Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 9, Issue, 05, pp.49851-49856, May, 2017

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

A COMPREHENSIVE SURVEY OF VARIOUS ROUTING ATTACKS IN MANETS

***,[1]Gaurav Kumar Singh, [2]Rishikesh and [2]Dr. Anil Kumar Sagar**

[1]School of Computing Science and Engineering, Galgotias University, Greater Noida, Greater Noida, India
[2]School of Computing Science and Engineering, Galgotias University, Greater Noida, India

ARTICLE INFO

Article History:
Received 22nd February, 2017
Received in revised form
16th March, 2017
Accepted 04th April, 2017
Published online 19th May, 2017

Key words:

MANET, Black hole,
Gray hole, Sink hole,
Wormhole attack,
AODV, DSDV,
Dynamic topology.

ABSTRACT

In this survey paper literature review of black hole attack in MANETs has been presented. MANET is a type of network where communicating devices can communicate to each other without any fixed centralized master device. That's why attack in between the communication of two more devices is not a challenging task. There are several types of attacks in MANET routing protocols such as black, gray, sink and wormhole attack and others also. But we can't deny the importance and popularity of MANETs in today's time scenario because such type of networks is very easy to design, implement at any time anywhere. Especially in those geographical locations where to setup the infrastructure based network of communicating devices is very challenging task like at remote locations, disastrous locations. So, it's a challenging task for researchers to implement better security protocols for mobile ah-hoc networks in order to service a very tight security against the attackers. So, in this area an ample of research and techniques have been proposed for securing routing protocols in MANETs. MANET routing protocol has been categorized under two broad categories that are Proactive and Reactive. Proactive routing protocols are DSDV, WRP, OLSR and others also. Reactive routing protocol i.e. AODV, DSR. There are various MANET routing protocols like AODV, DSDV, DSR and other. But in today's time the routing protocol which used most frequently are AODV, AOMDV, DSDV.

Citation: Gaurav Kumar Singh, Rishikesh and Dr. Anil Kumar Sagar. 2017. "A comprehensive survey of various routing attacks in manets", *International Journal of Current Research*, 9, (05), 49851-49856.

INTRODUCTION

MANETs are the group of mobile nodes that can communicate to each other in the absence of access point. The topology of the network is not fixed. It is somewhat dynamic. Each device/node acts as host as well as router. These kinds of networks cab be created at anytime, anywhere. And mainly in those areas where to create infrastructure network is very difficult like in battlefield. Communication between two devices becomes a bit difficult as compared to fixed networks. Mobile Ad Hoc Network (MANET) is a dynamic nature multi-hop wireless network which can be setup by two or more than two mobile nodes on a shared wireless channel. One of the major intricated task in MANETs is routing among mobile nodes due to the mobility nature of the nodes. Mobile Ad-hoc Networks as shown in Figurea. It is one of the challenged area of research. According to an ample of researchers now days (Krati patidar and Vandana Dubey, 2014). A MANET has a self-organizing property that's why every mobile node can get connected to each other without any use of wired link i.e. they can getconnected to each other with a wireless link, which establish a random topology (Harris Simaremare, 2014).

****Corresponding author: Gaurav Kumar Singh,***
School of Computing Science and Engineering, Galgotias University, Greater Noida, Greater Noida, India.

Topology of network changes very rapidly with respect to time. MANETs are resource constraints that is Battery powered, Low bandwidth for message transmission. So that's why this is very challenging area for researcher due to such type of characteristics of MANETs There are so many routing protocols in MANETs proposed by a lot of researchers have been broadly classified under three categories i.e. Reactive protocols, Proactive protocols and Hybrid protocols. Reactive routing protocol also named as On-demand routing protocols because in this type of protocol the route between two devices willing to communicate to each other are created only when they want to communicate to each other. In On-demand routing protocol, the link between two devices willing to communicate to each other are created in two phase, first phase is known as Route discovery phase (Nodes starts to discover the route on the basis of demand) and Second phase is known as Route maintenance phase (When there exists a problem such as link failure, wireless channel lost in between two devices, Maintenance is required to remove such problems). In Proactive, Each and every node carries the routing table and keeps all the basic information about the network structure (i.e. topology of network). Proactive protocols are not good for a MANET having high number of nodes because of the

bulkiness of table maintenance by each mobile node which may degrade the performance of the network.

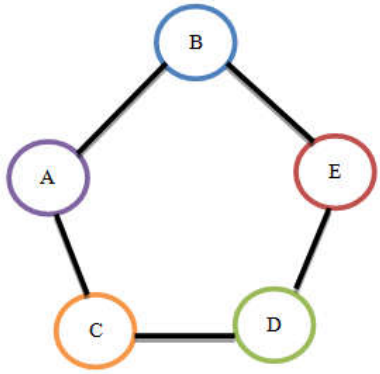

Figure 1. Mobile Ad-Hoc Network

Introduction To Routing Protocol

Routing protocols are always a major task and plays an important role in any type of network in order to present the network reliability, functionality, performance etc. Actually, routing protocols are the set of rules and properties used to find out the best route between two electrical/electronic devices wiling to communicate to each other. Routing protocols are broadly categorized under three categories i.e. Proactive (e.g. DSDV), Reactive (e.g. AODV) and Hybrid protocols (e.g. ZRF) [2][8].In Proactive protocols, Each and every mobile node keeps a routing table which contains the very useful information about the nodes participating in the MANETs and about the geographical structure of the network (i.e. Network topology). Whenever the changes in the mobile ad-hoc network topology occurs, routing table of each node are updated periodically. Whereas in Reactive protocols path discovering and path maintenance. In simple words the route is searched whenever required and route maintenance is done when the route fails due to link breakage etc. There are some problems with Proactive routing protocol that is it is not suitable for large size network because to hold the correct and accurate information about all participating nodes in MANETs is very challenging task and one more thing is that every node needs to send the control messages sporadically in order to maintain the route's correct information.

DSDV

Dynamic Destination Sequenced Distance Vector (Concepts and Protocols) is a type of proactive routing protocol which can be created by using Bellmen Ford Algorithm with some modification. As the name of this protocol, this protocol puts sequence numbers to the routing table of all the nodes. In the DSDV, all mobile nodes preserve a routing table and each routing table keeps the list of all the destination nodes and total number of hops to each. Routing table updated immediately when any topological change occurs in the network. The advertisement of routing table to each other among the mobile nodes can be done in two ways i.e. by broadcasting the routing tables or by multicasting the routing tables. Due to this advertisement, the mobile nodes become capable of updating their routing tables as the topological changes occurs in the network. Broadcasting and Multicasting of routing tables is done by all the mobile nodes in network periodically and incrementally. Actually, the DSDV routing protocol was developed by computer scientists with the purpose of reducing the broadcast messages and to avoid the routing overhead. So, each mobile node in the network transmits and updates its routing table sporadically in sort to keep the whole stable. In DSDV protocol, when node broadcasts their packets to their nearby (very close neighbors) nodes then they use two types of data packets that are incremental dump packets and full dump packets (Papadimitratos, 2002). Where incremental dump packets always keep all the required information which is available each time and full dump carries only those information that is updates in the previous dump. Therefore, DSDV routing protocol always minimizes the overhead. But this protocol cab be used for small size MANETs. The main advantage of DSDV routing protocol is that it always ensures and produces the loop free routes between communicating mobile nodes and avoids the count to infinity problem. Other important benefit of using the DSDV routing protocol is that it maintains only the best routes between the devices willing to communicate to each other instead of keeping and updating the various routes from source to destination node. But there are some disadvantages of the DSDV routing protocol is that multi-path routing among the mobile devices is not supported. One more thing is that there is unnecessary wastage of the network bandwidth occurs just because of the unnecessarily sharing the routing information among the mobile nodes even if there is not any topological changes in the mobile ad-hoc network.

AODV

AODV stands for Ad-Hoc On-Demand Distance Vector. AODV is an extend version of DSDV routing protocol but it is a type of Reactive protocol rather than Proactive. Reactive protocols are those routing protocols in MANETs which searches and maintains the links between the mobile nodes whenever required. It uses the theory of distance vector routing algorithm to work properly in MANETs (Chaitali Biswas Dutta, 2014), and uses the destination sequence number to show the route freshness between the mobile nodes willing to communicate to each other and the operation can be performed loop free (Mohamed, 2013; Satria Mandala, 2013; Mohemad A. Abdelshafy, 2013). AODV routing protocols provides services to mobile nodes as they can send messages to each other. By using AODV routing protocol mobile nodes becomes capable of transmitting the messages via their neighbors to those nodes it can't be able connect directly. AODV routing protocol is used to determine the route for transmitting the packets and it always ensures that the path between two communicating devices will be loop free and It always tries to provide the shortest path for communication between a mobile node pair. This protocol has such type of mechanism which can control the route changes due to the topological change in the network and establishes the new fresh routes between mobile nodes in case of ant route error due to some other reasons. AODV routing protocol first discovers the routes and after that maintains the routes. So AODV protocol discovers the routes by broadcasting the route-request (RREQ) packets to all its nearby nodes (neighbors) with the help of new sequence number. Each mobile node that receives the broadcasted message, further broadcasts that particular message to the next level of neighbors and the process continues repeatedly until the destination mobile node receives that particular message originally transmitted by source node. So, whenever a desired destination or any intermediate mobile node which have new fresh path destined the destination receives the RREQ packet, and it unicasts a reply packet by sending the route reply packets (RREP) towards the counter path implemented at the

intermediary nodes during the route discovery process. Such type of process continues until the original sender of RREQ packet receives the RREP packet. And then source node just starts to broadcast the packets to the destination node with the help of next door neighbors which responded the with RREP packet firstly. Mobile nodes in the network don't receives those RREQ packets which have already seen by it and the RREQ packet uses the sequence numbers to guarantee that the routes are loop free. Whenever any route link breakage problem occurs then route error (RERR) packet has been sent to every active nearby node. All the essential routing information is stored in the source node, destination nodes and the nearby nodes from where the data packet has been transmitted (Chaitali Biswas Dutta, 2014; Mohamed, 2013). Such type of mechanism decreases the space complexity or we can say that the reduction in required memory complexity for whole network, minimizes the frequency rate of resources available in the MANETs, and runs very well in a high mobility conditions (Mohamed, 2013 and Monika, 2013). If the source node changes its position in network that means network topology changes then it'll re-initiate the link (route) discovery process for transmitting the packets to the destination and if one of the intermediate node moves away from the network or leaves the network then the nearby node sends links letdown message to the other nearby nodes in order to alert them about the network topology. Such type of functioning continuing until the source node re-initiates the route discovery for transmitting the packets from source to the destination. Main advantage of the AODV routing protocol is that the routes between mobile nodes are discovered whenever needed and the sequence numbers are used to indicate that the route is fresh route from source to destination. Route maintenance is done by using 'Hello' message. Major disadvantage of the AODV routing protocol is that the intermediary node can create the problem of inconsistent route if the source node has the previous old sequence number of the destination and intermediate node are not having the latest destination sequence numbers.

DSR

Full form of DSR is dynamic source routing protocol. DSR routing protocol is a type of Reactive protocol that is on demand routing protocol. In this protocol, Source node is always responsible for routing the links between mobile nodes (Monika, 2013). In this protocol, the required information for routing stored in the packet header. In DSR routing protocol the intermediate nodes are not responsible for maintaining the routing information just because of the required information is always maintained by the data packet header. Main advantage of the DSR routing protocol is that it always contains a route cache which enables every node to detect or discover the link between two mobile devices willing to communicate very fast with very small energy consumption rate. There for by using this mechanism, before forwarding the data packets nodes always first crosscheck its route cache data.

Differentation among various routing protocol

The Table a shown below represents the comparative values in between AODV, DSR and DSDV routing protocols.

Different attacks on different layers

In computer network, there are various attacks on different layers of protocol suit used in the network. Attacks like Denial of services (DOS), pocket mistreating attack, routing table poisoning, hit and run attack, routing attacks etc. Denial of services attacks are those attacks which includes the system's software application or other hardware part of network not able to Process the user's request and query in order to provide the desired output to the user. Denial of services attacks includes activities like ICMP flooding, UDP flooding, SYN flooding etc. Actually, flooding of such type of packets creates the uncontrollable traffic over the network which is not easily processed by routers and that makes the router unable to process such type of packet traffic. That means router is unable to provide services to their user. Routing attacks are also classified under several categories that are Black-hole attack, Grey-Hole attack, Worm-hole attack, and Sink-hole attack. In this paper, Brief overview over routing attacks has been done.

Table 1. Routing protocols comparison

Comparison parameters	DSR	Ad-Hoc On Demand Distance vector	Destination sequence distance vector
Protocol Type	Protocol nature is reactive	Protocol nature is reactive	Protocol nature is proactive
Based On	Source routing	Distance vector routing	Distance vector routing
Approaches used for routing	Demand based approach	Uses On-Demand approach	Uses table driven approach
Loop free routing	Provides loop free routing	Provides loop free routing	Provides loop free routing
Route maintenance	Path is handled by Route cache	Path is updated by Route Table	Path is handled by Route Table
Unicasting/Multicasting	Unicasting only	Both Unicasting and Multicasting	Unicasting only
Duplex between mobile nodes	Both Unidirectional and Bi-directional links	Bi-directional links	Bi-directional links
Broadcast	No periodic broadcast	Uses periodic broadcast	Uses periodic broadcast
Security	Not a good security	Not a good security	Not a good security
Overhead	Message overhead is high	Message overhead is high	Message overhead is low
Route matric	It uses shortest path	It uses shortest path	It uses shortest path
End to End delay	High	Lower	Moderate

Table 2. Layer-wise Attack List

Mobile Ad-Hoc Network Layers	Various routing attacks
Application Layer	Various attacks via virus and worms
Transport Layer	Session Hijacking attack and Jelly Fish attack
Network Layer	Black-hole, Grey-hole, Sink-hole, Worm-hole attacks
Data Link Layer	WEP targeted attacks
Physical Layer	Malicious attacks

The table 2 mentioned below shows the various attacks list on several layers of protocol used in network.

Various attacks on manet routing protocol

Black-hole attack: Black hole attack is type of active attack in MANETs. Black-hole attack (Rajinder Singh, 2014), is a very uncertain grave problematic for the MANETs, in which a malicious mobile node always transmits false routing information to the requesting original sender, showing that it is able to provide the shortest path to the destination mobile node with the intension to interrupt and unnecessarily drop or consume the data packets receiving from that particular node. That means such type of malicious nodes never promotes or forwards the data packets received from a node to their destination node. For example, in AODV routing protocol the malicious node can transmit the fake route reply packet (RREP) to the source nodes, guaranteeing that it can offer a fresh and shortest path to the end node. This enables the source node to select the route and transmitting the data packets. Due to which all the traffic of data packets goes through that particular malicious (Black-hole) node and thus the black-hole node can misuse or reject those data packets.

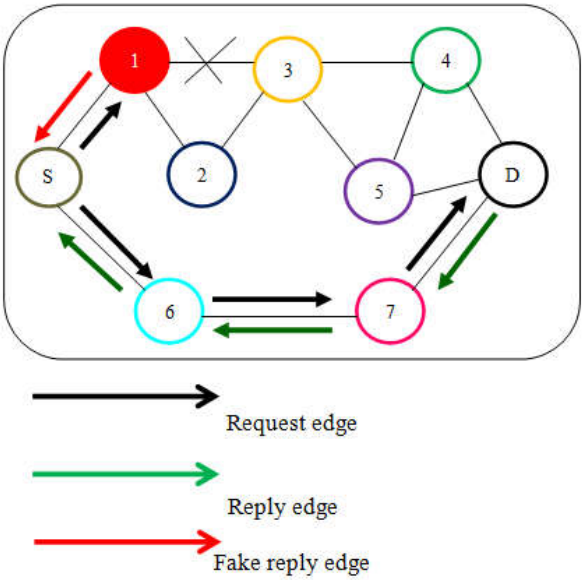

Figure 2. Black-hole Attack

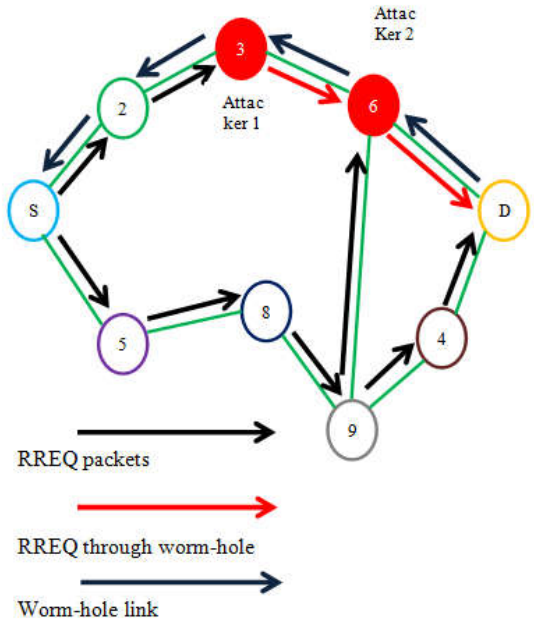

Figure 3. Worm-hole Attack

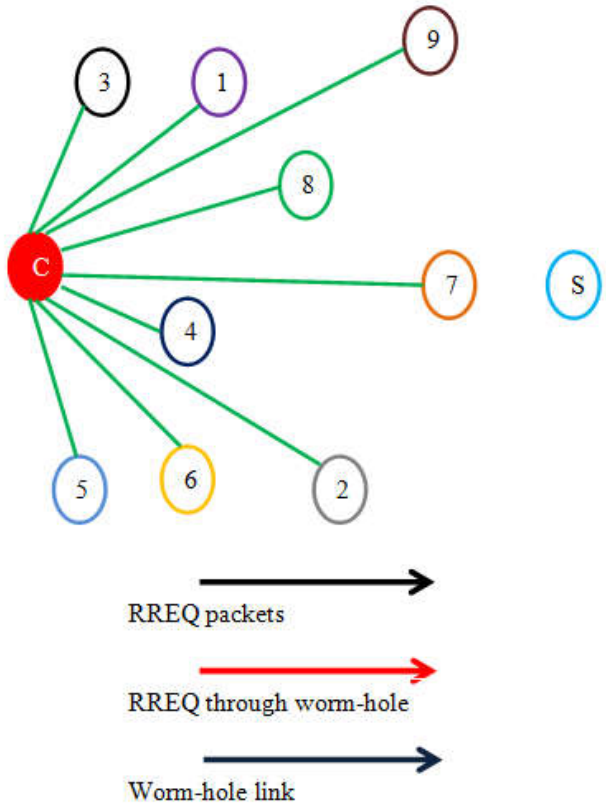

Figure 4. Sinkhole Attack

In the figure b, Mobile nodes labeled as S and D are source and Destination mobile nodes in a MANET with topological structure as shown in figure b. Whereas mobile nodes labeled as 1,2,3,4,5,6,7 are the intermediate nodes. Node labeled as 4 is also a fake malicious node (black-hole node). The sender node S sends the route request (RREQ) packet to the intermediate nodes which are very close to node S or we can say neighboring nodes. Nodes 1,2, and 6 are neighbor nodes of Source Node S. So, after receiving RREQ packet from node S they further forward that particular RREQ to next level of neighboring nodes except node 4. Node 4 transmits the false routing information to source node S guaranteeing that it offers the fresh and shortest route to the destination node 'D'. The source node 'S' once received the route reply (RREP) packet; it'll transmit the data packets to the malicious node '4' as it is having the shortest path to the destination.

Gray-hole attack

Gray-hole attack is a variation of Black-hole attack and also a type of active attack in MANETs. In this type of attack mobile nodes drops the data packets selectively. Data packet forward attack based on selection can be classified under two categories:1) Don't forward any UDP packets while forward every TCP packets. 2) This type of attack can drop and forward the data packets on the basis of probabilistic distribution. For example, if gray-hole node forwards 40% of total data packets then it will drop remaining 60% data packets. Therefore, this type of attack is very challenging task for security providers to detect these attacks in the MANETs. Gray hole node can switch its behavior during the data transmission through it that is it can switch from behaving correctly to a node like black hole node. So, it is an attacker actually and it'll act as a normal behaving node. Generally, in

the gray hole attack, the attacker (i.e. gray hole node) acts with malicious intention for a time period in which the data packets are dropped by it and after that it can switch to behaving as a normal node in MANETs.

Worm-hole attack

Wormhole attack (Bounpadith, 2007), can also be known as tunneling attack or co-operative black-hole attack. Such type of attacks are very bad for a Mobile ad-hoc network because in this two or more than two nodes co-operative to each other in order to create a tunnel of black-hole nodes and guaranteeing that it will provide the fresh and shortest path to destination and take full admin of the source node.

Sink-hole attack

The sinkhole attack is also a type of active attack in MANETs and in simple words its very severe attack in the MANETs. The main purpose of such type of attacking nodes is to attract all the mobile nodes traffic towards itself which may lead to an unreliable and very poor performance network. Sink-hole node always does such type of activity by stating that it has the shortest and fresh path to destination. After receiving all the intermediate mobile node traffic, it changes the topology of the network as well as secret information also like modification in the packets or delete the received data packets. A compromise node always enchains all the secret data through its surrounding mobile nodes as much as possible. So, any routing algorithm like AODV, DSDV etc. couldn't perform efficiently. In the figure c, Nodes labeled as S and D are considered as Source and Destination node respectively. And remaining mobile nodes labeled as 1,2,3,4,5,6,7,8,9 are considered as the intermediate nodes and node 'C' can be considered as sinkhole node which enchains largest portion of the mobile node from the intermediate nodes by offering them a fake shortest and fresh path to the end node.

Solution to remove Attacks from manets

Solution to Black-hole problem in MANETs

In (Krati patidar and Vandana Dubey, 2014), Kriti Patidar *et al*. has been given an algorithm to protect the mobile ad-hoc network from black hole attack and worm-hole attack. It will improve the network durability, performance as well as reliability level of the network. Author has been developed the intrusion detection system on the basis of specification concept. The proposed routing security technique uses the counter idea for indicating the correct and fresh AODV routing behavior and the intermediate mobile nodes tries to check the performance and character of the other internal nodes in order to detect those nodes which are going to violate the specification rules.

In (Vimal Kumar, 2015), Vimal Kumar *et al*. designed a rich efficient solution for catching the black hole attack which causes very high communication cost in the MANETs. The designed technique is a technique which will secure the routing protocols used in MANE from black hole attack and provide the communication cost very low. This technique is merely the improvisation over the AODV routing protocol. In this solution, a coming route reply table (CRRT) is maintained by the source node. Coming route reply table saves the routes replied by packets for establishing link (path) between the mobile nodes willing to communicate. CRRT table contains the very useful information like next hop, hop counts, destination sequence no., Source IP address, Destination IP address, and lifetime.

In (Rutvij, 2013), Rutvij H. Jhaveri has been introduced a mechanism to catch and to be far from Black-hole attacks and Gray-hole attacks while discovering route from source to destination. Author has been designed the a modified AODV protocol that is R-AODV. The Time, false (fake) nodes has been caught with the help of this new technique after getting RREP packet, R-AODV points that route reply as DO_NOT_CONSIDER and set the received route reply packet as MALICIOUS_NODE in the routing table. After that, the route reply packet (RREP) is given away to the source node and update the routing tables.

In (Saurabh Gupta, 2011), Saurabh Gupta *et al*. has been given a protocol to avoid black hole attack over routing protocols. The author has been named his technique as black hole attack avoidance protocol (BAAP). BAAP technique uses Ad-hoc On-demand Multipath distance vector, which always creates the disengage multiple-route with the help of path discovery process. The time, intermediate nodes respond to the source node, some mobile nodes can have multiple links (paths) to the destination node but it always tries to select merely single route to that destined node. In BAAP technique, total mobile node keeps a legitimacy table of their neighbor nodes to find the right path (link) to the destination. Message formats of RREQ and RREP packets are changed according to BAAP protocol. The Modified RREQ and RREP packets according to this protocol are shown below:

Solution to Sink-hole attack

In (Fang-jiao Zhang, 2014), Fang-Jiao Zhang *et al*. has been presented a solution for detecting the sinkhole attack problem by using a redundancy mechanism. The path formation is dependent on three phases that are: Route request, Route reply, and Route establishment.

Solution to Worm-hole attack

In (Yudhvir Singh, 2012), Yudhvir Singh *et al*. has been designed themechanism for avoiding wormhole attack. Solution can be used for finding the malicious nodes in the mobile ad-hoc network. According to this technique, alternative paths are searched repeatedly in a loop by using route discovery process. This technique easily finds the malicious mobile nodes in the MANETs and avoids all those nodes from the network without affecting the performance of network. In (Krati patidar and Vandana Dubey, 2014), Kriti Patidar *et al*. have been introduced a solution to safe mobile ad-hoc network from black hole attack and wormhole attack and enhanced the total network stability, performance, and reliability. The researcher has been introduced the technology which used the routing information with variations among the intermediary nodes to catch wormhole attack. This technology used the concept of hop count.

Conclusion and future work

By doing such type of literature review, ithas been observed that an ample of problems are there in MANETs like various types of attacks in MANET routing protocols etc. So MANETs

are facing the issues regarding to the security level in MANET routing protocols. An ample of techniques, protocols, algorithmic approaches have been provided by the researchers in this domain in order to provide security against the misbehaving nodes causing the security issue in the network. And Solutions can be used to remove such type of problems in routing protocol and to enhance the performance level Of routing protocols. The objective of the researches is merely to endow the unique technical approaches in order to endow the safety against the black hole attacks over routing protocols and can enhance the overall efficiency of the network routing protocols. The masterly algorithmic approaches can be designed and implemented with the help of popular software tools like network simulator (NS 2,3), Opnet, MATLAB etc. to check the performance level and outcomes from the network.

REFERENCES

Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto and Nei Kato," A Survey of Routing Attacks in Mobile Ad-hoc Networks" IEEE Wireless Communication 2007, pp.85-91.

Chaitali Biswas Dutta, Utpal Biswas," A Novel Blackhole Attack for Multipath AODV and its Mitigation", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.

Concepts and Protocols "Wireless and Mobile Networks" book by Dr Sunilkumar S. Manvi and Mahabaleshwar S. Kakkasageri.

Fang-jiao Zhang, Li-Dong Zhai, Jin-Cui Yang and Xiang Cui, "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks", Information Technology and Quantitative Management (ITQM 2014).

Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao,"A survey of blackhole attacks in wireless mobile ad-hoc networks", Springer 2011,pp. 1-16.

Harris Simaremare, AbdelhafidAbouaissa, RiriFitri Sari and Pascal Lorenz, "Performance Analysis of Optimized Trust AODV using ANT Algorithm", IEEE ICC 2014 - Communications Software, Services and Multimedia Applications Symposium,pp. 1843-1848.

Jiven CAI, Ping YI, Jialin CHEN, Zhiyang WANG and Ning LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad-hoc Network", 2010 24th IEEE International Conference on Advanced Information Networking and Applications,pp. 775-780.

Krati patidar and Vandana Dubey, "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks", IEEE 2014.

Mohamed A. Abdelshafy, Peter J. B. King," Analysis of Security Attacks on AODV Routing", IEEE 2013, pp. 290-295.

Mohemad A. Abdelshafy, Peter J. B. King, "Analysis of Security Attacks on AODV Routing", IEEE, pp 290-295, 2013.

MS Monika Y. Dangore, Mr Santosh S. Sambare," Detecting and Overcoming Blackhole Attack in Aodv Protocol" 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, pp.77-82.

Nirbhaya Chaubey AkshaiAggarwa, Savita Gandhi, Keyurbhai A Jani, "Effect of Pause Time on AODV and TSDRP Routing Protocols under Blackhole Attack and DoS Attack in MANETs", IEEE 2015, pp. 1807-1812.

Papadimitratos P. and Z. J. Haas. "Secure routing for mobile ad hoc networks," "SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)", Jan 2002.

Rajinder Singh, Parvinder Singh and Manoj Duhan, "An effective implementation of security based algorithmic approach in mobile ad-hoc networks" Singh *et al*. Human-centric Computing and Information Sciences 2014, pp. 1-14.

Rutvij H. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs", IEEE 2013, pp.254-260.

Satria Mandala, Abdul Hanan Abdullah, Abdul Samad Ismail, HabibollahHaron, Md. AsriNgad, YahayaCoulibaly," A Review of Blackhole Attack in Mobile Ad-hoc Network", IEEE 2013, pp. 339-344.

Saurabh Gupta, Subrat kar, S Dharmaraja," BAAP:Blackhole Attack Avoidance Protocol for Wireless Network", International Conference on Computer & Communication Technology (ICCCT)-2011,pp.468-473.

Vimal Kumar, Rakesh Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad-hocNetwork", ScienceDirectProcedia Computer Science 48 (2015) 472 – 479.

Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika and Dheer Dhwaj Barak, "Wormhole Attack Avoidance Technique in Mobile Ad-hoc Networks", 2012 Third International Conference on Advanced Computing & Communication Technologies, pp. 283-287.

****