Indian Journal of Science and Technology, *Vol 7(4), 401–408, April 2014*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Black Hole Attacks Detection by Invalid IP Addresses in Mobile Ad Hoc Networks

Reza Amiri[1], Marjan Kuchaki Rafsanjani[2*] and Ehsan Khosravi[3]

[1]ACECR Kerman Branch, Kerman, Iran; amirish60@ut.ac.ir
[2]Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran; kuchaki@uk.ac.ir
[3]Department of Computer Science, Sirjan University of Technology, Kerman, Iran; ehsan_k81@yahoo.com

Abstract

A mobile ad hoc network is a set of nodes without the required intervention of any fixed infrastructure. Therefore, these networks have particular application in risk and crisis management should a natural disaster such as flood and earthquake befall and destroy communications infrastructures. In the absence of a fixed infrastructure, nodes in a network need to cooperate with each other. In circumstances as such, a malicious node can easily locate itself on the route and reduce network performance by deleting packets. In this paper, we have proposed a method which enables to detect the malicious nodes using valid and invalid addresses, without triggering false detection across the network. According to the simulation results, this method is capable of detecting malicious nodes faster compared to similar methods.

Keywords: Mobile Ad hoc Networks (MANETs), Risk and crisis management, Intrusion detection, Black hole attack

1. Introduction

Mobile nodes in mobile ad hoc networks play both router and host and are connected by wireless. Mobile ad hoc networks do not require a pre-established communication infrastructure and the nodes are free to move in or move out of the network at any time[1].

As a result of dynamic topology, independence from infrastructures, self-organization, and facility of movement, mobile ad hoc networks are considered a desirable option for risk and crisis management[2]. In critical situations, such as flood, earthquake, and war, when the communications network infrastructure is destroyed, mobile ad hoc networks can be easily organized and employed to connect the forces[3,4].

Mobile ad hoc networks benefit from characteristics different from wired or even standard wireless networks. Due to their dynamic nature, these networks are more vulnerable. Accordingly, numerous studies have been conducted on designing an intrusion detection system to detect misuse and abnormal behavior.

Design of an intrusion detection system for ad hoc networks as well as the transfer of an intrusion detection system to ad hoc environment are extremely difficult due to lack of central controller, bandwidth limitations, and dynamic typology in mobile ad hoc networks[6].

The present paper proposed a method based on misuse detection in which, employing an invalid address in its disposal, the intrusion detection system attempts to deceive and entrap the intruder.

In the following section (Section Two) intrusion detection systems and black hole attack are discussed; Section Three presents a number of methods formerly proposed for black hole attack detection; the proposed method shall be explained and compared to one of the previous methods, simulated and analyzed in Section Four; and in Section Five, conclusion will be provided.

2. Background

There are basically two defensive lines to save the network from being damaged by intruders[1]. The first defensive line is referred to as intrusion prevention systems. Intrusion prevention methods focus on protecting the network from malicious attackers by strengthening the cryptosystem or developing secure protocols. However, the sole pres-

*Author for correspondence

ence of an intrusion prevention system is not sufficient to secure the ad hoc network; since in the case of internal attacks, the malicious nodes easily pass the first defensive shield as they have their own usernames and passwords[6]. Consequently a second defensive line will be necessary for network security, referred to as intrusion detection systems, which detect the intruder and provide him with a proper response.

2.1 Intrusion Detection System

Intrusion detection systems are divided into two major classifications according to the 'detection regulation'[7]:

2.1.1 Anomaly Detection Systems

Anomaly-based detection defines a profile of normal user behavior and compares it to all the behaviors which a node monitors in the network. In case of any deviation of a behavior, the behavior will be considered as an intrusion. This technique may detect previously unknown attacks, but may exhibit high rates of false positives.

2.1.2 Misuse Detection Systems

Misuse-based detection monitors the occurrence of predefined signatures or sequences that indicate an intrusion. The monitored behaviors are compared to the signature database, and in case of correspondence are introduced as attacks. This method may not detect previously unknown attacks, however its false positive rates are much lower than that of anomaly detection systems.

2.2 Black Hole Attack

The black hole attack is one of the most common attacks against the reactive routing protocol in MANETs. The black hole attack involves in a malicious node(s) fabricating the sequence number, hence pretending to have the shortest and the most recent route to the destination[8]. In this attack, a malicious node sends a forged Route Reply (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. Through comparing the destination sequence number contained in the RREP packets, upon the receipt of multiple RREPs, the source node judges the greatest one as the most recent routing information and selects the route contained in that RREP packet. The malicious node fabricates its forged RREP packet as having the shortest route to the destination as well as the greatest sequence number. The malicious node can place itself along the route and drop data packets and thus reduce network functionality.

Black hole attacks are generally divided into two classes of single and collaborative attacks.

Single black hole attacks occur when one node introduces itself as a node with the shortest and most recent path to the destination and then tries to drop the packets.

The black hole nodes may work as a group. That means more than one black hole node work collaboratively to mislead other nodes. Most intrusion detection methods fail against collaborative black hole attacks[9].

3. Related Literature

As passed, the attacks are divided into single and collaborative. An example of the proposed methods to deal with each class will be presented below.

3.1 A Novel Security Approach for Detecting Black Hole Attack in MANET

Jaisankar et al.[8] proposed a security method for single detection in two steps of detection and reaction x. Field_next_hop is added to RREP in the first section. Before the source node forwards data packets, the leading PREP packet is assessed between the intermediate nodes and destination node. Every single node maintains a Black Identification Table (BIT) including the fields of 'source, destination, current node ID, Packet Received Count (PRC), Packet Forwarded Count (PFC), and Packet Modified Count (PMC)'. PMC is then updated by tracing of the BIT of the neighboring nodes. If the node functions properly, the corresponding number multiplies. Subsequently, in case the received packets differ from the forwarded packets, the malicious node will be detected. The second step is to isolate the black hole. Therefore the node maintains an Isolation Table (IT) and records the black node's ID. The ID is then broadcasted to every other node so that the malicious node is eliminated through checking the isolation table. Simulation results showed a 40 to 50 percent quicker packet delivery rate compared to that of AODV when attacked, as well as a 75 to 80 percent decrease in the number of dropped packets. The mentioned method, unlike the usual multi-stage method, corrects the original RREP packets for collecting the data of malicious nodes, instead of forwarding higher numbers of packets. The proposed method offers higher

packet delivery rate and lower packet drop rate compared to those of the major schemes.

3.2 Improving AODV Protocol against Black hole Attacks

This method was proposed for single intrusion detection in which a new table, Smg_RREP_Tab, a new timer, MOS_WAIT_TIME, and a new variable, Pre_ReceiveReply, shortly referred to as P packet, are added to the AODV routing protocol (Mistry, 2010). Definitions of the innovative functions are initially clarified. RREP_WAIT_T is a time period within which the source node forwards RREQ packet up to the point that receives the RREP's control message. MOS_WAIT_TIME is half the value of RREP_WAIT_TIME. RREP packets are stored in the newly developed table bearing the abbreviated names of Cmg_RREP_Tab. Mail_node is finally adopted to discard the control messages from these nodes. A brief description of the proposed method is presented below. As a first step, the Pre_ReceiveReply added function is executed. The source node analyzes every single stored RREP packet in the Cmg_RREP_Tab. Then the RREP packet with the higher sequence number than that of the source, is abandoned and the sender suspects the presence of a malicious node. As long as the attacker is identified, the control messages originated from it can be ignored. Therefore, the RREP packet with the highest sequence number in the Cmg_RREP_Tab is selected. The Mali_node is maintained continually, and ultimately the ReceiveReply is called in the original AODV. When the network size changes, PDR is improved up to 81 percent; whereas, upon variations in node movement, the improvement in this method reaches to 70 percent. Compared to that of the original AODV, this solution provides a higher packet delivery rate in the simulation results; however, end-to-end delay will inevitably rise. In a non-adjusted network size, the end-to-end delay reaches 13 percent, while in a network with adjusted movement it arrives at 6 percent. The above-gone method will also fail in dealing with collaborative black hole attacks.

3.3 Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile Ad Hoc Networks

Vishnu[10] proposed a mechanism for the detecting and removing of black and gray hole attacks. This method is capable of detecting collaborative malicious node with high packet drop rates. A more detailed account of the mentioned process follows. The first step of the solution develops one of the backbones of the network is developed from a set of strong nodes on the ad hoc network. These trusted nodes can be allocated to RIP when new nodes join the network. Every node obtains an RIP, meaning that it has acquired route verification. Prior to conveying the data packets, the source node sends a request to the nearest BBN for the allocation of an RIP. Then the RREQ is forwarded to the source node and RIP address. In case the source node receives only the RREP of the destination node, there are no black holes. Otherwise, upon receiving the RREP packet from the RIP, the source realizes that there is a possibility of the presence of an intruder in the network. The neighboring RIP nodes change in the promiscuous state as the source node alerts them via a monitored message. The neighboring nodes monitor the designated as well as malicious nodes. Moreover, the source node sends a few dummy data packets to test the malicious node. The neighboring nodes monitor the packet flow and in the case the dropping rate is higher than the normal threshold, they regard it as a black hole and inform the source node of the presence of the malicious node. This control message is then broadcasted across the network, and as a result, the malicious node is added to the black hole list. The approved malicious node is then dropped and all the nodes drop the respective responses in their black lists. This method is capable of detecting not only the black hole, but also the gray hole. Nevertheless, it is difficult to comprehend how this method enhances functionality, since no simulation or empirical results are provided. Moreover, the proposed method may face serious problems and fail if the number of attackers is higher than that of normal nodes.

3.4 Bait DSR (BDSR) based on Hybrid Routing Scheme

BDSR was proposed by Po-Chun Tsou et al.[11] to prevent collaborative black hole attacks. It is a combination of proactive and reactive methods in the form of a hybrid routing protocol, with a main nature of on-demand DSR routing protocol. Initially, in the routing stage, the source node forwards the bait RREQ packet prior to route discovery. The destination address of the bait RREQ is random and non-existent. To avoid bait RREQ traffic, BDSR adopts a method similar to that of DSR. Bait RREQ packets survive

only for a period. Malicious nodes are easily expelled from the first stage, since the bait RREQ is capable of separating the deceived RREQs from black hole nodes. The RREP generator, in the proposed method, is recorded in the additional field of the RREP. In this way the source node is enabled to detect the attacker's location from the reply location of the RREP. All the forwarded replies by the attacker need to be dropped. Subsequently, the original DSR route discovery procedure is utilized. If data delivery rate is less than that of the pre-defined threshold, the bait procedure will be once again initialized for investigating suspicious nodes. The simulation results, compared to the original DSR scheme and watch dog method, indicate that BDSR provides for a high packet delivery rate. The packet delivery rate for BDSR is 90 percent, which is by far higher than that of DSR and watch dog. Furthermore, the communication overhead is lower than that of watch dog, but slightly higher than that of DSR.

3.5 Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems (PSBA)

Intrusion detection nodes in this method are considered as fixed, and after they detect a malicious node, intrusion detection nodes broadcast an alert message throughout the network to inform the other nodes of the presence of the malicious node[12]. The ABM algorithm executed for intrusion detection nodes is comprised of two RQ and SN tables. The RQ table stores PREQ messages observed by the intrusion detection node in its transmission range. The SN table is employed for an intrusion detection node to store the degree of suspicion of nodes in its transmission range. The suspicion degree of a node is crucial for judgments made concerning the malicious node. In the case an intermediate node, is not a destination node, and does not broadcast an RREQ packet for a specified route but forwards an RREP for the route, the level of suspicion of this node is increased one unit in the SN table of the monitoring suspicion detection node. If the level of suspicion is lower than a threshold value, it will be considered as an inactive status, otherwise, the status is identified as active and the node will be blocked.

4. The Proposed Method

In most of the previously proposed schemes for black hole attack detection, it was assumed that the black hole attack occurs without any alterations, however, in reality, attackers are normally smart and specialist individuals who try to first identify the system's weak spots and use them for the attack. In the PSBA scheme for instance, the supposition is that after receiving the RREQ packet an attacker sends a RREP packet to the sender, without forwarding the packet. As a result, the only task of the intrusion detection system is to monitor whether a node sends a reply packet to the route without forwarding the RREQ packet. In such cases, with a slight change in the black hole attack, if the attacker forwards the RREQ packet and then transmits its forged RREP packet without waiting for the reply, the intrusion detection system fails to detect the attack. False detections are also higher in this intrusion detection system as shown by the following example:

As shown in (1a), node C is located outside the radio range of the intrusion detection system and maintains a route to node D. In (Figure 1b), however, node C moves to a location within the radio range of the intrusion detection system but still maintains a route to node D. Now suppose node A or B broadcasts an RREQ packet to node D. Since node C has a route to node D, it replies to the request and broadcasts an RREP packet to the source route. Here, because the intrusion detection system has failed to eavesdrop on the route request packet from node C to node D, thus it considers a false positive for node C. In order for reducing false detections, schemes as such adopt a threshold value. But the problem associated with thresholds is that if low, the probability of false detection rises, and if high, intrusion detection speed is reduced.

4.1 Introducing the Proposed Method

The present study attempts to propose a method which besides increasing the detection speed of malicious

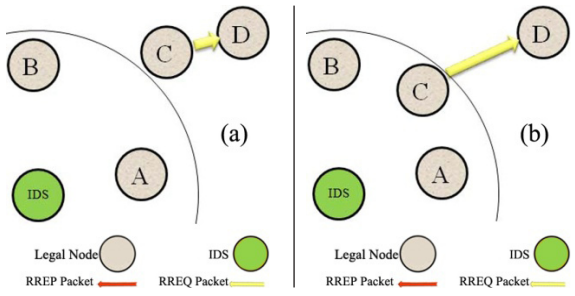

Figure 1. (a) Node C is located outside the radio range of the IDS; (b) Node C moves to a location within the radio range of the IDS.

nodes, obviates the probability of false detections by the intrusion detection system, and moreover prevent the malicious node from bypassing and defeating the intrusion detection system via administering slight changes.

In this paper, we have considered the following assumtions:

1. This method is not considered as appropriate for small networks in which all the nodes are aware of each others' addresses, and the hypothesis is that the network under discussion is a large network, the nodes of which are only aware of a small number of the addresses of the neighboring nodes.
2. As a first step in this method, every single node receives two IP addresses, one of which is used for the real IP address, and the other for intrusion detection operation.
3. The node may not optionally change its address, and to do so, it is required to obtain the permission from the network administrator and go through authentication for the new requested address.
4. The authentication is executed through secure methods in which the original data exchanged between network administrator and the mentioned node will not be accessible by the other nodes.
5. Network administrator cannot be malicious.

The procedure is as follows:

1. Login of the node to the network and being allocated a valid and an invalid address;
2. Network monitoring
3. Intrusion detection

The node, initially, presents its login request to the network administrator. The administrator executes the authentication operation to ensure the validity of the node. The node, then, receives an address by which it is identified in the network. An additional invalid address is also allocated to the node which is later on employed for intrusion detection procedure.

In the second step, every single node involves in monitoring for the detection of the black hole attack. Any of the formerly discussed black hole attack detection schemes can be utilized for this step[13]. The monitoring can be conducted irregularly or via the received packet specification protocols to reduce network administration expenses.

When a node is suspicious of the presence of an attack, the third step (intrusion detection) is initialized. The proposed steps for intrusion detection are presented below.

Initially, the node creates an RREQ packet intended for the invalid IP address allocated by the administrator on login, and broadcasts it across the network. Based on the definition of the black hole attack, upon receiving the RREQ packet, the malicious node forwards an RREP packet to the source node. When the source node receives the RREP packet, it identifies the sender node as malicious.

As shown in (Figure 2), suppose every node has been allocated with both a valid and an invalid address by the administrator when logging in. These addresses are shown in Table 1. For simplicity it is assumed that the network administrator has allocated odd addresses as valid, and even addresses as invalid addresses. Node S, for instance, is allocated with the valid address 1 and invalid address 2. In reality, however, the addresses must be selected randomly so that there is no possibility for the other nodes to figure out the address list.

In (Figure 3a), the node 'S' is suspicious of the presence of a malicious node in the network, consequently it initiates intrusion detection operation by creating and

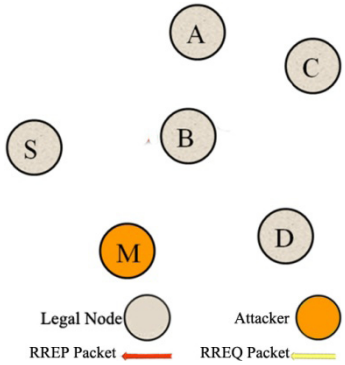

Figure 2. Sample of a mobile ad hoc network.

Table 1. The address list allocated to the nodes by the network administrator

Node	Valid Address	Invalid Address
S	1	2
A	3	4
B	5	6
C	7	8
D	9	10
M	11	12

forwarding an RREQ packet to a destination with the invalid address at its disposal (address for destination 2).

Nodes 'A' and 'B', in (Figure 3b), check the RREQ packet, and since the address is invalid, there is no route with this address and as a result they forward the packet. The malicious node 'M', on the other hand, based on the definition of black hole attacks, sends an RREP packet to the node 'S'.

The node 'S' waits for RREP packets and if any node sends an RREP packet to the invalid address, it will be considered as a malicious node. Thus, the malicious node 'M' is detected and reported to the network administrator. This report may include proofs such as the route reply packet, sent by the malicious node 'M' and other additional proofs. Upon receiving the evidences, the network administrator, executes the required investigations to prevent from a false detection. In the case the administrator accepts the proofs as well, a message is sent to the other nodes in the network and node 'M' is introduced as a malicious node.

4.2 Disadvantages of the Proposed Method

The attacker in this method is capable of ensuring the validity of an address as follows:

Upon receiving an RREQ, the attacker triggers the attack if it is certain of the validity of the destination address of the packet; otherwise, it behaves like an ordinary node and waits for the RREP. In the case the attacker eavesdrops on the RREP, it becomes certain of the validity of the address and can thenceforth conduct a black hole attack for this address as well. An example of what passed follows.

Consider the above example. As shown in (Figure 4a), suppose node 'S' sends an RREQ to node 'C' (address 7). Uncertain of the validity of address 7, the malicious node behaves like a normal node and forwards the packet. As observable in (Figure 4b), after some time, node 'C' sends an RREP packet to node 'S' via node 'B'. Neighboring node 'B', node 'M' eavesdrops on the packet and so becomes certain of the validity of Address 7, and thenceforth if any node sends an RREQ to Address 7, malicious node 'M' easily triggers the attack.

For the above-mentioned method, considering the fact that in a normal situation, the RREP packet is created only when the address is valid, hence, the malicious node can wait and become certain of the validity of the address when it eavesdrops on an RREP packet. To obviate such limitations, it is recommended that every single node be appointed a friend, and execute the intrusion detection procedure together with its friend node.

4.3 Obviating the Disadvantages of the Proposed Method

At the beginning of the network operation and upon the authentication stage, the administrator appoints a friend to every single node across the network and informs them of the validity as well as invalid addresses of their counterparts. In case the number of nodes in a network is an odd number, network administrator itself assumes the responsibility of friendship with one of the nodes.

Just as the above-said method, when a node suspects the possibility of an attack on the network, it sends an RREQ packet to its invalid address and here, the friend node replies and sends an RREP packet to the source node. Assume, for instance, that in (Figure 4), node 'S' is friends with node 'C' and is suspicious of an attack within the network, therefore it sends an RREQ for its invalid address (Address 2). With regard to the fact that node 'C' is aware of the node S's invalid address, it sends an RREP packet to the source node (node 'S'). The malicious node

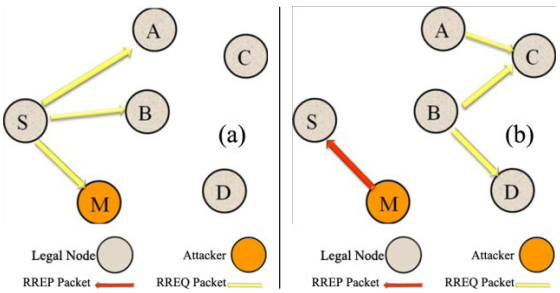

Figure 3. (a) Node 'S' sends an RREQ to the destination 'C'; (b) malicious node 'M' sends a forged RREP to 'S'.

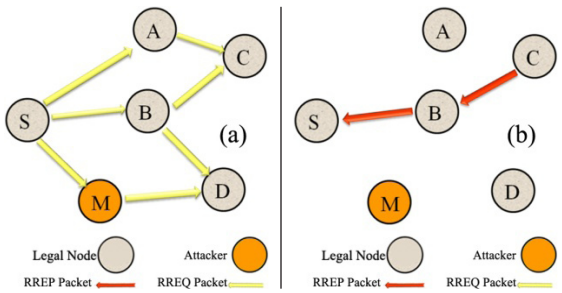

Figure 4. (a) Node 'S' sends an RREQ packet to node 'C'; (b) node 'C' sends an RREP packet to node 'S'.

'M', in this way, will not be able to realize whether the address 2 is valid.

4.4 Simulation and Evaluation of Results

As for simulation, the proposed method and the PSBA method were implemented in OPNET simulator. The simulation parameters are provided below:

A number of 50 nodes, were randomly placed in an environment of 5000 * 5000 m^2. The packet sizes were considered at an equal and fixed size of 1024 bytes. The packet dispatch interval was adjusted to 0.1 seconds. DSR protocol was adopted for routing. Subsequent to investigating different threshold values in the PSBA method, the acceptable threshold value for this method was designated in 5.

As for comparing the PSBA and the proposed method, two networks were considered in one of which 4 malicious nodes and in the other 6 malicious nodes were placed. The malicious nodes were randomly selected out of the available nodes. The simulation results in a network with 4 malicious nodes are given in Figure 5, and Figure 6 portrays the results for a network with 6 malicious nodes.

Simulation results indicate that the proposed method benefits from higher intrusion detection speed compared to the PSBA method.

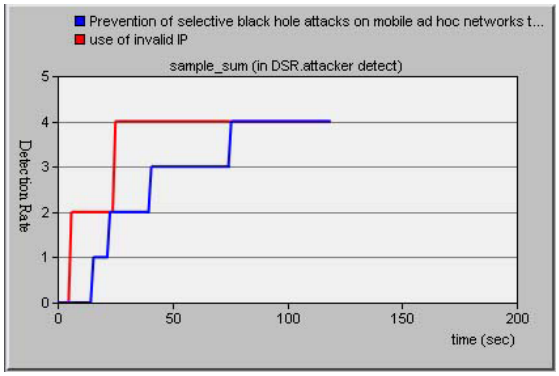

Figure 5. Network with 4 malicious nodes.

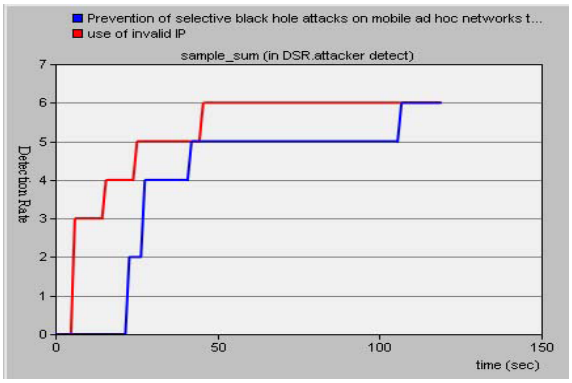

Figure 6. Network with 6 malicious nodes.

5. Conclusion

The black hole attack is one of the most important threats in mobile ad hoc networks, capable of significantly reducing network functionality. Based on the proposed method in this study, the node suspicious of the presence of an attack can deceive and entrap the malicious node by employing the invalid addresses. Considering the nature of black hole attacks, in which a malicious node, after receiving an RREQ packet, sends a forged RREQ packet to the source node, it seems that, by adopting the proposed method, malicious nodes can be easily detected. In this method, it is only malicious nodes which may reply to a packet with an invalid address, therefore there will be no possibility of false detection. On the other hand, this method does not require a threshold value for intrusion detection, thus, the rate of malicious node detection will also rise.

6. References

1. Ritonga MA, Nakayama M. Manager-based architecture in Ad Hoc network intrusion detection system for fast detection time. International Symposium on Applications and the Internet, SAINT 2008. 2008 Jul 28–Aug 1; Turku, Finland. IEEE. p. 76–82.
2. Moradiya P, Sampalli S. Detection and prevention of routing intrusions in mobile ad hoc networks. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing; 2010 Dec 11–13; Hong Kong. IEEE. p. 542–47.
3. Nasser N, Chen Y. Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks. IEEE International Conference on Communications. 2007 Jun 24–28; Glasgow. IEEE. p. 1154–59.
4. Cheng B-C, Tseng R-Y. A context adaptive intrusion detection system for MANET. Comput Comm. 2011; 34(3):310–18.
5. Cannady J. Distributed detection of attacks in mobile ad hoc networks using learning vector quantization. Third International Conference on Network and System Security. NSS'09. 2009 Oct 19–21; QLD: Gold Coast. p. 571–74.

6. Mishra A, Nadkarni K, Patcha A. Intrusion detection in wireless ad hoc networks. IEEE Wireless Comm. 2004; 11(1):48–60.
7. Srinivasan T, Mahadevan V, Meyyappan A, Manikandan A, Nivedita M, Pavithra N. Hybrid agents for power-aware intrusion detection in highly mobile ad hoc networks. Systems and Networks Communications. International Conference on Systems and Networks Communications, 2006. ICSNC '06. 2006 Oct; Tahiti. IEEE. p. 2.
8. Jaisankar N, Saravanan R, Swamy KD. A novel security approach for detecting black hole attack in MANET. Inform Process Manag. 2010; 70:217–23.
9. Mistry N, Jinwala DC, Zaveri M. Improving AODV protocol against blackhole attacks. Proceedings of the International MultiConference of Engineers and Computer Scientists MECS 2010 Mar 17–19. 2010; Hong Kong. p.17–19.
10. Vishnu K, Paul AJ. Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks. Int J Comput Appl Tech. 2010; 1(22):38–42
11. Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. 2011 13th International Conference on Advanced Communication Technology (ICACT). 2011 Feb 13–16; Seoul. IEEE. p.755–60.
12. Su M-Y. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comput Comm. 2011; 34(1):107–17.
13. Ben Othman J, Mokdad L. Enhancing data security in ad hoc networks based on multipath routing. J Parallel Distr Comput. 2010; 70(3):309–16.