ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (196-204), Month: July - September 2014, Available at: www.researchpublish.com

A WEIGHTED CLUSTERING ALGORITHM FOR IMPROVING MANET SECURITY

[1]Shirsty Chandel, [2]Prof. Ashish Tiwari

Computer Science & Engineering Department, Rajiv Gandhi Technical University
Airport Road, Gandhi Nagar Bhopal-462 033,India

Vindhya Institute of Technology and Science, Umrikheda, Khandwa Road, Indore (M.P.), India

Abstract: **Mobile ad-hoc network (MANET) is an autonomous system connected by mobile nodes with wireless links. Due to absence of infrastructure, MANET is used in various applications, such as battlefield, business applications, and remote areas. As, communication among the nodes is through the insecure wireless link, security is very important issue for this type of networks. MANET is vulnerable to attacks such as Black hole attack, Gray hole attack, wormhole attack, Sybil attack, and Route table modification attack. Which is based on cluster organization of network, this paper provides is approaches are detected and prevent the black hole attack over the MANET. Most of them use the properties of malicious activities of node and network during attack condition. These techniques are provides the efficient detection and prevention over MANET environment this techniques are limited to adopt a single problem of security from black hole detection.**

Keywords: **MANET, Black hole attack, MAC, AODV, QOS.**

I. INTRODUCTION

MANET is an autonomous and decentralized wireless system. It is also called self organized, infrastructure less networks. Each node not only operates as an end system, but also acts as a router to forward packets. Nodes cooperate with each other to route the control and the data packets from source to destination. Routing in MANET is classified in two types proactive (table driven) and reactive (On-Demand). In a proactive routing protocol, nodes periodically exchange routing information with other nodes. In a reactive routing protocol, nodes will exchange routing information only when needed. Due to dynamic changing topology, open medium, and no clear line defense attacks on MANET are possible. Attacks in MANET are classified into two types: passive attacks and active attacks. A passive attack does not disrupt operation of protocol; trap the information by listening to the traffic. An active attack involves action such as modification and deletion of exchanged data.[1] A MANET is a self configuration distribute dynamic network in which the nodes are mobile and communication is not via fixed access points. Since they act open medium any node in space can be a part mantes have a hug applicability potential as they have the potential to be anytime. Although features of MANET attack huge applicability , they also manifest vulnerability this vulnerability to attack imposes unreliability a condition that cannot be compromised especially in emergency situation that the MANET are exposed to , these attack can be classified as active and passive attack. In active attack the adversary breaks into the system and is able to insert and capture transmission thus modifying or corrupting the data whereas in passive attack the adversary merely listens to the transmission [2] In a MANET node can communicate directly with each other's wireless transmission range. So that a multi hop concept produces where various number of intermediate hosts transfer the packet which are sent by the source host before they reach the destination host the success of communication between two nodes is highly depends on other node cooperation.[3] The advantages of rapid network convenient communication and other advantages make it has been widely used in the aspects of military, commercial, emergency service and etc.[4] A Mobile Ad hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in

radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the node has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other; however the node 2 can be used to forward packets between node 1and nodes 2. The node 2 will act as a router and these three nodes together form an ad-hoc network. [5]

MANETs have some special characteristic feature such as unreliable wireless media (links) used for communication between hosts. Constantly changing network topologies and membership, limited bandwidth battery, lifetime and computation power of node etc while these characteristics are essential for the flexibility of MANETs they introduce specific security concerns that are absent or less servers in wired network.

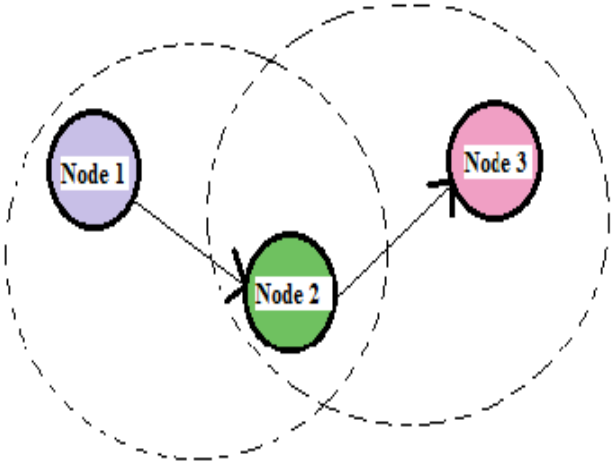


Figure 1 Example of Mobile Ad-hoc Network

A. ***Types of MANET***

1. Vehicular Ad-Hoc Networks (VANET's) - VANET is a type of Mobile Ad-Hoc network where vehicles are equipped with wireless and form a network without help of any infrastructure. The equipment is placed inside vehicles as well as on the road for providing access to other vehicles in order to form a network and communicate.
2. Intelligent Vehicular Ad-Hoc Networks (InVANET's)- Vehicles that form Mobile Ad-Hoc Network for communication using WiMax IEEE 802.16 and Wi-Fi 802.11. The main aim of designing InVANET's is to avoid vehicle collision so as to keep passengers as safe as possible. This also help drivers to keep secure distance between the vehicles as well as assist them at how much speed other vehicles are approaching. InVANET's applications are also employed for military purposes to communicate with each other.
3. Internet Based Mobile Ad-Hoc Networks (iMANET's) - These are used for linking up the mobile nodes and fixed internet gateways. In these networks the normal routing algorithms does not apply. [7]

B. ***Attack in MANET***

These attacks can be classified into two types:

1) External attack- External attack are carried out by nodes that do not belong to the network it causes congestion sends false routing information or causes unavailability of services
2) Internal attack- Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other node and may participate in other network activities

C. ***Application of MANET***

The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional

infra structured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include

1. Military Battlefield: Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.
2. Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.
3. Local Level: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.
4. Personal Area Network (PAN)**:** Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.
5. MANET-VoVoN**:** A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. Using MANET-JXTA, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signaling protocol based on the exchange of XML messages over MANET-JXTA communication channels [5]

D. *MANET's Challenges*

1) Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
2) Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.
3) Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.
4) Hidden terminal problem**:** The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
5) Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, and frequent path breaks due to mobility of nodes.
6) Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.
7) Battery constraints: Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.
8) Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks. [8]

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (196-204), Month: July - September 2014, Available at: www.researchpublish.com

II. BACK GROUND

MANET is susceptible to various types of routing attacks such as Black hole, Gray hole, Worm hole, Sybil attack, and resource consumption attack. A black hole attack is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and absorb them without forwarding them to the destination Fig. shows how the Black hole problem arises. In Figure 2, A wants to send data packet to node D. To initiate the process reactive routing protocol is involved. In the process of route discovery if node C is malicious node it replies to Node A as soon as it receives RREQ, the existence of a path through it to node D. Node A and receiving the reply from node C, will ignore another route replies from rest of nodes in MANET without checking the validity of path received from node C. Node C will consume all the packets or drops. The presence of misbehavior nodes packet delivery ratio was decreased. To identify misbehaved node in the route trust management is used. To improve security in MANET need a mechanism that allows a node to evaluate trustworthiness of other nodes. [1]

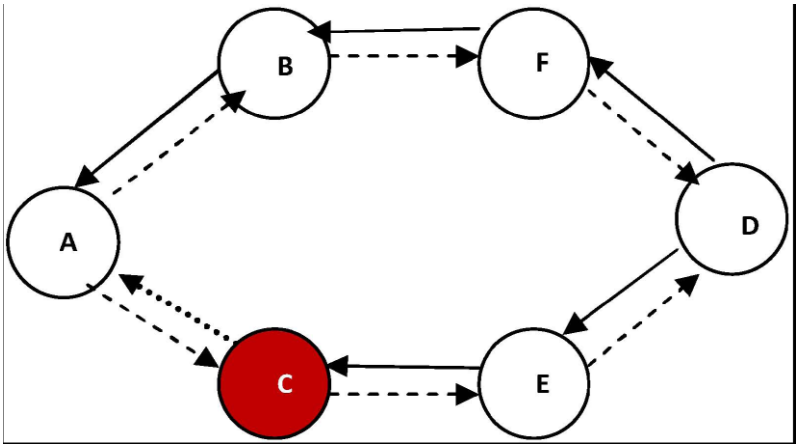


Figure 2 Black Hole Attack

A particular severe attack among several routing attack is called black hole attack. In this attack, a malicious node tries to capture the path toward itself by falsely claiming larger sequence number and smaller hop count to the destination and then absorb all data packet without forwarding them to destination node. Black hole attack have serious impact on routing algorithm which uses sequence numbers to determine fresh messages and select the shortest route based on the hop count such as Dynamic source routing (DSR) or Ad hoc On-Demand distance vector routing (AODV).[5] Sometime this black hole attack is also called as packet drop attack. This a type of denial of service in which the router or any device wait for reply from its destination but the packet dropped by the malicious node which is working as hop between source and destination. The black hole attack is much more serious problem the other attack on the wireless network. [9]

A. *Type of black hole attack*

1) Internal black hole attack

A name implies that it is present in the network internally. Here the internal malicious node fits in between the routes of source and destination. As its present internally so this node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is called an internal attack because here node itself belongs to the network internally. Internal attack is more severe to attack because here malicious node present inside the network actively.

2) External black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

External black hole attack can be summarized in following points:

1. Malicious node detects the active route and notes the destination address.

2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.

3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.

4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node. The new information received in the route reply will allow the source node to update its routing table. 5. New route selected by source node for selecting data. The malicious node will drop now all the data to which it belong in the route. [10]

B. *How black hole node affects MANET*

Black hole attack is one of many possible attacks in MANET. In AODV, during the route discovery phase when nodes receive a route request message it replies to the source node with the route reply. Message in which it consists of number of hops that were required in order to transfer the data to the destination and also the sequence number and on the basis of those route reply message, network judge which one will be the best route for sending the data to the destination. It will generate a route request massage (RREQ).This control message is forward the control message to their neighbors' node. This process of finding destination node goes on until it finding destination node goes on until it finds a node that has fresh enough route to the destination or destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node .A black hole node also operates by replying for a RREQ message come from any source in the network as the node itself is a nearest node to the destination and receive all the packet of data meant for some other node.[11]

C. *Detection and prevention techniques of black hole attack in ADVO*

i. ***Detection, Prevention and Reactive AODV (DPRAODV) Scheme:*** This is a new control packet used. This packet called ALARM is used in DPRAODV. While other concepts are the dynamic these hole value unlike normal AODV, the RREP sequence number is extra checked whether higher than the threshold value or not. If the value of RREP sequence number is higher than the threshold value, the sender is referenced as an attacker and updated it to black list. The ALARM is sent to its neighbors who includes the black list, thus the RREP from the malicious node is blocked but is not processed. DPRAODV simply detects multiple black hole rather than cooperative black hole attack. The advantage of DDPAODV is that it achieves an obviously higher packet delivery ration than the original AODV, except for it takes a little bit higher routing overhead and end to end delay, but DPRAODV simply detects multiple black hole rather than cooperative black hole attack.

ii. ***DRI Table and Cross Checking Scheme:*** this technique is used DRI table. This table cross checking method is use to identify the cooperative black hole nodes, and utilize modified AODV routing protocol to achieve this methodology. The table, 1 represents for true and 0 for false table is used two bit 'from' and 'through' which stand for information on routing data packet from the node and through the node respectively the advantage of this technique is it can identify multiply collaborative black hole nodes. The drawback of these techniques is that mobile node has to maintain an extra database of past routing experience in addition to a router work of maintaining the router table.

iii. ***Distributed Cooperative Mechanism (DCM):*** It is used to solve the collaborative black hole attack in AODV routing protocol, because the node works cooperatively, they can analyze and detect, multiple black hole attack. The DCM is composed of four sub modules like, local data collection, local detection, and cooperative diction and global reaction. Advantages of this technique is that DCM has a higher data delivery ration and there detection rate even if there are various black hole nodes

iv. ***Neighborhood-based and Routing Recovery Scheme:*** In this method source node sends a modify route entry control packet to destination node to renew routing path in the recovery protocol. In this scheme, not only a lower detection time and higher throughput are acquired, but the accurate detection probability is also achieved. The main limitation of this scheme is that it becomes useless when the attacker agrees to forge the take reply packets.

v. ***Redundant Route Method and Unique Sequence Number Scheme:*** In this scheme there are two techniques to prevent the black hole attack. The first technique is to find a true path to the destination. A method based on neighbor set information is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two steps are: 1- Collect neighbor set information. 2-Determine whether there

exists a black hole attack. In Response procedure, Source node sends a modify Route Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. This scheme effectively detects black hole attack without introducing much routing control overhead to the network find at least two routes from the source to the destination node. The working of this scheme is as follow: Firstly the source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route to the destination will reply to this RREQ packet and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are it represents that there are at least two routing paths existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are last-packet-sequence-numbers which is used identify the last packet sent to every node and the second one is for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not. Simulation result shows that these techniques have less numbers of RREQ and RREP when compared to existing AODV. Second technique is considered to be good as compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol. The limitation for this technique is these both techniques fail to detect cooperative black hole attacks. [10]

III. EXCLUSIVE METHOD

The proposed approach is a device specific approach of for optimizing the detection and prevention of Black hole attack. In the proposed system nodes and devices are organized using a fix infrastructure of MANET devices, where devices are categorized in the following manner.

1. ***Mobile Nodes:*** these nodes are collection of the mobile devices and follow the law of independent mobility, these nodes are those who are actually uses the network and their services. These nodes are frequently participating in communication. Additionally able to send, receive and route data during communication sessions as tradition of MANET. But they are only receives services from the nearest cluster heads.
2. ***Cluster Heads:*** these nodes are basically static access points which installed separately by the service provider. These nodes are participating in communication when intra-cluster communication occurs. The primary objective of these cluster heads, to monitor the communication between trusted nodes, when new mobile node trying to communicate with internal cluster or trusted node then data sending and receiving is the main responsibility of these nodes.
3. ***Monitoring Server:*** this device is used to calculate the trust value for securing the network from attack. In addition of that these nodes are also responsible for elimination of nodes that are performing malicious activities in Network. That is performed using MANET's Black hole characteristics.

The arrangement of these nodes are given by fig 3, where arrangements of above given nodes are provided. On the basis of their functionality of network attack formation and detection process is described.

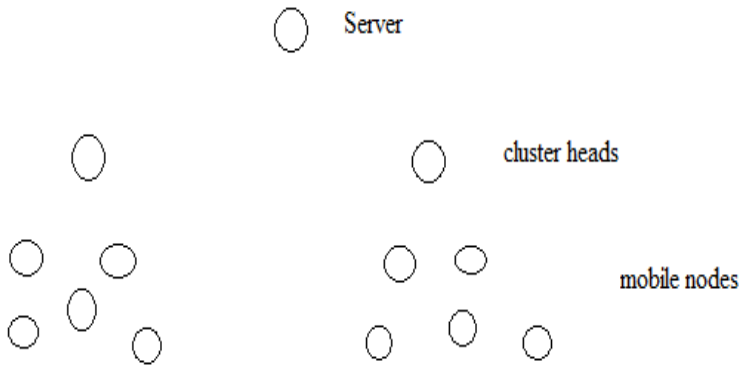
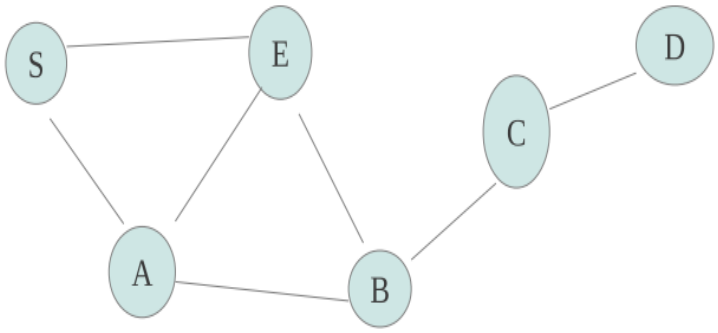


Figure 3 Shows Network the Proposed

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (196-204), Month: July - September 2014, Available at: www.researchpublish.com

In a MANET when we using ad-hoc types of routing ,if nodes want to communicate than the route search has been start, there are different types of packets in a MANET such as data packets and routing packets routing packets are which is used for path searching from source to destination so the source send a routing packets known as RREQ packets which also known as request packets contain all the information about source and destination and these packets flood to his neighbours nodes than they send it to their neighbours nodes so these packets travel hole network and then when they find out the destination they reply message were start to sending form destination ends and a route has been establish .The other types of packets are data packets which contains data .In above picture shows a MANET where solid lines shows the paths between all the nodes ,S is our source and D is our destination when source S want to send data it start sending RREQ packets and then D reply to other networks nodes when sending nodes received these packets it starts sending data packets from its shortest path. In our work we maintain a history table which contain send packets ,received packets and dropped ratio which is calculated by using received packets/ send packets for every node in our network than all the values of dropped ratio we calculate a average value which lies in between 0 to 1 and we set it to our threshold value than for finding out malicious node we apply a algorithm which is depend on the dropped ratio of every nodes if the node's average value of node is multiple of average value of dropped ratio is less than or equal to 0 ,than these node is set to know and data sending is continue , else the value is more than 0 than these node is set to suspected node and then we check by using other method by using these method we can set it to finally as know or unknown node ,in these method we send RREQ packets 3 times to these nodes for testing to it ,if these packets are dropped than it set to be unknown for our network if the condition false and packets are not dropped than the node are safe to communicate to other nodes.



The Median is the 'middle value' in your list. When the totals of the list are odd, the median is the middle entry in the list after sorting the list into increasing order. When the totals of the list are even, the median is equal to the sum of the two middle (after sorting the list into increasing order) numbers divided by two. Thus, remember to line up your values, the middle number is the median! Be sure to remember the odd and even rule.

Find the Median of: 9, 3, 44, 17, 15 (Odd amount of numbers)
Line up your numbers: 3, 9, 15, 17, 44 (smallest to largest)
The Median is: 15 (The number in the middle)

Find the Median of: 8, 3, 44, 17, 12, 6 (Even amount of numbers)
Line up your numbers: 3, 6, 8, 12, 17, 44

Add the 2 middles numbers and divide by 2: 8 12 = 20 ÷ 2 = 10
The Median is 10.

	Nodes	Sending packet	Receiving packet	dropped ration
A	**8**	**7**	**.8**	
B	**9**	**8**	**.8**	
C	**5**	**4**	**.8**	
D	**7**	**6**	**.8**	
E	**9**	**10**	**.8**	
Thres_value		**.8**		

Here we apply a neural network for evaluating the above table thus we the above table is provided as input for neural network and the neural network is trained using the given values. For training of neural network required some important parameters such as number of training cycle, input layers, number of training patterns and learning rate. Neural network uses the number of training cycles for correcting the error in output omitted. That error is evaluated as Error = actual output – output found and these values are adjusted in the neural network weights; the activation function of a node defines the output of that node given an input or set of inputs. The output calculation is performed as the below given function.

$$\mathcal{Y} = \sum_{i=0}^{n} w_i \quad x_i$$

n = the number of input units to the neuron
w_i = the i™ weight
x_i = the i™ input value to the neuron

IV. REVIEW

Summarize the different type of method used in different papers.

The research work which is done by, **Black hole attack and their counter measure based on trust management in MANET: A survey** in **2011**. In this research work, what is MANET and classified the MANET or introduction of black hole attack. There are many solution proposed for management and malicious node detention has been briefly explained.

GAODV: A modified AOV against single and collaborative black hole attack in MANET in their research work of **2013** showed that the type of attack in MANET, they are two type of attack active and passive attack. In this paper, which the control packet called CONFIRM, CHCKCNFRM and REPLYCONFIRM.

The paper published by **Sweta kaushik, Analysis of MANET security, Architecture and assessment** in **2013**, introduction of MANET. This paper we address the design issue of MANET network architecture, attacks, security issues, application of MANET.

MANET: Vulnerabilities, Challenges, Attack, Application in January 2011 published an article on, attack in MANET, application of MANET.

In the paper published by **Irshad ullah, A analysis of MANET using different MANET routing protocols i**n **2010** published on article on type of attack in MANET they there type of attack – VANET'S, INVANET'S,IMANET'S

Study of MANET: Characteristics, challenges, application and security attack in may 2013. Routing protocol in used MANET, different challenges of MANET,

An Introduction of black hole attack, this paper again published by Muhammad Raza and syed irfan hyder in 2011.

Type of black hole attack and different properties of black hole attack, detection and prevention techniques of black hole attack in MANET. **Black hole attack in AODV routing protocol; a review in April 2013**.

The black hole node attack in MANET in 2012 IEEE, how black hole node affects MANET'. Security of MANET is one of the important fractures for its deployment. We have analysed the behaviour and challenges of black hole attack in MANET with solution finding technique.

V. CONCLUSIONS

In this paper includes a way to produce and implement s simulation based solution, which is based on cluster organization of network. The proposed scheme is simulated over single black hole attack condition, but using the concept of authority as server node it than previous methods. In near future the proposed idea is converted into an adoptable algorithm which can help to detect and prevent the black hole attack over the MANET. The existing problem in MANET network is simulation using the NS2 network simulation environment.
Therefore the proposed method is provides the following contribution on MANET.

1. Providing security for Black hole attack
2. Efficient in detection and prevention

ACKNOWLEDGMENT

This research work is not related with any type of industrial research work. I would like to thank everyone who had contributed to the successful completion of this research. I would like to express my gratitude to my research supervisor, Prof. Ashish Tiwari for his invaluable advice, guidance and his enormous patience of the research. I also wish to acknowledge Lect. Mitesh Bargadiya and other to contribute in the preparation of this survey.

REFERENCES

[1] U.Venkanna, R.leela velusamy, proc. Of conf. on advance in recent technologies in communication and computing 2011

[2] Sanjay k. dhurandher, Isaac woungang, Raveena mathur and prashant khurana, CAITFS, Division of information technology netaji subhas institute of technology 2013 IEEE. International conference on advanced information network and application workshop.

[3] Li shi-chang, yang hao-lan, zhu qing–sheng College of computer science Chongqing university 2010 IEEE internation conference on signal acquisition and processing.

[4] Priyanka goyal, unti parmar, rahul rishi, research scholar dept. of CSE technological institute of textile and science IJCEM international eng. & management, vol 11, janvary 2011.

[5] Sweta kaushik, manorma koushik international journal computer science eng 2012.

[6] 2011 second internation conference on intelligent system , modelling and simulation.

[7] Irshad ullah shoaid urrehman IEEE2010

[8] Aarti may 2013 international journal of advanced research in computer science.

[9] Muhammad raza and syed irfan hyder 2011 IEEE proceeding of 2012 international bhurban conference on applied science & technology.

[10] Chanchal aghi, chander diwaker issue April 2013.Ms. Nidhi sharam, Mr. Sharam 2012 IEEE.