International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 6 ǁ 2022 ǁ PP. 1791-1797

Detecting and mitigating the effect of black hole attacks in Mobile Ad hoc Network

Sibomana Fabrice
Research Scholar
Department of Computer Science
Karpagam Academy of Higher Education
Karpagam University
Coimbatore – 21

E.J.Thomson Fredrik
Associate Professor
Department of computer Application
Karpagam Academy of High Education
Karpagam University
Coimbatore – 21

Abstract: *providing a feasible routing in MANET is a major challenge but immensely essential to the whole operation of MANET. Mobile devices in MANET communicate to each other via wireless link, thus making vulnerable to numerous attacks. One of those attacks is black hole attack. Black hole attack is a well-known routing attack. Black hole attack takes an advantage of the fact that in MANET, Nodes collaborate and cooperation to perform basic but essential functions such as route discovery, forwarding packet in case of multi hop etc. the whole operation of MANET relies on nodes collaborating and cooperating between each other. For example, if a node needs to send a packet to the node outside of its radio range, it relies on intermediate nodes to forward the packet to intended node. Black hole attack participate in route discovery process by advertising itself as having flesh and shortest path to the destination and in return, drops all packets that pass through it. Thus making it essential to detect and remove black hole from the network. In this paper, we propose a novel method that uses neighbor forward credit based mechanism to detect and mitigate the effect of black hole attack in MANET*

Keywords: *Mobile Ad hoc Network, RREQ forward credit table, data forward credit table, AODV*

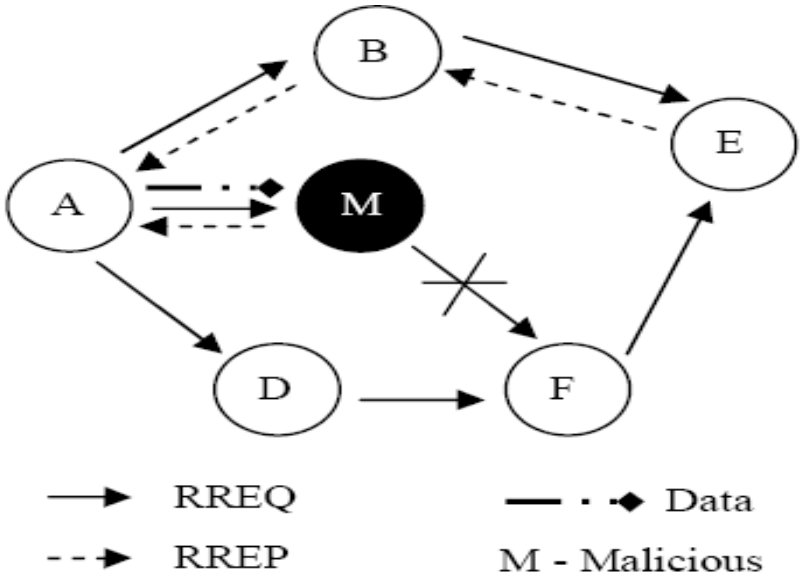
Date of Submission: 14-06-2022 Date of acceptance: 29-06-2022

I. Introduction

A mobile Ad hoc Network is a wireless infrastructure less network that consist of mobile devices linked via wireless link. MANET has unique characteristic such as mobility, self-organized, decentralized and dynamic topology. MANET is susceptible to various attacks because the lack of third party entity to control the network and it perform wireless communication between mobile nodes without any authentication system. In MANET, Nodes can leave or joint the network any time in the network without any authentication required. In addition, MANET characteristics like dynamic topology makeit difficult to apply any kind of security to MANET. One of the main challenges is securing MANET from routing attacks such as Worm hole, gray hole, black hole, selfish attack etc. AODV protocol is one of the most used to protocol to provide routing between nodes in MANET. Black hole attack has been known to attack MANET especially in case of on-demand routing protocol like AODV. [19]. Black hole attack acquires route from source node to the destination node by advertising itself as having a large sequence number and a shortest path to destination node [2,3,17,18]. A black hole node constructs a route reply with fake large sequence number and shortest path in order to forcefully acquire the route and the listen or drop to all data packets that pass through it. AODV works in the way that any intermediate node in ad hoc network could respond back to the route request if it has the route to the destination node in order to reduce the routing delay in the network.[] . However, Conventional AODV was made with the assumption that there is mutual trust between all nodes in the network. If this is not the case, it would be easy for malicious node to attack the network and compromise the whole network operation.

Black hole attack in AODV

Figure 1 shows how black hole node behaves in AODV. In this figure source node **A** wants to establish a route to destination node **E.** in AODV protocol, Node **A** broadcasts a Route Request (**RREQ**) message to search for destination node **E**. intermediate nodes D,F and B will received and rebroadcast the RREQ, whereas black hole attack M will send RREP with a large sequence number or hop count of 1 to the source node. **M** pretending that it is a neighbor of the destination node **E**. the actual RREPsfrom destination **E** containing the route B-Eand D-F-E will be discarded by source node **A.** Due to having more hop count value 2 and 3 compared to RREP sent by the black hole B whose hop count value is 1.



Therefore, according to AODV, a source node selects the largest sequence number and the shortest route to send data packet upon receiving multiple RREPs. Hence, the route would be selected by source node **A** Through black hole node. Black hole attack will drop all the data packets passing through it.

In this paper, we propose a neighbor forward credit based mechanism to detect and mitigate the effect of black hole attacks in MANET. The mechanism maintains two tables called Neighbor RREQ Credit Table (N(RREQ)CT) and Neighbor Packet Received Credit Table (NPRCT) in each and every nodes in the network to update the nodes activities. With help of records from both the tables the nodes are identified as black hole node and avoided or genuine node.

The remainder of the paper is organized a follows: in Section. 2, the related work is presented. Section 3,describes the details of our proposed scheme, while Section 4, experiments and results are presented. Finally section 5. Concludes the paper

II. Related work

Ramaswamy et al. [5] proposed a technique to detect multiple and coordinated black hole attacks working in a group by adding a Data Routing Information (DRI) table in each node. This table contains information of data sent and received by a node to and from its neighboring nodes respectively. Malicious nodes are detected on the basis of information contained in DRI table. This technique adds some delay in route discovery process due to cross checking of intermediate nodes. Kurosawa et al. [6] presented an anomaly detection technique using dynamic training method in which the training data is updated at regular time intervals. This scheme required to check whether the characteristic change of a node exceeds the threshold within a specified period of time. If yes, this node is considered as a black hole node, otherwise, latest observation data is added to the dataset for the purpose of dynamic updating. The characteristics under observation are the number of RREQs sent, the number of RREPs received, and the mean destination sequence number of observed RREQs and RREPs. This scheme requires additional processing as values are updated after specific time interval. So shorter updating time interval requires more processing overhead otherwise detection accuracy will decrease. Tamilselvan and Sankaranarayanan [7] proposed a solution called Prevention of a Co-operative Black Hole Attack (PCBHA) to prevent the cooperative black hole attack. The authors used a table called Fidelity Table, where each participating node is assigned with a fidelity level, which acts as a reliability measure of that node. In the beginning, a default fidelity level is assigned to each node. After broadcasting a route Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks 113 request, a source node waits to receive route replies from the neighboring nodes and then selects a node with a higher fidelity level to transmit data to the destination node. The destination node will return an acknowledgement (ACK) after receiving the data packets and the source node adds 1 to the fidelity level of the neighboring node upon receiving an ACK response. If no ACK is received by the source node, the value of 1 is subtracted from the fidelity level, which shows the possibility of a black hole node on this route. When the fidelity level becomes equal to 0, it is declared as black hole node. This solution adds more traffic to the network while exchanging fidelity table within the node and sending ACK message for each data packet. Another solution was presented by Weerasinghe and Fu [8] to countermeasure cooperative black hole attacks. This solution was basically an

enhanced form of a previous solution [5], which uses the Data Routing Information (DRI) table to detect wormhole attacks. The problem of delay in route discovery process still exists in the solution.

III. Proposed work

The proposed mechanism maintains two tables in each and every nodes the network:

- Neighbor RREQ Credit Table
- Neighbor Packet Received Credit Table

Neighbor RREQ Credit Table is maintained in every node to record the neighbor node activities. As the figure 1 shows, the black hole node does not rebroadcast RREQ to its neighboring instead; it instantly sends fake RREP containing the largest sequence number and the shortest route to the destination node. Therefore, black hole node RREQ count is always less compared to the neighboring nodes. Every node in the network update it Neighbor RREQ Credit Table whenever it received RREQ message from its neighboring nodes.

Table 1. Neighbor RREQ Credit Analysis Table

Status	Node ID	RREQ Count	Threshold No	Blackhole confirmed
Active	33	0	1	No
Inactive	51	12	1	No
Inactive	11	9	1	No
Active	3	7	1	No
Active	30	11	1	No

Table 2. Neighbor packet Received Credit Analysis Table

Status	Node ID	Packet Received Count	Threshold No	Blackhole confirmed
Active	33	0	1	No
Inactive	51	12	1	No
Inactive	11	32	1	No
Active	3	12	1	No
Active	30	3	1	No

Detection processes

Source node broadcasts RREQ to its neighbor nodes and waits for RREPs from neighbor nodes, up on receiving the Multiple RREPs from its neighbor node, source node first check its Neighbor RREQ credit table. If the RREQ with the shortest route destination node RREQ count greater that the threshold value, the source node uses the route to send the data to the destination. But if the RREQ count is less than the threshold value, the source node then check its Neighbor Received Credit table also if both RREQ count and Packet received count are less, then that node is considered as black hole attack and is avoided. But if RREQ count is less but Packet Received count is higher than the threshold value, that node is avoid and mark as suspicious and source node check the next RREP with the shortest path to destination with RREQ count that is high than the threshold value.

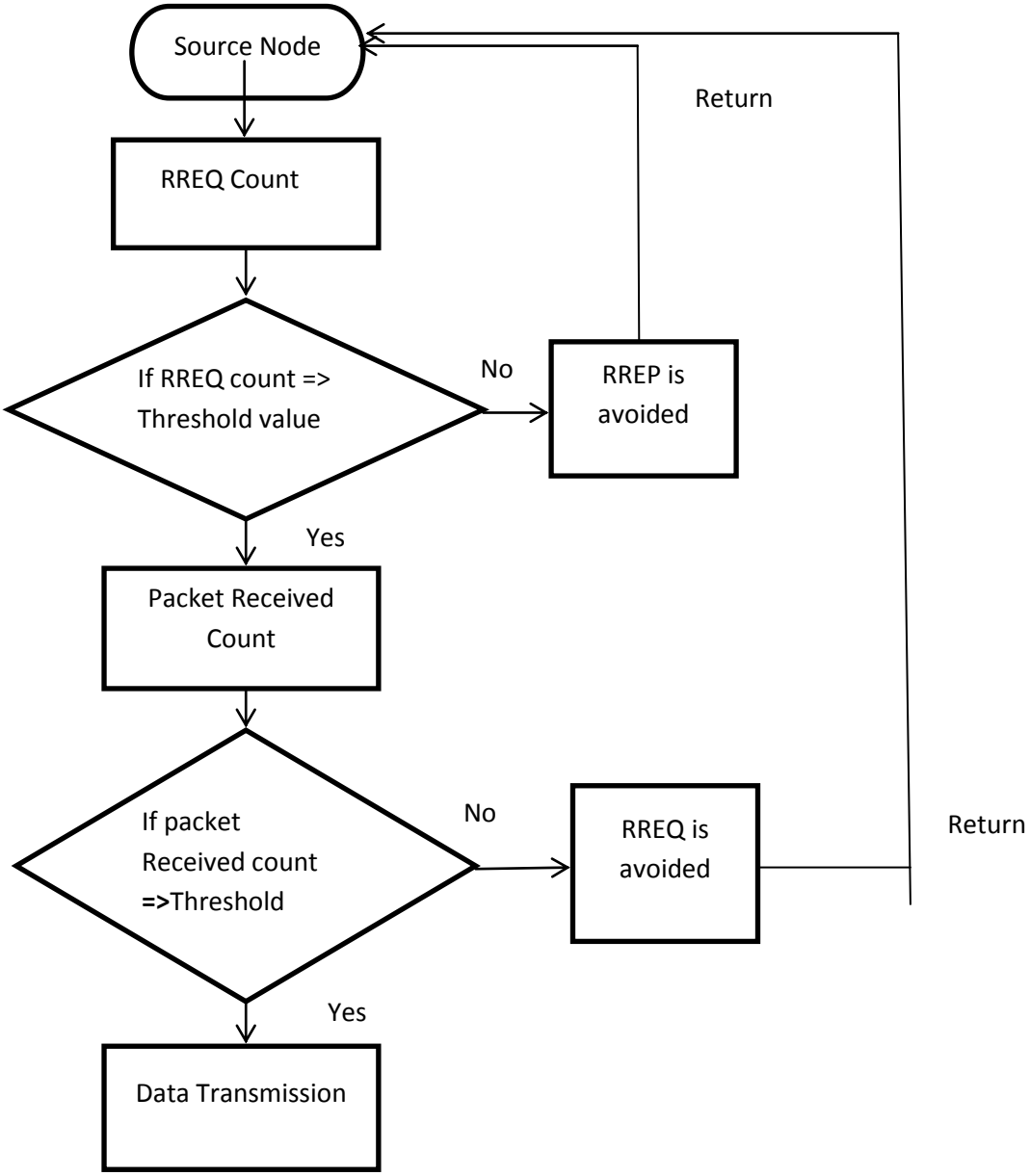


Figure 2: Proposed Mechanism Flowchart

IV. Experiment and Result

NS-2 Version 2.34 has been utilized to conduct experiment and evaluate the performance of the proposed mechanism. The parameter values used in the experiment are given in the table below

Table 3: Simulation Parameters

Parameters	Value
Simulation Area	800*800
Protocol	AODV Protocol
Normal Node	50(randomly deployed mobile node)
Black hole Node	0,1 and 2
Simulation Time	500 (s)
Transmission range	250 (m)
Mobility	0 – 20 m/s(random movement)
Max connection	20 pairs (40 nodes)
Traffic Type	UDP-CBR (constant bit rate)
Packet Size	512 bytes
Maximum speed	20 m/s

Pause time	0,5,10,15 and 20 s
AODV states	Normal AODV

For experiments, we made two cases; case-1 and case-2. In case-1, there is a single black hole node, whereas in case-2 there are two black hole nodes. Each case is tested with different pause times i.e. 0, 5, 10, 15 and 20. For each pause time, simulations have been performed multiple times and their average is used for further calculations. In each simulation, the numbers of packets sent, received, and dropped are recorded. In addition to that, the time of detection, false positive, true positive, and number of black hole nodes are also recorded

The results of experiments are analyzed on the basis of packet drop rate, transmission delay, detection time, and false positive rate.

Packet Drop Rate: Packet drop rate is the difference rate between packets sent by the source node and received by the destination node. By using proposed mechanism with AODV protocol, there is about 13 %–47 % decrease in packet drop rate as compared to AODV without proposedagainst different pause times in case of one black hole node. In case of two black hole nodes, packet drop rate reduces to 28 %–45 % against different pause times by using AODV with Proposed method. Table 2. Simulation parameters Parameter Value Simulation area 800 × 800 Protocol AODV Protocol Normal nodes **50 (randomly deployed mobile nodes) Black hole** nodes 0, 1 and 2 Simulation time 500 (s) Transmission range 250 (m) Mobility 0–20 m/s (random movement) Max connections 20 pairs (40 nodes) Traffic type UDP-CBR (constant bit rate) Packet size 512 bytes Maximum speed 20 m/s Pause time 0, 5, 10, 15 and 20 s

False Positive Rate: False positive rate is the rate of declaration of normal nodes as malicious nodes. The proposed method has very low false positive rate. During simulations, false positive rate dropped significantly because source node check the legitimacy twice.

Transmission Delay: It is the delay that is caused due to finding a valid route to the destination before sending data packets. By implementing the proposed method, there is some further delay added to route discovery process this is the only drawback of our proposed mechanism

Routing Overhead: Routing overhead is the extra amount of data, which is required to transmit other than actual data.

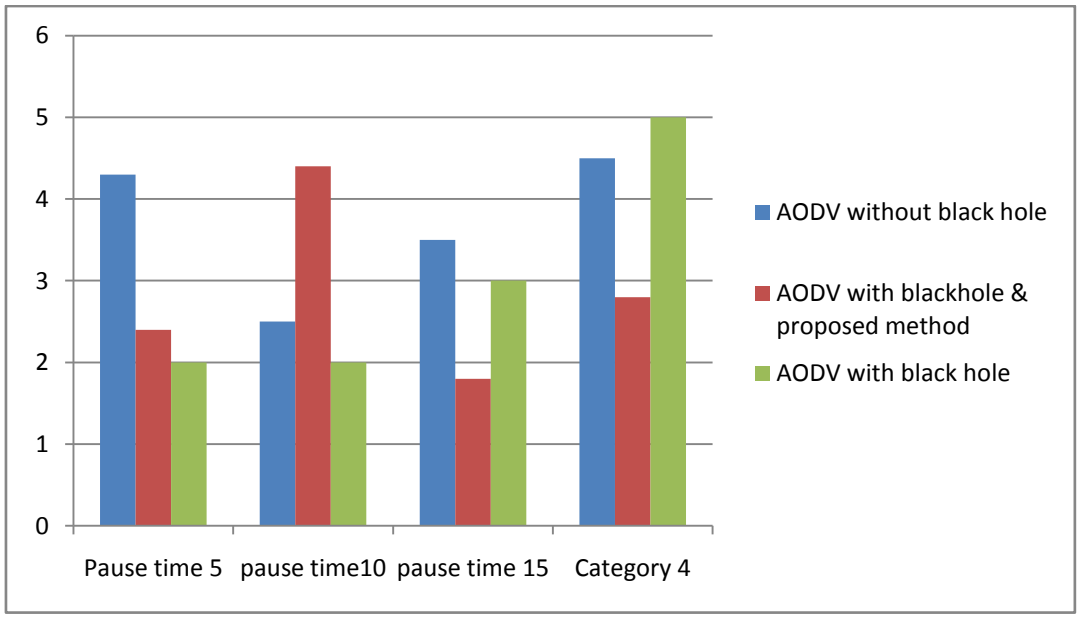


Figure 3. Packet drop rate with one black hole node

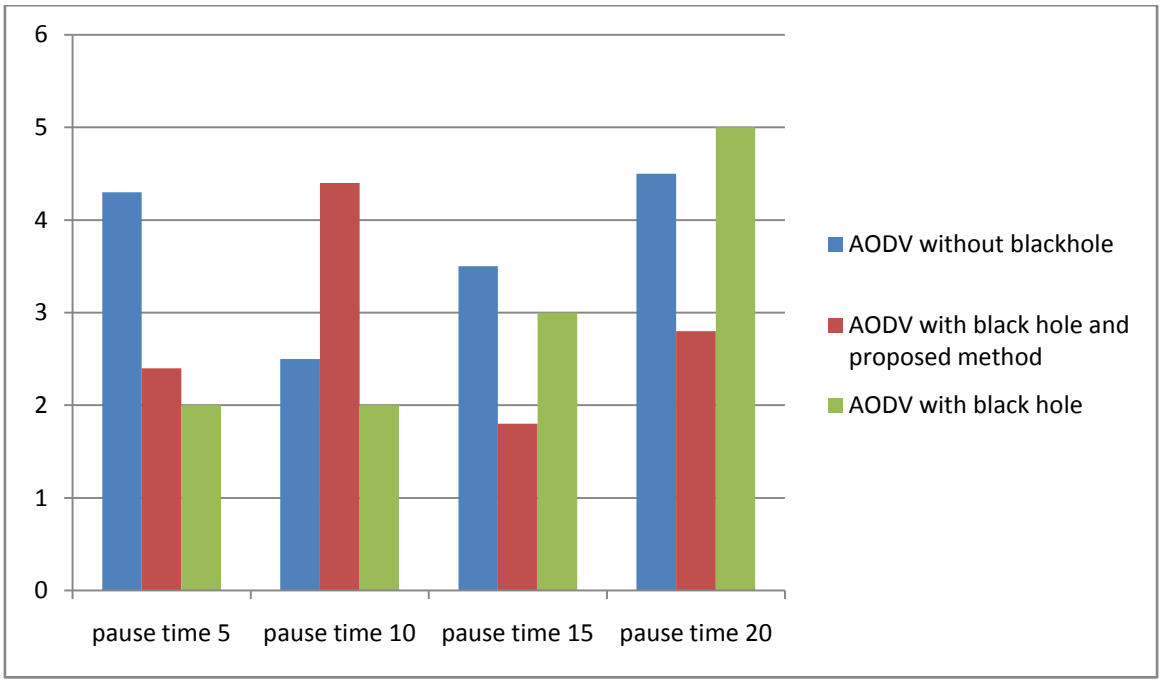


Figure 4: Packet drop rate with two black hole nodes

V. Conclusion

In this paper, we proposed a neighbor credit based on forwarding method to detect and mitigate the effect of black hole attack in MANET. the proposed method is based on the fact that black hole node does not rebroadcast the RREQ instead it sent a fake RREP containing the largest sequence number and the shortest routing route to destination. In this proposed mechanism, source node check its two table to check both RREQ count and Packet received count to see whether the node that sent their RREP are malicious node or not. The proposed method has been evaluated in network simulation and the result show improvement in packet drop rate but it present overhead problem. Overhead issue will be taken into account in the future work

References

[1]. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1999), New Orleans, LA, USA, pp. 90–100 (1999)
[2]. Mohebi, A., Scott, S.: A survey on detecting black-hole methods in mobile ad hoc networks. Int. J. Innovative Ideas. 13(2), 55–63 (2013)
[3]. Mandala, S., Abdullah, A.H., Ismail, A.S., Haron, H., Ngadi, M.A., Coulibaly, Y.: A review of blackhole attack in mobile ad hoc network. In: 3rd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), Bandung, pp. 339–344 (2013)
[4]. Tseng, F.-H., Chou, L.-D., Chao, H.-C.: A survey of black hole attacks in wireless mobile ad hoc networks. Hum.-Centric Comput. Inf. Sci. 1(4), 1–16 (2011)
[5]. Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J., Nygard, K.: Prevention of cooperative black hole attack in wireless ad hoc networks. In: International Conference on Wireless Networks (ICWN 2003), Las Vegas, Nevada, USA (2003)
[6]. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., Nemoto, Y.: Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. Int. J. Netw. Secur. 5(3), 338–346 (2007)
[7]. Tamilselvan, L., Sankaranarayanan, V.: Prevention of co-operative black hole attack in MANET. J. Netw. 3(5), 13–20 (2008)
[8]. Weerasinghe, H., Fu, H.: Preventing cooperative black hole attacks in mobile ad hoc networks: simulation implementation and evaluation. Int. J. Softw. Eng. Appl. 2(3), 39–54 (2008)
[9]. Su, M.-Y., Chiang, K.-L., Liao, W.-C.: Mitigation of black-hole nodes in mobile ad hoc networks. In: International Symposium on Parallel and Distributed Processing with Applications (ISPA), Taipei, Taiwan, pp. 162–167 (2010)
[10]. Gupta, S., Kar, S., Dharmaraja, S.: BAAP: blackhole attack avoidance protocol for wireless network. In: International Conference on Computer and Communication Technology (ICCCT), Allahabad, India, pp. 468–473 (2011)
[11]. Su, M.-Y.: Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comput. Commun. 34(1), 107–117 (2011)
[12]. Jhaveri, R.H., Patel, S.J., Jinwala, D.C.: A novel approach for GrayHole and BlackHole attacks in mobile ad-hoc networks. In: Second International Conference on Advanced Computing and Communication Technologies (ACCT), Haryana, India, pp. 556–560 (2012)
[13]. Chatterjee, N., Mandal, J.K.: Detection of blackhole behaviour using triangular encryption in NS2. In: 1st International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), Procedia Technology, vol. 10, pp. 524–529 (2013)
[14]. Tan, S., Kim, K.: Secure route discovery for preventing black hole attacks on AODV-based MANETs. In: International Conference on ICT Convergence (ICTC), Jeju, Korea, pp. 1027–1032 (2013) Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks 121

[15]. Thachil, F., Shet, K.C.: A trust-based approach for AODV protocol to mitigate blackhole attack in MANET. In: International Conference on Computing Sciences (ICCS), Phagwara, pp. 281–285 (2012)
[16]. Zhang, X.Y., Sekiya, Y., Wakahara, Y.: Proposal of a method to detect black hole attack in MANET. In: International Symposium on Autonomous Decentralized Systems, Athens, Greece, pp. 1–6 (2009)
[17]. Hu, Y.-C., Perrig, A.: A survey of secure wireless ad hoc routing. IEEE Secur. Priv. 2(3), 28–39 (2004)
[18]. Kant, R., Gupta, S., Khatter, H.: A literature survey on black hole attacks on AODV protocol in MANET. Int. J. Comput. Appl. 80(16), 22–26 (2013)
[19]. Ehsan, H., Khan, F.A.: Malicious AODV: implementation and analysis of routing attacks in MANETs. In: 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, pp. 1181–1187 (2012)