IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-5 , May 2019 E-ISSN: 2347-2693

Detection of Collaborative Wormhole Attack in Wireless Mobile Adhoc Network

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 and faculty at College of Engineering, University of Business & Technology, KSA
[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

DOI: https://doi.org/10.26438/ijcse/v7i5.652657 | Available online at: www.ijcseonline.org

Accepted: 22/May/2019, Published: 31/May/2019

***Abstract*—**A Wireless Mobile Adhoc network (MANET) is a self-controlled group of multiple nodes establishing a temporary network. MANET nodes have the tendency to change the location from one point to another due to it's vulnerable and dynamic nature topography, which may invite for several types of cyber-attacks. One of the most dangerous attack is wormhole attack in which two or more malicious nodes could establish a tunnel between them and attract all the neighbours to send the packets though that tunnel by assuring that packet would be delivered to destination through the tunnel's optimal-route and also assure to deliver all the packets by taking small amount of time delay. Most of the proposed methods to guard against wormhole attack use either clock synchronization or round-trip time technique but our proposed method uses hop-to-hop count technique. The purpose of this research work is to make a solution to detect the most risky and dangerous wormhole attack in the context of mobile Adhoc networks that can drift the normal traffic flow completely. We named this solution as Detection of Collaborative Wormhole Attack in Wireless Mobile Adhoc Network (DC-WAN). An attempt has been done to make an Algorithm to detect Wormhole malicious node(s) based on reactive Adhoc on demand distance vector (AODV) protocol. Several times experiments were conducted on our solution by using NS2 and found that the PDR and Throughput is similar to AODV protocol but the Packet Drop Ratio is fluctuating as time changes.

***Keywords*—** MANET, Cyber attacks, Wormhole attack, AODV, hop-to-hop count

I. INTRODUCTION

MANET consists of a group of unguided wireless nodes which may vary their positions frequently within the domain of network as they are ready to form an un-centralized infrastructure-less topology [1]. MANET has a common characteristic to insert or delete nodes dynamically at any time. Hence, it may be utilized where guided fixed wired network could not be installed properly. The nodes are very portable devices such as mobile handheld devices, Laptops and palmtops etc. which could work with little amount of battery backup. They are connected together and communicate with each other with the help of routing protocols [2]. Initially AODV was developed by IETF community to solve loop-creation and count-to-infinity problems with the help of sequence numbers. AODV depends upon two main steps such as Route Discovery and Route Maintenance that may utilize the following messages: RREQ, RREP, RERR and HELLO [3]. It is very difficult to eradicate wireless communication from our daily life. Therefore Adhoc network could be installed in situation of military battlefield and emergency services.

Several researchers are involved to make solutions on wormhole attack but they are not efficient. Our proposed solution is efficient as it can detect the wormhole attack efficiently based on the performance as shown in different graph. The following sections are used in our paper: Section-I is about introduction to AODV protocol, IDS and wormhole attack, Section-II is purely related work done by multiple researchers, Section-III is our actual work with the proposed solution, Flow chart, some part of coding of wormhole node. Section-IV is about Simulation, Section-V shows Results and discussion and the last Section-VI is about conclusion.

I. I. Adhoc on Demand Distance Vector Protocol

Adhoc on demand distance vector (AODV) is one of the routing Protocols developed for mobile Adhoc networks

(MANET). Our solution is tested with the combination of AODV protocol. It can establish a link between two nodes on demand. That's why this protocol is also known as on-demand routing protocol. AODV would work on routing tables which are required to forward packets from one node to another and also maintain the routes in the routing table to by using the following parameters: SA, DA, Seq.No., ID, h_count etc. Initially it starts with Route Discovery process later it maintain the routes by using Route Maintenance process [5]. In Route Discovery process the source node generates RREQ packets and broadcast to all neighbours that are connected to it. Flooding help us to broadcast RREQ packets. In turn, all the connected neighbours send the RREP to source and update their routing table in order to maintain the current status of nodes. Also the malicious node may generate the RREP and send back to source to assure that it has the best and shortest route to destination with minimum number of hops.

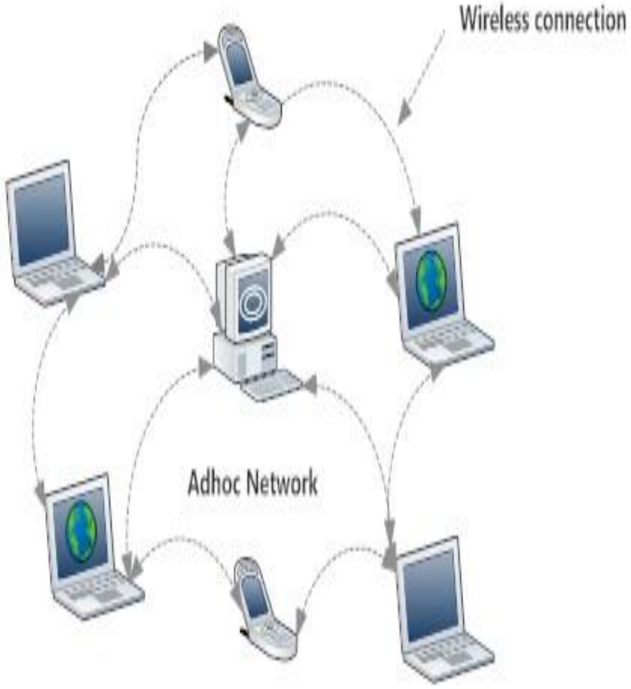

Fig-1: Mobile Adhoc Network

I.II. Intrusion Detection System (IDS)

Millions of people connect with each other through internet. As the size of internet grows there are more chances of cyber-attacks. To identify and detect the attacks we need to have some system which could monitor the entire Adhoc network.

This is exactly the role of Intrusion Detection System. Usually IDS try the look at the history of events and carry out the process to detect the malicious behaviour of a node by using simple rule of Algorithm. IDS can keep an eye on guided as well as unguided media types of networks. To have maximum level of security, it was suggested by many researchers to keep both Software and Hardware Intrusion Detection System in an organization. Over the two decades different categories of IDS have been developed.

I.III. Wormhole Attack

A Wireless Ad hoc network is vulnerable in nature and open for several types of cyber-attacks. One of the most dangerous attacks is wormhole attack in which two or more malicious nodes could establish a tunnel between them and attract all the neighbors to send the packets though that tunnel. It make sure that whenever data packets are send through that tunnel it would be delivered to destination with less number of hops and less delivery time. Most of the proposed methods to guard against wormhole attack use either clock synchronization or round-trip time technique but our proposed method uses hop-to-hop count technique.

Collaborative Wormhole attack consists of two or more malicious nodes that could make a strong tunnel between them and attract all the nodes to send data through it. Once they receive the packets they may either simply drop the packets or forward to any other malicious node if it is available in Adhoc network. This may lead to decrease the performance of system and eventually data packets may not be delivered to a particular destination. Therefore, our solution could identify and detects the malicious or bad guy(s) in MANET. The following Fig-2 consists of ten nodes from N1 to N10. We assumed that N1 is our source node and N10 is our destination. It is also assumed that a tunnel is formed between two bad guys namely N3 and N8. Initially N1 broadcast Route Request (RREQ) packets to all its adjacent neighbours in order to initiate communication. All the neighbours receive RREQ and try to generate a response in the form of Route Reply (RREP). Also one of the neighbours connected to Source is N3 which assure N1 that it has the optimal tunnel or channel to deliver data quickly with less amount of time delay. Every neighbour will be happy to deliver data though that tunnel but at the end both the bad guys will play with the packets and drop them. If the bad guys create the tunnel honestly and reliably than it is assumed that they will not harm the MANET and also provide useful service more efficiently [6].

In Fig-2 scenario, we assumed that N1, N2, N3……N10 are the nodes. N1 is a source, N10 is destination and N3 and N8 are malicious nodes which could establish a tunnel between them.

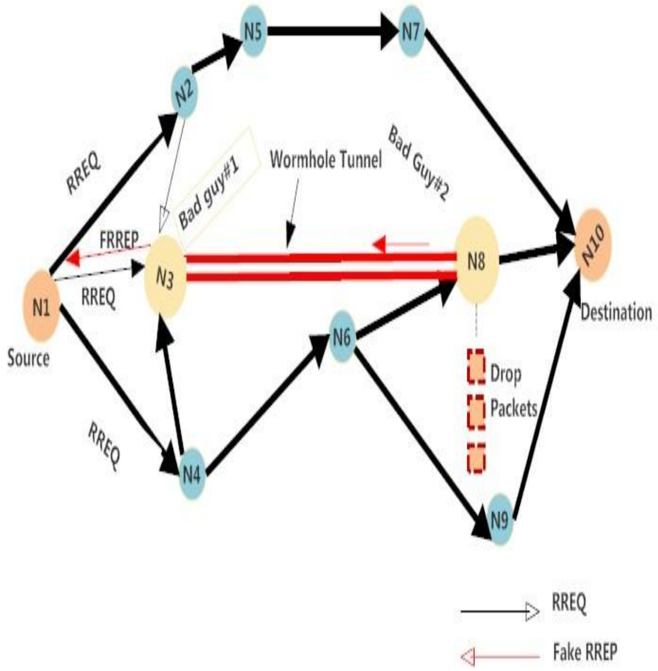

Fig-2: RREQ-RREP in Wormhole Adhoc Network

The Fig-2 is about RREQ-RREP and RREQ-FRREP which is purely based on AODV protocol:

- N1 floods RREQ to all adjacent neighbours (N2 and N4).
- N3 and N8 are malicious/bad guys which could form a tunnel.
- N3 will send FRREP to N1 in order to show best and optimal route through the tunnel.
- N1 update N3 route and store in database which is a false route to destination. N3 and N8 may drop the packets instead of forwarding to N10.

II. RELATED WORK

Several solutions have been developed to identify and detect Wormhole attacks in MANET which are as follows:

S.Young Shin, E.H. Hartono Halim [7] proposed a method to detect and separate wormhole attack in MANET. The idea here is to form multiple routes when sending Route Request packet (RREQ) from source to destination and these routes can be used as reference of each other to find malicious nodes with malicious behavior within the network. It is based on three steps: routes redundancy, routes aggregation and calculating round-trip time (RTT) of all listed routes.

M. Rmayti, Y. Begriche, R. Khatoun [8] proposed a novel detection model to allow a node to check whether a presumed shortest path contains a wormhole tunnel or not. This technique is based on the fact that the wormhole tunnel reduces significantly the length of paths passing through it.

R. Prakash, W. R Jeyaseelan [9] proposed a method in which a coordinator node is elected by wireless election algorithms to detect wormhole attack. The main function of the coordinator node is to separate and prevent any further attacks. Several experiments were carried out to check the performance under different situations. From the experiment results, they have identified that the suggested wireless protocol is adapted for improving the protection of resource constrained of wireless sensor networks.

T.Sundararajan, S. M. Ramesh [10] suggested a solution which is purely based on biological artificial intrusion detection system (BAIDS) and also combines the power of hybrid negative selection algorithm (HNSA) to identify and detect abnormal behavior in MANET. Also an action will be taken against the attackers. The detectors used in this research are involved to separate good behaving nodes from bad behaving with sufficient level of accuracy in a MANET.

R. Prakash, W. R. Salem [11] developed an algorithm for wormhole attack. Here the updated information of the packets can be changed frequently may give strong security. The solution of wormhole attack identifies the coordinator node which is selected by wireless election algorithms. The main task of the coordinator node is to monitor, and separate any further attacks in future.

III. METHODOLOGY

The following Algorithm will explain you the various steps of wormhole detection.

Assume [N1: Source, N2, N4 may be neighbours, RREQ: Route Request Packet, RREP: Route Reply Packet, Fake Route Reply (FREP), NL: Neighbours List THV: Threshold].

```
Procedure Wormhole( )
h_count=0;          //hop count is initialized to Zero
for i = 1 to N      // 1,2,3,….N number of neighbors
N0:Broadcast PREQ   // Route Discovery
Ni ← PREQ           // Neighbors receive PREQ
if (Ni(Addr) = = Destination Address && N1←
    NL   ) /* Check if there is an entry of source and
    destination Address in Routing table of source and
    Neighbor list stored in Source */

    N1←N2(RREP)     // Correct Route Reply
    else
    N3-N8←Tunnel  // Form a tunnel between N3 & N8
    N1 ←N3 (FRREP])  /* Wormhole node (N3 or N5)
    generate False FRREP & send to source */
```

```
7.  Ni+1← RREQ    /* RREQ is forwarded to another
    neighbor. */
8.  h_count  = h_count + 1  /* hop count is incremented
    by 1 */
    end if
9.  If (h_count > THV)        /* Check whether if the
    value of hop count is greater than threshold value or
    not. */
    Print "Wormhole Node"
    else
    Print "Normal Node"
    end if
10. All routes to Tunnel is  blocked
    end for loop
    end Wormhole Procedure
```

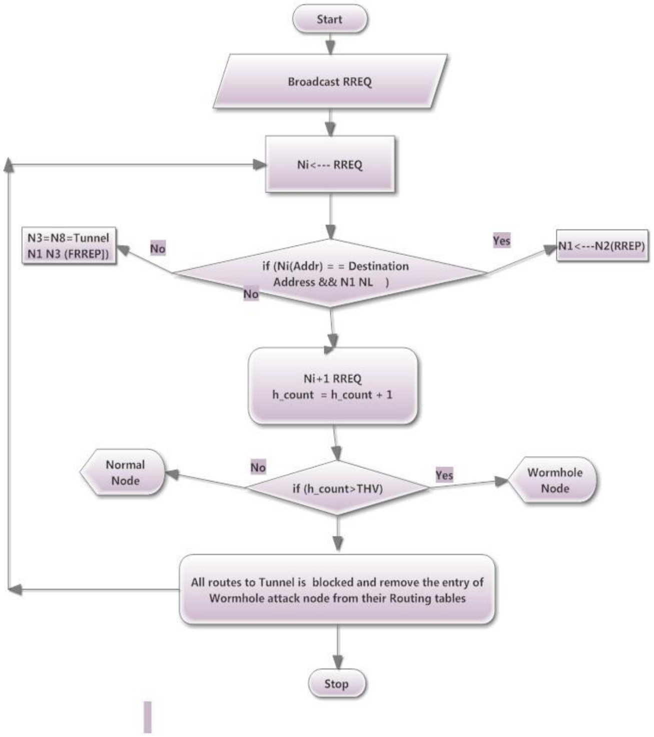

Fig-3: Flow chart of DC-WAN

1V. SIMULATION

To add Wormhole node just we need to update the following files which are available in ns-2.35/mac/ directory.

- **arp.cc**
- **ll.h**
- **ll.cc**

/* Under ll.h define elements for the wormhole peer list */

```
Class LL;

Typedef struct wormhole_peer_struct {

 LL* ll;

Int id;

Struct wormhole_peer_struct* next;

} wormhole_peer;
```

/* Under arp.cc add the following code for wormhole attack. */

```
wormhole_peer wormhole_head;
```

// For tracking overhead define the following integer variables

```
int routing_packet_count;
int routing_byte_count;
int data_packet_count;
int data_byte_count;
```

/* Under ll.cc add the following code for wormhole attack. */

```
Case NS_AF_INET:
dst=ch→ next_hop();

Case NS_AF_NONE:
If(IP_BROADCAST == (u_int32_t) dst)
{       mac_→     hdr_dst((char*)     HDR_MAC(P),
MAC_BROADCAST);
IS_broadcast = 1;reak;
}
```

V. RESULTS AND DISCUSSION

NS-2.35 tool is used for simulating for our proposed solution. The malicious nodes N3 and N8 may establish a tunnel between them as they are interested to play in the network by either drop packets or forward them to another malicious node, which may result in degradation of the overall performance of a network. The proposed solution helps us to detect the malicious node and update their information to other nodes. The simulation work have been carried out in combination of AODV protocol with the following parameters: Malicious nodes: 1 or 2, number of nodes varies from 10 to 50 each time there is a step of ten and it is distributed in an area size of 900*900m using CBR traffic type.

V.I. Performance Analysis of AODV and DC-WAN

Packet Delivery Ratio (PDR): It is defined as the ratio of total of data packets received to the total of data packets send. It is calculated by the following equation.

$$PDR(CD\_WAN) = (\sum packets\ Received/\sum Pakets\ send) * 100$$
------------ (I)

Throughput: it is the total number of data bits delivered per second. It is measured in Kbps.

$$Throughput(CD-WAN) = Receive\ Line * (End\ time - Start\ time) * (8/1000)$$
----------- (II)

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

$$Packet-Drop-Ratio\,(CD-WAN) = (Send\ Line - Received\ Line/Send\ Line) * 100$$
----------- (III)

Table-2: 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

Table-3: DC-WAN Data

Time (msec)	Packet Send	Packet Received	PDR:DC-WAN	P_Drop_Ratio: DC-WAN	Throughput: DC-WAN
10	1188	1020	85.85	14.14	326.4
20	3579	3254	80.91	9.08	780.96
30	6625	6243	94.23	6	998.88
40	9635	9210	95.58	4.41	736.8
50	12655	12246	96.76	3.23	0

The Fig-4 shows that Time and PDR for DC-WAN keeps on changing with respect to time but at 30msec the PDR ratio is almost 86.24% which is very close to AODV.

Table-1: Simulation Parameters

No#	Parameters	Items
1.	Simulator Software	NS-2.35
2.	Topography	900m x 900m
3.	Routing Protocol	AODV
4.	Wireless Standard	IEEE 802.11 Layer
5.	Packet Size (Bytes)	512
6.	Total Number of Nodes	10
7.	Minimum Number of wormhole Node	1
8.	Simulation Time	10-50 msec
9.	Traffic Type	CBR
10.	Propagation	Random Waypoint
11.	Link Layer Type	LL

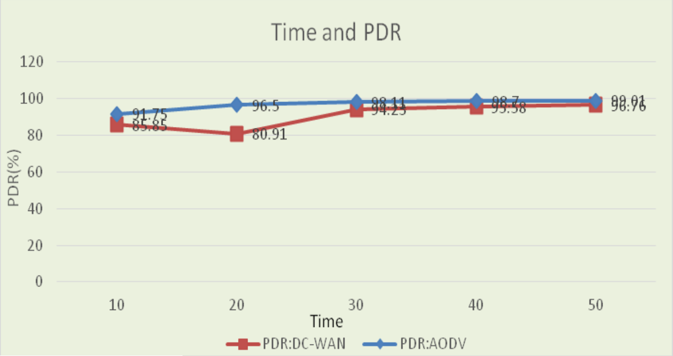

Fig-4: Time Vs PDR

The Fig-5 shows that Throughput also keep on changing with respect to time but It's close to AODV at 30 msec.

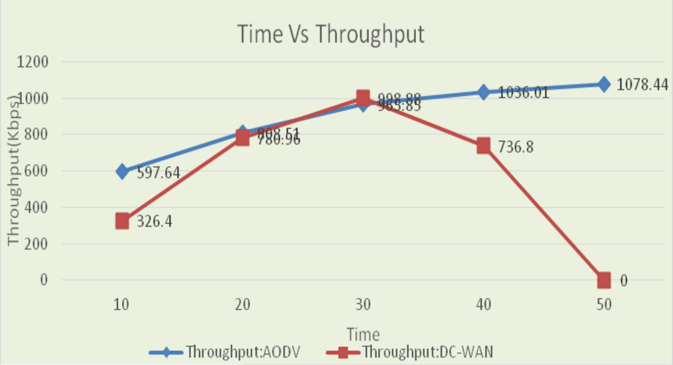

Fig-5: Time Vs Throughput

The Fig-6 shows that Packet-Drop-Ratio of CD-WAN. It keeps on changing with respect to AODV. The gap between AODV and DC-WAN throughout the graph is somewhat large but having a difference of 2.24% at time 50 msec.

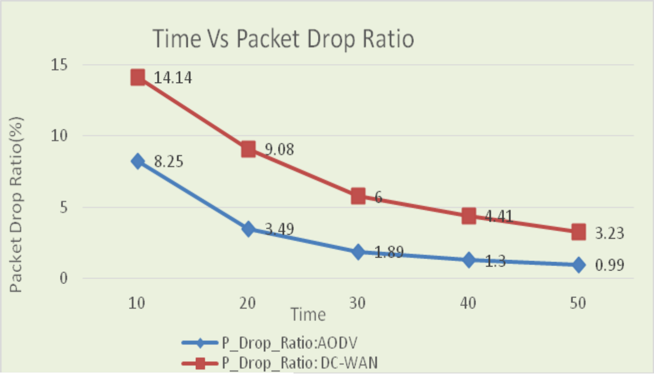

Fig-6: Time Vs Packet Drop Ratio

VI. CONCLUSION

MANET has no centralized infrastructure as it is setup with free of topology. So it is difficult to monitor what is happening in it. Thus we need to protect it from different types of attacks. One of the dangerous attacks in MANET is wormhole attack that creates a tunnel between malicious nodes that allow data packets to pass through it. Once packets are delivered to tunnel the wormhole attack is initiated and ultimately drops the packets. Our proposed technique uses hop-to-hop count technique to solve this issue. Our Simulation results as shown above are efficient with respect to PDR and Throughput, which is almost similar to that of original AODV protocol at time instant 30 msec. The Packet Drop Ratio keeps on changing but having 2.24% difference at 50 msec. Therefore, the proposed solution is efficient.

REFERENCES

[1] S. Singh, R. Kansal, “Novel Technique for Detection of Wormhole Attack in MANET”, International Journal of Computer Sciences and Engineering, Vol.6, Issue. 11, pp. 464-468, Nov 2018.

[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] N. Gandhewar, and R. Patel, “Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad Hoc Network”, In Proceedings of the Fourth International Conference on Computational Intelligence and Communication Networks, IEEE Computer Society, pp. 714-718, 2012.

[4] 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.

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

[6] S. Upadhyay and A. Bajpai, “Avoiding Wormhole Attack in MANET using Statistical Analysis Approach”, International Journal on Cryptography and Information Security,Vol.2, Issue.1, March 2012.

[7] S.Young Shin, E.H. Hartono Halim, “Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation”, International Conference on ICT - ieeexplore.ieee.org IEEE, 2012, India.

[8] M. Rmayti, Y. Begriche, R. Khatoun, “Graph-based wormhole attack detection in mobile ad hoc networks”, 4th International Conference on Mobile and Secure Services, 24-25 Feb. 2018, IEEE Xplore: 12 March 2018, USA.

[9] S. Majumder, D. Bhattacharyya, “Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach”, 2018, IEEE, India.

[10] T. V. P. Sundararajan, S. M. Ramesh, R. Maheswa, K. R. Deepak, “Biologically inspired artificial intrusion detection system for detecting wormhole attack in MANET”, © Springer Science + Business Media New York 2013, Wireless Networks May 2014, Volume 20, Issue 4, pp 563–578.

[11] R. Prakash , W. R. Salem and T. Jayasankar “Detection, Prevention and Mitigation of Wormhole Attack in Wireless Adhoc Network by Coordinator”, Applied Mathematics & Information Sciences, Vol. 12, Issue No. 1, PP. 233-237,2018.

[12] 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.

Author’s Profile

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. Currently Working as a faculty at College of Engineering, UBT, Kingdom of Saudi Arabia from 2010. He worked as a faculty at Nizwa College of Technology, Sultanate of Oman from 2008-2009. Also worked as Associate Professor and Head of CSE department at Deccan College of Engineering & Technology, Hyderabad, India from 1997-2008. He received M.Tech in Information Technology in 2003 and B.E in Computer Science & Engineering in 1997. He had published two papers and an article based on Intrusion detection system in International Journals. He is an author of Textbook Title: ‘Data Communication and Networking’, Sure Series, Hyderabad, India. His area of research is Data Communication, Wired and Wireless Network and its 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.