ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 6, December 2015

Malevolent detection techniques of MANETs in WSN: A Review

Priyanka V[1], Sumathi Poobal[2], Jose Anand[3]
[123]Electronics and Communication Engineering, KCG College of Technology, Chennai, India

Abstract*— In the next generation of wireless communication systems, there'll be a requirement for the fast preparation of freelance mobile users. Vital examples embrace establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network eventualities cannot deem centralized and arranged property, and may be planned as applications of Mobile impromptu Networks MANETs. A MANET is an associate autonomous assortment of mobile users that communicate over comparatively information measure affected wireless links. Since the nodes are mobile, the topology might amendment chop-chop and erratically over time. The network is redistributed, where all network activity together with discovering the topology and delivering messages lies on the nodes themselves, i.e., routing practicality are going to be incorporated into mobile nodes. MANETs suffers from intrusion within which a malicious node might or might not participate in route discovery mechanism with an significance to degrade the network performance. Intrusion has serious impact on routing and delivery magnitude relation of packets. Several researchers have conducted different techniques to detect the routing attacks and studied the performance. Here, varied attacks and a survey of the conferred solutions is analyzed.

***Index Terms*— MANET, AODV, ZRP, DSDV, Security, Black hole attack, Gray hole attack.**

I. INTRODUCTION

Wireless networks provide unprecedented freedom and mobility for a growing number of laptop and PDA users who no longer need wires to stay connected with their workplace and the Internet. Ironically, the devices that provide wireless service to these clients need lots of wiring themselves to connect to private networks and the Internet. A viable alternative to all those wires - the wireless mesh network. Unlike basic Wi-Fi that simply untethers the client; the wireless mesh untethers the network itself giving IT departments, network architects and systems integrators unprecedented freedom and flexibility to build out networks in record time - with high performance and without the expensive cabling. Wireless networks divided into two categories.

- Infrastructure wireless network
- Infrastructure less or ad hoc wireless network.

Infrastructure Networks

Infrastructure network have fixed network topology. Wireless nodes connect through the fixed point known as base station or access point. In most cases the access point or base station are connected to the main network through wired link. The base station, or access point, is one of the important elements in such types of networks. All of the wireless connections must pass from the base station. Whenever a node is in the range of several base stations then it connects to any one of them on the basis of some criteria.

Infrastructure less Ad-hoc Networks

Ad-hoc networks also called infrastructure less networks are complex distributed systems consist of wireless links between the nodes and each node also works as a router to forwards the data on behalf of other nodes. The nodes are free to join or left the network without any restriction. Thus the networks have no permanent infrastructure. In ad hoc networks the nodes can be stationary or mobile. Therefore one can say that ad hoc networks basically have two forms, one is Static Ad-hoc Networks (SANET) and the other one is called Mobile Ad-hoc Networks (MANET). From the introduction of new technologies such as IEEE 802.11 the commercial implementation of ad hoc network becomes possible. One of the good features of such networks is the flexibility and can be deployed very easily. Thus it is suitable for the emergency situation. But on the other side it is also very difficult to handle the operation of ad hoc networks. Each node is responsible to handle its operation independently. Topology changes are very frequent and thus there will be need of an efficient routing protocol, whose construction is a complex task. TCP performances are also very poor in mobile ad hoc network.

The remainder of the paper is structured as follows. In next section the characteristics, applications and advantages of MANETs are discussed. In Section 3, a number of the potential attacks in WSN are studied. Section four describes the routing protocols used in MANETs. A review of existing techniques to handle black hole and grey hole attack is given in section five. In section 6, comparative study specified in section five is provided. Finally, section seven concludes the work and points out future analysis directions.

II. CHARACTERISTICS, APPLICATIONS AND ADVANTAGES OF MANETS

MANETs is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self re-configuring multihop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The nodes in

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 6, December 2015

the network not only act as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes. MANETs rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies.

Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult; include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. In ad hoc networks, devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it.

Applications

Some of the applications of MANETs are

- Military or police exercises.
- Disaster relief operations.
- Mine site operations.
- Urgent Business meetings
- Robot data acquisition

It is easy to imagine a number of applications where this type of properties would bring benefits. One interesting research area is inter-vehicle communications. It is one area where the ad hoc networks could really change the way we communicate covering personal vehicles as well as professional mobile communication needs. Also, it is area where no conventional (i.e. wired) solutions would do because of the high level of mobility. When considering demanding surroundings, say mines for example, routing is accomplished via nodes i.e. ad hoc network is used. Such networks can be used to enable next generation of battlefield applications envisioned by the military including situation awareness systems. Ad Hoc networks can provide communication for civilian applications, such as disaster recovery and message exchanges among medical and security personnel involved in rescue missions.

Advantages

The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.
- These networks work without any pre-existing infrastructure.

III. ATTACKS IN MANETS

There are different types of attacks in Ad-hoc networks, they are:

- Black hole attack
- Wormhole attack
- Flooding attack
- Grey hole attack

Black hole attack

An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order to reduce the quantity of routing information available to the other nodes.

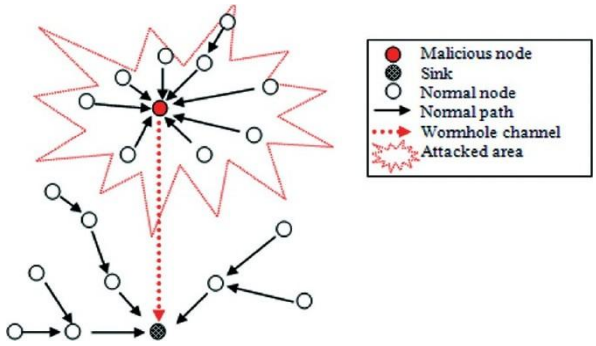


Fig 1: Black hole attack

This is called black hole attack which is shown in figure 1, and it is a "passive" and a simple way to perform Denial of Service attack. The attack can be done selectively (drop routing packets for a specified destination, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

Wormhole attack

The wormhole attack is quite severe, and consists in recording traffic from one region of the network and replaying it in a different region. For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link (see Figure 2) The wormhole link can be established by a variety of means, e.g., by using an Ethernet cable, a long-range wireless transmission, or an optical link.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 6, December 2015

Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

The severity of the wormhole attack comes from the fact that it is difficult to detect, and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation (via encryption, digesting, and digital signature) are preserved.

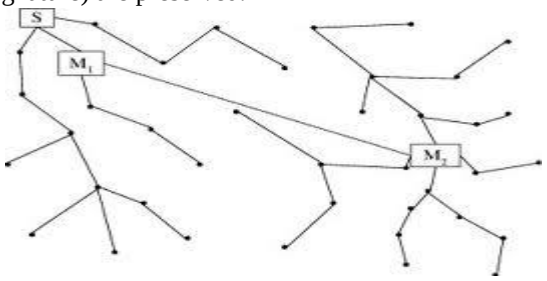
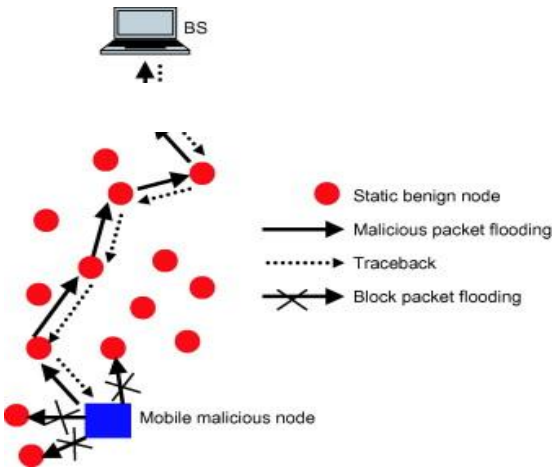


Fig 2: Wormhole Attack

Flooding attack

There are different types of flooding attacks, which have the goal to disrupt the routing discovery or the maintenance phase within Manet. Basically, via flooding attack a malicious node/an attacker aim the exhaustion of the network resources (e.g. network bandwidth) as well as consuming the resources of an authentic network user (e.g. computational and battery power). Furthermore an attacker can influence the network performance, by hindering the proper execution of routing algorithm (in routing discovery phase). By Route request (RREQ) flooding (or routing table overflow)it is possible for an attacker to send multiple RREQs to non-existing recipient in a very short period of time (see Figure 3), using the Ad hoc On demand vector (AODV) protocol of MANET. In other words the malicious node represents false (non-existing) routes to all authentic nodes within the network, preventing the creation of new actual ones and causing routing table overflow by the authentic users. The avalanche of RREQs all over the network leads to consummation of the battery power and the network



bandwidth, causing Denial of Service (DoS).

Fig 3: Flooding attack

As a countermeasure against the flooding attack every network participant (actual authentic user or simply node) can compute and monitor the evaluation of all neighbors RREQ, and in case of outmatching of the RREQs' limit, which is preliminarily defined, the specific neighbor node comes with its ID in a blacklist. By this way the authentic/actual node "knows", that it should not receive any RREQs from its neighbors, recorded in its blacklist. Furthermore the efficiency of this countermeasure can be enhanced if the RREQ limit is not preliminarily defined (fixed), but is computed on hand of statistical analysis over RREQ, so the risk of attack with varying flooding rates to be minimized.

Gray hole attack

Gray hole is one of the attacks found in ad hoc network which act as a slow poison in the network side (i.e) we cannot suppose how much data can be lost. In grayhole attack a malicious node trashes to precede certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,when a source node want to route a packet to the destination node , it uses a particular route if such a route is accessible in its routing table. If not, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighboring nodes. By getting the RREQ message, the intermediate nodes bring up-to-date their routing tables in a reverse route to source node. A Route Reply (RREP) message is sent backward direction of the source node after the RREQ query reaches either the destination node itself or any other intermediate node that has a recent route to destination.

IV. ROUTING PROTOCOLS IN MANETS

Ad-hoc networks require multi-hop routing and all nodes can potentially contribute in the routing protocols. Routing protocols are organized as:

Reactive/On-demand routing protocols

Reactive or on-demand routing protocols route is discovered when needed. Reactive protocols tend to decrease the control traffic messages overhead at the cost of increased latency in discover a new routes. Source initiates route discovery in reactive routing protocols with less delay. In reactive protocols there is no need of distribution of information. It consumes bandwidth when we transfer data source to destination. Reactive Protocols are AODV, DSR (distance vector routing) and ABR (Associatively Based Routing) protocols. Manet is also called Mesh network. It is high adaptable and rapidly deployable network.

AODV: AODV stand for Ad-hoc On-Demand Distance Vector routing .AODV establishes a route to a destination only on demand. AODV is capable of both unicast, broadcast and multicast routing. AODV have some join feature of DSR and AODV.AODV avoids the counting to-infinity problem of

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 6, December 2015

other distance-vector protocols by using sequence numbers on route updates. AODV reacts relatively quickly to the topological changes in the network and updating only the hosts that may be affected by the change, using the RREQ message. Hello messages, dependable for the route maintenance, are also imperfect so that they do not create unnecessary overhead in the network. The RREQ and RREP messages are responsible for the route discovery.

Advantages

- The AODV protocol is basically flat routing protocol so it does not require any inner organizational method to handle the routing process.
- In AODV routes are established on demand and that destination sequence numbers are applied to find the latest route to the destination.
- The connection setup delay is lower.
- The AODV protocols are loop free and avoid the counting to infinity problem.
- At most one route per destination is maintained at each node

Disadvantages

- It can lead to heavy control overhead
- In AODV unnecessary bandwidth consumption.

Proactive or table-driven protocols

In Proactive routing protocols every node store information in the form of tables and any type of change accrue in network topology need to update these tables according to update. The node swaps topology information so they have route information any time when required. There is no route discovery delay associated with finding a new route. In proactive routing fixed cost generate, as normally greater than that of a reactive protocols. Proactive routing protocols are DSDV (destination sequenced demand vector), OLSR (optimized link state routing protocol)

DSDV: Every node will maintain a table listing all the other nodes it has known either directly or through some neighbors. Every node has a single entry in the routing table. The entry will have information about the node's IP address, last known sequence number and the hop count to reach that node. Along with these details the table also keeps track of the next hop neighbor to reach the destination node, the timestamp of the last update received for that node. The updates are accepted based on the metric for a particular node. The first factor determining the acceptance of an update is the sequence number. It has to accept the update if the sequence number of the update message is higher irrespective of the metric. If the update with same sequence number is received, then the update with least metric (hopCount) is given precedence. In highly mobile scenarios, there is a high chance of route fluctuations, thus we have the concept of weighted settling time where an update with change in metric will not be advertised to neighbors. The node waits for the settling time to make sure that it did not receive the update from its old neighbor before sending out that update.

Hybrid routing protocols

Hybrid routing protocols combination of both reactive and proactive routing protocols. It was proposed to reduce the control overhead of proactive routing protocols and also decrease the latency caused by route discovery in reactive routing protocols. Hybrid routing protocols are ZRP (Zone routing protocol) and TORA (Temporarily Ordered Routing Algorithm)

***ZRP*:** ZRP was planned to decrease the control overhead of proactive routing protocols and discovery in reactive routing protocols and also decrease the latency caused by route. It can be safely be assumed that most communication takes place between the node close to each other. ZRP provide framework to other protocols. The behavior of ZRP is adaptive. ZRP is based on the Zone, these are local neighbors, each node within have many overlapping zones and each zone may be have dissimilar size. ZRP consists of several component, these component together give the benefits of ZRP. Each component work independently to give the efficient result.

***Components of ZRP*:** IARP Intrazone Routing Protocol, IERP Interzone Routing Protocol, BRP Border cast resolution protocol. IARP is first component of ZRP.IARP is used to communicate with the interior node inside the zone if network topology may change rapidly. It allows for only local route. IERP is global reactive component of ZRP. It used reactive approach to communicate with nodes outside the zone. It changes the way route discovery handled. Route queries are issued by IERP when request for the route issue. BRP is used to direct the route request initiated by global reactive IERP. It is used to maximize efficiency and increase disused queries

V. RELATED WORKS

Y. Zhang et al., [14] and Seungjoon Lee et al., [8] have introduced the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the black hole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source node. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path.

Hongmei Deng [4] proposed a solution for the black hole problem for ad hoc on-demand distance vector routing protocol. One possible solution to the black hole problem is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense we avoid the black hole problem and implement a secured AODV protocol. But there

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 6, December 2015

are two associated disadvantages. First, the routing delay is greatly increased, especially for a large network. Second, a malicious node can take further action such as fabricate a reply message on behalf of the destination node. and another method is considered in this paper, in that method the source node will verify the each next node information by forming the new route, but in this method, the overhead increases and the security is not much better.

Yanchao Zhang et al., [12] proposed a novel anonymous on-demand routing protocol, termed MASK, to enable anonymous communications thereby thwarting possible traffic analysis attacks. Based on a new cryptographic concept called pairing, he first proposed an anonymous neighborhood authentication protocol which allows neighboring nodes to authenticate each other without revealing their identities. A pairing-based anonymous on-demand routing protocol MASK provides strong sender and receiver anonymity, the relationship anonymity between senders and receivers, the unlocatability of mobile nodes, and the untraceability of packet flows under a rather strong adversarial model but the routing information is not authenticated in the current design of MASK.

Dokurer [3] proposed a solution that is based on ignoring the first established route to reduce the adverse effects of black hole attack. He assumed that first RREP message would normally come from a malicious node. Unfortunately, this solution has some limitations. For example, the second RREP message received may also come from malicious node if the real destination node is nearer to the source node than the malicious node. This method also does not address how to detect and isolate malicious node from the network.

Nidal Nasser et al., [7] overcame the weakness of Watchdog and introduced intrusion detection system called ExWatchdog. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. ExWatchdog solves a fatal problem of Watchdog, i.e., a malicious node can partition the network by falsely reporting other nodes as misbehaving. Our solution decrease the overhead greatly, though it does not increase the throughput obviously. It is not reliable, because the solution is based on assumption only.

Sukla Banerjee [10] proposed an approach that consists of an algorithm which works as follows. Instead of sending the total data traffic at a time they divide the total traffic into some small sized blocks. So that malicious nodes can be detected and removed in between the transmission of two such blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before start of the sending any block to alert it about the incoming data block. Flow of the traffic is monitored by the neighbors of the each node in the route. After the end of the transmission destination node sends an acknowledgement via a postlude message containing the no of data packets received by destination node. Source node uses this information to check whether the data loss during transmission is within the tolerable range, if not then the source node initiate the process of detecting and removing malicious node by aggregating the response from the monitoring nodes and the network. This Proactive detection schemes are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted.

Ming-Yang Su et al., [6] discussed a mechanism known as ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds the limit, the nearby IDS broadcasted a block message with id of IDS, the identified black hole node and the time of identification will place the malicious nodes on their blacklists to isolate the malicious node in the network cooperatively. The advantage of this mechanism is that it can be able to detect cooperative black hole nodes in the MANETs. The main drawback of this mechanism is that mobile nodes have to maintain an extra database for training data and its updating, in addition to the maintenance of their routing table.

Alem, Y.F et al., [1] proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent attacks by the both single and multiple black hole nodes. IDAD assumes every activity of a user can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole node IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data is collected, it is given to the IDAD system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system isolates the particular node from the network. The reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication.

S. S. Bajwa and M. K. Khan [2] proposed Grouped Black Hole Attack Security Model (GBHASM) to prevent grouped black hole attacks in Ad hoc On-demand Distance vector (AODV) protocol in wireless ad hoc networks. This model is based on two modules. First module describes how a new node becomes member of network. After having joined the network, this node is assigned node codec(NC) pkk1 and pkk2. When node requests for shortest path to destination with a packet having pkk2, then each node matches Node Code pkk1 with pkk2. If they match within Time to Live (TTL), routing information is shared with intermediate node otherwise packet is forwarded to next node. This model has low delay and high performance

R. Tanuja et al., [11] proposed technique to eliminate Black Hole and False Data Injection attacks initiated by the malicious nodes, severally employing a new acknowledge theme with low overhead. Advantage with this theme is that it

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 6, December 2015

will with success establish and eliminate 100 % black hole nodes and ensures more than 99 % packet delivery with increased network traffic.

Siddiqua et al., [9] proposed a secure knowledge algorithm to detect and mitigate black hole attack on AODV by taking packet drop reasons into consideration before declaring a trusted node as black hole node. Each node monitors the behavior of its neighbor by listening to packet transmission wirelessly. Every node compares the neighbor information with its knowledge table information. The nodes monitor the control packets as well as data packets to prevent selective dropping. When packet dropping reaches to a threshold then before declaring a node to be malicious the algorithm first checks whether suspected node is destination or not. It also checks packet drop reasons such as Time to live (TTL) and residual energy. If suspected node is detected to be a black hole, its id is broadcasted to all other nodes in network so that malicious node can be avoided in routing process. Secure AODV shows better performance in terms of throughput and delay as compared to existing AODV.

Jian-Ming Chang et al., [5] designed a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. CBDS method implements a reverse tracing technique that detects the black hole attack. Simulation results were provided, which depicts that CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio (chosen as performance metric).

VI. COMPARISON OF VARIOUS SOLUTIONS

Techniques proposed by	Techniques	Type of attack	Merits	Demerits	Protocol
Ming-Yang Su; Kun-Lin Chiang;Wei-Cheng Liao	An Anti-Blackhole Mechanism using IDS	Multiple black holes	High detection rate	Time delay	Reactive
Alem, Y.F.;Zhao Cheng Xuan	Intrusion detection using anomaly detection	Single and multiple black hole nodes	Minimum network overhead	Neighbour nodes may give false information	Reactive
Tanuja, R., M. K. Rekha, S. H. Manjula, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik Delta	BhnFDIA	Black Hole and False Data Injection attacks	more than 99 % packet delivery	Increased network traffic	Reactive
S. Bajwa and M. K. Khan	Grouped Black Hole Attack Security Model	grouped black hole attacks	low delay and high performance	Overhead is high	Reactive
Y. Zhang and W. Lee	Confirmation request (CREQ) and route confirmation reply (CREP)	Single and multiple black hole nodes	Low cost	Time delay and false positive	Reactive
Sukla Banerjee	Divide the total traffic into small sized blocks.	Black hole and grey hole	Packet delivery rate increased, Latency reduced	Hacker involve by fake message, Overhead will be high	-
Hongmei Deng, Li, Wei, Agrawal D.P.	To disable the ability to reply in a message of an intermediate node	Black hole	Preventing black hole attack in rural area network	Routing Delay is increased in a large network	Reactive
Yanchao Zhang, Wei Liu and Wenjing Lou	MASK	Eavesdropping	Strong sender and receiver anonymity,	The routing information is not authenticated in the current design of MASK.	-
Nidal Nasser and Yunfeng Chen	Exwatchdog	Intrusion detections	Decrease the overhead greatly	It does not increase the throughput.	-

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 6, December 2015

Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai	Co-operative Bait detection scheme	Black hole	Increased packet delivery ratio	Overhead is high	Hybrid

VII. CONCLUSION AND FUTURE WORK

In this survey paper, an overview of characteristics, routing protocols and several attacks of MANETs have been discussed and comparative study on various technology implemented to improve the security issues of MANETs have been attempted. MANETs is an emerging technology field and is an active area of research. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. As ad hoc networks are vulnerable to many types of attacks the security of this network is a major issue. Many researchers are trying to prevent the attacks done on ad-hoc networks at various levels. A variety of such attacks have been discussed. We have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. A lot of research is still being carried out to identify new threats to ad hoc networks and to provide security. As a future work, the detection and prevention mechanism of the several routing attacks in MANET environment can be developed. An effective method to eliminate the attacks should be found, thereby ensuring a secured packet transfer communication.

REFERENCES

[1] Alem, Y.F.; Zhao Cheng Xuan, "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2nd International Conference, vol.3, May 2010, pp.V3-672-V3-676, 21-24.

[2] Bajwa, ShahidShehzad, and Muhammad Khalid Khan. "Grouped Black hole Attacks Security Model (GBHASM) for Wireless Ad-Hoc Networks." In Computer and Automation Engineering (ICCAE), The 2nd International Conference, IEEE, vol. 1, 2010, pp. 756-760.

[3] Dokurer, Semih, "Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, Atılım University, 2006

[4] Hongmei Deng., Li, Wei., Agrawal D.P, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, Volume 40 , issue 10, Cincinnati Univ., USA ; Oct 2002

[5] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A Cooperative Bait Detection Approach", Member, IEEE, IEEE Systems Journal, Vol. 9, No. 1, March 2015

[6] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), International Symposium, Sept. 2010, pp.162-167, 6-9

[7] Nidal Nasser and Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks", IEEE International Conference, Communications, 2007

[8] Seungjoon Lee, Bohyung Han, Minho Shin; "Robust Routing in Wireless Ad Hoc Networks", international Conference, 2002

[9] Siddiqua et al., "Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm", SPACES-2015, Dept of ECE, K L UNIVERSITY, 2015, pp. 421-425.

[10] Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science (WCECS), San Francisco, USA, October 22 - 24, 2008,

[11] Tanuja, R., M. K. Rekha, S. H. Manjula, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik. "Elimination of black hole and false data injection attacks in wireless sensor networks." In Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, Springer New York, 2013, pp. 475-482.

[12] Yanchao Zhang, Wei Liu and Wenjing Lou, "Anonymous Communications in Mobile Ad Hoc Networks", IEEE, 2005

[13] Y.Zhang and W.Lee, "Intrusion detection in wireless ad-hoc networks", 6th annual international Mobile computing and networking conference proceedings, 2000.

AUTHOR BIOGRAPHY

First Author Priyanka V, PG Scholar, ME Communication systems.

Second Author Sumathi Poobal M.E., Ph.D, Professor, Vice Principal.

Third Author Jose Anand M.E., Associate Professor