmahdi, E., Yoo, S.-M., and Sharshembiev, K., "Securing data forwarding against blackhole attacks in mobile ad hoc networks," in [*2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*], 463–467, IEEE (2018).

[17] Kaur, T. and Kumar, R., "Mitigation of blackhole attacks and wormhole attacks in wireless sensor networks using aodv protocol," in [*2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*], 288–292, IEEE (2018).

[18] Djahel, S., Nait-Abdesselam, F., and Khokhar, A., "An acknowledgment-based scheme to defend against cooperative black hole attacks in optimized link state routing protocol," in [*2008 IEEE International Conference on Communications*], 2780–2785, IEEE (2008).

[19] Raj, P. N. and Swadas, P. B., "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet," *arXiv preprint arXiv:0909.2371* (2009).

[20] Kozma, W. and Lazos, L., "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*], 103–110 (2009).

[21] Singh, J., "Fuzzy logic based intrusion detection system against blackhole attack on aodv in manet," *Computing* , 28–35 (2011).

[22] Cho, Y., Qu, G., and Wu, Y., "Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks," in [*2012 IEEE Symposium on Security and Privacy Workshops*], 134–141, IEEE (2012).

[23] Nath, I. and Chaki, D. R., "Bhapsc: A new black hole attack prevention system in clustered manet," *International Journal of Advanced Research in Computer Science and Software Engineering* **2**(8) (2012).

[24] Ullah, I. and Anwar, S., "Effects of black hole attack on manet using reactive and proactive protocols," *International Journal of Computer Science Issues (IJCSI)* **10**(3), 152 (2013).

[25] Chavda, K. S. and Nimavat, A. V., "Removal of black hole attack in aodv routing protocol of manet," in [*2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*], 1–5, IEEE (2013).

[26] Thakur, N., Bisen, D., and Gupta, N., "Proposed agent based black hole node detection algorithm for ad-hoc wireless network," *International Journal on Computational Science & Applications* **5**(2), 69–85 (2015).

[27] Kumar, S. R. and Gayathri, N., "Trust based data transmission mechanism in manet using solsr," in [*Annual Convention of the Computer Society of India*], 169–180, Springer (2016).

[28] Hu, Y.-C., Johnson, D. B., and Perrig, A., "Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad hoc networks* **1**(1), 175–192 (2003).

[29] Visconti, A. and Tahayori, H., "A biologically-inspired type-2 fuzzy set based algorithm for detecting misbehaving nodes in ad-hoc wireless networks," *International journal for infonomics* **3**, 373–82 (2010).

[30] Wahengbam, M. and Marchang, N., "Intrusion detection in manet using fuzzy logic," in [*2012 3rd National Conference on Emerging Trends and Applications in Computer Science*], 189–192, IEEE (2012).

[31] Barani, F. and Abadi, M., "Bee id: Intrusion detection in aodv-based manets using artificial bee colony and negative selection algorithms," (2012).

[32] Mitrokotsa, A. and Dimitrakakis, C., "Intrusion detection in manet using classification algorithms: The effects of cost and model selection," *Ad Hoc Networks* **11**(1), 226–237 (2013).

[33] Baadache, A. and Belmehdi, A., "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks," *Computer Networks* **73**, 173–184 (2014).

[34] Lohi, C. and Sharma, S. K., "A fortify approach to secure aodv protocol against black hole attacks," *International Journal of Computer Applications* **114**(7) (2015).

[35] Siddiqua, A., Sridevi, K., and Mohammed, A. A. K., "Preventing black hole attacks in manets using secure knowledge algorithm," in [*2015 International Conference on Signal Processing and Communication Engineering Systems*], 421–425, IEEE (2015).

[36] Mahmoud, T. M., Aly, A. A., and Makram, O., "A modified aodv routing protocol to avoid black hole attack in manets," *International Journal of Computer Applications* **109**(6), 27–33 (2015).

Table 1. Existing Schemes for Black-hole detection in MANET

Ref. No	Scheme	Routing Protocol	Year	Result
18	Acknowledgement based scheme	OLSR	2008	The number of false alarms reduces with the increasing timeout value
19	Detection Prevention and reactive AODV (DPRAODV)	AODV	2009	PDR of DPRAODV is improved by 85% than AODV under attack
20	REAct-Resource Accountability based on Random Audits	DSR	2009	Communication overhead grows upto three times larger compared to the single misbehaving node
21	MANET-Black hole detection mitigation scheme–enhanced Route Discovery for AODV (ERDA)	AODV	2012	When the number of malicious node increases,AODV with ERDA method provide significant improvement in the packet delivary
22	Watchdog Mechanism	AODV	2012	Improves the data security in mobile adhoc network
23	BHAPSc:A new Black-hole attack prevention system in clustered MANET	AODV	2012	PDR increases with decrease in the number of malignant nodes. The control overhead is also less
24	Detection of Black hole attack in MANET under AODV protocol	AODV	2013	PDR of the proposed AODV is immune to the malicious nodes whereas AODV is not. There is very less packet loss percentile in the proposed AODV
25	Detecting and overcoming Black hole attack in AODV protocol	AODV	2013	The network parameters like PDR, throughput are tested for the honest network and malicious one
26	Advanced AODV protocol for the Detection and Elimination of Black Hole Attack in MANET's	AODV	2015	PDR increased in this new adaptive AODV
27	ACKNOWLEDGEMENT Based Multipath Routing Scheme for Detecting Malicious Nodes in MANET	AODV	2015	The proposed methodology detects malicious nodes, maintains blacklist of such nodes, finds multipath to destination and decrease the route discovery time

Table 2. Various intrusion detection systems for addressing black-hole attack

Ref. No	Scheme	Routing Protocol	Year	Result
28	SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks	NS2	2003	The PDR increases in SEAD but overhead also increases which is disadvantage
14	Promiscuous Listening Routing Algorithm (PLRSA)	NS2	2006	PLRSA uses only passive observation to isolate the black holes. DSR with PLRSA provides better throughput performance than DSR
9	Anomaly detection scheme using dynamic training method	NS2	2007	The average detection rate is increased by more than 8% and the average false positive rate is decreased by more than 6%
18	Two hop acknowledgement technique	GloMoSim	2008	Proposed protocol clearly outperforms the Watch Dog, with a minor cost in energy consumption
29	Artificial Immune System based on Type2 FUZZY Sets of MANET IDS	None	2010	Partial anomaly based detection technique is deployed. Active Immune based response on attacked system is used
30	Energy based trust solution using fuzzy logic for IDS	NS2	2012	Anomaly based detection is used to detect selfish nodes
21	Fuzzy logic based IDS	NS2	2012	Misuse based detection technique is used to detect black hole attack and alarm response mechanism is used
31	BeeID: Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony Negative Selection Algorithms	NS2	2012	BeeID increases the average detection rate of DCAD and WPCA and decreases the average false-alarm rate of them
32	Sequential cross validation procedure	GlomoSi-m	2013	Effective usage of weighted cost matrices with statistical classifier was analysed
33	End-to-End acknowledgement based approach	OPNET	2014	PDR is better than two hop approach and watch dog approach
34	A Fortify Approach to Secure AODV Protocol against Black Hole Attacks	NS2	2015	The mechanism is integrated into route decision making process of the AODV protocol to defend the black hole attack. Thus PDR increases with the proposed mechanism
35	Intrusion Detection scheme based on hop count mechanism	NS2	2015	The PDR increases by the proposed method and the data drop increases if the count of malicious node increases
36	Modified AODV protocol to avoid Black hole attack	NS2	2015	When the number of nodes is increased, the packet deliver ratio and routing load of the proposed IASAODV protocol is better