IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Mechanism for Detecting Black Hole Attack in Infrastructure-Less MANET (MDB-MAN)

Syed Muqtar Ahmed[1*], Syed Abdul Sattar[2]

[1]Department of Computer Science, Research Scholar of Rayalaseema University, ID: PP.COMP.SCI & ENG.083, Kurnool, Andhra Pradesh, India
[2]Department of Electronics and Communication, Nawab Shah Alam College of Engineering and Technology, Hyderabad, Telengana, India

[*]*Corresponding Author: syedmuqtar@yahoo.com, Tel.: +00-9963102912*

Available online at: www.ijcseonline.org

Accepted: 27/Dec/2018, Published: 31/Dec/2018

Abstract— Mobile Adhoc Network (MANET) is a self-organized group of wireless nodes forming a tentative network. In MANET nodes would be randomly changing their positions due to its dynamic infrastructure-less property. Therefore it is more susceptible to Black-Hole & Gray-Hole attacks, which are considered as serious attacks to the network. So far several solutions have been developed for MANET but many of them are not efficient. The main purpose of this paper is to present a solution known as mechanism for detecting Black Hole Attack in Infrastructure-Less MANET (MDB-MAN). An Algorithm is developed to detect Black-Hole node based on reactive Adhoc on demand distance vector protocol (AODV), where routes are established on demand. Several times simulations were conducted on proposed model using Network Simulator and found that the Packet Delivery Ratio (PDR) and Throughput is almost similar at time instant 50 msec. as compared to original AODV protocol. The Packet Drop Ratio keeps on changing as time changes and it can be tolerable.

***Keywords*—** MANET, AODV, MDB-MAN, Black-Hole attack, Gray-Hole attack

I. INTRODUCTION

Mobile Adhoc network consists of group of wireless nodes which are moving freely from one end to other within the domain of network without the help of pre-existing infrastructure. The MANET is self-organized network in which mobile nodes or devices would be added or deleted dynamically at any time [1]. Therefore, MANET is suitable for that type of areas where fixed wired network could not be setup easily. In MANET, different movable & portable devices are assumed to be connected with the help of routing protocols [2]. Routing protocols have been classified into three categories namely Reactive protocols: Example: AODV & DSR Proactive Protocols: Example: OLSR and Hybrid protocols: Example: ZRP [3]. In today's wireless communication, the Adhoc network could not be isolated from our daily routine work; especially in military and emergency services.

Many researchers have been involved to show different solutions on Black-Hole attack but still they are not effective. In this paper, we present a solution to identify and detect the Black-Hole attack. Our paper is organized as follows: Section-I contains the introduction to Adhoc on demand distance vector protocol, Intrusion Detection System and Black-Hole attack, Section-II contains a related work done by several researchers with their solutions, Section-III is about the proposed Algorithm with Flow chart and configuration of Black-Hole node. Section-IV is about Simulation, Section-V describes Results and discussion and Section-VI concludes the research work.

I. I. Adhoc on Demand Distance Vector Protocol

Adhoc on demand distance vector (AODV) Protocol has been designed for mobile Adhoc networks (MANET). Our proposed solution is based on AODV protocol. This protocol would establish the link from source to destination, whenever it is required. I.e. on-demand policy. AODV would maintain the routes in the routing table with the help of different packet parameters like Source Address, Source Sequence number, Broadcast Id, Destination Address and Hop-Count. AODV works on two strategies like Route-Discovery and Route-Maintenance [4]. The first step of this protocol is to send a RREQ (Route-Request) to all the adjacent nodes that are directly connected to source node. The process of sending a RREQ simultaneously to all nodes is known as flooding. Once RREQ is received, every node would update its routing table to maintain current status. The RREP (Route-Reply) is send back to source either by intermediate neighbour or destination node to complete the round trip journey in the form of acknowledgement and to ensure that it has the optimal route to destination with less number of hops.

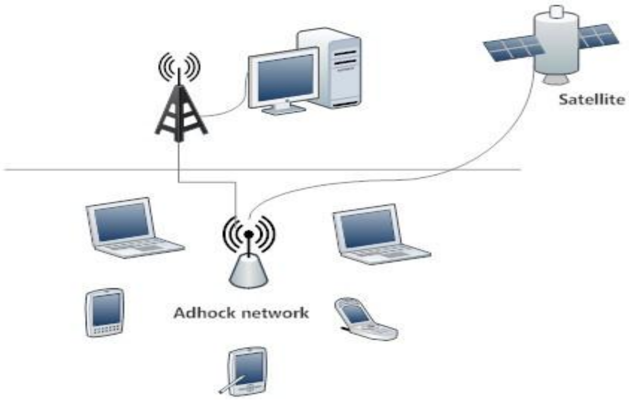

Fig-1 Mobile Adhoc Network

I.II. Intrusion Detection System

The main purpose of Intrusion Detection System (IDS) is to identify and detect the malicious behaviour of Intruder in the network. Intrusion Detection System is basically used for monitoring all operational parameters of Wired or Wireless networks. Over two decades different categories of IDS have been developed. The traditional types of IDS were failed to analyse the data properly as they work on log-files within the Operating Systems. Therefore, we need both software and hardware IDS solutions to provide full security to our data and network as well. One of the categories of IDS is Distributed IDS which could be used on several nodes to collect and analyse parameters. The main design issue in the Distributed IDS is the communication between Components within the System Architecture [5].

I.III. Black-Hole Attack

Black Hole attack is one of the most dangerous threat to the network security, which could degrade the overall performance of MANET. One of the nodes could be a Black-Hole-Node (B-H-N) node that acts like an attacker. As soon as B-H-N node receives RREQ from source, it will send RREP, ensuring that it has the best route to destination with less number of hops in order to deceive the other nodes in the network. Hence, the packets are delivered to a B-H-N and ultimately packets are drop or may be forwarded to any other B-H-N (if it is available in the network). Black Hole Attacks have been divided into two categories namely Single Black-Hole Attack and Collaborative-Hole Attack [6]. In this paper, we are working on Single-Hole Attack. To explain the Single-Hole Attack, we assume the scenario of Fig-2. In this, N0, N1, N2……N14 are the nodes. N0 is a source, N5 is Black-Hole-Node and N14 is considered as Destination.

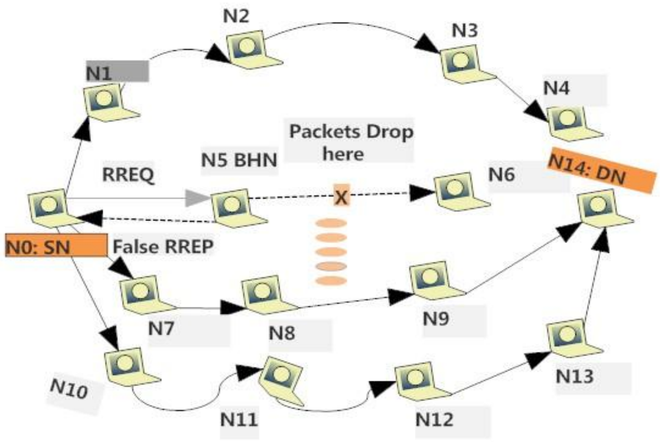

Fig-2: RREQ-RREP in Black-Hole Node (B-H-N)

The Summary of Fig-2 RREQ-RREP is conducted with AODV protocol as follows:

- N0 broadcast RREQ to all neighbours (N1, N5, N7 and N10).
- Assume that N5 is Black-Hole Node (BHN).
- N5 will backtrack to N0 by false RREP, saying that it has the optimal route to destination with less number of hops.
- N0 store the false information in its routing table and deliver packets to N5 (B-H-N). Simply N5 discard the packets instead of forwarding to N14.

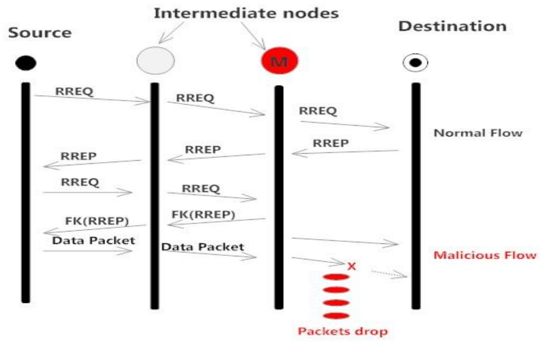

Fig-3 Sequence diagram of Black-Hole node

II. RELATED WORK

Many solutions have been presented with different techniques to solve the Black-Hole Attack in MANET which are discussed in this section:

Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre proposed a Watchdog technique which uses two different tables namely Pending-Packet table (PPT) and Node-Rating table (NRT). Both the tables store the data related with Source-Address (SA), Destination-Address (DA), Next hop-Count (H-Count) and Packet-ID (P-ID). In PPT, initially the packets are placed in the queue and later on it check the address of next neighbour and forward to it. NRT holds the data related with drop packets. In order to detect Black-Hole node, the watchdog technique uses the ratio between Packets delivered and Packets drop. If the ratio is above the Threshold value (TH) then it is assumed that node as a Black-Hole-Node [7].

BDSR scheme for DSR based MANET was proposed by Po-Chun Tsou, Jian-Ming Chang, Yi-Hsuan Lin, HanChieh Chao and Jiann-Liang Chen, which is based on Dynamic Source Routing. It uses Virtual-Address to make sure that Black-Hole node must send RREP when source node delivers RREQ [8].

Raj and Swadas presented a technique that compares the Sequence-number (SN) with Threshold updated value. If the SN>THV then the neighbour node is considered as malicious and this node is send to black list [9].

Lalit and L. Himral, V. Vig, and N. Chand, presented a method to prevent intruder node by checking the First RREP received from neighbour. If the Sequence-Number (SN) of neighbours node is much greater than the SN of Source node then it is assumed as Black-Hole node and the entry will be erased from the Routing Table [10].

Helio Mendes Salmon et al. presented a method based on Artificial-Immune System for Intrusion Detection. This method shows the results with Low-Positive value and increases efficiency of system but the Total End-End-delay is also increased [11].

Sanjay K. Dhurandher , Isaac Woungang , Raveena Mathur , Prashant Khurana proposed a GAODV Protocol which is based on Acknowledgement packets (RREP) send by neighbours to source for detecting Black hole attack. The technique shows that Data-Delivery ratio is improved compared to original AODV [12].

Rutvji proposed an approach to mitigate Black-Hole and Gray-Hole attacks. They have modified the name of previous Algorithm known as R-AODV to MR-AODV and even they have removed the limitastions from R-AODV. During Discovery phase they could able to separate Black-Hole and Gray-Hole nodes and establish a new secure path to deliver data. MR-AODV is a reliable solution configured with multiple simulation parameters that increases the Packet Delivery Ratio and acceptable Average End-End-Delay [13]. Murugan et.al presented a method which uses cluster technique and cryptography to detect Black-Hole attack. It provides better security using Secret-key and Threshold-Cryptography with in the network [14]. Michiardi and Molva proposed a Core scheme in which every node calculate a reputation value for every neighbour, based on watchdog scheme [15]. The Black-Hole attack effects on the overall performance of MANET. Its simulation is carried out in OPNET [16].

III. METHODOLOGY

This section explains an Algorithm of MDB-MAN with comments as shown below in green text.

Assume [S0: Source, Ni may be any intermediate node, RREQ: Route Request Packet, RREP: Route Reply Packet, TL=Time to live, mxt: maximum Threshold, PSA: Packet Source Address, FL: False Route, DP: Data Packet].

```
---------------------------------------------------------------------------
1.  Procedure Black_Hole( )
2.  h_count=0;          //hop count is initialized to Zero
3.  for i = 1 to N      // 1,2,3,….N number of neighbors
4.  S0:Broadcast PREQ   // Send PREQ simultaneously
                        //to all neighbors
5.  Ni ← PREQ           // Neighbors receive PREQ
6.  if (Ni(Addr) = = PSA)   /* Check if there is an entry
    of source and destination Address in
    Routing table of neighbor. */
    S0 ←Ni (FL[RREP])       /* Black-Hole node(N5)
    generate False RREP & send to source */
     else
    Ni+1← RREQ      /* Otherwise; RREQ is appended
    to another neighbor. */
    end if

7.  Ni ← S0[DP]         /* Source send Data Packet to
    Malicious node and it will drop packets. */

8.  If (RREQ = = TRUE && (hop_count=TL)
    Display "Drop Packets"          // Drop packets
    else
    hop_count - = hop_count     /* hop count is
    decremented by one. */
    Display "Forward Packets" // Forward packets to
    other node. */
    end if
9.  Ni-1 ← RREP
    If (hop_count > mxt)        /* Check whether hop
    count is greater than maximum threshold value. */
    Display "Dangerous: Black Hole Node"
    else
    Display "Normal Node"
    end if
10. All routes to Black-Hole node are blocked
    end for loop
    end Black-Hole Procedure
---------------------------------------------------------------------------
```

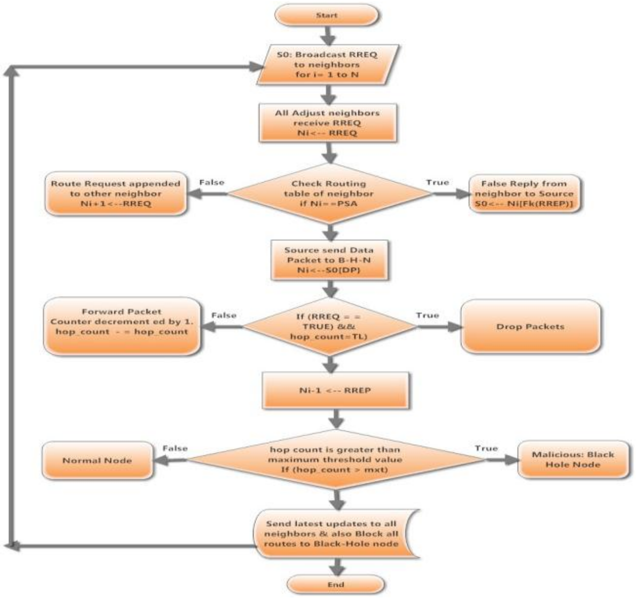
Start
S0: Broadcast RREQ to neighbors for i= 1 to N
All Adjust neighbors receive RREQ Ni<-- RREQ
Check Routing table of neighbor if Ni= =PSA
False
Route Request appended to other neighbor Ni+1<--RREQ
True
False Reply from neighbor to Source S0<-- Ni[Fk(RREP)]
Source send Data Packet to B-H-N Ni<--S0[DP]
If (RREQ = = TRUE) && hop_count=TL)
False
Forward Packet Counter decrement ed by 1. hop_count - = hop_count
True
Drop Packets
Ni-1 <-- RREP
hop count is greater than maximum threshold value If (hop_count > mxt)
False
Normal Node
True
Malicious: Black Hole Node
Send latest updates to all neighbors & also Block all routes to Black-Hole node
End

Fig-4 Flow chart of MDB-MAN

1V. SIMULATION

Simulation of MDB-MAN for adding Black-Hole node can be done with the following Steps:

1. Install ns-allinone package under Ubuntu Operating system.
2. Under Aodv.h & Aodv.cc add Black-Hole (malicious) agents.

Under Aodv.h add the following code:

bool BHN_malicious;

a) Under Aodv.cc add the following code to the constructor of Aodv class:

BHN_malicious = false;

b) Goto Aodv::command( ) class, add the following code:

```
If(Strcmp(argv[1], "BHN_malicious") = = 0)

 {

BHN_malicious = true;

return TCL_OK;

}
```

c) Goto AODV: rt_resolve(packet *) class, add the following code:

```
#define DROP_MALICIOUS "BHN_malicious"

If (BHN_malicious = = true)

{

drop (p, DROP_BHN_malicious);
```

d) Goto project and clean

3. Initial route is assumed as **N0→N8→N9→N10→N14** where N0: Source node, N14: Destination node and N8, N9, N10 are Intermediate nodes.
4. Configure Black-Hole node in TCL Script (N6 is Black-Hole node for our network) with the following code:

```
$ ns at 0.0 "[N6 set ragent _ ] BHN_malicious"
$ ns color brown
$ns at 0.0 "$N6 label BHN_malicious"
```

V. RESULTS AND DISCUSSION

The simulation of our solution is done under NS-2.35. The Black-Hole node in our network either drops the packet or play with in the network to forward packets to another malicious node, which may degrade the overall performance of system. To resolve this issue, we have combined some functionality of our solution into AODV protocol. The proposed technique identify and detects the Black-Hole node and broadcast information to all neighbours to delete its entry from their routing tables and block all further packet transmission. The following Fig-5 is the Screenshots of simulation and table-1 shows the simulation parameters.

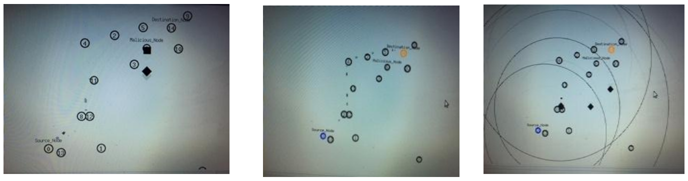

Fig-5 Screenshots of Simulation

V.I. Metrics for Simulation

Packet Delivery Ratio (PDR): The ratio of total of received packets to the total of send packets. If we want to have the optimal performance of network then we need to have high PDR. It is calculated by the following equation.

$$PDR(MDB) = (\sum packets\ Received/\sum Pakets\ send) * 100 \quad \text{--- (1)}$$

Throughput: The total number of bits delivered/sec.

The unit of throughput is in Kbps.

$$Throug\,hput\,(MDB) = Receive\ Line * (End\ time - Start\ time) * (\frac{8}{1000})$$

--- (2)

Packet Drop Ratio: It is the difference between Packets send & Packets received divided by packets send.

$$Packet - Drop - Ratio(MDB) = (Send\ Line - Received\ Line / Send\ Line) * 100$$

--- (3)

Table-1: AODV Data

Time (msec)	Packet Send	Packet Received	PDR (%) AODV	P_Drop_Ratio (%) AODV	Throughput (Kbps) AODV
10	1188	1090	91.75	8.25	597.64
20	3579	3454	96.5	3.49	808.51
30	6625	6500	98.11	1.89	965.85
40	9635	9510	98.7	1.3	1036.01
50	12655	12530	99.01	0.99	1078.44
60	15684	15559	99.2	0.8	1068.67

Table-2: MDB-MAN Data

Time (msec)	Packet Send	Packet Received	PDR (%) MDB-MAN	P_Drop_Ratio (%) MDB-MAN	Throughput (Kbps) MDB-MAN
10	1188	750	63.45	36.86	413.29
20	3579	2432	67.95	32.04	596.3
30	6625	5212	78.61	21.32	773.84
40	9635	8305	86.19	13.8	904.61
50	12655	11446	90.46	9.55	985.31
60	15684	14027	89.43	10.56	963.41

The Fig- shows that PDR for MDB-MAN is almost similar to AODV protocol at time instant 50 msec. Its keep on changing for rest of the time.

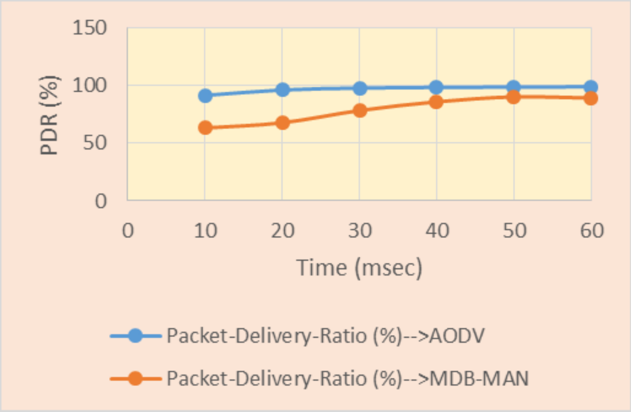

Fig-6: Time Vs Packet Delivery Ratio

Table-3: Simulation Parameters

#No.	Parameters	Items
1.	Software	NS-2
2.	Topology Area Size	850m x 850m
3.	MANET Protocol	AODV
4.	Wireless Standard	IEEE 802.11
5.	Packet Size (Bytes)	512
6.	Total Number of Nodes	15
7.	Number of Malicious Node	1
8.	Simulation Time (msec)	10,20,30,40,50,60
9.	Traffic Pattern	CBR/TCP
10.	Propagation	Two ray ground

The Fig-7 shows that Throughput of MDB-MAN is similar to AODV protocol at time instant 40 and 50 msec.

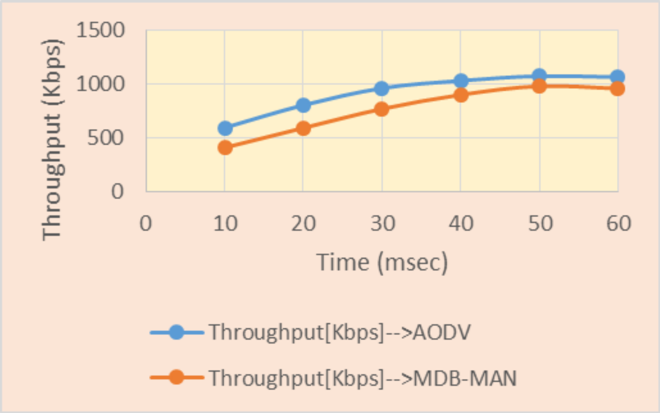

Fig-7: Time Vs Throughput

The Fig-8 shows that Packet-Drop-Ratio of MDB-MAN. It is near to AODV curve at time instant 50 msec. and for rest of the time it keeps on changing.

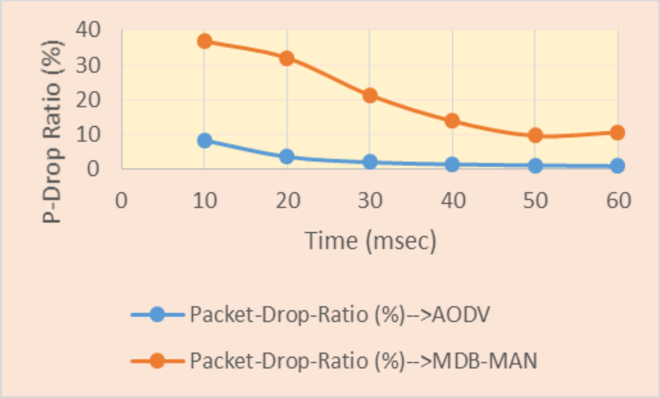

Fig-8: Time Vs Packet-Drop-Ratio

VI. CONCLUSION

The Wireless mobile Adhoc network is infrastructure–less network and it is subjected to be vulnerable. Hence, security issues arises. The bad behaviour of malicious node would take the advantage of this network and try to attack on it. The proposed MDB-MAN Algorithm identify and detect the Black-Hole node, which is considered as one of danger attack on MANET. Our Simulation results presented are efficient in terms of Packet Delivery Ratio and Throughput, which is almost near to the original value of AODV protocol at time instant 50 msec. The Packet-Drop-Ratio is varied as time changes and it can be tolerable. Therefore, the proposed solution is efficient. In future, our solution could be extended with Clustering of nodes.

REFERENCES

[1] S. Jain, N. Hemrajan, S. Srivastava, “Simulation and Analysis of Performance Parameters for Black Hole and Flooding Attack in MANET Using AODV Protocol”, International Journal of Scientific & Technology Research Vol. 2, Issue. 7, pp. 66-69, July 2013.

[2] A. Patel and A. Jain, “A study of various Black Hole Attack techniques and IDS in MANET”, International Journal of Advanced Computer Technology, Vol. 4, Issue. 3, pp. 58-62, 2016.

[3] R. Garg, V. Mongia, “ Mitigation of Black Hole Attack in Mobile Ad-Hoc Network Using Artificial Intelligence Technique”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology , Vol. 3, Issue. 1, pp. 1168-1174, 2018.

[4] S. Muqtar Ahmed and S. Abdul Sattar, “International Journal of Computer Science and Engineering”, Vol. 6, Issue. 11, pp. 77-82, 2018.

[5] M. Jahnke, J. T¨olle, S. Lettgen, M. Bussmann, and U. Weddige, “A Robust SNMP Based Infrastructure for Intrusion Detection and Response in Tactical MANETs”, Springer-Verlag Berlin Heidelberg, pp. 164–180, 2006.

[6] I. Saada, M. Z. Rashad, R. H. Sakr, “Implementing and Comparing LIDBPP (Local Intrusion Detection by Bluff Probe Packet)”, International Journal of Computer Science and Network Security, Vol.16 Issue.8, pp. 20-24, August 2016.

[7] A. A. Bhosle, T. P. Thosar and S. Mehatre, “Black-Holeand Wormhole Attack in Routing Protocol AODV in MAN”, International Journal of Computer Science, Engineering and Applications, Vol. 2, No.1, February 2012.

[8] P.C. TSOU, J. Ming CHANG, Y.Hsuan LIN, H.Chieh CHAO, J. Liang CHEN, “Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs”, 13th International Conference on Advanced Communication Technology, ICAC-2011.

[9] P. N. Raj and P. B. Swadas, “DPRAODV: A dyanamic learning system against black hole attack in aodv based manet”, IJCSI International Journal of Computer Science Issues, vol. 2, pp. 54–59, 2009.

[10]. L. Himral, V. Vig, and N. Chand, "Preventing Aodv Routing Protocol From Black Hole Attack", International Journal of Engineering Science and Technology (IJEST), Vol .3, 2011.

[11]. H. M. Salmon, C. M. d. Farias, P. Loureiro, L. Pirmez, "Intrusion Detection System for Wireless Sensor Networks Using Danger Theory Immune-Inspired Techniques", International Journal of Wireless Information Networks, Vol. 20, Issue.1, pp. 39-66, 2013.

[12] S. K. Dhurandher, I. Woungang , R. Mathur , P. Khurana, “GAODV: A Modified AODV Against Single and Collaborative Black Hole Attacks in MANETs”, 27th International Conference on Advanced Information Networking and Applications Workshops, 2013.

[13] Rutvij, H.J., “MR-AODV: A solution to mitigate black hole and gray hole attacks in AODV based MANETs. Pro”, 3rd International Conference on Advanced Computing and Communication Technologies, CCT-2013.

[14] R. Murugan, A. Shanmugam, “Cluster Based Node Misbehaviour Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks”, International Journal of Computer Science and Security 3 Vol. 6; Issue. 3; Start page: 188, 2012.

[15] U. K. Singh, J. Patidar and K. C. Phuleriya, “On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks”, International Journal of Scientific Research in Computer Science & Engineering”, Volume-3, Issue-1, pp. 11-16, 2015.

[16] P K. Sharma, S. Mewada and P. Nigam, “Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network”, International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue. 4, pp. 8-11, 2013.

Author’s Prifile

Syed Muqtar Ahmed is pursuing Ph.D. in Computer Science & Engineering, from Rayalaseema University, Kurnool, Andhra Pradesh, India. He is having 20 years of teaching experience. Worked as Assistant, Associate Professor and Head of CSE department at Deccan College of Engineering & Technology, Hyderabad, India from 1997-2008. He also worked as a faculty at Nizwa College of Technology, Sultanate of Oman from 2008-2009. He received M.Tech in Information Technology in 2003 and B.E in Computer Science & Engineering in 1997. Recently published articles in Intrusion detection system and also an author of Textbook Title: ‘Data Communication and Networking’, Sure Series, Hyderabad, India. His area of research is Data Communication, Wireless Network and Network Security.

Dr. Syed Abdul Sattar is a Professor, Director (R&D) at Nawab Shah Alam College of Engineering and Technology, Hyderabad, India. He had received national award as Young Scientist in year 2006 with a Gold medal from NESA New Delhi. He obtained his first Ph.D. in CSE from GSU USA in 2004 on WLAN’s Efficiency and Second Ph.D. in ECE from JNTU, Hyderabad on WLAN security in year 2006. He passed Bachelors of Engineering in 1990 and obtained Master’s in 2002. His publications are more than 170 in National and International Journals like IEEE, ELSEVIER and SPRINGER etc. He has guided 17 Ph.D. scholars so far and more than 20 are in pipeline. His area of Research is in Wireless communication and Image processing.