International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 5458-5463

Mitigating Black Hole Attacks in MANETs Using a Trust-Based Threshold Mechanism

Biswaraj Sen[1], Moirangthem Goldie Meitei[2], Kalpana Sharma[3], Mrinal Kanti Ghose[4], and Sanku Sinha[5]

[1,2,3]Computer Science and Engineering Department, Sikkim Manipal University, Majitar, Sikkim, India.
[4] Sikkim University, Tadong, Gangtok, India.

[5] Sikkim Manipal University, Gangtok, India.

Abstract

A MANET (Mobile Ad hoc Network) is a wireless network which is mobile and is deployed for an immediate or short term purpose. MANETs operate by sharing information among its neighbours and each node in a MANET takes responsibility for information propagation since central coordination is absent. Hence, each node in a MANET implicitly trusts its neighbours for information sharing. Nodes in a MANET are vulnerable to various security threats which seek to exploit the weaknesses of the network. A Black Hole attack is one such attack which seeks to compromise the network by dropping information that is meant for a certain destination. This paper looks at utilizing the inherent trust relationship among the nodes in a MANET by formulating a trust model to recognize the trustworthiness of a node. This trust model makes use of intrusion detection to detect, identify and mitigate Black hole attacks.

Keywords: Black hole attack, MANET, intrusion detection system, threshold, trust model.

INTRODUCTION

Ad hoc networks are wireless networks that are designed to meet an immediate requirement or a particular situation (hence the name *ad hoc*). Ad hoc networks differ from traditional networks in the sense that they do not require a centralized coordinator or a prior infrastructure to be in place, i.e., the participants in an ad hoc network can communicate with each other directly without an intermediate infrastructure (e.g. base station). Thus, ad hoc networks are also called *infrastructureless networks* [1]. A MANET (Mobile ad hoc network) refers to a network in which the nodes forming the ad hoc network are mobile [2]. MANETs are characterised by their highly random and dynamic topologies [3]. MANETs have been used to set up communications in areas where there is no pre-existing infrastructure (e.g. battlefield) or where the infrastructure has failed (e.g. earthquake rescue) [4]. Hence, the characteristic properties of MANETs have enabled them to be used in areas such as emergency search and rescue operations, military battlefields, and in academic and commercial sectors [5, 6].

In a MANET, nodes cooperate with each other to share information. A node wanting to send information transmits the information to its neighbour which in turn propagates it to its neighbours until it reaches the required destination. This system places an inherent trust in among the other nodes in the network for information propagation. An 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 dropped because of the intrinsic network characteristics or the presence of an attacker.

This paper briefly discusses the latent trust relationship among nodes in a MANET and seeks to develop a trust model to handle threats. The rest of the paper is organized as follows: Section 2 discusses the trust among nodes in MANETs. Section 3 covers a short explanation about intrusion detection system (IDS). Section 4 gives a brief explanation of the Black hole attack. Section 5 highlights some of the work done in this area. Section 6 describes the proposed trust model. Section 7 discusses the results. Section 8 provides the conclusion.

TRUST IN MANETS

Ad hoc networks operate by establishing an intrinsic 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, ad hoc networks are vulnerable to attacks from other devices within the transmission range.

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 [7]. MANETs are susceptible to DoS attacks as they do not have a clear line of defence [8, 9]. Ad hoc networks operate by establishing an intrinsic trust relationship among its participating nodes. Hence each node in a MANET is able to function as a router. Each node in a MANET completely trusts its neighbours to carry out network activities such as packet forwarding and packet delivery until each packet reaches the intended destination. Often, attackers try to take advantage of this particular trait present in the nodes in a MANET. Thus, managing trust also becomes an important issue [10, 11].

INTRUSION DETECTION SYSTEM (IDS)

Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system [12]. Intrusion detection system (IDS) is the mechanism by which this monitoring activity is achieved. An IDS monitors and collects network activity information and then analyzes it to check for any anomalous behaviour in the network. If an IDS determines that an anomalous behaviour 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 behaviour while misuse detection (also called signature based detection) uses databases that contain signatures or patterns of known attacks [13].

BLACK HOLE ATTACK

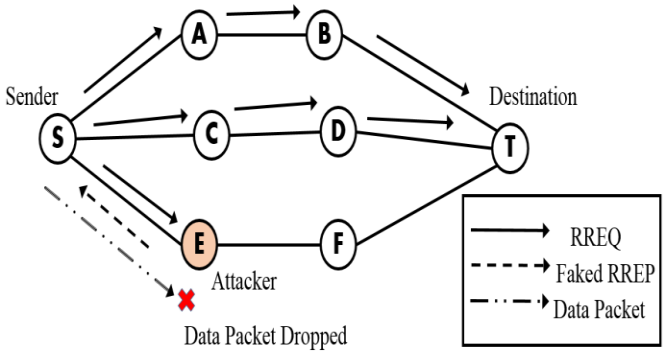

Figure 1. Black hole attack

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. This attack is carried out by an attacker sending fake routing information [14]. When an attacker node receives a Route Request message from a sender node, it 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.

RELATED WORK

Huang and Lee [15] proposed an intrusion detection system based on their previous work on anomaly detection which used cross feature analysis to detect intrusions [16]. Their work focused on detecting anomalies by implementing IDS on every node, and anomaly detection by implementing IDS for a cluster based system. Trivedi et al. [17] proposed a detection mechanism based on reputation to deal with intrusions in MANETs. Their proposed mechanism has been termed as RISM (Reputation based intrusion detection system for mobile ad hoc networks), which is a modification of the CONFIDANT protocol [18]. Nadeem and Howarth [19] proposed an IDS mechanism called IDAR (intrusion detection and adaptive response) which uses both anomaly detection and knowledge based intrusion detection. Hu et al. [20] proposed RAP (Rushing Attack Prevention) which is a generic route discovery mechanism for handling Rushing attacks. Prathapani et al. [21] proposed the use of mobile honeypot agents to detect Black hole attacks in Wireless Mesh Networks (WMNs).

PROPOSED STRATEGY

The overview of the proposed strategy is shown in the following diagram.

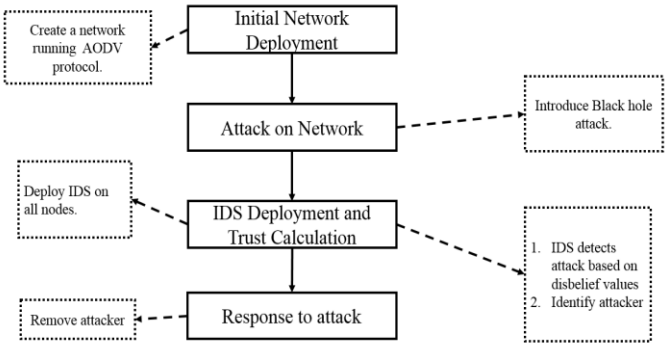

Figure 2. Workflow diagram of proposed methodology

The proposed methodology consists of the following phases:

Phase 1: Initial Network Deployment

Initially, the network is made to function on its own using a standard routing protocol. This helps in calculating a baseline observation of the network under normal circumstances. Once we know how the network behaves normally, we can differentiate it from the conditions arising due to malicious behaviour in the network.

Phase 2: Attack on Network

The network is now subjected to a routing attack, viz. Black hole attack. The attack is carried out in four scenarios as follows:

a) One Black hole attacker.

b) Ten percent of total nodes as Black hole attackers.

c) Twenty percent of total nodes as Black hole attackers.

d) Thirty percent of total nodes as Black hole attackers.

Phase 3: IDS Deployment and Trust Calculation

In this phase, IDS is deployed in all the nodes of the network. Each IDS node keeps track of the trust levels of its immediate neighbours. This tracking is done at run time. The trust values at are calculated based on three parameters:

a) The belief that a node has for its neighbour (b): The belief factor is calculated by taking into account positive events that occur during a transmission. Here, positive events are the events that signify a successful transmission in the network. The positive events chosen are:

   i) Successful packet reception

   ii) Successful packet forwarding

   The belief factor is calculated as follows:

$$b = \frac{p}{p+n+2}$$

   where, p = number of positive events and n = number of negative events

b) The disbelief that a node has for its neighbour (d): Contrarily, the disbelief factor is calculated by taking into account negative events that occur during a transmission. Negative events are the events that signify an unsuccessful transmission in the network. The negative events chosen are:

   i) Unsuccessful packet reception

   ii) Unsuccessful packet forwarding

   The disbelief factor is calculated as follows:

$$d = \frac{n}{p+n+2}$$

   where, p = number of positive events and n = number of negative events

c) The uncertainty that a node has for its neighbour (u): Uncertainty factor is initially set to 1 before any transmission begins after a node has just discovered its neighbours.

   The uncertainty factor is calculated as follows:

$$u = \frac{2}{p+n+2}$$

   where, p = number of positive events and n = number of negative events

   Hence, these three parameters are taken in such a way that:

$$b + d + u = 1$$

   at all times.

So initially, a node will have uncertainty value of 1, belief value of 0 and disbelief value of 0 for its neighbour before transmission. As communication begins in the network, these values get updated based on positive and negative events. This trust value calculation is done periodically.

An anomaly in the system is detected when the disbelief factor rises above a certain threshold. In this case, the anomaly is first verified as an attack by applying identification rules for recognizing attacks such as a Black hole attack. This step ensures that network congestion factor is taken into consideration. Once positively identified as an attack, the node under question will be treated as malicious and it will not be allowed participate in the network.

Threshold calculation

The threshold value is set based on experimental values. This is done by calculating the average value of PDF (packet data fraction) of several simulations of the network in its initial phase. This provides a measure of how the network performs normally in the absence of any malicious attacker. This average PDF value thus obtained serves as a threshold for discovering anomalous behaviour in the network.

Phase 4: Response to attack

When an attack such as a Black hole attack occurs, the intrusion is detected by the periodic update of the trust values. Once the attacker node is identified, it is not allowed to participate in routing and will be removed from the network. The node will then seek alternate routes to reach the destination after removing the attacker.

This process is explained as follows:

a) Since each node will be running IDS, each node can monitor its neighbour's activities. Hench each node keeps track of the belief, disbelief and uncertain factors of its neighbours.

b) If the disbelief factor of a certain neighbour node rises above the calculated threshold value (as explained above), then appropriate action is taken by:

   - Identifying the attack and the attacker: This is necessary to differentiate between network congestion and a routing attack, viz. black hole attack in this case. For this the following formula for identifying black hole attack is used:

$$PFP = \frac{pr(n)}{ps(nn)}$$

where,

PFP = packet forward percentage

pr(n) = no. of packets received by a node n

ps(nn) = no. of packets sent by n's neighbours and not destined for n

If n keeps dropping packets for a sufficiently long period, or more precisely, if the denominator is not zero and PFP = 1, then a Black hole is detected and n is identified as the attacking node.

   - Removing the attacker from the routing process: Once the attacker is identified, the node that detected

the attacker removes the malicious node from the network.

RESULTS

Simulations were carried out in ns-2.35 using AODV protocol. The simulation parameters are as follows:

Table 1. MANET simulation parameters

Method	Type
Channel type	Channel/wireless channel
Radio propagation	Propagation/TwoRayGround
Network Interface	Phy/WirelessPhy
Mac Type	Mac/802_11
Interface Que	Queue/DropTail/PriQueue
Link Layer type	LL
No. of Nodes	30, 60
Routing Protocol	AODV
Area	1000*1000 sq. m.
Simulation Time	1200 sec
Mobility	Random Waypoint

The results of the simulations can be viewed in the following graphs.

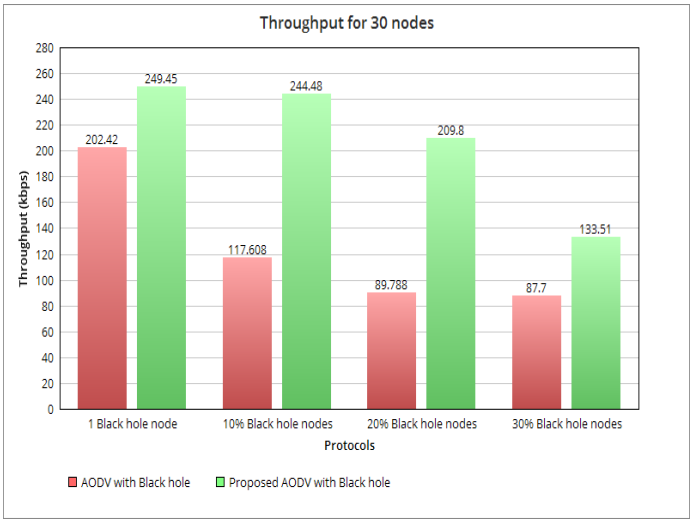

Figure 3. Throughput of 30 nodes

For 30 nodes, it is seen that the proposed solution gives a much better performance in terms of throughput as compared to the native AODV protocol when both are exposed to black hole attackers. This is because the proposed method is able to detect, identify and remove the attacker thereby increasing the throughput.

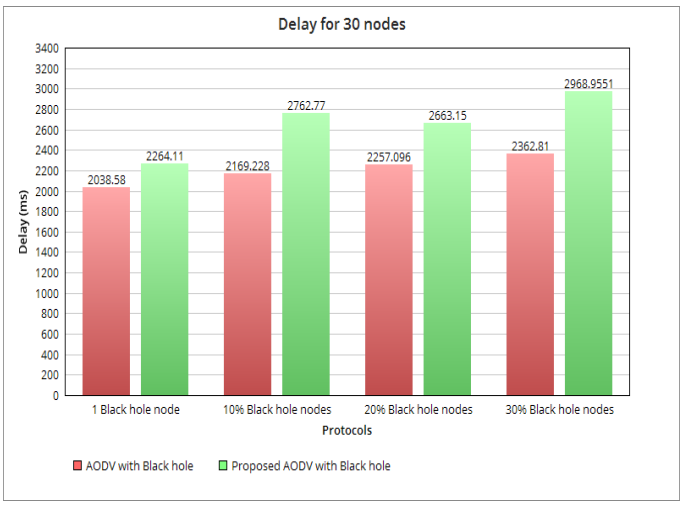

Figure 4. Delay of 30 nodes

But in terms of delay for 30 nodes, it is seen that the proposed solution suffers in performance as compared to the native AODV protocol when both are exposed to black hole attackers. This is because the proposed method has to find a new path after detecting and removing the attackers from the network, thereby increasing the delay.

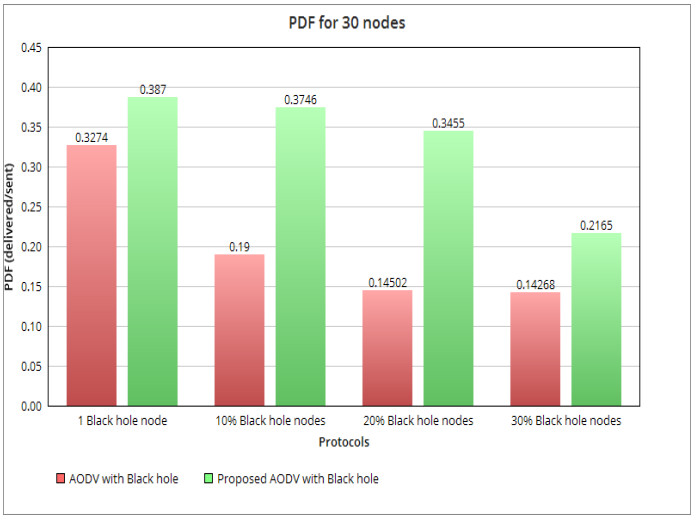

Figure 5. PDF of 30 nodes

However, for 30 nodes, the proposed solution gives better PDF performance as compared to the native AODV protocol when both are exposed to black hole attackers. This is because the proposed method is able to detect, identify and remove the attacker thereby increasing the packet delivery ratio.

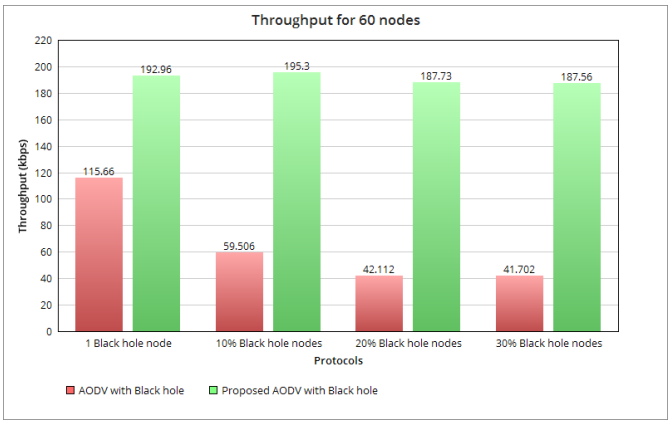

Figure 6. Throughput of 60 nodes

For 60 nodes, it is again seen that the proposed solution gives a much better performance in terms of throughput as compared to the native AODV protocol when both are exposed to black hole attackers.

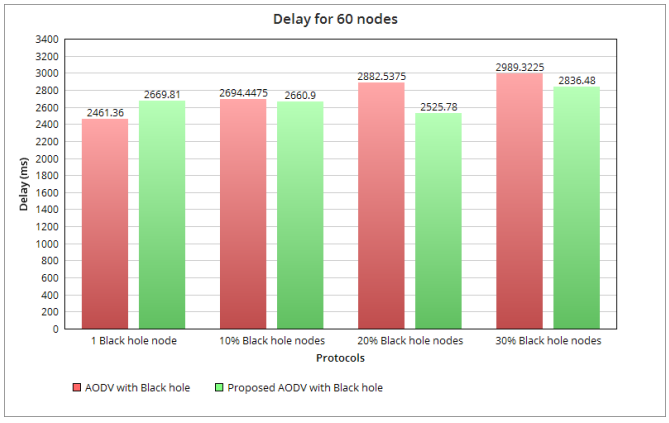

Figure 7. Delay of 60 nodes**.**

In terms of delay for 60 nodes, it is seen that the proposed solution experiences lesser delays as compared to the native AODV protocol when the number of black hole attackers are increased. This is because the network is denser as compared to 30 nodes and alternate routes to the destination can be found faster.

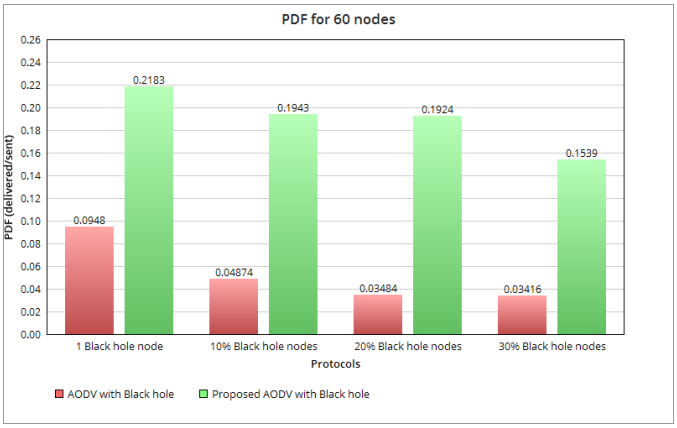

Figure 8. PDF of 60 nodes

As in the case for 30 nodes, for 60 nodes the proposed solution gives better PDF performance as compared to the native AODV protocol when both are exposed to black hole attackers. This is because the proposed method is able to detect, identify and remove the attacker thereby increasing the packet delivery ratio.

It can be seen that the black hole attack causes a big decline in network performance running AODV protocol. This drop in performance is easily seen across different parameters such as throughput, average end to end delay and PDF (packet delivery fraction).

When the proposed trust based IDS mechanism is applied, it can be seen that the network shows great improvement in terms of throughput and PDF, although the resultant benefit of this improvement is slightly lesser than the original network performance. However, it can be seen that the proposed mechanism suffers in average end to end delay parameter for 30 nodes. This can be explained by the fact that in a large network area, with the number of valid nodes reduced due to removal of the attackers, it becomes harder to find alternate routes to reach a destination. Hence, the overall time taken to find an alternate route increases because of the lack of eligible neighbour nodes in the network.

CONCLUSION

MANETs are susceptible to different kinds of attacks and threats because of their characteristic properties such as trust based relationship and lack of central coordination. It is possible to use this characteristic feature of MANET and devise a trust model to monitor network activity. Therefore, this document has made use of the trust behaviour among nodes in MANETs and devised a trust based IDS system against Black Hole attacks. To achieve this, a threshold value for judging the trustworthiness of a node has been implemented. The proposed mechanism is able to provide a substantial improvement in the affected network in terms of throughput and PDF, although it experiences higher end to end delays.

REFERENCES

[1] Deng, H., Li, W., and Agrawal, D. P.: Routing security in wireless ad hoc networks. IEEE Communications magazine, 40(10), 70-75 (2002)

[2] Chandra, P.: Bulletproof Wireless Security: GSM, UMTS, 802.11, and Ad Hoc Security. Elsevier (2011)

[3] Stojmenovic, I.: Handbook of wireless networks and mobile computing (Vol. 27). John Wiley & Sons (2003)

[4] Mohapatra, P., and Krishnamurthy, S.: AD HOC NETWORKS: technologies and protocols. Springer Science & Business Media (2004)

[5] Murthy, C. S. R., and Manoj, B. S.: Ad hoc wireless networks: Architectures and protocols, portable documents. Pearson education (2004)

[6] Güneş, M., Juraschek, F., Blywis, B., Mushtaq, Q., and Schiller, J.: A testbed for next generation wireless network research. PIK-Praxis der Informationsverarbeitung und Kommunikation, 32(4), 208-212 (2009)

[7] Zhang, Y., Lee, W., and Huang, Y. A.: Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9(5), 545-556 (2003)

[8] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. IEEE wireless communications, 11(1), 38-47 (2004)

[9] Wu, B., Chen, J., Wu, J., and Cardei, M.: A survey of attacks and countermeasures in mobile ad hoc networks. In: Wireless network security (pp. 103-135). Springer US (2007)

[10] Li, W., Parker, J., and Joshi, A.: Security through collaboration and trust in manets. Mobile Networks and Applications, 17(3), 342-352 (2012)

[11] Cho, J. H., Swami, A., and Chen, R.: A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 13(4), 562-583 (2011).

[12] Anantvalee, T., and Wu, J.: A survey on intrusion detection in mobile ad hoc networks. In: Wireless Network Security (pp. 159-180). Springer US (2007)

[13] Nishani, L., and Biba, M.: Machine learning for intrusion detection in MANET: a state-of-the-art survey. Journal of Intelligent Information Systems, 46(2), 391-407 (2016)

[14] 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)

[15] Huang, Y. A., and Lee, W.: A cooperative intrusion detection system for ad hoc networks. In: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (pp. 135-147). ACM (2003)

[16] Huang, Y. A., Fan, W., Lee, W., and Yu, P. S.: Cross-feature analysis for detecting ad-hoc routing anomalies. In: Distributed Computing Systems, 2003. Proceedings. 23rd International Conference on (pp. 478-487). IEEE (2003)

[17] Trivedi, A. K., Kapoor, R., Arora, R., Sanyal, S., and Sanyal, S.: RISM--Reputation Based Intrusion Detection System for Mobile Ad hoc Networks. arXiv preprint arXiv:1307.7833 (2013)

[18] Buchegger, S., and Le Boudec, J. Y.: Performance analysis of the CONFIDANT protocol. In: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (pp. 226-236). ACM (2002)

[19] Nadeem, A., and Howarth, M. P.: An intrusion detection & adaptive response mechanism for MANETs. Ad Hoc Networks, 13, 368-380 (2014)

[20] Hu, Y. C., Perrig, A., and Johnson, D. B.: Rushing attacks and defense in wireless ad hoc network routing protocols. In: Proceedings of the 2nd ACM workshop on Wireless security (pp. 30-40). ACM (2003)

[21] Prathapani, A., Santhanam, L., and Agrawal, D. P.: Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents. The Journal of Supercomputing, 64(3), 777-804 (2013)