ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

Design and Implementation of Black-hole Attacks in AODV Routing Protocol for Mobile Ad-hoc Networks

P.Gowrisankar[1], N.Srinivasulu[2], Dr.Ch.Balaswamy[3]

Student, ECE Department, QIS College of Engineering and Technology, Ongole, India [1]

Student, ECE Department, JNTU College of Engineering, Hyderabad, India [2]

Prof& HOD, ECE Department, QIS College of Engineering and Technology, Ongole, India [3]

Abstract: A black hole attack is a severe attack that can be easily employed against routing in mobile ad-hoc networks. A black hole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. In this paper, we are implementing Black hole attack considering the routing protocol: Ad-hoc On Demand Vector Routing Protocol (AODV) evaluate the network performance metrics like throughput, First route failure lifetime, Packet-Delivery Ratio, Average end-end Delay, Drop rate. The Experiment show that (1) Implementation of AODV for MANET without Black hole attacks (2) AODV for MANET suffers from Co-Operative Black hole attack (3) Comparison of AODV without Black hole attacks and with Black hole attacks in terms of Network Performance Metrics.

Keywords: MANET, Black hole attack, Network Performance , Security, Throughput, Packet loss and Packet Delivery Ratio.

I. INTRODUCTION

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems. Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network.

The Characteristics of Ad-hoc networks are Mobility, Multihoping, Self-organisation, Energy Conservation, Scalability and Security.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

Security is the Important Design Criteria Because Ad-hoc networks are much more easily harmed to security attacks than conventional wired networks. An active attacker tends to interrupt the continuity of operations. Due to the complexity of the ad-hoc network protocols these active attacks are by far more difficult to detect in ad-hoc than infrastructure networks. Passive attacks are unique of ad-hoc networks, and can be even more harmful than the active ones. The active attacker may eventually discover and physically disabled/eliminated. The passive attacker is never discovered by the network. Like a "bug", it is placed in a sensor field or at a street corner. It monitors data and control traffic patterns and thus infers the motion of rescue teams in an urban environment. This information is relayed back to the enemy headquarters via special communications channels with low energy and low probability of detection. To avoid the passive attacks require powerful new encryption techniques coupled with careful network protocol designs.

II. ROUTING PROTOCOLS

The Ad hoc routing protocols are broadly classified into three categories those are

- Proactive routing protocols or Table driven routing protocols

Example: DSDV

- Reactive Routing protocols or On-Demand routing protocols

Example: DSR, AODV

- Hybrid routing protocols

Example: ZRP

Proactive Routing Protocol (Table Driven: In a network utilizing a proactive routing protocol, every node keeps one or more tables representing the complete topology of the network. These tables are updated constantly in order to keep up-to-date routing information from each node to every other node. To maintain the up to- date routing information, topology information needs to be alternate between the nodes on a regular basis, leading to comparatively high overhead on the network. On the other hand, routes will be available on request. Many proactive protocols arise from conventional link state routing, along with the Optimized Link State Routing protocol (OLSR).

Reactive Routing Protocol (On-Demand Driven): Reactive routing protocols are on-demand protocols. These protocols do not try to keep correct routing information on all nodes at all times. Routing information is collected only when it is required, and route determination based on sending route queries throughout the network. The primary benefit of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be consumed. While reactive protocols do not have the fixed overhead needed by keeping continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network because of query flooding. Because of these weaknesses, reactive routing is less applicable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

Hybrid Routing Protocol: Wireless hybrid routing is depends on the idea of organizing nodes in groups and then allowing nodes different functionalities inside and outside a group. Both routing table size and update packet size are decreased by involving in them only part of the network (instead of the whole); thus, control overhead is decreased. The most popular way of building hierarchy is to group nodes geographically close to each other into definite clusters. Each cluster has a leading node (cluster head) to communicate to other nodes on behalf of the cluster hierarchy. In this way, each node has a local scope. Different routing strategies are used hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be acquired through this flexibility. Since mobile nodes have only a single unidirectional radio for wireless communications, this type of hierarchical organization will be mentioned to as logical hierarchy to distinguish it from the physically hierarchical network structure.

III. DESCRIPTION BLOCK HOLE ATTACK AND AODV ROUTING PROTOCOL

MANETS are vulnerable to various types of attacks. On the basis of different characteristics the attack on mobile ad hoc network is classified as passive and active attacks. One such active attack is Black hole attack. A black hole is a node that has the characteristics that it always responds with a RREP message to every RREQ, even though it does not really have a legitimate route to the target node. A Black Hole attack is a kind of denial of service where a malicious node can absorb all data packets by fallaciously claiming a new and fresh route to the destination and then drops them without delivering them to the destination. Cooperative Black hole means the malicious nodes act in a group. In black hole attack the malicious node waits for the neighbours to initiate a RREQ packet. As the black hole node receives the RREQ packet, it will immediately send a forged RREP packet to the source node advertising itself as having the shortest and optimum route path to the target destination. On receiving of RREP the source node thinks discovery

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

of route process is over, discards other RREP messages from other nodes and choose the path through the malicious node to route the data packets and starts to transmit the data packets over malicious node. When the data packets reach the black hole node that malicious node absorbs the entire packet and dropped them instead of forwarding them to the intended destination which results in denial of communication. Cooperative Black hole means the malicious nodes act in coordination. When the source node wants to initiate a transfer of data packet to the destination, it first broadcast the RREQ packet to the neighbouring nodes. The malicious nodes present in the network, also receive the RREQ. The Black hole nodes respond first to any RREQ, it immediately sends out the RREP.

AODV Routing Protocol:

Ad-hoc On-demand Distance Vector Routing (AODV) is an improvement on the Destination Sequenced Distance Vector routing (DSDV). AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. To find a path to the destination, the source broadcasts a route request packet. The neighbours in turn broadcast the packet to their neighbours till it reaches an intermediate node that has recent route information about the destination or till it reaches the destination. A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only. When a node forwards a route request packet to its neighbours, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet.

IV. SIMULATION SETUP

The Proposed protocol is implemented with the object oriented discrete event simulator. In our simulation, 7mobile nodes move in a 500 meter x 500 meter square region for 200 Seconds simulation time. The Simulator Environment is created by using TCL Script with the help of following parameters included in the table.

Propagation	Two Ray Ground Propagation
No. of Nodes	7
Area Size	500x500 m^2
MAC	802.11
Simulation Time	200 Sec
Traffic Source	CBR
Packet Size	512 bytes
Antenna type	Omni directional
Packet Transmission Power	0.4 mw
Packet Receiving Power	0.1mw
Routing Protocols	AODV
Initial Energy of nodes	X joules (Different Energies are used)

Table.4.1. Simulation Environment

The simulation environment observes by using the Network Animator (NAM). The below figures are the snapshots of simulation environment

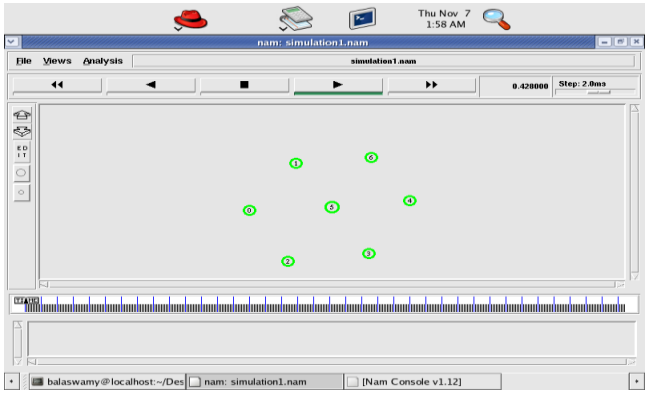

Fig.4.1.Simulation Network Setup

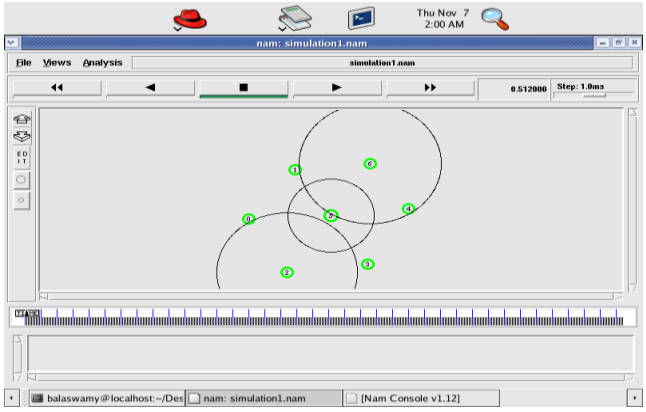

Fig.4.2.Brodcasting

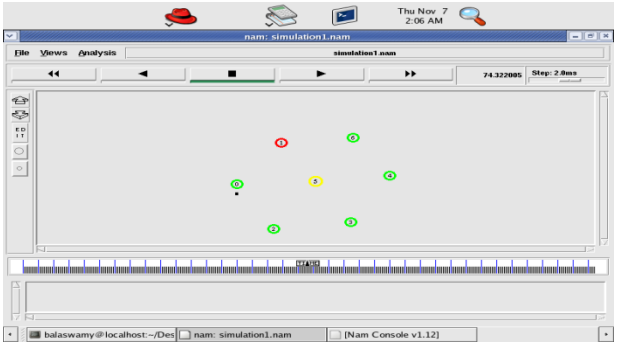

Fig.4.3. First Route Failure without Block hole attack

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

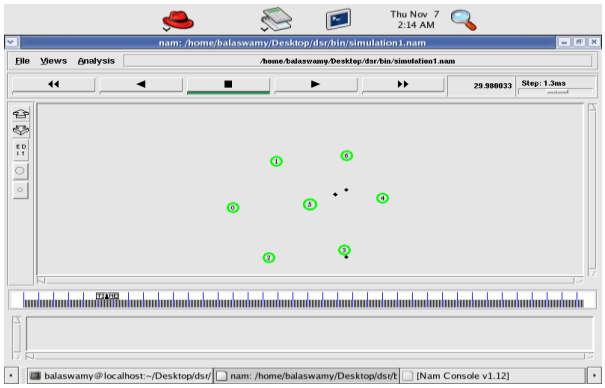

Fig.4.4. the Malicious Node Created 6th Node Dropped Information

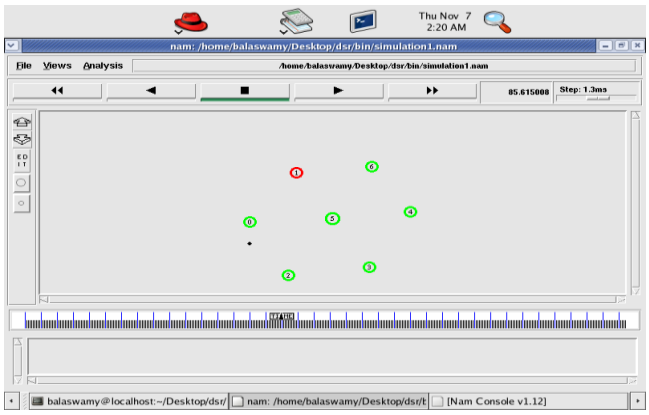

Fig.4.5. First Node Failure time with Block-hole attack

Performance Metrics

Packet delivery ratio: The ratio of the data packets delivered to the destinations to those generated by the CBR sources. Received packets and sent packets number could be easily obtained from the first element of each line of the trace file.
Packet delivery ratio (%) = (received packets/sent packets)*100

Average end-to-end delay: This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.
For each packet with id (Ii) of trace level (AGT) and type (cbr), we can calculate the send (s) time (t) and receive (r) time (t) and average it.

Routing overhead: It is the ratio of the routing packets sent and the total packets sent. Each hop-wise transmission of a routing packet is counted as one transmission.

Calculation of the routing overhead:
Routing overhead = routing packets sent / total packets sent

Network Lifetime: It represents the lifetime of network when the all routes are fail.

Throughput: Throughput refers to the performance of tasks by a computing service or device over a specific period. It measures the amount of completed work against time consumed and may be used to measure the performance of a processor, memory and network communications. It can be represents Bits per Second.

V. EXPERIMENTAL RESULTS

The Results based on the trace files the AODV protocol without Block-hole attacks and AODV protocols with Black hole attack consider the different performance metrics those are First node failure time, Average end to end delay, Packet Delivery Ratio, Drop rate and Throughput.

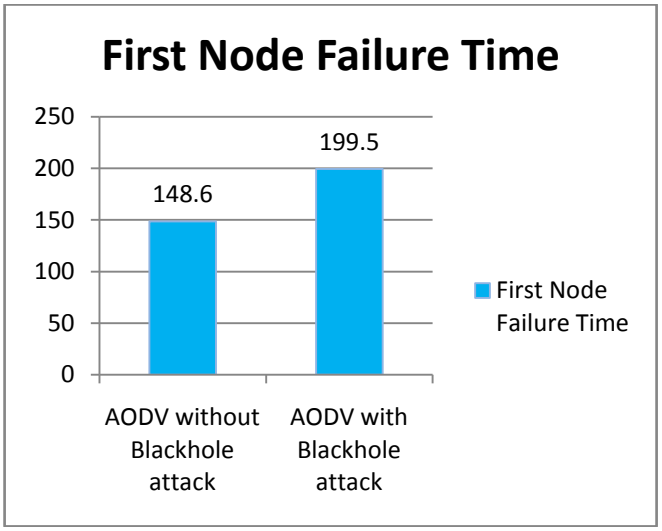

Fig.5.1.First Node Failure Time
The diagram 5.1 shows First Node Failure time consider routing protocol AODV with and without Black-hole attacks

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

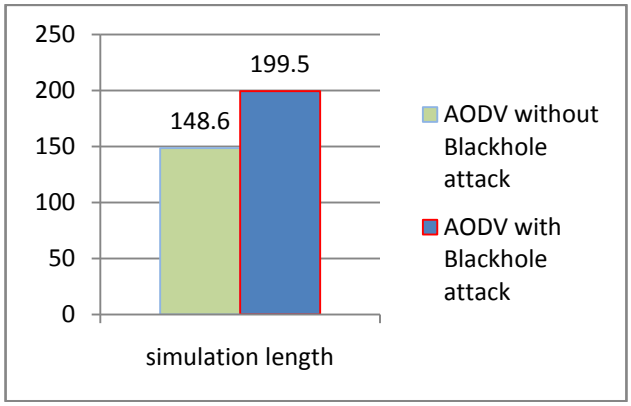

Fig.5.2.Simulation Length
The diagram 5.2 shows Simulation Length consider routing protocol AODV with and without Black-hole attacks

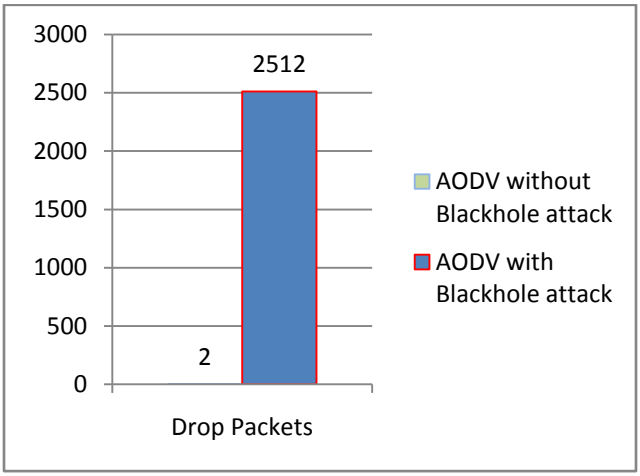

Fig.5.4. Drop Packets

The diagram 5.4 shows Drop Packets consider routing protocol AODV with and without Black-hole attacks

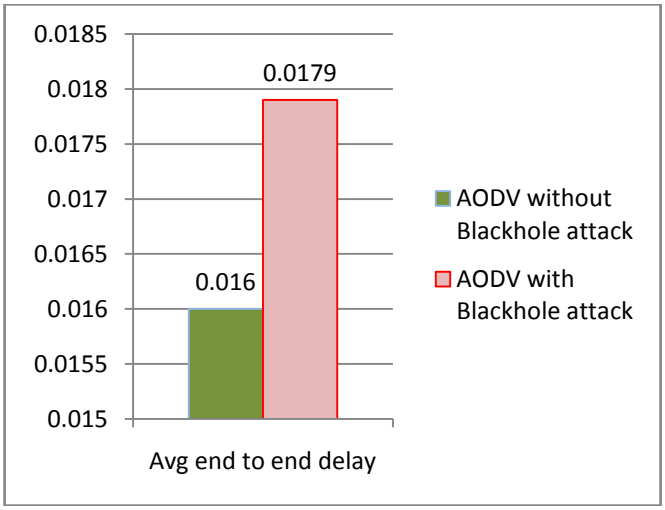

Fig.5.3. Avg end to end delay
The diagram 5.3 shows Avg end to end delay consider routing protocol AODV with and without Black-hole attacks

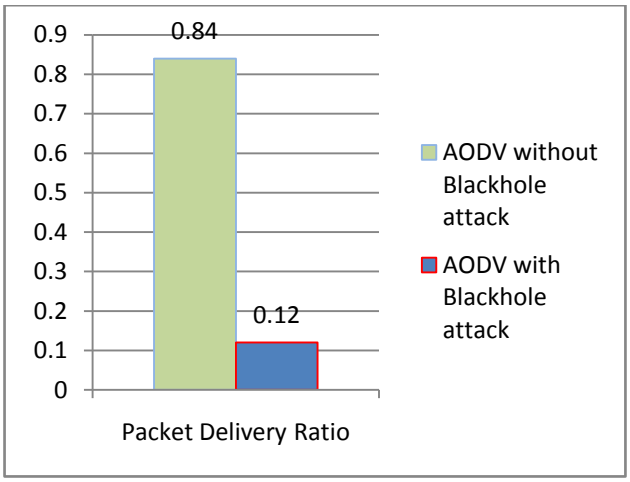

Fig.5.5.Packet Delivery Ratio
The diagram 5.5 shows Packet Delivery Ratio consider routing protocol AODV with and without Black-hole attacks

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 12, December 2013

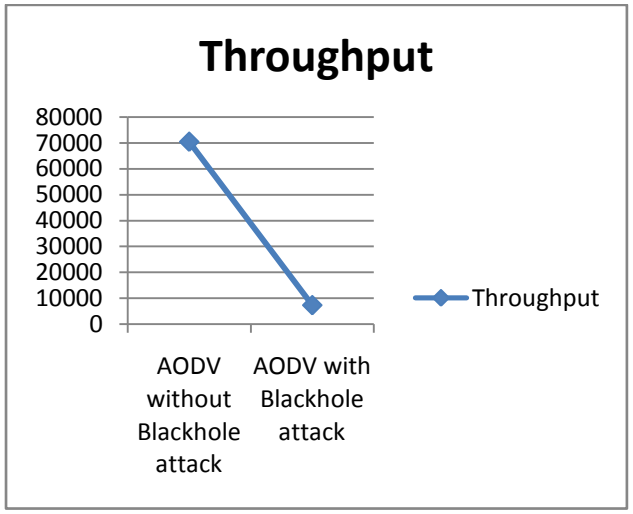

Fig.5.6.Throughput

The diagram 5.6 shows Throughput consider routing protocol AODV with and without Black-hole attacks

VI. CONCLUSION

Generally in MANET the design of Routing protocols are very important criteria because the performance of network depends on the design of routing protocols. In this paper, we are using ad-hoc routing protocol Ad hoc on Demand Vector Routing Protocol (AODV) the main objectives were achieved those are (1). The Black-hole attacks implemented by creating malicious node, (2). Analysed the Cooperative Black-hole Attacks, (3).The Comparison of AODV analysis with Black-hole attacks and without Block-hole attacks through considering the performance metrics First node failure time, Packet Delivery Ratio, Average End to End Delay, Simulation Length, Throughput and Dropped Packet Information analysed the performance of the Mobile Ad-hoc Network with the help of CBR traffic using the NS 2 Software.

REFERENCES

[1] Hesiri weera singhe and Huirong Fu "Preventing Cooperative Black hole attacks in Mobile Ad hoc Network: Simulation Implementation and Evolution" IJSEA Vol.2 No.3 July 2008.

[2] Igor kotenko and Mikhail stepashkin " Attack graph based evolution of Network Security"

[3] Amol A.Bhosle, Tushkhar P.Thosar and Shehal Mehatre "Black hole and worm hole attack in routing protocol in MANET", IJCSEA vol.2, No.1 Feb 2012.

[4] Fan-Hsum Tseng, Lider Chou and Ham- chiehchao " A Survey of Black hole attack in wireless mobile ad hoc networks", Human-Centric Computing and Information Sciences 2011, 1:4

[5] Jim Binkley " Network Security Attacks"

[6] Silbers chatz,Galvin and Gagne " System Security from the operating system principles" 2005.

[7] Xiang- yangli " Cryptograpy and Network Security"

[8] T.Sakthivel, R.M. Chandrasekharan "Detection and Prevention of Worm-hole attacks in MANETs using Path Tracing Approch ", Europian Journal of Scientific Research.

[9] Atteq Ahmad " Types of Security and It's Prevention" International Journal of Computer Technology and Its Application, Vol 3(2) 750-752.

[10] Shinnimittal, Harish taliya " Analysis of Cooperative Black hole Attack using Dynamic Source Protocol" , IJARCSSE, Vol.2, issue 8, Aug-2012.

BIOGRAPHIES

P.Gowrishankar received the B.Tech in Electronics and Communication Engineering from JNTU Kakinada in the year 2010. Now he is pursuing M.Tech from JNTU Kakinada. His area of interest in wireless networks and Mobile Ad-hoc Networks.

N.Srinivasulu presently pursuing his MS degree from JNTU Hyderabad. He received the B.Tech Degree in ECE from JNTU Kakinada. He has published Four Research papers in International Conferences and Three International Journals. His area of Interest is Mobile Ad-hoc Networks, Wireless Communication Networks and VLSI. He is EDAS Identifier and Active Member of IAENG, IAEST and IACSIT Professional Societies.

Dr.Ch.Balaswamy received the B.E degree in ECE from S.R.K.R. Engineering College, Bhimavaram in 1998. He received the M.Tech degree in ECE from Inad College of Engineering , Hassan, India in 2001. He received his Ph.D. from JNTU Ananthapur in 2010. He has 13 years' experience in teaching for U.G and P.G students. He guided many B.Tech and M.Tech projects. He has published Nine International Journals and Seven Research papers in National and International Conferences. His area of Interest is Mobile Ad hoc Networks, Micro Processors & Controllers and Embedded System. He is active member of ISTE, IAENG and IAEST Professional Societies.