International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Issue 11, November 2015
www.ijates.com
ijates
ISSN 2348 - 7550

DESIGN AN INTELLIGENT PROTOCOL FOR SECURITY CHALLENGES IN MANET

E.r Mandeep Singh[1], E.r Ashu Bansal [2]

[1]M.Tech Research Scholar, [2]Assistant Professor, Dept of CSE,
Baba Farid College of Engineering & Technology, Bathinda, Punjab, (India)

ABSTRACT

Mobile Ad Hoc Networks (MANETs) is a self-configuring network of wireless mobile nodes that formed network capable of dynamic changing topology. Each node in the network acts as a router, forwarding data packets to other nodes. MANET have many potential applications such as military services in battlefield, disaster relief operations and in commercial environments. Black hole and Gray hole are two of many attacks that take place in MANET and is considered as one of the most common attacks made against the DSR routing protocol. The black hole attack involves malicious node pretending to have the shortest and freshest route to the destination by constructing false sequence number in control messages.Our approach uses the concept of the trust value which is calculated from the friendship table. Source node starts sending the route request to the nodes in the network. Trust value is calculated by checking the packet delivery ratio of the nodes.The proposed scheme showed better performance over route caching technique. This is primarily due to the fact that the detection of the malicious nodes in the network has been done in the basis of friendship table in the proposed scheme which consists of the trust value of the nodes. The proposed scheme detects the malicious nodes in the network without causing much loss of data which leads to better results.

Keywords: **Manets, Blackhole, Grayhole, DSR, Trust Value.**

I. INTRODUCTİON

In recent years, there have been noteworthy developments in the technology used to build Micro-Electro-Mechanical Systems (MEMS), digital electronics, and wireless communications. This has empowered the advancement of minimal effort, low-force, multi-purpose little sensor nodes that can convey crosswise over short distances. There has been a ton of exploration into routing in wireless sensor networks. Routing in wireless sensor networks is critical, as communication that utilization them.

A network is a framework that comprises of an aggregation of computers and other hardware identified with it connected via communication channel for sharing data and information. There are two sorts of networks Wired and Wireless Networks. Wired network are those network in which computer apparatuses are connected with one another with the assistance of wire. The wire acts as medium of communication for transmitting data from one point of the network to other point of the network. While a wireless network is a network in which computer devices communicates with each other without requiring any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with any alternate device, the

objective device must lie within the radio range of each other. The transmission and reception of data in wireless sensor network networks is done using the electromagnetic waves. Recently wireless networks are getting well known as a result of its versatility, simplicity and extremely moderate and cost sparing establishment. Mobile Ad-Hoc Networks comes under Wireless Networks. Wireless networks are getting well known because of their convenience. User is no more subject to wires where he/she is, easy to move and appreciate being connected to the network. One of the incredible characteristics of wireless network that makes it fascinating and unique amongst the conventional wired networks is mobility. This characteristic gives client the capability to move freely, while being associated with the network. Wireless networks are relatively easy to install than wired networks. There is nothing to worry about the establishment of the hardware outlays. Wireless networks could be designed consistent with the need of the clients. These can run from little number of clients to substantial full foundation networks where the amount of clients is in thousands.

II. RELATED WORK

Effect of Black Hole Attack on MANET Routing Protocols by Jaspal Kumar, M. Kulkarni, Daya Gupta (2013). In this paper, the effects of Black hole attack on mobile ad hoc routing protocols have been analysed. Due to the massive existing vulnerabilities in mobile ad-hoc networks, they may be insecure against attacks by the malicious nodes. Mainly two protocols AODV and Improved AODV have been considered. Simulation has been performed on the basis of performance parameters and effect has been analysed after adding Black-hole nodes in the network. Finally the results have been computed and compared to stumble on which protocol is least affected by these attacks.

A Survey of Attacks on Manet Routing Protocols by SupriyaTayal, Vinti Gupta (2013).This paper states that an Adhoc network is a network in which nodes communicate without using any network infrastructure and move in random order. MANET is an attractive technology for many applications, such as rescue and tactical operations, due to the flexibility provided by their dynamic infrastructure. MANET is an autonomous system of wireless mobile hosts without fixed network infrastructure and centralized access point such as a base station. Due to lack of a defined central authority, MANETs are more vulnerable to security attacks and thus security is essential requirement in MANET as compared to the wired network. In this paper an attempt has been done to represent an overview of AODV, the possible attacks on MANET and some security mechanism to these attacks.

Black Hole Attack in Manet's: A Review Study by Dr. A. A. Gurjar,A. A. Dande (2013). Black hole attack is one of the possible attacks in MANET. In black hole attack, a malicious node sends the route reply message to the source node in order to advertise itself for having the shortest path to the destination node. The malicious node reply will be received by the requesting node before the reception of the any other node in the network. When this route is created, malicious node receives the data packet, now it's up to the malicious node whether to drop all the data or forward it to the unauthenticated nodes. This paper deals with the study aspect of this black hole attack.

Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview by Swati Jain, Naveen Hemrajani (2013). This paper describes the features, application, and vulnerabilities of mobile ad hoc network also presents an overview and the study of the attacks and their mitigation in routing protocols. As the

increase of wireless networks, use of mobile phones, smart devices are gaining popularity so the adhoc network is also an uprising field. Each device in a MANET is free to move independently in any direction, linking to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, and quality of service, limited bandwidth and limited power supply etc.

A Survey on Detection of Blackhole Attack using AODV Protocol in MANET by Ms Monika Y. Dangore, Mr Santosh S. Sambare (2013). In this paper, an attempt is made to understand the possible solutions to Blackhole attack with various methodologies proposed earlier. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. AODV (Ad-hoc On-demand Distance Vector) is a loop-free routing protocol for ad-hoc networks. It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviors such as node mobility, link failures etc. Blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

An Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network by Arnab Mitra, Rajib Ghosh, Apurba Chakraborty, Debleena Srivastva (2013). This research work reports on Alive and Black Hole node detection if it exists in any Mobile ad hoc networks (MANETs). The dynamic topology of MANETs allows nodes to join and leave the network at any time instance. This general feature of MANET has exposed to major security attacks including existence of black hole nodes, which adversely affects the entire routing practice. To deal with this routing mess, an Artificial Neural Network (ANN) based automated Black Hole node detection tactic has been proposed, which is capable of detecting the existence of Black hole node(s) in the MANET and thus helps to minimize the smash up in reliable routing procedure. Experimental results in network simulation confirm the hazards caused by presence of Black hole node(s) in MANET, which is same as our earlier research on black hole node detection using Cellular Automata (CA).

Survey on Prevention of Black Hole Nodes in Mobile Adhoc Networks by Pooja Vij, V. K. Banga, TanuPreet Singh (2012).This paper states that a wireless Adhoc network is a collection of mobile nodes with no pre-established infrastructure, forming a temporary network. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality.

One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc On-Demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack. In this paper, Black hole nodes or malicious nodes are detected and after detecting it those nodes are removed and also shortest path from source to destination is found by using GLOMOSIM. It is proposed that this protocol is increase the throughput, security and life time of the network by reducing the delay than the other conventional AODV protocols.

Detection and Prevention of Blackhole Attack in MANET Using ACO by Sowmya K.S, and Deepthi P Hudedagaddi (2012).This paper presents introduction about MANET and brief description of attacks in MANET. With the increase in use of MANETS, security has become an essential requirement to provide

protected communication between mobile nodes. In this paper, a method to detect and prevent blackhole attacks by notifying other nodes in the network of the incident.To overcome the challenges, there is a need to build a multi fence security solution that achieves both broad protection and desirable network performance. It has been explained that MANETs are vulnerable to various attacks and Blackhole is one of the possible attacks. It has been explained about ANT NET, where ACO system and pseudocode of it has been proposed.

Preventive Aspect Of Black Hole Attack In Mobile Ad Hoc Network by RajniTripathi and Shraddha Tripathi (2012). In this paper the prevention mechanism for black hole in mobile ad hoc network is presented. The routing algorithms are analysed and discrete properties of routing protocols are defined. The discrete properties support in distributed routing efficiently. The protocol is distributed and not dependent upon the centralized controlling node. Important features of Ad hoc on demand vector routing (AODV) are inherited and new mechanism is combined with it to get the multipath routing protocol for Mobile ad hoc network (MANET) to prevent the black hole attack. When the routing path is discovered and entered into the routing table, the next step is taken by combined protocol to search the new path with certain time interval. The old entered path is refreshed into the routing table. The simulation is taken on 50 moving nodes in the area of 1000 x 1000 square meter and the maximum speed of nodes are 5m/sec. The result is calculated for throughput verses number of black hole nodes with pause time of 0 sec. to 40 sec., 120 sec. and 160 sec. when the threshold value is 1.0.

III. BLACK HOLE ATTACKS IN MANETS

Because of the way of occasions that prompts the utilization of MANETs such as communication during natural disasters, on the battlefield, and business conferences, there is a need for ensured security of data transfer between two communicating nodes. Thus, secure routing protocols have been recently proposed. Secure routing protocols are mostly intended to prevent hazards to safety properties, such as: (i) identity authentication and non-reputation; (ii) availability of resources; (iii) integrity; (iv) confidentiality and privacy.

MANETs must possess a secure way for transmission and communication and this is highly challenging and crucial issue as there are increasing threats of attack on the Mobile Networks. Security is the cry of the day. With a specific goal to provide secure communication and transmission, it is most extreme vital to understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more prone to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

A Black Hole attack scrambles the route by forging a routing message, and then, further either eavesdrops or drop the packets, posing a possible threat to safety properties. A Black Hole attack forges the sequence number and hop count of a routing message to forcibly acquire the route, and then eavesdrop or drop all data packets that pass. A malicious node impersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery.

A Black Hole node has two properties: (1) the node exploits the ad hoc routing protocol and advertises itself as having a valid route to a destination, even though the route is spurious, with the intention of intercepting packets, and (2) the node consumes the intercepted packets.

The method how malicious node fits in the data routes varies shows how black hole problem arises. Node 1 is source node whereas node 4 is destination node. Source node broadcasts route request packet (RREQ) to find a route to destination node; with the normal intermediate nodes receiving and continuously broadcasting the RREQ, except the Black Hole node. Everything works well if the RREP from a normal node reaches the source node first. Here node 3 is attacker and acts as black hole. Node 3 sends a route reply packet (RREP) to the source node. But a route reply from node 3 reaches to source node before any other intermediate node. This makes the source node to conclude that the route discovery process is complete, ignoring all other RREPs and beginning to send data packets. The Black Hole node would directly send a route reply (RREP) to the source node S, with an extremely large sequence number and hop count of 1. The destination node D would also select a route with a minimum hop count upon receiving RREQs from normal nodes, and send a RREP packet. In this case source node sends the data packet to destination node through node 3. But as the property of black hole node that this node does not forward data packets further and dropped it. But source node is not aware of it and continues to send packet to the node 3. In this way the data, which has to be reached to the destination, fails to reach there. There is no way to find out such kind of attack. These nodes can be in large number in a single MANET, which makes the situation more critical.

The malicious node always sends RREP as soon as it receives RREQ without performing standard DSR operations, while keeping the Destination Sequence number very high. Since DSR considers RREP having higher value of destination sequence number to be fresh, the RREP sent by the malicious node is treated fresh. Thus, malicious nodes succeed in injecting Black Hole attacks. DSR is a reactive routing protocol. It verifies the best possible route only when packet needs to be forwarded. The process to find a path is just executed when a path is required by a node, which leads to On-Demand Routing. The DSR protocol is made out of two main mechanisms route discovery and maintenance. Route Discovery: When a source node S wishes to send a packet to the destination node D, it obtains a route to D. This is called Route Discovery. Route Discovery is used only when Source needs to send a packet to Destination and has no information of a route to it. Route Maintenance: The existing routes are no longer usable when there is a change in the network topology. In such a scenario, the source S can use an alternative route to the destination D, or invoke Route Discovery. This is called Route maintenance.

IV. FRIENDSHIP TABLE TECHNIQUE

1. Deploy the nodes in the network.
2. Choose source and destination node.
3. Source node starts sending the route request to the nodes in the network.
4. Trust value is calculated by checking the packet delivery ratio of the nodes.
5. If any node is not correctly forwarding the packets and is dropping them then the trust value of -1 is assigned to it.
6. If the node is correctly forwarding all the packets then the trust value is assigned to be +1.
7. All the trust value of the nodes along with ID of the nodes is printed into table referred to as friendship table.
8. When the route request reaches the destination node, the trust value of all the nodes in the path is calculated and added up to get the trust value of the path.

9. The path having the highest trust value is selected to send the data.
10. The destination node replies to the source node via path having highest trust value.

V. RESULTS AND DISCUSION

The proposed system was implemented in NS2.35. The figures shown below are the graphs for the parameters that were analyzed to check the performance of the network. The parameters used were : Energy Consumption, Routing overhead, Packet Delivery Ratio and Throughput.

1. Energy Consumption - It is one of the most important parameter that is important to the life of the network. Lesser the energy consumption better is the performance of the network. The proposed scheme not only detects the malicious nodes in the network but it is also efficient in terms of energy consumption.

2. Routing overhead - It is defined as ratio of number of routing packets sent in the network to the number of data packets received. If the routing overhead is less, it would mean that less routing is required to received the data in the network and better is the performance of the network.

3. Packet Delivery Ratio - It is ratio if number of data packets received to the number of data packets sent in the network. If the malicious nodes are present in the network, this parameter becomes important to analyze as it tends to reflect how much dropping is occuring in the network. More the PDR, lesser the packet dropping and better the performance of the network.

4. Throughput - It is amount of data received at the destination node. More the throughput better is the performance of the network. If the algorithm is able to detect the malicious nodes in the network then the throughput tends to be more.

The parameters that were used in simulation are shown in table below :

Simulator	NS2.35
Channel	Wireless Channel
Propagation Model	Two Ray Ground
Queue	CMU
Antenna	Omni-Directional
Energy Model	Radio Energy Model
Simulation Area	1000*1000

Table1:Simulation Parameters

Comparison Graphs between Proposed technique and Route caching technique.

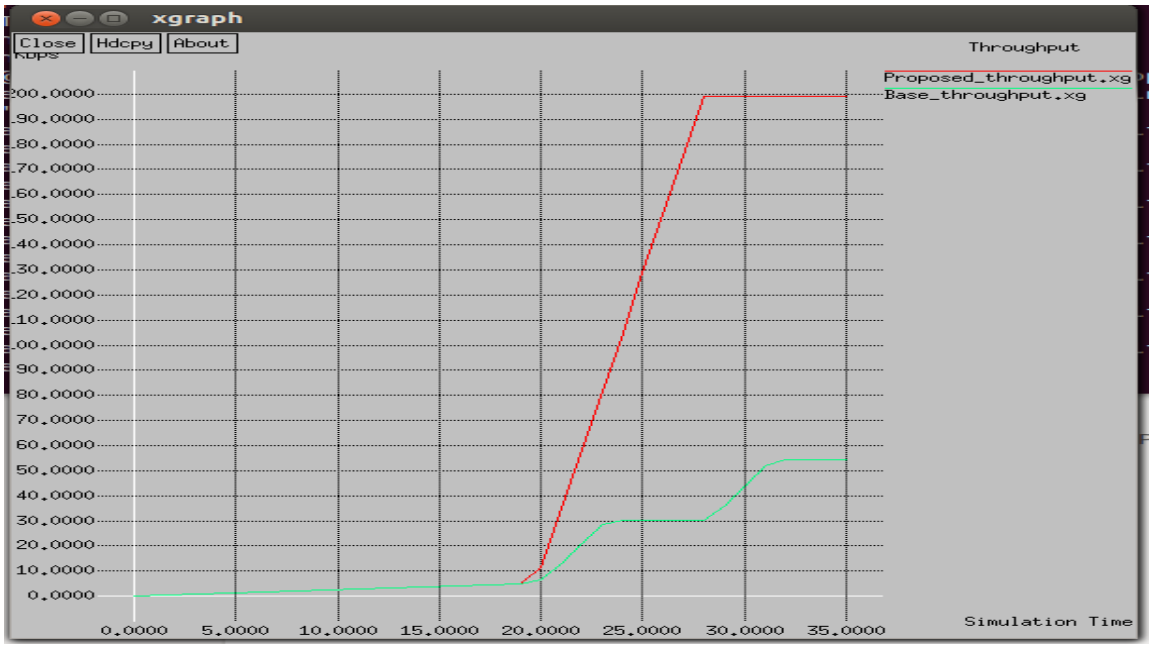

Fig: Comparison of Throughput (Proposed And Route Caching Technique)

The throughput of the proposed scheme is found to be better than the one obtained by route caching Technique.The throughput is found to be 200 Kbps.

Fig: Comparison of PDR (Proposed Scheme and Route Caching Technique)

The Packet Delivery Ratio for the proposed scheme has shown better performance over the route caching technique.

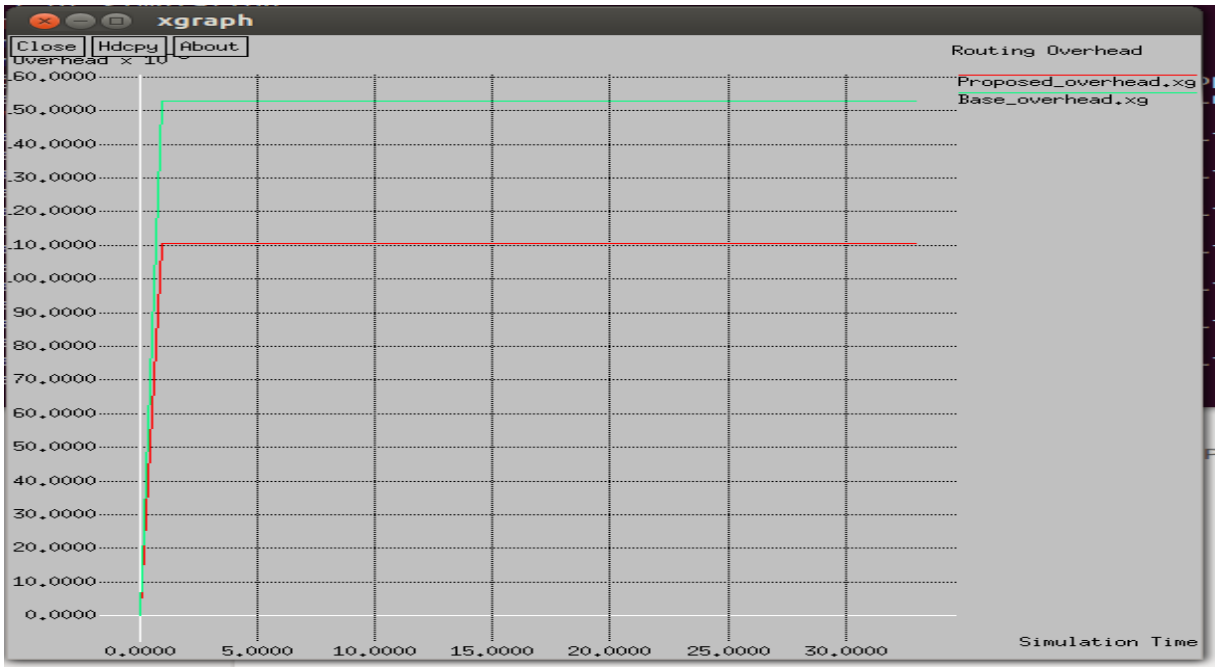

Fig: Comparison of Routing Overhead (Proposed scheme with Route Caching Technique)

The routing overhead for the proposed scheme is found to be 0.11.

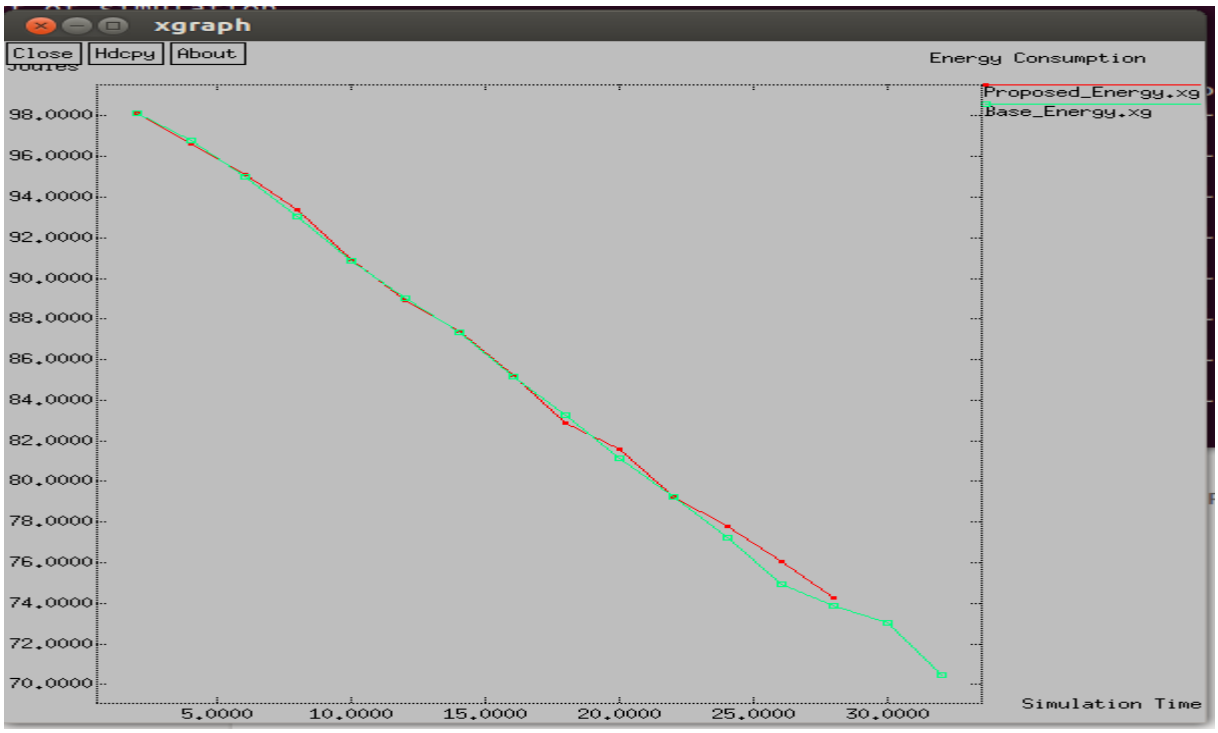

Fig: Energy Consumption Comparison(proposed scheme and route caching technique)

The proposed scheme has found to consume less energy than the route caching technique.

VI. CONCLUSION

The proposed scheme as well as route caching technique was implemented on NS2.35. The performance of the both the schemes was analyzed in the presence of gray hole and black hole nodes. The parameters that were used to check the performance of the network was packet delivery ratio, throughput, energy consumption and routing overhead. The proposed scheme showed better performance over route caching technique. This is primarily due to the fact that the detection of the malicious nodes in the network has been done in the basis of friendship table in the proposed scheme which consists of the trust value of the nodes. The proposed scheme detects the malicious nodes in the network without causing much loss of data which leads to better results.
In the future work, we can also take into account various other attacks like clone attacks in which the nodes are clones of each other, wormhole attacks etc. and analyze the performance of friendship table technique.

VII. ACKNOWLEDGEMENTS

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

REFERENCES

[1] Jaspal Kumar, M. Kulkarni, Daya Gupta, " Effect of black hole attack on manet routing protocols",Volume 5, Issue 5, April 2013, ISSN: 2074-9090 International Journal of Computer Network and Information Security (IJCNIS).

[2] Supriya Tayal, Vinti Gupta, "A Survey of attacks on manet routing protocols," Volume 2, Issue 6, June 2013 International Journal of Innovative Research in Science, Engineering and Technology.

[3] AA Gurjar, AA Dande, " Black hole attack in manet's: A review study", Volume 2, Issue 3, March 2013, ISSN: 2319-4413 International Journal of IT, Engineering and Applied Sciences Research (IJIEASR).

[4] Ms Monika Y. Dangore, Mr Santosh S. Sambare, "A survey on detection of blackhole attack using AODV protocol in manet", 2013 Internation conference on cloud & ubiquitous computing, IEEE.

[5] Arnab Mitra, Rajib Ghosh, Apurba Chakraborty, Debleena Srivastva, "An alternative approach to detect presence of black hole nodes in mobile Ad-Hoc network using artificial neural network", Volume 3, Issue 3, March 2013, ISSN:2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering.

[6] Puja vij, V. K. Banga, Tanu Preet Singh, " Survey on prevention of black hole nodes in mobile ad hoc networks ", Volume 12, Issue 5, July 15-16, 2012 International Conference on Trends in Electrical, Electronics and Power Engineering.

[7] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, "Detection and Prevention of blackhole attack in manet using ACO", Volume 12, Issue 5, May 2012 IJCSNS International Journal of Computer Science and Network Security.

[8] Swati Jain, Naveen Hemrajani, "Detection and mitigation techniques of black hole attack in manet: An Overview", Volume 2, Issue 5, May 2013, ISSN:2319-7064 International Jounral of Science and Research (IJSR).

[9] Rajni Trioathi And Shraddha Tripathi, "Preventive aspect of black hole attack in mobile adhoc network", July 2012, ISSN: 2231-1963, International Journal of Advances in Engineering & Technology.