A Study on Few Approaches to Counter Security Breaches in MANETs

Moirangthem Goldie Meitei and Biswaraj Sen

Abstract Mobile ad hoc networks (MANETs) represent a class of networking that is quite essential and different from the traditional systems. Though the use of MANETs is gaining popularity in academic and commercial domains, MANETs have been initially designed to be deployed in areas such as emergency search and rescue operations, military battlefields, and other hostile or challenging environments. Because of the demanding environments that they have to operate in, MANETs do not have well-defined infrastructure unlike wired networks. All the participating nodes in a MANET work via cooperation and hence central coordination is absent. This places an inherent trust among the nodes forming the network in a MANET. Another major consideration regarding MANETs is that they have to often deal with limited resources such as power and bandwidth. These characteristic properties of MANETs make them susceptible to different kinds of attacks which aim to find vulnerabilities in the MANET protocols or target the limited resources. Hence, it becomes essential to recognize these threats and find ways to mitigate and tackle them. This paper will emphasize in understanding threats in ad hoc networks and the approaches to deal with these threats.

Keywords MANET · Intrusion detection · Trust · Software agent

1 Introduction

Ad hoc networks, as the term ad hoc suggests, refer to wireless networks that are constructed for a particular purpose or an immediate need. Ad hoc networks differ from traditional networking systems in that they do not require a centralized

M. G. Meitei (✉) · B. Sen
Computer Science and Engineering Department, Sikkim Manipal Institute of Technology, Majitar, Sikkim, India
e-mail: mgmeitei@gmail.com

B. Sen
e-mail: biswaraj.s@smit.smu.edu.in

H. K. D. Sarma et al. (eds.), *Advances in Communication, Cloud, and Big Data*, Lecture Notes in Networks and Systems 31,
https://doi.org/10.1007/978-981-10-8911-4_12

coordinator or prior infrastructure to be in place. Thus, ad hoc networks are also called infrastructure less networks [1]. Such networks use a wireless medium for communication. A mobile ad hoc network (MANET) refers to a network in which the nodes forming the ad hoc network are mobile [2].

In a MANET, the nodes cooperate with each other to share information. If a destination node falls beyond the transmission range of a node that wants to transmit information, the sender node transmits the information to its neighbor which in turn propagates it to its neighbors until it reaches the required destination. It can be seen that this infrastructure places an inherent trust in all other nodes in the network for information propagation. A malicious attacker can take advantage of this trust relationship among the nodes, thereby compromising the network. Also due to the mobility of the nodes and the dynamically changing network topology, it is hard to determine if a packet is getting dropped because of the intrinsic network characteristics or because of the presence of a malicious attacker in the network. Hence, care must be taken when detecting threats that the generation of false alarms should be minimal.

This paper briefly discusses the different types of attacks that can take place in a MANET and the different strategies that can be used to tackle the security threats. The rest of the paper is organized as follows: Sect. 2 discusses the various security threats in MANETs. Section 3 explores some of the different mechanisms that have been proposed to tackle some of the security threats. Section 4 gives a brief summary of the attacks and security mechanisms, and Sect. 5 provides the conclusion.

2 Security Threats in MANETs

Security is a very important aspect in MANETs, especially since ad hoc networks are deployed in hostile environments such as military battlefields. The task of routing in MANETs faces several challenges because of its innate network characteristics and the areas of deployment. Some of these challenges are as follows [3]:

(a) Mobility
(b) Bandwidth constraint
(c) Error-prone and shared channel
(d) Hidden and exposed terminal problems
(e) Location-dependent contention
(f) Other resource constraints such as computing power, battery power, buffer storage, etc.

MANETs face vulnerabilities because of shared wireless medium, lack of physical protection for the mobile nodes, and complete trust among nodes because of lack of centralized decision-making entity [4]. MANETs operate by establishing an inherent trust relationship among its participating nodes. Hence, each node in a MANET is able to function as a router. But since the wireless medium is shared and

there is a lack of central coordination, MANETs are vulnerable to attacks from other devices within the transmission range. Thus, managing trust also becomes an important issue [5].

Also MANETs lack a clear line of defense since there is no well-defined place where traffic monitoring or access control mechanisms can be deployed [6]. Although cryptography can be used to provide security services such as confidentiality, authentication, integrity, and non-repudiation, it is not sufficient to deal with attacks that compromise on availability, such as DoS attacks [7]. MANETs face different kinds of security threats as follows:

(a) Denial of service
(b) Resource consumption in the form of energy depletion and buffer overflow
(c) Host impersonation
(d) Information disclosure
(e) Interference

The attacks against mobile ad hoc wireless networks can be generally classified into two types [1]:

(a) Passive attacks

Passive attacks are those attacks in which the malicious nodes do not disrupt the working of the network, but they listen to the data being transferred without altering it. These kind of attacks can violate the confidentiality of the data being sent in the network.

Some examples of passive attacks are eavesdropping, traffic analysis, and monitoring. These attacks are associated with the Physical layer and Link layer [7].

(b) Active attacks.

Active attacks, on the other hand, are those attacks that disrupt the working of the network by either altering or destroying the data. These attacks can be divided into two types as follows:

- External attacks: These are the attacks that are performed by nodes that do not belong to the network.
- Internal attacks: These are the attacks that are performed by nodes from within the network.

Examples of active attacks include jamming, spoofing, modification, replaying, DoS. These attacks are associated with Physical layer, Network layer or across multi-layers [7].

Some of these attacks in MANETs are discussed as follows:

Eavesdropping:

The act of intercepting messages and reading them by unauthorized attackers without actually modifying the messages is known as eavesdropping. In MANETs, the mobile nodes share a wireless medium in which messages are usually broadcast

over the network. These broadcast messages over the wireless medium can be easily intercepted by tuning to the particular frequency of the message.

Black hole attack:

A black hole attack is a DoS attack in which a malicious node falsely claims that it has the shortest path to the destination node. It is an active attack type which targets vulnerabilities in on-demand routing protocols such as DSR and AODV (Fig. 1).

Black hole attack is carried out by an attacker by sending fake routing information [8]. In this attack, an attacker node first claims that it has the shortest route to a given destination when it receives Route Request message from a sender node. For this, the attacker replies to the Route Request message with a Route Reply having a very high destination sequence number, hence ensuring that the attacker gets included in the route from the sender to the destination. On receiving the subsequent data packet from the sender, the attacker will not forward the data packets but instead drop them, thus preventing them from reaching the intended destination. A subtler version of Black hole attack can selectively forward data packets which makes it even harder to detect the attacker.

Gray hole attack:

A gray hole attack is an active attack type which causes dropping of messages. It can also be considered as a variant of Black hole attack. In this attack, the attacking node first honestly replies to Route Request message with correct Route Reply message. Then when the attacker receives data packets to be sent to the destination, it drops either some or all of the data packets intended for the destination node. Gray hole attacks are harder to detect than black hole attacks because it is difficult to conclude whether the packets are being dropped intentionally or because of a genuine network congestion.

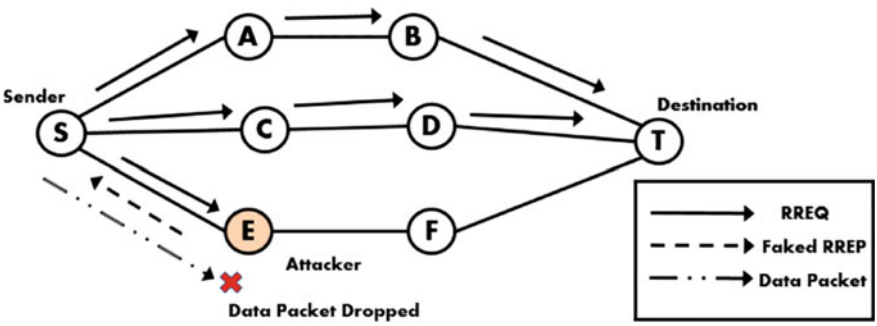

Fig. 1 Black hole attack

Rushing attack:

In rushing attack, a malicious node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same Route Request packet can react [3]. This is possible because the malicious attacker ignores the delays imposed by the network protocol. Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the malicious node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the malicious node (Fig. 2).

Sleep deprivation

Sleep deprivation is a resource consumption attack which attacks the limited battery life of a MANET node. In this attack, an attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node [7]. This leads to exhaustion of battery life of the node, thus compromising the performance of the network.

Wormhole

A wormhole attack is an attack carried out by two colluding attackers in the network. In this attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point [9]. Often, the colluding attackers are connected by a private high-speed network which provides faster transmission than the wireless medium of the network (Fig. 3).

In ad hoc routing protocols such as AODV and DSR, a wormhole attack may be launched in such a way that an attacker receiving a Route Request message will forward it to its colluding attacker who in turn rebroadcasts the request to its neighbors. The neighbors will discard all subsequent Route Requests thinking them

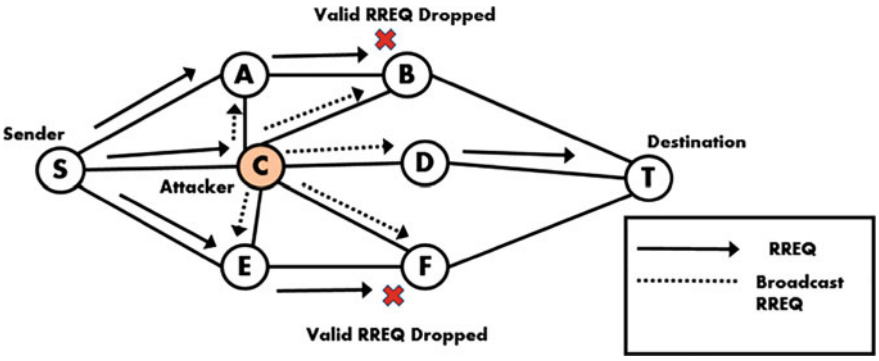

Fig. 2 Rushing attack

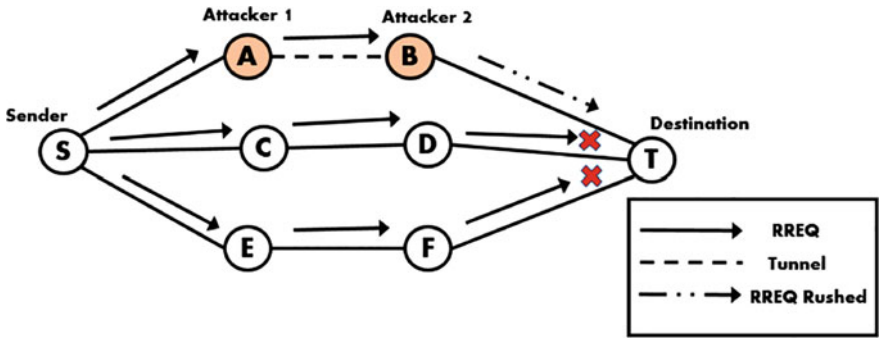

Fig. 3 Wormhole attack

to be duplicates. Thus, this prevents all other routes to the destination except the one containing the colluding attackers.

It can be seen that because of the vulnerabilities of MANETs, attacks can take place in several layers. However, this paper will look at security measures for attacks in the Network layer only.

3 Mechanisms for Dealing with Security Threats

Many scholars have proposed several types of defense mechanisms for dealing with the security threats mentioned in the previous section. Some of these defense mechanisms that are being addressed by this paper are:

(a) Intrusion Detection System (IDS)-based approach
(b) Authentication-based approach
(c) Software agent-based approach

These approaches are further discussed as follows.

3.1 Intrusion Detection System (IDS)-Based Approach

Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system [10]. The mechanism by which this is achieved is called an intrusion detection system (IDS). An IDS monitors and collects network activity information and then analyzes it to check for any anomalous behavior in the network. If an IDS determines that an anomalous behavior is occurring, it alerts the security administrator by generating an alarm. Also, IDS can initiate a proper response to the malicious activity.

Intrusion detection can be categorized into two methods: anomaly detection and misuse detection. Anomaly detection is the method of monitoring the network for deviations from normal behavior while misuse detection (also called signature-based detection) uses databases that contain signatures or patterns of known attacks [11].

Huang and Lee [12] proposed an intrusion detection system against several types of attacks in MANETs. Their paper is based on their previous work on anomaly detection which used cross-feature analysis to detect intrusions in a MANET [13]. Their latter work can be divided into two approaches: one based on detecting anomalies by implementing IDS on every node, and the other based on anomaly detection by implementing IDS for a cluster-based system.

In the first approach, they have used feature selection to identify anomalies. They have used a total of 141 features, and this approach can be used to detect new and unknown attacks. They have used certain features based on Monitoring node and Monitored node to classify and detect attack types. Then they further refined their work by proposing identification rules for identifying some well-known attacks such as black hole, random packet dropping, etc.

In the second approach, they proposed a cluster-based IDS as opposed to local IDS running on all the nodes to deal with limited power issue of MANET. Since running IDS on each node consumes battery power, the task of collecting network information is assigned to a single node in each cluster, which acts as the cluster head. Each cluster has a cluster head, called a Monitoring node, which monitors the other nodes in the cluster, which are called Monitored nodes. The cluster head can overhear the traffic from its neighbors by using the promiscuous mode in MANET routing algorithms. They also devised an election mechanism to select the cluster heads fairly in such a way that each node has an equal chance of being selected as the cluster head.

Results: Comparing the two approaches, it can be seen that the cluster-based IDS approach performs much better in terms of CPU speed up and network overhead as compared to the first approach of running IDS every node. Although the accuracy in terms of detection is minimally better in the first approach, the overall benefits of the second approach outweigh the first.

Trivedi et al. [14] proposed a reputation-based mechanism to deal with intrusion in MANETs. They have named this mechanism as RISM (reputation-based intrusion detection system for mobile ad hoc networks) and it is a modification of the CONFIDANT protocol [15]. RISM has been designed as a "semi-distributed nature" which implies that it is neither restricted locally nor immediately propagated to the whole network.

RISM has the following modules:

(a) **Monitor**: which takes the responsibility of monitoring the network. It collects network information at fixed time intervals, called as Timing Windows.
(b) **Reputation System**: which assigns reputation values to the nodes. The reputation system can assign a node to be either Normal, Suspicious, or Malicious. The reputation is assigned on the basis of a threshold for dropped packets,

called MaliciousDropThreshold. This MaliciousDropThreshold is flexible in the sense that its value can be updated according to the network traffic in each Timing Window.

(c) **Path Manager**: which calculates a new path when a node is deemed as Malicious.

(d) **Redemption and Fading**: which is a mechanism by which a node deemed as Malicious is given the chance to improve its reputation. This is implemented by carrying out a knock test to see if a Malicious reputed node behaves normally on receiving the knock test. If a Malicious node successfully passes the knock test, it can be moved to Suspicious category.

Results: RISM performs better than normal DSR in terms of packet delivery ratio up to a certain extent but when the number of malicious nodes increases, RISM incurs a routing overhead as compared to DSR because of recalculation of a new node when a malicious node is detected.

Nadeem and Howarth [16] proposed intrusion detection and adaptive response (IDAR), an IDS mechanism that deploys both anomaly detection and knowledge-based intrusion detection. This is an enhancement over their previous work in which they dealt with intrusion detection in a predetermined way. Their proposed mechanism implements an adaptive intrusion response after the intrusion has been detected. This adaptive response takes into account parameters such as attack severity, network degradation, and impact of the response action on the network performance.

IDAR employs a cluster-based IDS in which all nodes can be either manager node (MN), cluster head (CH), or cluster node (CN). IDAR uses two matrices for keeping track of the network. They are network characteristic matrix (NCM) and performance matrix (PM).

The architecture of IDAR consists of the following stages:

(a) **Network Monitoring and Data Collection**: In this phase, the CHs collect data from CNs and store them in NCM and PM.

(b) **Training**: In this phase, CHs continuously gather NCM and PM information and report to MN at fixed time intervals.

(c) **Testing**: Testing is carried out in four further phases as follows:

- **Intrusion detection**: MN uses anomaly-based intrusion detection to identify if any intrusion has occurred.
- **Attack identification**: This phase uses a rule-based approach to identify the attack. This is done with the help of a knowledge base maintained by IDAR.
- **Intruder identification**: In this phase, MN applies intruder identification rules that a specific for a known attack.
- **Adaptive intrusion response**: It consists of three actions: Isolation, Route around attacker, and No punishment.

Results: IDAR performs better when compared to fixed intrusion detection response as the overall network degradation of IDAR is lower as compared to fixed intrusion detection response. For severe attacks such as black hole attack and sleep deprivation, IDAR can isolate the attacker node for most of the time. For rushing attacks, choosing No punishment response by IDAR gives the most optimal network performance.

3.2 Authentication-Based Approach

Hu et al. [17] proposed a generic route discovery mechanism for handling rushing attacks. Rushing attacks are DOS attacks which prevent on-demand routing protocols to find routes longer than 2 hops. In rushing attacks, the attacker forwards Route Requests much faster than other nodes. This is possible because the attacker ignores delays at the MAC or the delays imposed by the routing protocol. Although one solution is to ignore delays at all nodes altogether, it can cause degradation in network performance because of the resulting collisions in the network. To tackle this, Hu et al. have proposed a Secure Route Discovery mechanism for defending against rushing attacks.

The proposed mechanism consists of three phases:

(a) **Secure Neighbor Detection**: This phase uses a three round mutual authentication protocol to determine if two nodes are neighbors so that they can communicate. This is carried out by deploying three messages:

- Neighbor Solicitation packet sent by the initiating node to a neighbor.
- Neighbor Reply packet sent by the neighbor on receipt of the previous packet.
- Neighbor Verification packet sent by the initiator which includes broadcast authentication of a timestamp and the link from source to the destination.

The protocol uses nonces to ensure freshness of the reply messages.

(b) **Secure Route Delegation**: In this phase, all nodes verify that secure neighbor detection protocols were executed correctly. A node receiving a Route Request verifies that the request came from its neighbor.

(c) **Randomized Message Forwarding**: In this phase, a node first collects a number of Route Requests and selects a random request to forward. This random selection is done to ensure that attacker cannot dominate all the routes returned.

Results: The proposed mechanism is able to detect alternate routes in case of a rushing attack most of the time as compared to existing on-demand routing protocols which are in general unable to deliver packets over paths longer than two hops. However, the proposed mechanism has very low packet delivery ratio as compared to DSR in normal traffic conditions. The packet overhead is also large in the proposed mechanism as compared to DSR.

3.3 Software Agent-Based Approach

Prathapani et al. [18] proposed the use of mobile honeypot agents to detect black hole attacks in Wireless Mesh Networks (WMNs). Honeypot agents are software agents that are used in IDS to detect malicious attackers. They are used to monitor the network and also can be used as decoys that lure attackers. Honeypots are deployed as mobile software agents that can traverse the entire network, and as such, they are not confined to individual nodes.

The use of honeypots in determining whether a node is malicious or not is illustrated as follows:

(a) A honeypot first places itself next to a node to be tested, called as testee node.
(b) It generates a Route Request bearing the address of a known destination node to the testee. That is, the honeypot already knows route the destination and it is trying to verify whether the testee node behaves normally or not.
(c) The testee node then sends its Route Reply in response to the Route Request from the honeypot.
(d) The honeypot node, in turn, sends a dummy data packet to the testee node to be sent to the known destination.
(e) Then, the honeypot queries the known destination whether it has received the dummy data packet via the testee.

Results: Simulations were carried out in AODV protocol using two kinds of topologies: Grid topology and Random topology. It is observed that employing the honeypot scheme increases network throughput significantly in Grid topology and in Random topology as compared to normal AODV under black hole attack.

4 Summary

MANETs face various challenges because of their inherent characteristics, their areas of deployment, and the limited resources. We have seen that attacks in MANETs try to exploit these native network properties and routing protocol deficiencies. The different kinds of attacks discussed in this paper can be summed up in Table 1.

We have also seen various approaches to counter the above-mentioned threats. A brief summary of the techniques discussed for handling the security threats in MANETs is shown in Table 2.

Table 1 Summary of attacks in MANET

Attack	Type of attack	Layer of attack	Security feature compromised	Effect
Eavesdropping	Passive	Physical layer	Confidentiality	Message interception
Black hole	Active	Network layer	Availability, integrity	Packet drop
Gray hole	Active	Network layer	Availability	Packet drop
Wormhole	Active	Network layer	Availability, integrity	Route manipulation
Rushing	Active	Network layer	Availability	Route manipulation
Sleep deprivation	Active	Network layer	Availability	Battery consumption

Table 2 Summary of security approaches

Authors	Mechanism	Routing protocol	Type of attack(s)	Effect
Huang and Lee [12]	IDS	AODV	Black hole, sleep deprivation	CPU speed up and low overhead
Trivedi et al. [14]	IDS	DSR	Packet drop	Improved packet delivery ratio
Nadeem and Howarth [16]	IDS	AODV	Black hole, gray hole, sleep deprivation, rushing	Successfully isolate attacker node
Hu et al. [17]	Authentication	DSR	Rushing	Detects alternate routes in case of rushing attack
Prathapani et al. [18]	Honeypot agents	AODV	Black hole	Improved throughput

5 Conclusion

The characteristic properties of MANETs (viz. trust-based relationship, lack of central coordination) make them vulnerable to different kinds of attacks. Moreover, MANETs have to often operate in challenging environments with limited resources (e.g., bandwidth, battery life). Hence, security is of prime importance in MANETs.

In this paper, we have looked at some of the attacks that can take place in MANETs and a few approaches to tackle these attacks. It is seen that more often than not, deploying security measures against these attacks acts as a double-edged sword in that the implementation cost of security mechanisms causes a compromise in overhead and/or efficiency of the network.

Still, research has been going on to optimize the cost of implementing these security measures [19, 20]. One future scope in this direction may be the application of Big Data to monitor, analyze, make inferences, and take decisions to tackle different attacks in MANETs.

References

1. Deng Hongmei, Li Wei, Agrawal Dharma P (2002) Routing security in wireless ad hoc networks. IEEE Commun Mag 40(10):70–75
2. Chandra P (2011) Bulletproof wireless security: GSM, UMTS, 802.11, and ad hoc securit. Elsevier, Armsterdam
3. Murthy CSR, Manoj BS (2004) Ad hoc wireless networks: architectures and protocols, portable documents. Pearson Education, London
4. Zhang Yongguang, Lee Wenke, Huang Yi-An (2003) Intrusion detection techniques for mobile wireless networks. Wirel Netw 9(5):545–556
5. Li Wenjia, Parker James, Joshi Anupam (2012) Security through collaboration and trust in MANETs. Mob Netw Appl 17(3):342–352
6. Yang H, Luo H, Ye F, Lu S, Zhang L (2004) Security in mobile ad hoc networks: challenges and solutions. IEEE Wirel Commun 11(1):38–47
7. Wu B, Chen J, Wu J, Cardei M (2007) A survey on attacks and countermeasures in mobile ad hoc networks. Wireless Network Security. Springer, US, pp 103–135
8. Kannhavong B, Nakayama H, Nemoto Y, Kato N, Jamalipour A (2007) A survey of routing attacks in mobile ad hoc networks. IEEE Wirel Commun 14(5):85–91
9. Hu Yih-Chun, Perrig Adrian, Johnson David B (2006) Wormhole attacks in wireless networks. IEEE J Sel Areas Commun 24(2):370–380
10. Anantvalee T, Jie W (2007) A survey on intrusion detection in mobile ad hoc networks. Wireless Network Security. Springer, US, pp 159–180
11. Nishani L, Biba M (2016) Machine learning for intrusion detection in MANET: a state-of-the-art survey. J Intell Inf Syst 46(2):391–407
12. Huang Y, Lee W (2003) A cooperative intrusion detection system for ad hoc networks. In: Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks, ACM, New York
13. Huang YA, Fan W, LeeW, Yu PS (2003, May) Cross-feature analysis for detecting ad-hoc routing anomalies. In: Proceedings of the 23rd international conference on distributed computing systems, IEEE, pp 478–487
14. Trivedi AK, Kapoor R, Arora R, Sanyal S, Sanyal S (2013) RISM–reputation based intrusion detection system for mobile ad hoc networks. arXiv preprint arXiv:1307.7833
15. Buchegger S, Le Boudec JY (2002, June) Performance analysis of the CONFIDANT protocol. In: Proceedings of the 3rd ACM international symposium on mobile ad hoc networking and computing, ACM, pp 226–236
16. Nadeem A, Howarth MP (2014) An intrusion detection and adaptive response mechanism for MANETs. Ad Hoc Netw 13:368–380
17. Hu YC, Perrig A, Johnson DB (2003, September) Rushing attacks and defense in wireless ad hoc network routing protocols. In: Proceedings of the 2nd ACM workshop on wireless security, ACM, pp 30–40
18. Prathapani A, Santhanam L, Agrawal DP (2013) Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents. J Supercomput 64(3):777–804
19. Mitrokotsa A, Dimitrakakis C (2013) Intrusion detection in MANET using classification algorithms: the effects of cost and model selection. Ad Hoc Netw 11(1):226–237
20. Wang SH, Tseng CH, Levitt K, Bishop M (2007, September) Cost-sensitive intrusion responses for mobile ad hoc networks. In: International workshop on recent advances in intrusion detection, Springer, Berlin, Heidelberg, pp 127–145