A NEW IDS SCHEME AGAINST BLACKHOLE ATTACK TO ENHANCE SECURITY IN WIRELESS NETWORK

Shalini Sharma[1], Girish Tiwari[2]

[1]*ME Scholar, Department of Electronics and Communication Engineering, UEC, Ujjain, M.P. (India)*
shalini09.2010@gmail.com
[2]*Associate Professor, Department of Electronics and Communication Engineering, UEC, Ujjain, M.P. (India)*
tiwari_girish@yahoo.com

Abstract

The aim of this paper is to protect the wireless network against the blackhole attack. Blackhole attack, as the name suggest, drops all the packets forwarded to it. In this paper, we have proposed an intrusion detection system (IDS) scheme to detect the malicious node (blackhole node) and to nullify its effect in the network. The proposed IDS scheme in the presence of blackhole attack gives approximately similar result as that of in the absence of attack. The network comprises for the three modules (i) Default AODV, (ii) AODV in the presence of blackhole attack and (iii) IDS scheme in the presence of attack by considering some parameters such as end to end delay, throughput, packet delivery ratio, normalized routing load etc. The proposed algorithm has been simulated on Network Simulator version-2 (NS-2).

Key Words: *AODV, Blackhole attack, DSN, IDS scheme, routing misbehavior, security.*

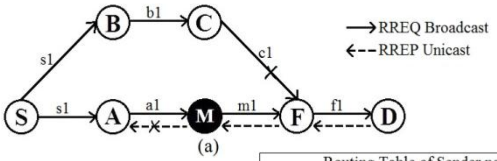
---***---

1. INTRODUCTION

In real-world, a network is used for supporting many applications, ranging from civilian to military, such as data collection, virtual classroom, conferences, search and rescue operations, etc. At that instant of time, many domains are working together to which a secure communication link is needed in between them. A security issue is always there while the communication is happening either in between a single domain or between different domains, but it is more difficult to find out the attacker when attacker belongs to in between a single domain because an insider attack has always more routing information than an outsider so it can harm the network easily. An inside attacker can act like two or more (virtual) destination node at a time and thus showing the shorter path for the packets to expel the data traffic which may lead to falsification.

Blackhole (BH) attack is one of the impersonation attacks, aims to enhance the congestion in the network. This attacker does not forward the received packets further, rather drops all of them. The effect of this attack is that the congestion in the network increases due to the continuous retransmissions from the sender node [1]. It sends the falsifying route request (RREQ) and route reply (RREP) packets to the route. It reduces the hop count (HC) or increases the destination sequence number (DSN) or do both to misguide the target nodes.

When sender node S broadcast RREQ to all its neighboring nodes to find a route to the destination D, malicious node M does not follow the routing protocol. Node M ignores to increase the hop count but intensely increases the DSN of the packet and forwards this false packet further to node F. Node F receives RREQ packet from both the nodes M and C but it considers packets from node M only because it has minimum hop count (Figure 1(b)). It rejects the legitimate RREQ from node C and updates its routing table according to the RREQ from node M (Figure 1(d)) and forward the routing packet further. Moreover, node F receives RREP from destination node and passes it to node M after updating its own routing table but node M does not forward this RREP packet further because it has the control over the link for sender node S. Therefore, sender node S never founds a route to the destination node D.



(a)

RREQ Packet

Last Hop	S	S	A	B	M	C	F
Next Hop	A	B	M	C	F	F	D
Source	S	S	S	S	S	S	S
Destination	D	D	D	D	D	D	D
RREQ	s1	s1	a1	b1	m1	c1	f1
Hop Count	0	0	1	1	1	2	2
DSN	1	1	1	1	2	1	2

(b)

Routing Table of Sender node			
Destination	Next Hop	DSN	Hop Count
S	0	0	0
D	-	-	-

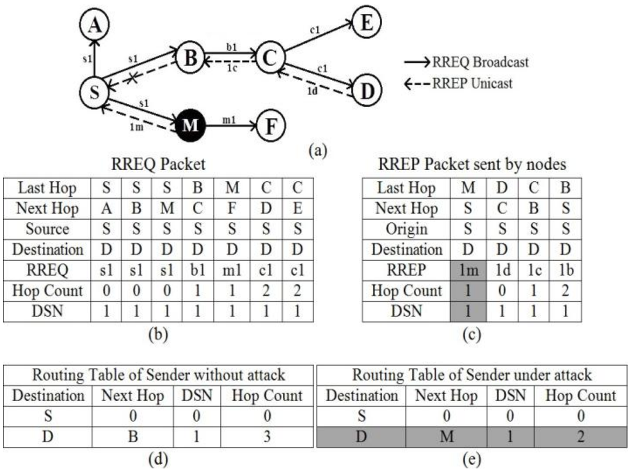
(c)

Routing Table of node F			
Destination	Next Hop	DSN	Hop Count
F	0	0	0
S	M	2	2
D	F	0	1

(d)

Figure 1: Blackhole Attack (RREQ Falsification)

In addition, malicious node also sends false RREP to the sender (Figure 2). When malicious node listens to the sender node to find a route to the destination node D, it sends forged RREP to the sender telling that it has the valid and the shortest path to the destination. As sender node does not have the knowledge of destination node, it receives RREP from node B also telling that it has a valid path to the destination but sender node considers node M as the legitimate node because node M gives the RREP with least hop count. Node S updates its routing table (Figure 2(e)) and sends the data packet to malicious node M.



RREQ Packet

Last Hop	S	S	S	B	M	C	C
Next Hop	A	B	M	C	F	D	E
Source	S	S	S	S	S	S	S
Destination	D	D	D	D	D	D	D
RREQ	s1	s1	s1	b1	m1	c1	c1
Hop Count	0	0	0	1	1	2	2
DSN	1	1	1	1	1	1	1

(b)

RREP Packet sent by nodes

Last Hop	M	D	C	B
Next Hop	S	C	B	S
Origin	S	S	S	S
Destination	D	D	D	D
RREP	1m	1d	1c	1b
Hop Count	1	0	1	2
DSN	1	1	1	1

(c)

Routing Table of Sender without attack			
Destination	Next Hop	DSN	Hop Count
S	0	0	0
D	B	1	3

(d)

Routing Table of Sender under attack			
Destination	Next Hop	DSN	Hop Count
S	0	0	0
D	M	1	2

(e)

Figure 2: Blackhole Attack (RREP Falsification)

2. PREVENTING BLACKHOLE ATTACK

Many researches have been done to secure the routing from Blackhole attack. They can be categorized into 3 categories, i.e. (i) Protocol Modification; (ii) Cryptography based protection and (iii) Intrusion Detection.

2.1 Protocol Modification

There are many modification mechanism have been proposed to enhance the existing protocol to provide the prevention from the blackhole attack. The cross-check method proposed by Deng et. al. [2] was a very common method to prevent the blackhole attack. The further researches have been done on cross check method by Weerasinghe et. al. [3], Yu, C.W. et. al. [4] and Zhang et. al. [5]. The degree of trust proposed by Raza et. al. [6], Al. Sharbaz et. al. [7] and Li, Jia et. al. [8] provides authority to each node in the network to calculate the level of trust of its all neighboring nodes.

2.2 Cryptography Based Protection

Cryptography has been done to protect the integrity of message and also to detect the false messages by using a digital signature. When a packet is damaged, it is easily recognizable if it cryptographically protected than if it is unprotected [9][10][11]. A hash function is also proposed by Sachan et. al. [12], Junhai et. al. [13], Basil et.al. [14] and Tsai et. al. [15] to maintain the probity of the routing packets.

2.3 Intrusion Detection System

IDS have been proposed for wired network previously where it can easily be installed in the wired devices but in the wireless infra-structureless network in a domain, it needs modification to be implemented to that network. R. Chaki [16] proposed a collaborative IDS which offers an architecture compatible with the heterogeneous nodes. Also, there are several distributed Agent-based IDS [17][18] developed at the lowest level of the analysis process of the different types of collected data. In this paper, our main aim is to propose a blackhole detection algorithm for an infra-structureless network in a domain.

3. PROPOSED WORK

In an infra-structureless network, there are various nodes which need to dynamically coordinate with each other to provide the routing service and to transmit the packets. Due to the open exposure and dynamic topology, security issues may raised in such wireless network. The presence of a malicious node in such types of network degrades the network performance in terms of throughput, packet delivery ratio, etc. The aim and role of the attacker node can be summarized in the following four steps:

Step. 1: Initially, the malicious node sends the forged information.
Step. 2: All the packets are dropped out by the malicious node by controlling the link.
Step. 3: Then, sender node continuously tries to retransmit the request packet after failure.
Step. 4: Therefore, the congestion in the network increases due to large number of routing packets which leads to degrade the performance of the network.

For an infra-structureless network, an adversary can act as blackhole attack while finding a route since it knows the routing information of the network. A blackhole attacker misguides the sender node by forwarding a false RREP which contains the least hop count and larger DSN. By sending false RREPs, it assures that sender will transmit the data packet and then it starts to drop them and hence drops the traffic at that route. In this paper, we assume that the malicious node increases its DSN only to misguide the sender node so that it can show itself as the destination node and receive all the data packets instead of the destination node.

This paper proposes an IDS algorithm to find out the malicious node by comparing the DSN of each neighboring node with threshold at each node in the network. If DSN of any node exceeds the threshold, the node that gets the knowledge at first spread the information about the node with exceeded DSN to all other nodes. Therefore, the sender node does not send the data packet to that route where the malicious node belongs, rather chooses one of the multiple route for the transmission. In this paper, we consider three following modules of routing to evaluate the performance of the network:

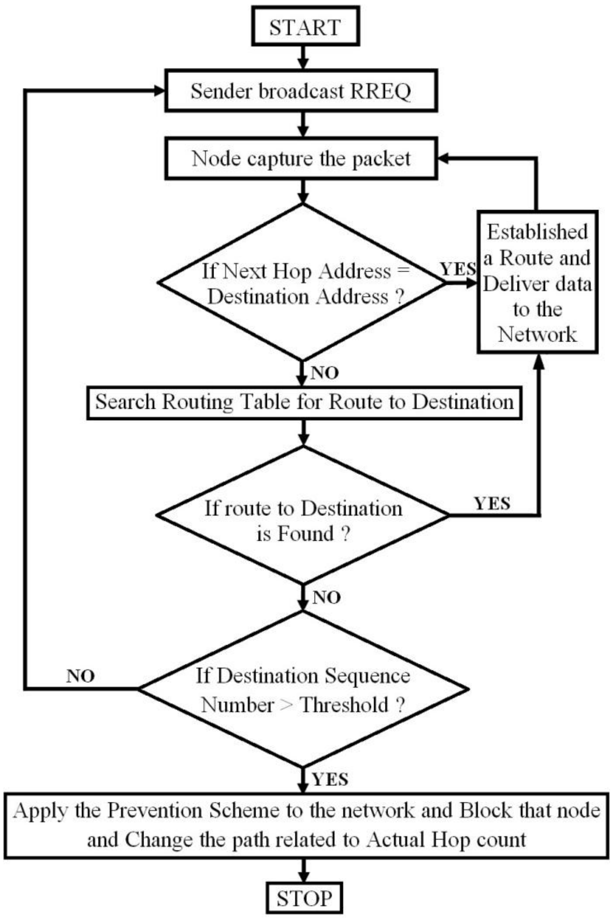
3.1 Default AODV (DAODV): To evaluate the performance of network in the absence of any attacker. AODV stands for Ad-hoc On demand Distance Vector routing protocol which is specially designed for the infra-structureless networks. It is capable to both the unicast and broadcast of the packets.

3.2 AODV in the presence of Blackhole Attack (BHAODV): To evaluate the performance of network in the presence of blackhole attack. The blackhole attack degrades the performance of the network by dropping the traffic at that route so that no sender can transmit the data through that route.

3.3 The proposed IDS algorithm in presence of blackhole attack (BHIDS): When IDS algorithm is applied to the network, malicious node acts as the simple node with no misguidance and valid routing information which leads to better performance even in the presence of attacker while it continuously eyed to disturb the routing.

4. PROCEDURE FOR PROPOSED IDS SCHEME

A flowchart for the proposed IDS scheme represents the steps followed by the participating nodes in the communication to identify the blackhole attack and to block the attacker to provide a secure transmission.


START
Sender broadcast RREQ
Node capture the packet
If Next Hop Address = Destination Address ?
YES
Established a Route and Deliver data to the Network
NO
Search Routing Table for Route to Destination
If route to Destination is Found ?
YES
NO
If Destination Sequence Number > Threshold ?
NO
YES
Apply the Prevention Scheme to the network and Block that node and Change the path related to Actual Hop count
STOP

Flowchart 1: The proposed schemeThe following steps describe the activity of an individual node participating in the communication:

Begin

Step. 1: The sender node broadcast the RREQ which contains both the sender address and destination address to all its neighbor nodes.

Step. 2: The destination node replies with RREP which contains source address and destination sequence number (DSN).

Step. 3: After receiving the reply packets, sender picks the packet with highest DSN.

Step. 4: Sender node updates its routing table as per given in the packet with highest DSN.

Step. 5: Then sender chooses the next hope from its routing table and send packet to that node for the destination node.

Step. 6: The next hop node captures the packet

Step. 7: It checks the destination address:

Step. 8: If next hop address = destination address; then Next hop node receives the packet.

Step. 9: Else; check its routing table step 4 (for next hop node).

Step. 10: If a route is found to the destination; then Next hop node receives the packet.Else;

Step. 11: If DSN > Threshold; the prevention scheme is applied and the node is kept silent and change the path to route the destination.

Step. 12: Else; Sender needs to broadcast the packet again.

Step. 13: End.

5. SIMULATION DESCRIPTION

The simulation for all the three modules i.e. DAODV (Default AODV without attack), BHAODV (AODV under Blackhole attack) and BHIDS (AODV with IDS algorithm against the attack) have been done in the Network Simulator version 2.35 (NS-2.35). The TCL (Tool Command Language) of these modules is simulated for 20, 40, 60, 80 and 100 nodes separately. The two ray ground radio-propagation model is used and the 802.11 IEEE standard is considered for the MAC layer. For this paper, a network with 750×750 meters dimension is created in a domain where all the nodes are kept under the AODV routing protocol. The simulation time is set to 500sec and the time of connection end is set to 451sec. Each node is selected with the transmission range of 250 meter. Initially, the nodes are allocated and then a mobility scenario file is generated to define the original location of the nodes and also the movement of nodes from one location to another location with the mobility of 20 meter per second. The simulation is considered for all the 20, 40, 60, 80 and 100 nodes, out of them 18 nodes are kept as the communicating nodes to evaluate the performance of network in all the three modules.

5.1 Performance Parameters

1. End to End Delay: The time taken for the actual delivery of the packet from the sender node to the intended recipient node is known as end to end delay. Generally it is measured in milliseconds and it takes into account the time taken for finding route, processing at intermediate nodes, retransmissions etc. The average end to end delay is defined as below

$$\text{Average End to End Delay} = \frac{\text{Total End to End Delay}}{\text{Number of packets sent}}$$

2. Average Throughput: Throughput is defined as the rate of successfully delivered packets over the communication link. The rate of received file by a host at any instant of time is called as the instantaneous throughput while the average throughput is the rate of delivered packets over a long period of time. Unit of the throughput is bits per time.

$$\text{Average Throughput} = \frac{\text{Total number of bits transmited}}{\text{Total time taken for transmission}}$$

3. Packet Delivery Ratio: PDR can be defined as the total number of packets delivered to the destination nodes per the total number of packets transmitted from sender nodes. It illustrates the level of delivery to the destination nodes.

$$\text{PDR} = \frac{\text{Total number of Packets Delivered}}{\text{Total number of Packets sent}}$$

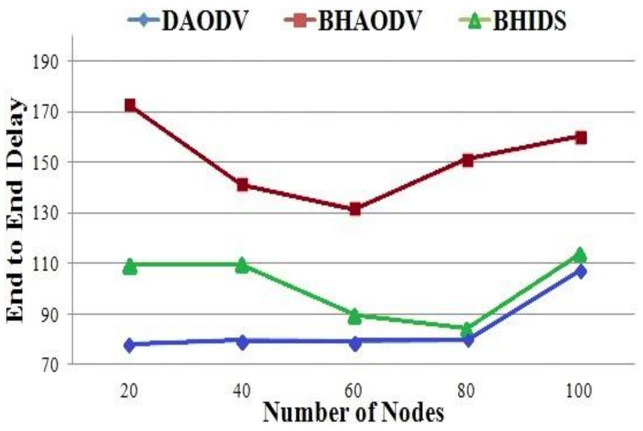
4. Normalized Routing Load: NRL can be defined as the ratio of total number of routing packets such as RREQ, RREP, etc. to the total number of data packets sent to the destination node. Each forwarded packet from the sender is considered as a single packet.

$$\text{NRL} = \frac{\text{Number of routing packets sent}}{\text{Number of data packet sent}}$$

6. RESULTS AND DISCUSSIONS

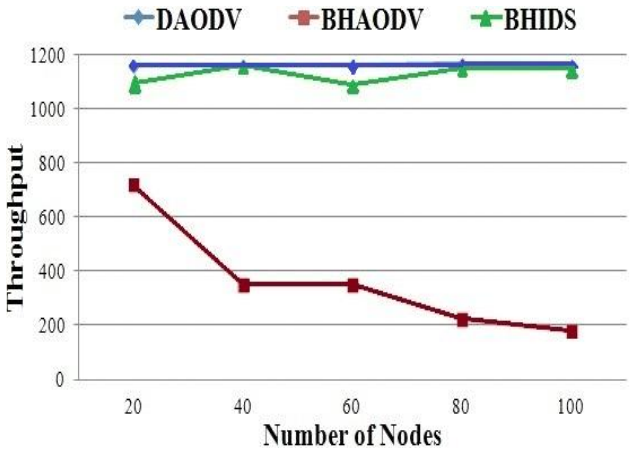
The result is evaluated by considering the performance parameters.

In Graph 1, the analysis of end to end delay is measured in case of default AODV, AODV with attack and proposed IDS scheme with node density of 20, 40, 60, 80 and 100. By observing this, we can see that the end to end delay is increases in the presence of attack as the attacker drops the packets transmitted through it which makes the sender to check its routing table again and again which leads a considerable delay in the transmission of the packets from the sender node. Moreover, delay is also advertised with the un-stable routes which have same DSN. End to end delay increases due to the attacker which can be shown easily in the trace file. This delay is considerably reduced when the IDS algorithm is applied to the network which identifies the adversary and obstructs its activities and provides an attack free network.



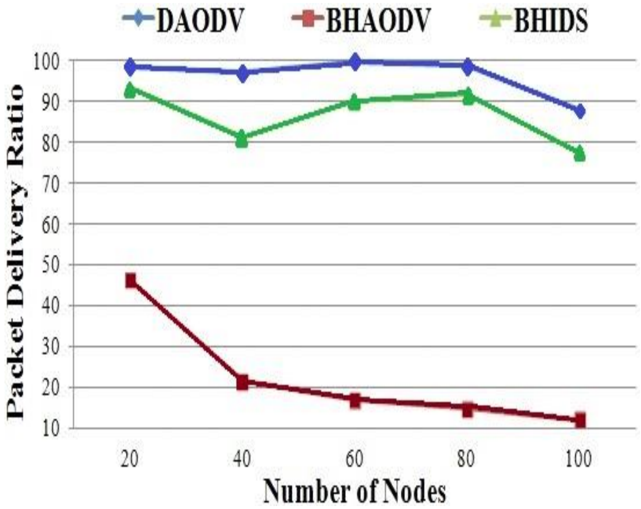
Graph 1: Analysis of End to End Delay vs. Node Density

Graph 2 shows the analysis graph of throughput for all the three modules with node density of 20, 40, 60, 80 and 100. Delivery of data is not safe when an attacker exists in the network; attacker drops all the data packets coming to it which tends minimum delivery of the packets. Thus, throughput decreases in the presence of attacker which can be seen easily in the graph. The throughput in case of IDS scheme is approximate equal to the range of default AODV which shows the better performance of routing in presence of IDS scheme over the attacker's effect. The reason behind is that the IDS scheme block the route where attacker exists and establish an alternative route for the reliable transmission of data packets.



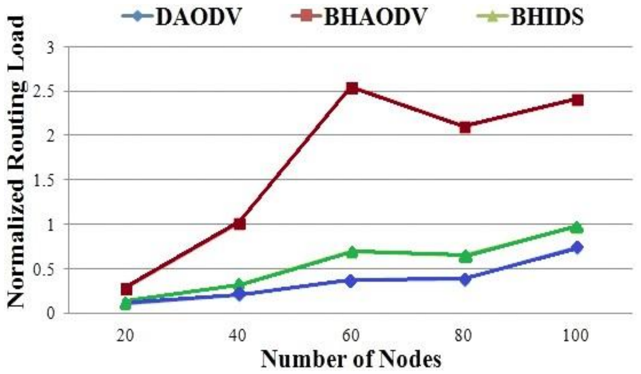
Graph 2: Analysis of Throughput vs. Node Density

In Graph 3, packet delivery ratio is measured with respect to the number of nodes for the default AODV, attack and IDS scheme. Packet delivery ratio shows the percentage of the packets which are successfully delivered out of the total transmitted packets. Packet delivery ration is direct related to the throughput i.e. when through is decreases, packet delivery ration is also decreases. Delivery of packets are reduces in the presence of attack and it improves when IDS scheme is proposed to the network. The PDR is increases about 90% in case of IDS scheme and it is almost equal to the performance of the default AODV.



Graph 3: Analysis of Packet Delivery Ratio vs. Node Density

The routing load is accounted through the delivered number of routing packets. As comparing both the throughput and normalized routing load, it is considerable that as throughput decreases, NRL increases simultaneously increases (Graph 4) which means that when attacker drops the data packets and does not send the recipient acknowledge to the sender, sender considers that data packet is failed to reach to the destination and then it checks it routing table and send RREQ again to the network which increases the congestion that tends to increase the load on route. This load is reduces by blocking that attacker which is done by IDS scheme which leads a considerable improvement in the throughput through which the normalized load is also decreased.



Graph 4: Analysis of NRL vs. Node Density

7. CONCLUSION

The aim of the IDS scheme is seem to detect the attacker; however the goal is not only to identify the attacker but also to stop its activities to provide an accurate and secure routing to the network. To provide an accurate route, the scenario has better throughput and minimized routing load but it compromises with the delay due to the alternative selection of the path for the best transmission of data packets. The performance of the IDS scheme for AODV is nearly equal to the performance of default AODV. In this paper, we have considered only one malicious node in a single domain network. In future, we can extend our research work by taking into account multiple malicious nodes and a multi domain network.

REFERNCES

[1]. Satria Mandala, Abdul Hanan Abdullah, Abdul Samad Ismail, abibollah Haron, Md. Asri Ngadi, Yahaya Coulibaly, "*A Review of Blackhole Attack in Mobile Adhoc Network*", International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME) 339 Bandung, November 7-8, 2013.

[2]. Hongmei Deng, Li, W., and Agrawal, D.P., "Routing security in wireless ad hoc network", Communications Magazine, IEEE (Volume: 40, Issue: 10), pp. 70-75.

[3]. Hesiri Weerasinghe, Huirong Fu, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation", Proceedings of the Future Generation Communication and Networking, Vol. 2, pp. 362-367.

[4]. Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Algorithm for the Detection and Elimination of Multiple Black Hole Nodes in Ad Hoc Networks", IEICET Commun, 2009, E92b, (2), pp. 483-490.

[5]. XiaoYang Zhang, Sekiya Y., Wakahara Y., "Proposal of a Method to Detect Black Hole Attack in MANET", International Symposium on Autonomous Decentralized Systems, IEEE, 2009, pp. 149-154.

[6]. Imran Raza, S.A. Hussain, "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes", Computer Communication, 2008, Vol. 31, pp. 1796-1802.

[7]. Li, F.Z., Al-Sharbaz, A., Jassim, S., and Adams, C., "Credibility based secure route finding in wireless ad hoc networks", Mobile Multimedia/Image Processing, Security, and Applications, 2008.

[8]. Li, X., Jia, Z., Zhang, P., Zhang, R., and Wang, H., "Trust-based on demand multipath routing in mobile ad hoc networks", Information Security, IET, 2010, Vol. 4, pp. 212-232.

[9]. Stallings, W., "Cryptography and Network Security Principles and Practice", Pearson Education, Inc, 2011, 5Ed.

[10]. Stallings, W., "Network Security Essentials: Applications and Standards", Pearson Education, Inc., 2011, 4Ed.

[11]. Girish Tiwari, Shalini Sharma, "Wireless Multi-Domain Network: A Study of Routing Protocols and Security Enhancements", International Journal of Computer Science and Information Technologies, Vol. 6 (3), 2015, pp. 3017-3022.

[12]. Preeti Sachan, P.M. Khilar, "Authenticated Routing for Ad-Hoc On- Demand Distance Vector Routing Protocol", Advances in Network Security and Applications, 2011, 196, pp. 364-373.

[13]. Junhai Luo, Mingyu Fan, Danxia Ye, "Black hole attack prevention based on authentication mechanism", Proc. 11th IEEE International Conference on Communication Systems, Singapore, 19-21 Nov 2008, pp.173-177.

[14]. C. Basile, Z. Kalbarczyk, R.K. Iyer, "Inner-Circle Consistency for Wireless Ad Hoc Networks", Transactions on Mobile Computing, IEEE, 2007, 6, (1), pp. 39-55.

[15]. Yuh-Ren Tsai, Shiuh-Jeng Wang, "Routing security and authentication mechanism for mobile ad hoc networks", IEEE 60th Vehicular Technology Conference, 2004, Vol. 7, pp. 4716-4720.

[16]. R. Chaki, N. Chaki, "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network", Proceedings of the IEEE International Conference on Computer Information Systems and Industrial Management Applications (CISIM 2007), pp. 179-184, 2007.

[17]. Semih Dokurer,Y.m. Erten, Can Erkin Acar, "Performance Analysis of ad hoc network under black hole attack" 1-4244-1024-0, IEEE, 2007, pp. 148-153.

[18]. D. Dasgupta and H. Brian, "Mobile Security Agents for Network Traffic Analysis", Proceedings of DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01, Volume: 2, 2001, pp. 332–340.