IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Robust Design of Intrusion Detection System in Wireless Mobile Adhoc Network (RDIDS-WMAN)

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

[1] Dept. of Computer Science, Research Scholar of Rayalaseema University, ID: PP.COM.SCI & ENG.083, Kurnool, Andhra Pradesh, India
[2] Dept. 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: 25/Nov/2018, Published: 30/Nov/2018

***Abstract*—** Presenting cutting edge research- A mobile Adhoc network is a collection of wireless devices in which nodes interact with each other in a tentative topology without using pre-defined infrastructure. Almost all networks are protected using multilayer firewalls and encryption methods, but many of them are not so effective. Therefore we proposed a Robust Design of Intrusion Detection System in Wireless Mobile Adhoc Network (RDIDS-WMAN) to detect anomalies for multi-hop networks. The purpose of this paper is to design a detail architecture of Analysis Process that operates on simple rules including four different phases namely Event management, Authentication, Duplicate request generation and Message alert monitoring phase to detect the malicious node. This paper also conducted the simulation of proposed RDIDS-WMAN with a combination of AODV protocol to show its effectiveness and resists the attacks. Meanwhile, the performance of network, such as Packet Delivery Ratio, Average End-to-End delay, Throughput and Packet Drop Ratio is tolerable according to the NS-2.35 simulation results. Our solution also uses an authentication process with hash method.

***Keywords*—** MANET, AODV, RDIDS-WMAN, Multi-hop network, Authentication, Intusion

I. INTRODUCTION

Wireless network have dynamic nature due to which it forms clusters with nearest neighbouring nodes [1]. An intrusion may be defined as "any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource". Intrusion Detection Systems (IDS) help us to identify the behaviour of malicious activity in Adhoc network. IDS is broadly classified into two techniques: Signature based IDS & Anomaly based IDS. Signature based IDS uses signatures of attacks to detect the intrusion, whereas Anomaly based IDS technique help us to protect destination machine and networks against malicious behaviour. The function of an Adhoc network routing protocol is to make a correct and efficient route between neighbours so that messages would be send within the active time interval [2]. The traditional way of securing network with firewalls and encryption methods may not be sufficient. Therefore, we proposed Robust Intrusion Detection System which may provide best solution for Mobile Adhoc Network (MANET) as its applications are directly related to military, airports, university and the whole community. Many researchers have been working on Adhoc network to provide better solutions for security, but still we need to work on it.

The paper is organized as follows: Section-I discuss about the introduction to MANET, Section-II discuss about related work of different researchers with solutions, Section-III have complete Architecture of RDIDS-WMAN, Section-IV is about Simulation results and finally Section-V is about Conclusion. Our main goal is to work on the following points:

- Provide better Authenticated solution.
- Identify and detect malicious node.
- Protect legal user of MANET.

I. I Vulnerabilities of MANET

Vulnerability is the weakness in the system. MANET is open and decentralized. The use of wireless link provides the network susceptible to attack from passive eavesdropping to active interfering. Damages would be node impersonation; message contamination & leaking of secrete information. Every node in a network must be prepared to confront unexpected attacks. Some of the vulnerabilities are Dynamic nature of topology, Scalability & limited power supply and Lack of centralized management etc.

I.II Attacks in MANET

One of the challenging tasks in MANET is to provide good security. MANET would be dynamically changing it's topology as the time passes. So its mechanism and shared wireless medium among nodes would be more vulnerable to attacks. Before developing any solution for MANET security, one has to understand different types of attacks which are as follows:

DOS and DDOS Attacks

The purpose of Denial-of-Service (DOS) attack is to stop all the services to the legitimate users by interrupting Server. Perpetrator generates a single request from his machine and sends it through internet, which may create thousands of copies of similar request through flood to disrupt all services of host. Routing is one of the biggest challenges in MANET with various security problems. DOS attacks namely Black-hole, Gray-hole are serious threats for MANETs [3].
Distributed Denial-of-Service (DDOS) attack is a malicious activity to interrupt normal traffic of a targeted server with a flood of Internet traffic. DDOS is more dangerous than DOS.

I.III Routing Protocols in MANET

Our Research is based on AODV. Routing protocol plays a significant role in MANET. They can control the number of nodes with restricted resources and provide optimal routes to deliver data packets quickly. The following are the routing protocol often used in MANET.

I.III.I AODV Protocol

The abbreviation of AODV is Adhoc on demand distance vector protocol. AODV protocol was developed by Nokia, University of California and Santa Barbara. AODV is a reactive protocol as it has the capability to establish the link on demand. It was developed for wireless MANET with range of 10's—100's mobile nodes and utilizes Sequence numbers for route updates. AODV works on Route Discovery and Route maintenance. The source can establish the route to destination that may have minimum number of hops through neighbours. The route established between the nodes by flooding RREQ message. One neighbour would forward the request to other neighbour and record the entry in there routing tables. The neighbour sends the RREP to source, assuring that it can provide best route to destination. AODV protocol ignore count-to-infinity problem when ever route change occur by using sequence numbers.

I.III.II Malicious Activity in AODV Protocol

Let 'A' as source, 'G' as destination and D as malicious node. Node A broadcasts a RREQ packet to all adjacent neighbours as shown in Fig-1. Neighbours scan their routing tables to check the possibility of having rout to destination. They could reply with RREP if there is a route available, otherwise, the RREQ is forwarded to another node and store a backward path in the source. The routing table store path details of the neighbour, the distance and the latest biggest sequence number [4]. If topology changes in the network then the route maintenance starts. When a broken path is detected, a RERR message is generated to inform the neighbours that the line is lost. The RREP message identifies those nodes which are not reachable by the way of the lost link. The D act as a malicious node would send a fake reply to ensure that it has the optimal route to source. When it receives data from source, simply it drops the packets or it may forward to any other malicious node.

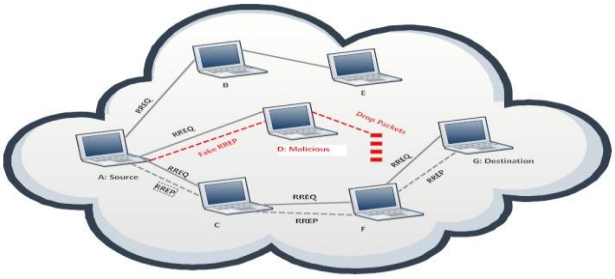

Fig-1: Establishing a new route using AODV protocol

I.III.III DSR Protocol

The abbreviation of DSR is Dynamic Source Routing protocol. It was developed for multi-hop wireless ad hoc networks. The protocol has two main characteristics, "Route Discovery" and "Route Maintenance", which could work altogether to explore and maintain routes to any destinations in MANET. DSR supports multiple routes to any destination and also manage the route while sending the packets to have load balancing. DSR support loop-less routing operations in network that may have single path using only "soft RREQ - RREP Source Destination state", and there will quick recovery when paths are updated [5].

II.RELATED WORK

This section reviews related work on IDS in MANET. Wireless Mobile Adhoc Network is an excellent field of research and less attention is paid to security aspects of routing protocols. The research community is involved to test and implement ad hoc network routing protocols. Wireless mobile ad hoc network is less secure compared to wired network. Therefore, researchers need to make new IDS systems which can handle new security challenges. Cooperative intrusion detection system has been proposed to have good security in mobile Adhoc network [6], where all the available nodes are guided to run their IDS in order to collect and identify possible intrusions. If any abnormal

behaviour is found, then a global detection process is started for detecting advance intrusions. Later on, enhancement of this model was developed in, where all possible intrusions can be detected with their adjacent sources. The watchdog solution belongs to a part of IDS. The concept in this solution is to keep an eye on neighbour of each node by sensing the channel to find out whether it forwards to its successor or drops the packet. In [7], authors developed a method that resolves some of watchdog's problems. In this proposal, each node quickly checks its neighbour and authenticates Two-way-hop acknowledged message. In [8], authors, sketch an intrusion detection system to avoid the black hole attacks in AODV. In this solution, an agent is utilized to know the attacks that use the route request and the route reply packets. An agent can keep an eye on two-way packets. If any activity is non ethical, then black hole is identified. In [9], Ms. Nidhi Sha and rma Mr.Alok Sharma developed couple of solutions for black hole attack, later they compare their solutions to the original AODV based on the pause time and found low delay in MANET. In [10] a solution was proposed known as channel aware detection (CAD) that rely on two techniques, namely hop by hop loss observation and traffic overhearing. An intermediate node checks the behaviour of its predecessor and successor neighbours to find the malicious node.

III. METHODOLOGY

This section explains the Architecture, Pseudocode and Algorithm of RDIDS-WMAN.

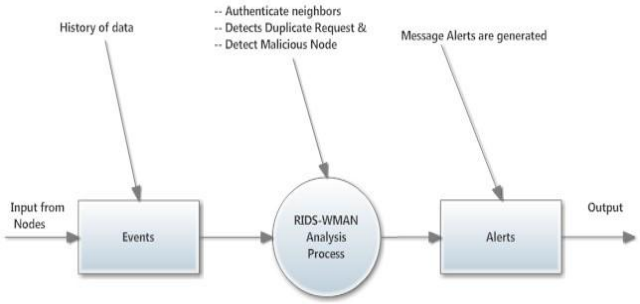

Fig-2: Top Level Architecture of RDIDS-WMAN

Events: This phase checks and store the history of data related to a particular event.
Analysis Process: carry out processes on the collected data to detect malicious signs based on Simple rules of Algorithm.
Alerts: one of the nodes would be selected for monitoring alerts that generates response to the administrator.

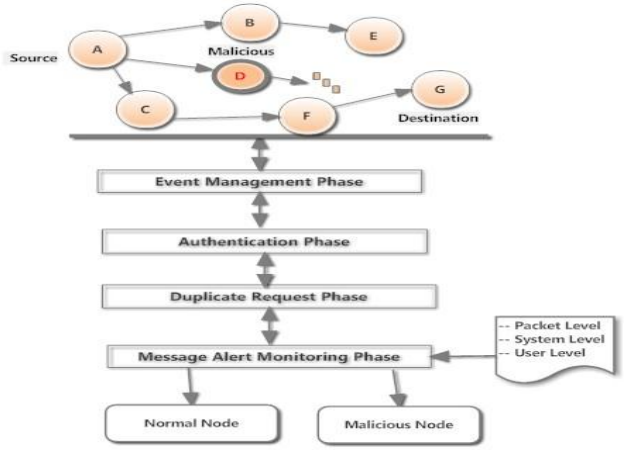

Fig-3 : Detail Architecture of Analysis Process

III.I Architecture of RDIDS-WMAN

The RDIDS-WMAN has been proposed to identify the malicious node in adhoc network with AODV Protocol. The Detail Architecture is displayed in Fig-3, with the following phases:
Event Management Phase : Keeps history of events.
Authentication Phase : Authenticates the nodes
Duplicate Request Phase : Find out whether a message is Duplicate or not.
Message Alert Monitoring Phase : Malicious node can be detected here and the alerts are sent to administrator.
Initially RDIDS-WMAN broadcast RREQ packet to all its Neighbours. In the next step the internmediate node receives a RREP, then it will calculate its hop counter value, which is bigger than Threshold value to detect as a malicious node. RDIDS-WMAN was proposed to perform the detection of malicious node and also block control messages effectively, and at the same time it reduces the tranmission of duplicate RREQ to reduce the network overhead and the time delay.

III.II Pseudocode of RDIDS-WMAN

1. Source node generates RREQ packet and broadcast to all neighbors using flooding.
2. Select one route from several routes.
3. Authentication process with hash method.
4. Check whether the packet received is duplicate or original RREQ.
5. Check whether the node is intermediate or destination node.
6. Identify the malicious node by checking hop counter value that must be greater than Time to live value.

7. If malicious node is found then intermediate node will update its routing table and also broadcast its updates to all its neighbors in order to block messages.

III.III Algorithm of RDIDS-WMAN

Let {SN: Source Node, DN: Destination Node, X1, X2, X3……Xn-1…...X…...Xn+1 are Intermediate nodes, RREQ: Route Request Packet, RREP: Route Reply Packet, PTOS: Present time of System, T: Timer, TTL=Time to live, THV: Threshold Value to find malicious node, ∀ : Logical symbol for All }

Boolean: RREQ = 0; //0: false & 1: true
h_cnt=0; //Hop counter initialize to zero

Step 1: //SN generates RREQ and broadcast to all its //neighbours using flooding
for ∀ packets of SN do send RREQ by flooding
Step 2: Procedure Select route (); // Select one route from several routes
Step 3: // Authentication process with hash method,
// Where EKpub is an encryption with public key, Hs() is a
// hashing function and + is a concatenation symbol.
C ← EKpub (Hs (xi+xi-N)
Step 4: // if the node is not the DN then it should be
// One of the Intermediate nodes.
If (Xk != DN) then //Xk may be any one
// Intermediate node such as X1, X2…Xn
Print "Intermediate Node"
else
Print "Destination Node"
end if
Step 5: // Check whether duplicate RREQ is
//received by neighbour. Here 1 indicates Boolean true.
If (RREQ =1) && (h_cnt=TTL) then
Print "Duplicate RREQ"
else
h_cnt=h_cnt-1; // Decrement counter by 1 for next hop
Print "Original RREQ"
end if
Step 6: // When Xn-1 receives a RREP, concludes that it's a //malicious or Normal node.
// RREP is in the range of hop count limit and threshold value
// to decide about malicious node.
Xn-1← RREP // Intermediate node may receive Route Reply
If (h_cnt>THV) then
Print" Malicious Node"
else
Print "Normal Node"
end if
Step 7: // if malicious node is found then Xn-1 will update
// its routing table and also broadcast updates to all its
// neighbours.
Xn-1 ← malicious
Print "Xn-1 broadcast updates to all neighbours to block message and Xn broadcast message to Xn+1"
end for

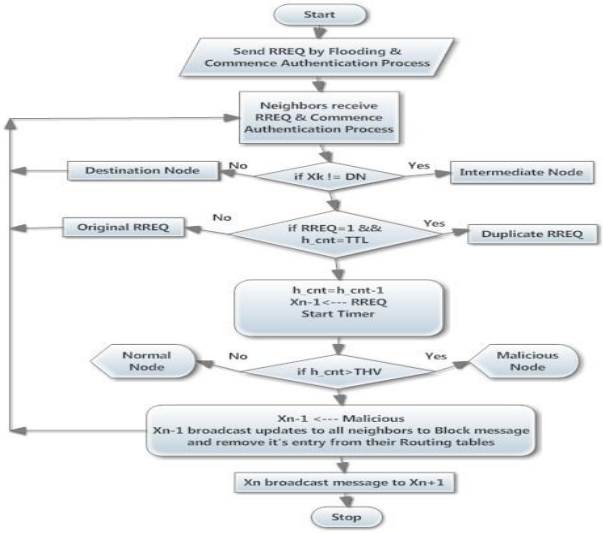

Fig-4: Flowchart of RDIDS-WMAN

1V. SIMULATION RESULTS AND DISCUSSION

We have simulated our proposed algorithm using NS-2.35. The functionality of malicious node is to either drop the packets or to forward to other malicious nodes. We took the original AODV protocol and configured one node as malicious. Our solution detects the malicious node and later immediately blocks that node by sending information to neighbours. The following table shows the simulation parameters

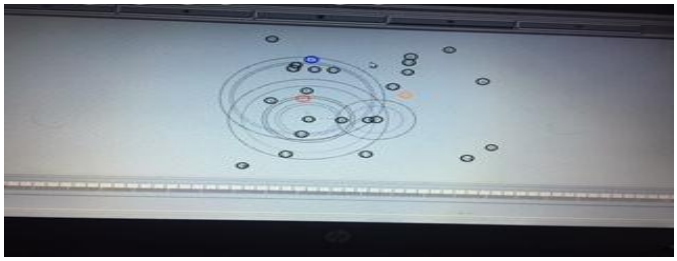

Fig-5: Simulation Screen Shot

1V.I Metrics for Simulation

Packet Delivery Ratio (PDR): It is defined as the ratio of sum of data packets received at destination to the sum of data packets that were send by the source. If the PDR ratio is high then the performance of the routing protocol is high. PDR is calculated as follows:

$$PDR = \sum Packets\ Received / (\sum Packets\ Send) * 100 \quad (1)$$

Average End to End Delay: It is the defined as delay between the packets send by the source and its delivery at the receiving node.

$$AVG.\,End-End-Delay = delay/(Packets\ Received) \quad (2)$$

Throughput: The total number of bits forwarded to higher layers per second. It is measured in Kbps.

$$Throughput = bytes * (8/(End\ time\ of\ Packet\ transmission - Start\ time\ of\ Packet\ transmission))/1000 \quad (3)$$

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

$$Packet\ Drop\ Ratio = (Packet\ Send - Packet\ Received)/(Packets\ send) * 100 \quad (4)$$

Table-2: Simulation of AODV without malicious node

Number of Nodes	Packet Send	Packet Received	PDR (%) AODV	Avg_End-to-End delay (ms) AODV	P_Drop_Ratio (%) AODV	Throughput (Kbps) AODV
5	300	267	89.00	164.44	11	18.83
10	300	298	99.33	149.71	0.67	20.77
15	300	296	98.67	151.12	1.33	21.19
20	300	298	99.33	149.99	0.67	21.57
25	300	300	100	149.5	0	20.83
30	300	299	99.67	149.99	0.33	21.25

Table-3: Simulation of RDIDS-WMAN with a malicious node

Number of Nodes	Packet Send	Packet Received	PDR (%) RDIDS-WMAN	Avg_End-to-End delay (ms) RDIDS-WMAN	P_Drop_Ratio (%) RDIDS-WMAN	Throughput (Kbps) RDIDS-WMAN
5	300	270	90.00	166.28	10	12.23
10	300	295	98.33	148.67	1.67	15.43
15	300	290	96.66	181.98	3.33	15.21
20	300	292	97.33	179.82	2.66	17.18
25	300	298	99.33	149.99	0.66	18.01
30	300	295	98.33	181.67	1.66	17.27

The below Fig-6 graph shows that PDR for our proposed RDIDS-WMAN solution. It has been observed that our solution PDR is reduced only by 0.67% compared to AODV protocol with 25 nodes.

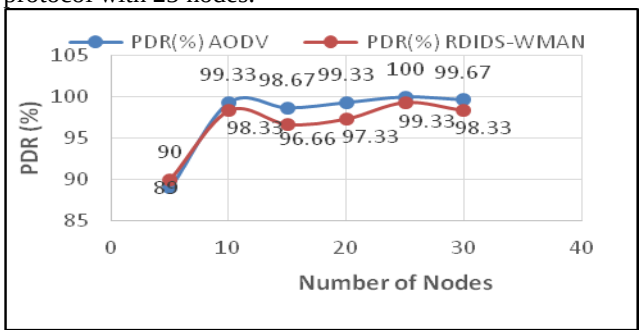

Fig-6: Number of Nodes Vs Packet Delivery Ratio

Table-1: Simulation Parameters

S. No	Simulation Parameters	Values
1	Simulator tool	NS-2.35
2	Number of Nodes (Experiment repeated 6 times to have accurate Performance)	5,10,15,20,25,30
3	Number of Malicious Node	1
4	Area Size	900m x 900m
5	Routing Protocols used	AODV
6	Wireless Standard	IEEE 802.11
7	Packet Size in Bytes	512
8	Source of Traffic	CBR/UDP
9	Model of Propagation	Two ray ground

The below Fig-7 graph shows that Average End-to-End delay of RDIDS-WMAN is almost similar to AODV at 10 and 25 nodes simulation, showing differences of 1.04ms and 0.06 ms respectively. It may vary for other number of nodes.

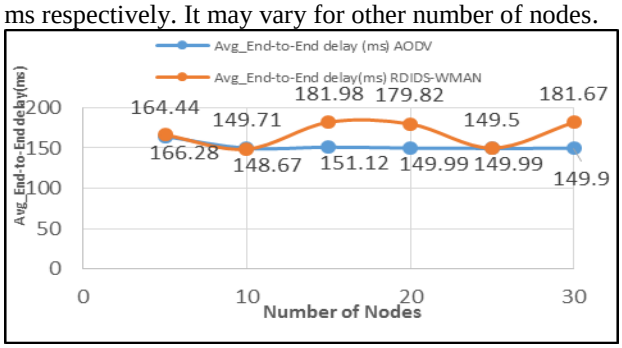

Fig-7: Number of Nodes Vs Average End-to-End delay

The below Fig-8 graph shows that Throughput of RDIDS-WMAN is close to AODV at simulation of 25 nodes, showing differences of 2.82 kbps. It may vary for other number of nodes.

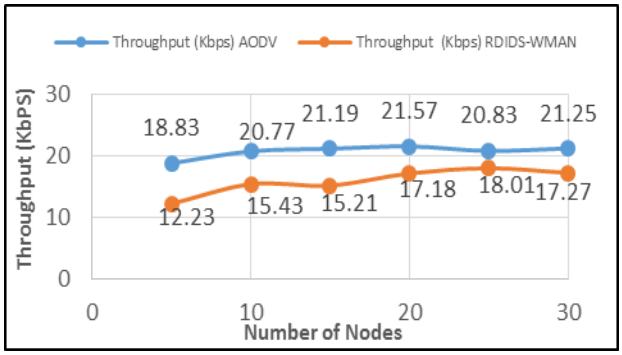

Fig-8: Number of Nodes Vs Throughput

The below Fig-9 graph indicates that Packet Drop Ratio of RDIDS-WMAN is close to AODV showing only the difference of approximately 1% in throughout.

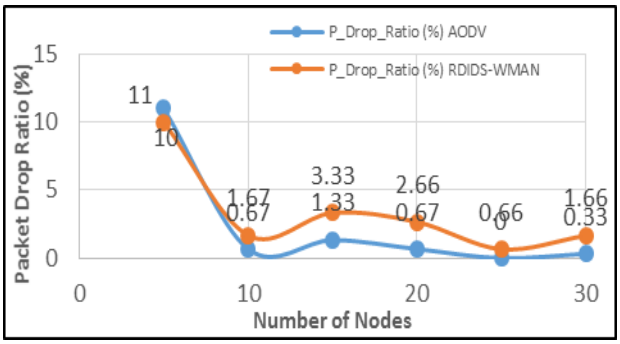

Fig-9: Number of Nodes Vs Packet Drop Ratio

V. CONCLUSION

MANET is vulnerable in terms of security. Attacker gains the access to it due to decentralized nature and undefined topology. The algorithm and architecture proposed in this paper composed by four stages namely Event Management Phase, Authentication Phase, Duplicate Request Phase and Message Alert Monitoring Phase The simulation results shows that the PDR and Average End-End-Delay of proposed solution is approximately similar to AODV. It signifies that the solution is efficient. Meanwhile, the Throughput introduced by authentication is tolerable.

REFERENCES

[1]. J. Srilakshmi1, S.S.S.N. Usha Devi N2, "Secure and Efficient Multipath Routing Using Overlay Nodes", International Journal of Scientific Research. Computer Science and Engineering, Vol.6, Issue 5, pp.16-19, October 2018.

[2]. Lubdha M. Bendale, Roshani. L. Jain, Gayatri D. Patil, "Study of Various Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Scientific Research in Network Security and Communication", Vol. 6, Sp.issue.01, pp.1-5, January 2018.

[3]. Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala "DOS Attacks in Mobile Ad-hoc Networks: A Survey", In the Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, India, Pages 535-541, 2012.

[4]. Swaijit Kaushal, Reena Aggarwal," A study of different types of attacks in MANET and performance analysis of AODV protocol against wormhole attack", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 4 Issue 2, February 2015.

[5]. Naveen Bilandi and Harsh K Verma, "Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET", International Journal of Electronics and Computer Science Engineering Vol. 1, Issue 3, pp.1660-1667,

[6]. Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, USA, Pages 135-147, 2003.

[7] D. Djenouri and N. Badache, "Struggling against selfishness and black hole attacks in MANET", Wireless Communication. Mobile Computing, vol. 6, pp. 689–704, 2008.

[8] Morigere Subramanya Bhat, Shwetha .D, Manjunath .D and DevarajuJ.T,"Scenario Based Study of on demand Reactive Routing Protocol for IEEE-802.11 and 802.15.4 Standards", Vol. 1(2), 128-135, November 2011.

[9] Ms. Nidhi Sha rma and Mr. A. Sharma, "The Black-hole node attack in MANET", Proceedings of 2012 Second International Conference on Advanced Computing & Communication Technologies, pp. 546-548, 2012.

[10] S. D. Manikantan, C. Yu and A. Trisha, "Channel-aware detection of gray hole attacks in wireless mesh networks", IEEE global telecommunications conference, pp. 1–6, December 2009.

Author's Biography

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.

