A New Intrusion Detection System to deal with Black Hole Attacks in Mobile Ad Hoc Networks

Maryam Fathi Ahmadsaraei *, Abolfazl Toroghi Haghighat

Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran

Abstract

By extending wireless networks and because of their different nature, some attacks appear in these networks which did not exist in wired networks. Security is a serious challenge for actual implementation in wireless networks. Due to lack of the fixed infrastructure and also because of security holes in routing protocols in mobile ad hoc networks, these networks are not protected against attacks. For example in black hole attack, an attacker catches packets and throw them away, instead of forwarding them to their destinations. By using wireless intrusion detection systems, wireless networks can be protected. In this study, we introduce a new intrusion detection system to encounter black hole attack. This system is based on a combination of anomaly based intrusion detection (ABID) and specification based intrusion detection (SBID), we also use a new intrusion response. The analysis of simulation results (with NS-2) show that our method is success by using three measures: throughput, packet loss rate and packet delivery rate in comparing with ABID and SBID.

Keywords: Black hole attack, intrusion detection systems, mobile ad hoc networks

1. Introduction

There is no central node for network management In mobile ad hoc networks (MANETs). Nodes can move freely. These networks Flexibility decrease the level of security. Establishing Security becomes a major issue in MANETs. Many researchers have researched in this field. We can divided their approaches in to two main categories: a) approaches which are based on the encryption, due to the decentralized structure of these networks, there is no possibility of using this method. b) Intrusion detection approaches which can identify suspicious behaviors and possible attacks. The target of Intrusion detection system (IDS) is to detect suspicious behavior or known attacks [1].

Increasing using ad hoc networks and the importance of securing these networks are the reasons to research so much in this field. In [2], authors changed ad hoc on demand distance-vector (AODV) routing protocol. They use ABID to ensure of the network against black hole attack and expel the malicious node. This method Increases packet delivery rate and have no overhead. In [3], they use Intrusion detection system and consistent response. Group heads collect and store data from cluster members and send them to manager node. Manager node use anti-black hole intrusion detection. Then in

* Corresponding author. Email: fathimaryam2000@yahoo.com

the next step, manager node detects the attack and implement intrusion response. In [4], they proposed anti-black hole algorithm. In this algorithm if a middle node is not destination and does not send route requests packet for a specific path yet, but forwards route reply packets, in this situation, intrusion detector node should increase the amount of the node suspicious one unit. When the amount of node suspicious exceeded from threshold, a block message will sent by Intrusion detector node to block hole node. In [5], they have changed dynamic source routing protocol. In this method source node sends number of packets which wants to transmit to the destination from a different path. By receiving packets destination will start counting packets. If the number of packets which were not received was greater than packet loss threshold, destination will begin to identify the attacker node. The proposed approach has lower packet loss rate than dynamic source routing. In [6] they proposed a system which surveillance unit review traffic and send suspicious data to logging unit. By using this Information, attack detection unit, detect attack and inform to counter-attack unit. This unit decreases attack effect. In [7], they proposed a method which use digital signature to deal with using channel unfairly. To deal with the anomalies in forwarding packets, this method is done in several steps: source node suspects to a middle node which transmits the most number of steams. Because this node is dropping packets with extremely rate. If bad behavior counter of a node exceed from threshold, this node is known as a malicious node. In [8], they use cooperative and distributed method to prevent black hole attack. This method has four steps: Step one: each node listens to his neighbors to finds if his neighbors is malicious or not. Step two: to analysis if the suspicious node is a black hole attacker or not. Step three: intrusion detector node warns his one neighbors to participate detections process and decide if suspicious node an attacker or not. Step four: send alarms to entire network. This method has overhead. In [9], they proposed which do not selected path by receiving the first route reply packet arrivals. In this method source waits until all route reply packets receive. It is because most of the time the first route reply packet is from black hole node. In [10], system is divided into two parts: local intrusion detection which creates a list of trusted neighbors and global produces intrusion detection which is used to identify common attacks. In local intrusion detection system a list of trusted neighbors is created which is used in global intrusion detection system to identify common attacks. In [11], if a node forwards packets less than forwarding packets threshold, intrusion detector node knows that node as a black hole node. In [12], they proposed a new secure routing protocol based on reputation. Node reputation is based on his behavior. By using incentive mechanism, the chance of node activity will increase in the network. In [13], they proposed a method which some of the nodes are selected randomly as checkpoint nodes. The duty of these nodes is to produce acknowledgement for each received packet. If suspicious behavior is detected, a warning packet will delivered to the source node. In [14] they proposed a method. In that method each node monitor his neighbors, so nodes waste a lot of energy. Nodes compare packet loss rate and packet loss threshold and then judge their neighbor behavior. In [15], they proposed an adaptive intrusion detection system. If suspicious score exceeds from threshold, intrusion detector node sends block message to the network and Isolates the attacker node. In this paper, they do not discuss about the threshold value.

To encounter black hole attack, no one composed two methods: ABID and SBID yet. In this article, we combine these two methods. In the most of proposed ABID methods, due to high error rate of this method, the attacker allowed to return to the network [16] and it is assumed that the node is wrongly knew as an attacker. Therefore, the node should be allowed to return to the network. In any articles, researchers do not mention that they may detect the malicious node correctly and they were not wrong. So returning this malicious node to the network may be very dangerous. Therefore, we mention this issue in our proposed solution. The following article in the second part we discuss about the main content of the research. In the third part we present conclusion and recommendations for future work.

2. Main Content

In this section we discuss about some basic concepts, issue, proposed solution and analyzing results.

2.1. Define Basic Concepts

Mobile ad hoc network is a set of wireless nodes which constitute multi-hop radio network without the need for infrastructure or the central management [17]. Variable nature or decentralized configuration of these networks, leads them to be vulnerable [18]. We use AODV routing protocol which is in reaction routing category. In AODV routing protocol source node broadcasts route request message. Other nodes reply to source node according to their routing table. Source node checks replies and select a middle node which has the highest sequence number and lowest hop [19]. Black holes attack uses this secure hole of AODV routing protocol and send the greatest sequence number to source node. So source node sends his packet through this black hole node. After the black hole node acquired the path between source and destination, this node will drop all the packets. There are two kinds of black hole attacks: a) Single black hole attack which one black hole node attacks the network. b) Cooperative black hole attack which some black hole nodes attack the network and work together to destroy the network performance. To prevent the kinds of attacks simultaneously, we should use intrusion detection systems [14]. An intrusion detection system monitors users and network behaviors dynamically to recognize network intrusions [5]. Intrusion detection systems divide into three categories: a) anomaly based intrusion detection, which Identifies activities that are different from normal activities. ABID has two steps: Training and testing. Training is a process to model normal or expected behavior of network or users. Also this model acts as a user profile or network behavior. Building an effective profile consist of collecting information about normal activities and behavior of a network [3]. This method is good for small networks and has high wrong alarms rate. This method uses some techniques to model users' behavior in the network such as: statistics, chi-square test, decision tree and Markov chain. b) knowledge-based intrusion detection which has known attacks in its knowledge base and if these suspicious behavior were seen in the network. Intrusion detector node will warn. If an intrusion detector node seen that the network performance is decreased and could not find any attacks with these specifications, it adds this behavior as a new attack to its knowledge base. This method uses some techniques such as: expert systems, forward or backward chaining. c) Specification based intrusion detection which defines specifications a set of rules to monitor routing protocol behavior and detect network attacks [20].

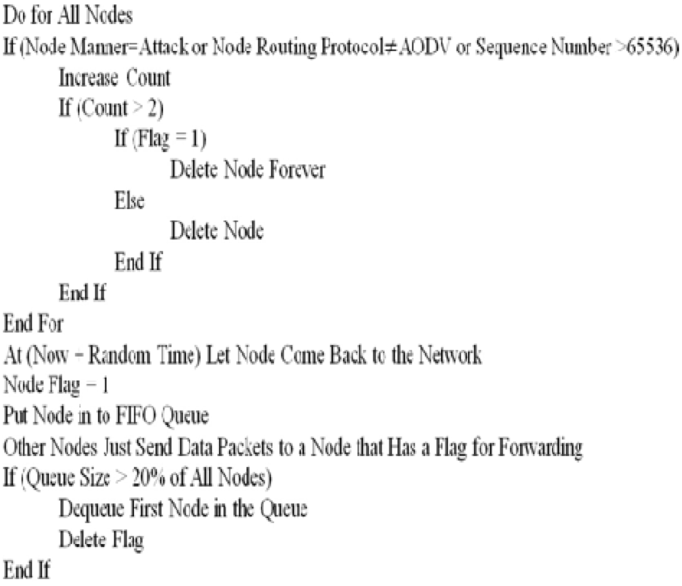
2.2. Issue

Mobile ad hoc networks are without infrastructure and use reaction routing protocols more, because these routing protocols have less overhead. Reactive routing protocols are prone to black hole attacks. The Implementation of black hole attacks is simple [21]. The intensity of black hole attacks is so high and these types of attacks disrupt network performance [3]. So we use intrusion detection systems to prevent network performance degradation by black hole node(s).

2.3. Proposed Solution

We implement our proposed solution on all network nodes. To detect intrusion we combine two Intrusion detection systems: ABID and SBID. For ABID we use standard profile in NS simulation which uses statistical methods. In this method if the route reply messages of a node in 10 times more than its route request messages, this is a suspicious behavior and this node is an attacker.

This module is called “attack” in NS simulator. For SBID, our limitations are on the routing protocol of each node and the sequence number. If routing protocol behavior of a node was different from AODV routing protocol behavior (NS simulator does this comparison) or if the sequence number was higher than the threshold, this node behavior will be known a suspicious behavior and suspicious counter will increase one unit. The Threshold to limit the sequence number is 65536. This number is equivalent to 2^{16}. This number is based on try and error method. By using this threshold number we obtained the highest throughput and the lowest packets loss rate. We assumed the threshold number to be 65536 because the black hole node uses 32-bit sequence number which all of the bits is filled with 1. So if a node used 16-bit sequence number (which all of the bits is filled with 1), that node behavior will be considered as an attack. After detecting attacker, we offer a new intrusion response approach to encounter with this node. By viewing abnormal behavior in the network Nodes abnormal sequence number or abnormal routing protocol (from AODV routing protocol) on a node, its suspicious counter will increase one unit. If the suspicious counter of any node exceeded from number two, that node will be known as an attacker and should expel that node from the network. With try and error technique we assumed the threshold to be number two. Because ABID methods has high error rate and in most of the times detect normal as an attacker, so if a node is known as an attacker that node should expel from the network for a random time. After random time that suspicious node will be allowed to return to the network. After returning to the network, this node will be put in FIFO queue. We assign a flag with value one to this. If a node has been expelled and then has been forgiven and is in FIFO queue, this node has a flag with value one in its header. From now, other nodes send only information packets to nodes which are in FIFO queue and do not send them control packets (such as AODV control packets, route request packets, route reply packets and route error packets). It is for this reason that if the node was an attacker and the detection were not wrong, the attacker could not degrade AODV routing protocol performance. If 20% of the network nodes were in FIFO queue (They are forgiven nodes) we should exit them from queue with first in first out order and treat them like normal nodes and send them information and control massages. We should also omit their flag. Because of wrong detection rate of ABID, it is possible to detect a lot of nodes as an attacker node wrongly and then forgive them and put them in FIFO queue. After some time most of the network nodes will be in FIFO queue and other nodes won’t send them control massages, so there won’t be any routing process in the network and it would be a reason to degrade network performance. The 20% threshold is also based on try and error method. If a node were known as an attacker for the second time, this node will expelled from the network forever. This is because that if a node has suspicious behavior in limit circumstances that we create for a forgiven node, that node is an attacker with very high probability and our proposed IDS were not wrong in detecting and expelling this attacker node. A black hole node can attack the network in our limit circumstance again, because this node puts its sequence number the greatest 32-bit integer number and does not need other nodes to send him control packets. Pseudo code of this algorithm is proposed in Figure 1.



```
Do for All Nodes
If (Node Manner=Attack or Node Routing Protocol$\neq$AODV or Sequence Number $>65536$)
        Increase  Count
        If (Count $> 2$)
                If (Flag $= 1$)
                        Delete Node Forever
                Else
                        Delete Node
                End If
        End If
End For
At (Now - Random Time) Let Node Come Back to the Network
Node Flag $= 1$
Put Node in to FIFO Queue
Other Nodes Just Send Data Packets to a Node that Has a Flag for Forwarding
If (Queue Size $>$ 20% of All Nodes)
        Dequeue First Node in the Queue
        Delete Flag
End If
```

Fig. 1. Pseudo code of the proposed IDS algorithm.

3. *Analyze and Evaluating the Results of Proposed on*

We use NS-2 simulator. We simulate to simulate in different situations: An under black hole attack network which is not equipped with IDS, An under black hole attack network which is equipped with our proposed IDS, ABID, SBID large and small networks and with one and two black hole nodes. The details of our network simulations are proposed in Table 1.

Table 1

Parameters of simulation environments

Parameter			**Value**
Simulation area	*In small networks*		750m x 750m
	In large networks		1500m x 300m
Simulation time			500 s
Number of normal nodes	*In small networks*	*Single black hole attack*	19 nodes
		Cooperative black hole attack	18 nodes
	In large networks	*Single black hole attack*	59 nodes
		Cooperative black hole attack	58 nodes
Number of black hole nodes	*Single black hole attack*		1 node
	Cooperative black hole attack		2 nodes
Traffic type			UDP - CBR
Packet size			512 KB
Packet rate			10 kbps
Maximum node speed			20 m/s

Our simulation criteria in this paper are throughput, packet loss rate and packet delivery rate. First we define of each of these criteria: a) Throughput: The number of bits which will be sent per a unit time by source node to destination node in the network. b) Packet loss rate: The number of lost packets to the total Sent packets, c) Packet delivery rate: The number of packets which have been successfully transmitted to the sent packets [22].

We investigated the throughput of a small network which is under single black hole attack in different conditions in Figure 2. We investigated packets loss rate and packet delivery rate in these situations in Figure 3. We show in Figure 2 that the throughput in a network which is under single black hole attack has the lowest throughput, because no action is done to encounter black hole attack. The network throughput which is equipped with our IDS has the highest throughput in compare with the network which is equipped with ABID or SBID. Because our proposed IDS is the combination of ABID and SBID, our IDS can detect black hole node and encounter black hole attack earlier. Therefore, we decrease damage of black hole attack and increase throughput. Also, because of our intrusion response, we reduce wrong intrusion detection rate.

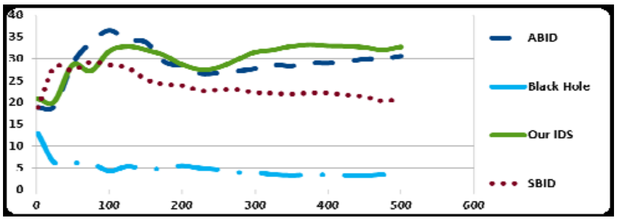


Fig. 2. Network throughput diagram in a small network which is under single black hole attack in different situations.

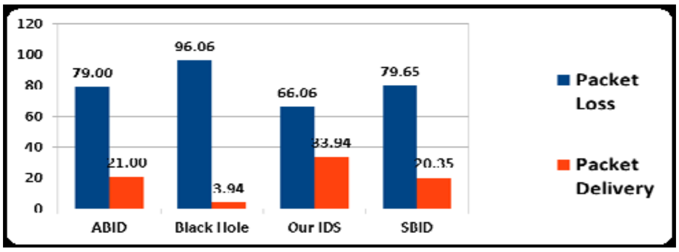


Fig. 3. Packet loss rate and packet delivery rate in a small network which is under single black hole attack in different situations.

We show the average of packet loss rate and the average of packet delivery rate in figure 3. The average of loss rate is the highest in a network which is under black hole attack because no action has been done to encounter black hole attack. The network which is equipped with our IDS and is under black hole attack has the lowest packet loss rate in compare with ABID and SBID. It is because our IDS is a combination of ABID and SBID, so our IDS can detect attack earlier and encounter with black hole node, there for we would have lower packet loss rate.

In figure 4, we present the throughput of a large network which is under single black hole attack in different situations. In Figure 5, we show the packet loss rate and packet delivery rate in a large network which is under single black hole attack in different situations. The results of these charts are similar to figures 2 and 3, but because the network is large and because of higher transmission the throughput is higher than small networks.

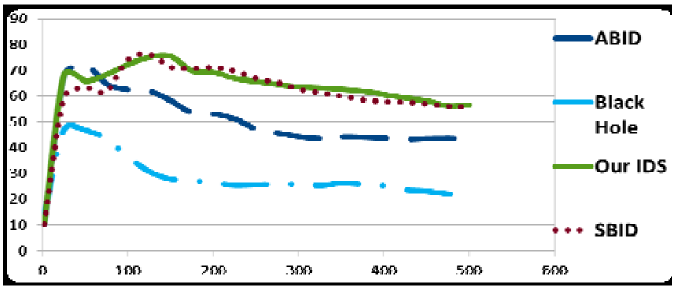


Fig. 4. The throughput of a larger network which is under single black hole attack in different situations.

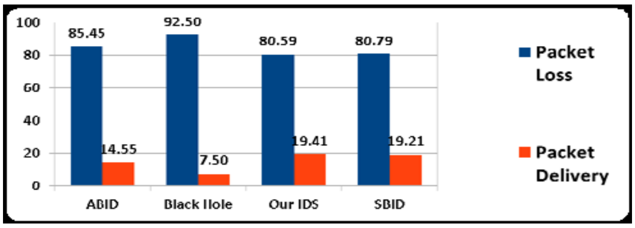


Fig. 5. The average of packet loss rate and the average of packet delivery rate in a large network which is under single black hole attack in different situations.

In figure 6 we can see the throughput of a small network which is under cooperative black hole attack in different situations and in figure 7, we can see the packet loss rate and the packet delivery rate in a small network which is under cooperative black hole attack in different situations. The results of these charts are similar to figures 2 and 3, but because of cooperative black hole attack we see the lower throughput and lower packet delivery rate. In Figure 8, we can see the throughput of a large network which is under cooperative black hole attack in different situations and in figure 9, we see the packets loss rate and the packet delivery rate of a large network which is under cooperative black hole attack in different situations. The results of these charts are similar to figures 4 and 5, but because of cooperative black hole attack we see the lower throughput and lower packet delivery rate.

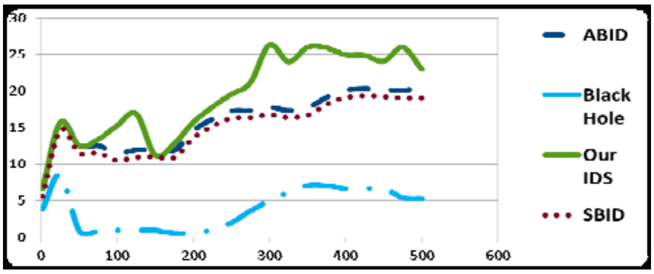


Fig. 6. The throughput of a small network which is under cooperative black hole attack in different situations.

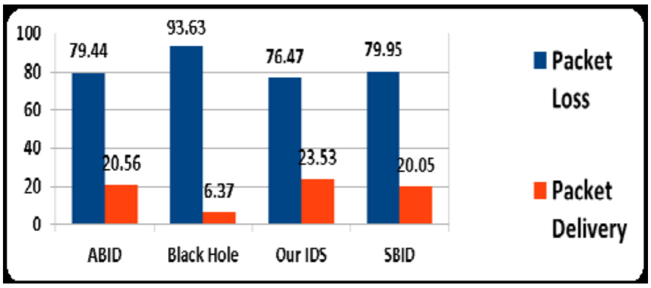


Fig. 7. The average of packet loss rate and the average of packet delivery rate in a small network which is under cooperative black hole attack in different situations.

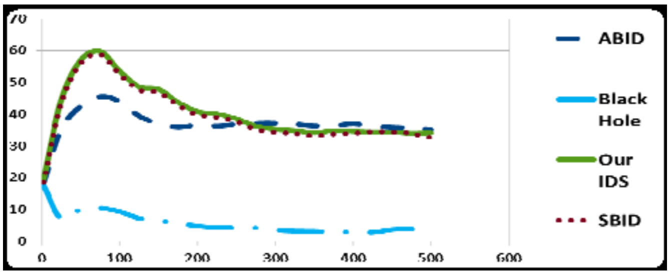


Fig. 8. The throughput of a large network which is under cooperative black hole attack in different situations.

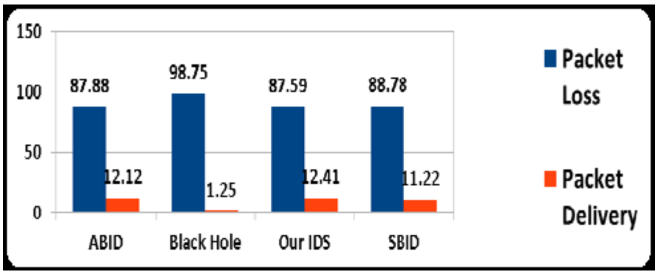


Fig. 9. The average of packet loss rate and the average of packet delivery rate in a large network which is under cooperative black hole attack in different situations.

3. Conclusion

In this paper we investigate a network in different situations: A normal network, an under attack with no IDS, with our IDS, with ABID and with SBID in large and small networks and with single and cooperative black hole attack. We found that the network throughput which is under black hole attack and is equipped with our IDS is higher than this network which is equipped with ABID or SBID. Also we found that the packet loss rate in our IDS is lower than ABID or SBID. These results are true in both large and small networks which are under single or cooperative black hole attacks. It is because our IDS is a combination of ABID and SBID, and also our IDS uses a new intrusion response. But, our IDS has high overhead.

To troubleshoot our proposed solution, we recommend that this IDS algorithm to deploy just I some nodes to reduce overhead. We recommend to deploy ABID and SBID in our IDS with other techniques. We also recommend to combine SBID and KBID.

References

[1] M.S. Isfahani and M. Aboali, "The intrusion detection system for encountering DoS attack by high route request", the third Conference of Information technology and knowledge, Ferdosi University of Mashhad, pp. 86-94, 1386.

[2] A. Bhandare, S. Patil and B. Pail, “Modified AODV Protocol to Prevent MANET Against Black Hole Attack and its Performance Analysis”, International Journal of Advanced Scientific and Technical Research, Vol. 4, 2013.

[3] A. Nadeem and M. Howarth, “An Intrusion Detection & Adaptive Response Mechanism for MANETs”, Elsevier International Journal of Ad Hoc Networks, Vol. 12, 2013.

[4] A. Deepa and V. Kavitha, “A Comprehensive Survey on Approaches to Intrusion Detection System”, Elsevier International Conference on Modeling Optimisation and Computing, Vol. 19, pp. 138-149, 2012.

[5] M. Mohanapriya and I. Krishnamurthi, “Modified DSR Protocol for Detection and Removal of Selective Black Hole Attack in MANET”, Elsevier International Journal of Computers and Electrical Engineering, Vol. 3, 2013.

[6] M. Su, “Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems”, Elsevier International Journal of Computer Communications, Vol. 34, 2011.

[7] S. Manikantan, C. Yu and A. Tricha, “Channel – Aware Detection of Black Hole Attacks in Mobile Ad Hoc Networks”, IEEE Global Telecommunications Conference, Vol. 3, pp. 100- 116, 2009.

[8] C. She, J. Wang, and H. Yang, “Intrusion Detection for Black Hole and Gray Hole in MANETs”, KSII Transactions on Internet and Information Systems, Vol. 9, pp. 70-77, 2013.

[9] S. Madhavi and H. Tai, “An Intrusion Detection System in Mobile Ad Hoc Networks”, International Journal of Security and Its Applications Vol. 2, 2008.

[10] H. Shahnawaz and S. Gupta, “Black Hole Attack in AODV & Friend Features Unique Extraction to Design Detection Engine for Intrusion Detection System in Mobile Ad Hoc Network”, Journal of Engineering Science and Technology, Vol. 7, 2012.

[11] M. Su, K. Chiang and W. Liao, “Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks”, IEEE International Symposium on Parallel and Distributed Processing with Applications, Vol. 10, 2010.

[12] Y. Yu, G. Lei, W. Xingwei and L. Cuixiang, “Routing Security Scheme Based on Reputation Evaluation in Hierarchical Ad Hoc Networks”, Wiley International Journal of Computer Networks, Vol.5, 2010.

[13] M. Su, “A Study of Deploying Intrusion Detection Systems in Mobile Ad Hoc Networks”, Elsevier International Conference on Electronic Engineering and Computer Science, Vol. 14, pp. 214-225, 2012.

[14] A. Nadeem and M. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”, IEEE Communications Surveys & Tutorials, Vol. 15, 2013.

[15] B. Xiao, B. Yu and G. Chemas, “Identify Suspect Nodes in Selective Forwarding Attacks”, Elsevier International Journal of Parallel Distributed Computing, Vol.67, 2007.

[16] T.Araghi, M. Zamani and A. Manaf, “A Survey for Prevention of Black Hole Attacks in Wireless Mobile Adhoc Networks Using IDS Agents”, International Journal of Latest Trends in Computational Science, Vol. 2, 2013.

[17] W. Wei, Z. Guosun, Y. Jing, W. Hanli and T. Daizhong, “Towards Reliable Self - Clustering Mobile Ad Hoc Networks”, Elsevier International Conference of Computer and Electronic Engineering, Vol. 10, pp. 38–62, 2012.

[18] S. Pathak and S. Jain, "A Survey: On Unicast Routing Protocols for Mobile Ad hoc Network", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, January 2013.

[19] K. Al–Omari and P. Sumar, "An Overview of Mobile Ad hoc Networks for the Existing Protocols and Applications", International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks, Vol. 2, March 2010.

[20] D. Roy, B. ebdutta and C. Rituparna, “BHIDS: A New, Cluster Based Algorithm for Black Hole IDS”, Wiley International Journal of Security and Communication Networks, Vol. 11, 2010.

[21] F. Tseng, L. Chou and H. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, Springer International Journal of Human - centric Computing and Information Sciences, Vol. 5, 2011.

[22] U. Venkanna and L. Velusamy, “Black Hole Attack and Their Counter Measure Based on Trust Management in MANET: A Survey” ,IEEE International Journal of Advances in Recent Technologies in Communication and Computing, Vol. 6, 2011.