International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 6, Issue 6, June 2017 **ISSN 2319 - 4847**

AN APPROACH TO DETECT AND ENHANCE BATTERY POWER FROM POWER DRANING ATTACK IN MOBILE AD-HOC NETWORK

[1]Mr. Ankit Barve, [2]Mr. Balwant Prajapat

[1]M.Tech (Cyber Security), VITM College Indore

[2]Asst. Professor & Head CS & IT Department VITM College Indore

ABSTRACT

Mobile Ad hoc Network (MANET) it is vulnerable to different routing attacks. One of the severe network layer attack is "Battery life draining attack", In this attack modifies targeted packets. It does so by preparing long routes or misguiding the packets. Malicious nodes use false messaging, or modify routing information. This action affects the bandwidth and node's battery power. Network resources will get protection from attack. In this paper, we have discussed about battery life draining attack, its behavior and technique of its detection and prevention available currently. It is energy efficient method in this method we will enhance the battery power life.

Keywords: MANET, Vampire attack, Routing Protocol AODV.

1. INTRODUCTION

According to the structure, a network has categories in two main domains first wired oriented and second wireless oriented. While, according to their utility and applications the wireless communication is also illustrated in two parts, first short range or indoor communication and second broad range or outdoor communication. Wireless mobile ad-hoc network be a locate of various nodes or terminals which converse by every new by means of decentralized manager and has advantage of wireless message and system ability [1]. MANET is a type of ad-hoc system and generally has a routable network background taking place scheduled pinnacle of connection level of wireless ad-hoc system. every nodule within mobile ad-hoc system participates as the sender or receiver in addition to a router. Routing has to be enabled within every node in the direction of further the incoming packet to the receiver. The information shared between two nodes in the mobile ad-hoc network required to determine a way from the sender to the receiver. A variety of routing algorithms exist with each direction-finding approach be able into single mode or the other depending upon the range of the network [2]. Because of restricted property in MANET, designing an effective routing algorithm has become complicated task. A well-organized routing algorithm is requisite to be considered for the restricted property within the MANET and at the equivalent time it has to be adjusted to changing network conditions like topology, passage, the amount of nodes etc.

Proposed work investigates the wireless ad-hoc network designed for their safety plus presentation issue. appropriate to study these issue be essentially needy happening the routing strategy the methods in which the network nodes identify to provide data. These technologies are easy to use attacking work on such networks, the attack technique to tuppavarkalul used by majority.

There are several forms-based attacks. Wireless advertising network needs more work about vampire attacks
Several routing based attacks exist. More work is required for the vampire attacks in wireless ad-hoc networks. The study is for finding an optimum solution for the vampire attacks which causes the energy loss and performance losses in wireless ad-hoc network.

2. AD-HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOLS (AODV)

AODV is a responsive pathway set of rules planned for ad hoc wireless network. To connect two nodes, AODV routes only when demand is required. AODV routing algorithm is particularly suitable for active self-configured network such as mannet. AODV provide a loop-free route with root managing designed for not working relations. Bandwidth

demand of mobile nodes is relatively in AODV, but as an alternative protocol, AODV does not require routine advertising from time to time.
There are 3 forms of management messages in AODV, which are mentioned below.

Route Request Message (RREQ):

The starting place node that transmits RREQ messages should communicate with any other node within the network. AODV Flood RREQ Message, Increasing Ringer Technology of Torture There is a time (TTL) value to live in every REE message, the value of TTL indicates that RREC has to be forced to broadcast

Route Reply Message (RREP):
Having a requested identification or any intermediate node that joins a route to the requested node generates a route path RREP message back to the mastermind join.

Route Error Message (RERR):

Within the system, each node keep the vertical link on the nodes of your neighbor in the neighborhood. Once the node has detected a link crack that is very full of life, (RERR) is generated from the message node, thus giving different notes to those nodes that are below the link

3. EXISTING SYSTEM LIMIT
A malicious node can meet the following attacks in AODV.

The source node can be impersonated through malicious node by modifying the source address with its address inside the RREQ package.

To analyze communication in the route and to become a part of it, the malicious node RRQ can also change the other packet contents such as hop count for hop calculation to increase the likelihood of being selected into the pathway involving starting place and target. Reduces.

The destination node can be cloned in RREP by establishing a destination deal with via its individual address.
Malicious nodes can capture entire network and can act as a network leader by broadcasting the largest sequence number. This can be a black hole for the entire sub-network

This can pick up some RRQ packets and RREP packets and save them from other packets.

It can create a RER message and can avoid further communication between the nodes because they can not reach the destination with different serial numbers.

To create a delay in communication, malicious nodes can send two different RREQs in the neighboring node with different sequence numbers.

4. VAMPIRE ATTACK
Originally a vampire attack is a type of DDOS attack, which onsumes resources on neighboring nodes. so, targeted packet are being prepared during the invasion of the vampire, due to which the prepared routes can be prepared or misleading packets. In addition, malicious nodes square measure conspiracy the network create persistent property with false management message exchange from neighboring nodes. The malicious node use battery power of the network devices and when consumption not forward the initial packet, through the traditional additional shortest energy expenses of O (d) where d is the system distance, make d/2 the likely length of the pathway to an random destination.

Malicious node creates loop with the help of same number of nodes including many time in a selected path. This attack is known as carousel attack and it uses for increasing the path length away from the number of nodes in the network, simply restricted via amount of authorized entry in the source route.

Attackers do not employ or else go back prohibited route otherwise check communication in the small expression.

Battery power consumption is considered meant for the slightest no of packets requisite towards transport particular packet, therefore the power of attack raise linearly pending bandwidth diffusion with the many packet transformed.

TYPE VAMPIRE ATTACK

The three types of vampire attacks, which are used to attack the carousel, vibe visits and malicious invasion attacks, have been described.

Carousel Attack: Carousel attack is a kind of vampire attack. Malicious node creates packet intentionally introduces routing loops in this attack. It focuses on source routing protocols and modify a few information of packet headers at received route reply, allow a single packet to continually move through the same set of nodes.

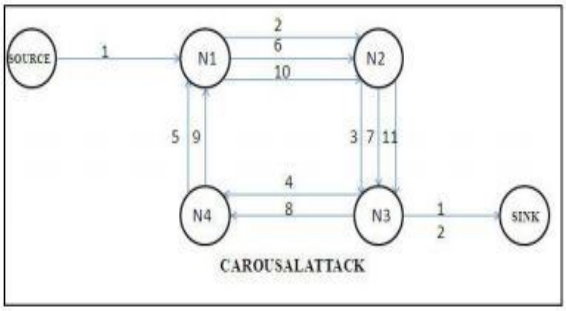


Figure:1 Carousel Attack

Stretch Attack: Stretch attack is also a type of vampire attack. This attack also targeting source routing. Malicious node creates falsely extended route in this attack therefore, packet moving possibly throughout the network. This attack is known as stretch attack, because it extend path of the packet, and all packets processed through almost every node that is free from hop count next to the shortest path among the malicious node and packet destination.

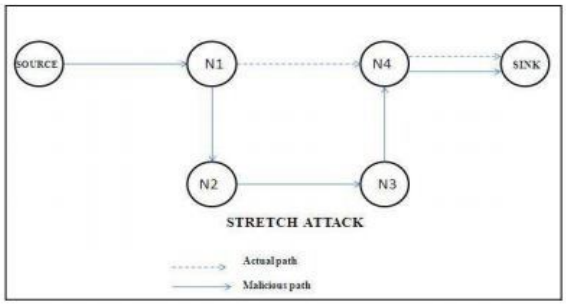


Figure:2 Stretch Attack

Malicious Discovery Attack: Malicious discovery attack is a variant of vampire attack. This attack targeting on-demand routing. Malicious nodes have various paths to make supposed topology using malicious discovery attack. Topology change means attacker may incorrectly declare that connection losing or a connection to node that is not available to the current network. Malicious discovery attack is formed with modifying the packet header's information and continuously flood that modified packet. That flooding consumes node's battery power and disable the network.

Current protocols are not focused on the attack of this vampire. Vampire attacks are on the routing layer, hence nearby are two type of attacks, that is to say carousel and vandal attack. Therefore, a major energy loss is referred to as the new protocol PLGP, a valuable and secure protocol is estimated with important management protocols referred to as the Alpatic Diffie-Hellman Key Exchange Protocol to avoid the attack of this vicious vampire. With the employment of this approach, existing issues is overcome.

5. PROBLEM DOMAIN

The major security problem with the ad hoc network is unsafe routing. However, however, this place has been eliminated in large quantities of labor, although all schematic techniques area unit supports static methods. They are not taking the current network traffic, with safety issues of Midway Nodes and the selected route. Apart from this, the position of routing technology, in order to mislead routing techniques, distorts the attackers to compromise with detector nodes or intermediate messages, or bring the network to an endless position. In one of the most important draws of an unsafe routing, limited accessibility conditions have been expanded during routing time, highest energy usage, resource consumption with communiqué.

Ad hoc network are weak for various types of attacks. These attacks are mainly: Attacks on secrecy and authentication (external appearance attacks, packet replley attacks, and improving or spoofing of packets), attacks on network availability (attacks on exchange of swap networks are often denied. (DoS attacks), aggravated attack against service integrity (target network of attacker to accept false data value.

6. PROPOSED TECHNIQUES

The following methodology describes the implementation of the proposed approach to detect the battery life exhaust attack. Actually, battery life dragon attack is a type of DDOS attack, which consumes the battery power of the nodes in the network. Therefore, long routes have been designed to modify the targeted packet or are packing the rumble during the attack. Using the false control message exchange in the malicious node network, they are constantly communicating with neighboring nodes. Due to this, neighboring nodes answer a false request for connectivity, so that energy burns fast. Therefore, in order to identify malicious packets in the network, a new type of scheme is needed which monitors the activity of the network node and provides decisions for malicious packets.

The attacker nods the packet information received during the attack. For the purpose of simulation, when a malicious host receives RREQ packet (route request packet), it changes the destination address to an unreadable or unknown host IP address. This results all the packets are continues floods in the network. Once the host floods false packets the network bandwidth consumption increases. Both the activities on the network cause the frequently energy losses and bandwidth consumption.

7. ALGORITHM FOR DETECTING & AVOIDING MALICIOUS NODES OR PACKETS.

The secure routing protocol finds the malicious packet in network and reduces the impact on performance. Routing protocol detects issues in packet and prevents it when a malicious host transmits the altered packets thus the entire detection technique is required to implement in route discovery phase. The nodes will check host and might discard the malicious packet throughout route discovery section. then, projected work perform test on the expected packet information by forward toward further host. Therefore, broadcast ID of acknowledged packets in conjunction with Destination ID of usual packet is check within the algorithmic rule.

ALGORITHM:
Step1: Initialize with range of Received RREQ Packets but limit.

Step2: IF (Received_RREQ_Packet==1) THEN

Forward the RREQ packet

ELSE IF (Received_RREQ_Packet==2) THEN

Ignore RREQ and wait for new one

ELSE IF (Received_RREQ_Packet< RREQ limit)

REPEAT i =1 to Received_RREQ_Packet-1

Extract bid[i], dadd [i]

IF (bid[i] == bid [i+1] && dadd[i] == dadd [i+1]) THEN Flag=1

ELSE Flag=0

Step3: IF (Flag===1) THEN

Forward the RREQ packet

Else

DISPLAY (“Malicious RREQ Packet”)

Drop RREQ Packet

Step4:Exit

-

The desired algorithm steps are summarized using the flow diagram of the activities. When a source initiates the communication it broadcast a RREQ packet for finding the dedicated route between source and destination. At that time the RREQ receiver initiate two variables named flag and received RREQ. When a receiver finds the first RREQ packet it checks the received RREQ value. If received RREQ value is 1 then check source address and forward the packet. while node receive two RREQ packets then ignore packets with wait for original one. If received RREQ value is more than two then protocol extracts broadcast id and destination address from RREQ packet and compare them. If broadcast id with target address of all RREQ packets are same then set flag to one otherwise zero. If flag value is 1 then forward the RREQ packet else display that packet as malicious packet.

8. SIMULATION PARAMITERS AND NETWORK

SCENARIO :
This section explains the entire analysis methodology at the side of simulation atmosphere and network state of affairs thoroughly.

Number of nodes	13
Dimension of simulated area	1000×800
Simulation time (seconds)	70
Radio range	300m
Traffic type	CBR, 3pkts/s
Packet size (bytes)	512
Routing Protocol	AODV
Connection Type	TCP

A.Performance Metrics:-
Following are the performance metrics considered to demonstrate the performance of our proposed AODV under different environment network scenario.

i) Packet delivery ratio:-
The whole quantity of packet send via starting place device and successfully received packets ratio is responsible for PDR packet delivery ratio which. The packet delivery ratio is estimated using the below given formula.

$$PDR = \frac{\text{NO. OF RECEIVED PACKET}}{\text{NO. OF PACKET SEND}}$$

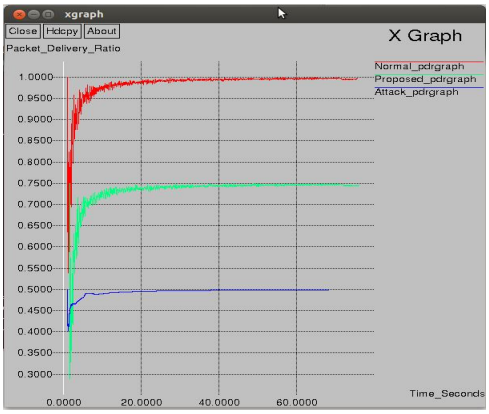
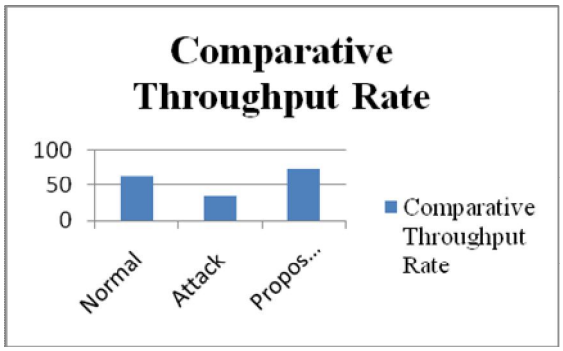


Figure 4: Comparative PDR

ii)Throughput rate :
Network throughput is the rate of successful data or message transfer over a communication link. Data may be delivered over a physical or logical link, or exceed through a definite network node. The throughput is frequently

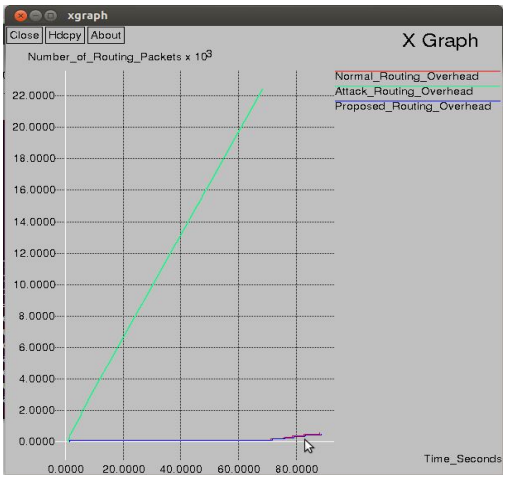
considered in bits or bytes per second (bit/s or bytes/s), with from time to time in data packet for every second or data packet for each time period.

$$\text{THROUGHPUT(BYTES/SEC)} = \frac{\text{TOTAL NO. OF RECEIVED PACKET AT DESTINATION}}{\text{TOTAL SIMULATION TIME}}$$



iii) Routing overhead:

The amount of routing packets such RREQ, RREP, RERR injected into the network is known as the routing overhead. When a node needs to communicate with other node in the network then it initiates route discovery process. For sending a data packet in the network there are many packets like MAC packets, Beacon packets in the network which are not data packet. It creates overhead in the network.



iv) Remaining Energy :

Ad-hoc system nodes initially contains a fixed amount of energy, the measurement of energy describes how long a network device is live in the network. The amount of energy consumption enlarges as the number of nodes (traffic) increases. Initial energy is set for nodes and for graph generation, read value from trace files and calculates remaining energy with the help of awk file.

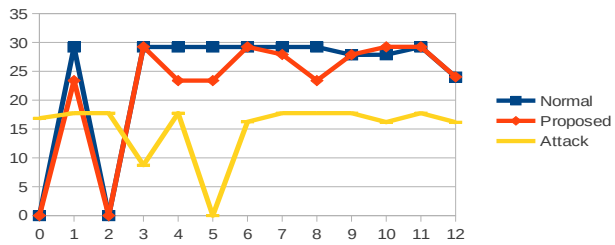


Figure 4: Comparative Remaining Energy

9. CONCLUSION

The wireless ad-hoc system be single of the popular networks in now days. A rich amount of applications are designed with the help of wireless ad-hoc network. The routing algorithms are responsible for route discovery and management in such networks. The transmission of data in such network is performed in ad hoc manner. Therefore, any mobile suspicious node can join the communication. It may causes loss in privacy and security therefore; different kind of routing deployment based attacks is studied in this work. After examining various routing-based attacks, an interesting type of attack was recovered, in which the battery life was attacked. Drainage attack in battery life Resources consumption in wireless networks is a type of attack, it can reduce network performance and reduce the life of infected network nodes.

A new solution has been proposed to detect malicious packets in the network. The proposed solution first compares all REEC (route requests) received in each node. By compiling a packet header information (broadcast ID and destination address), a comparison is made. When the broadcast ID and destination address are the same in each packet, leave that packet or leave them.

Comparative performance study is done in relation to the current approach to correct the effectiveness of the proposed approach. It has been concluded that the performance of the proposed approach is favorable appropriate to high bandwidth accessibility, near to the ground energy consumption, high packet delivery ratio and low routing overhead.

REFERENCES

[1] S. Buruhanudeen, "Existing MANET routing protocol and metrics used toward the efficiency and reliability-An Overview," IEEE Telecommunication and Malaysia International Conference on communication, pp. 231-236, 2007.
[2] T. W. Mehran Abolhasan, "A review of routing protocols for mobile ad hoc netwok," ELSEVIER, Ad Hoc Networks, vol. 2, pp. 1-22, 2004.
[3] N. H. Eugene Y. Vasserman, "Vampire Attack: Draining Life from Wireless Ad-hoc Sensor Networks," IEEE Transaction on Mobile Computing, vol. 12, no. 2, pp. 1-15, February.
[4] J. L. Th. Arampatzis, "A Survey of Application of Wireless Sensor and Wireless Sensor Network," in Proceeding of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 2005.
[5] A. T. Kartik Kumar Srivastava, "Secure Data Transmission in MANET Routing Protocol," International jounral of Computer Technology & Applications, vol. 3, no. 6, pp. 1915-1921, 2012.
[6] M. B. Harjeet Kaur, "Performance of AODV, OLSR AND ZRP Routing Protocol under the black hole Attack in MANET," International Journal of Advanced Research in Electricals, Electronics and Instrumentation Engineering, vol. 2, no. 6, pp. 2320-3765, June 2013.
[7] H. M. Amirhossein Moravejosharieh, "Performance Analysis of AODV, AOMDV, DSR, DSDV Routing Protocol in Vehicular Ad-hoc Network," Research Journal of Recent Sciences, vol. 2, no. 7, pp. 66-73, July 2013.
[8] P. K. S. Kapang Lego, "Comparative Study of Ad-hoc Routing Protocol: AODV, DSR, DSDV in Mobile Ad-hoc Network," Indian Journal of Computer Science and Engineering, vol. 1, no. 4, pp. 364-371.
[9] A. P. Dr S.S. Dhenakaran, "An Overview of Routing Protocol in Mobile Ad-hoc Network," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 2, pp. 251-259, February 2013.[10] J. KIM, 8 April 2011. [Online]. Available:http://www2.engr.arizona.edu/~junseok/AODV.html.
[11] V. V. P. Rajipriyadharshini, "Vampire Attacks Deploying Resources in Wireless Sensor Network," Internatinaol Journal of Computer Science and Information Technologies, vol. 5, no. 3, pp. 2951-2953, 2014.
[12] J. D. B. Umakanth, "Detection of Energy draining attack using EWMA in Wireless Ad- hoc Sensor Network," International Journal of Engineering trends and Technology, vol.4, no. 8, pp. 3691-3695, August 2013.
[13] P. D. P. R. Sundaram, "Exhausting energy by Vampire's in wireless ad-hoc Sensor Netwok," International Journal of Computer Science and Mobile Computing, vol. 3, no.2, pp. 856-861, February 2014.
[14] P. Chandragiri, "Early Detection and Prevention of Vampire Attack in Wireless Sensor Network," in Proceeding of the Intl. Conference on Information, Engineering, Management and Security, Warangal, 2014.
[15] D. J. A. P. Preethi Monoline, "Cache Consistency and IDS for Handling Attacks in Routing Ad-hoc Network," International journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 4, 2007.
[16] S. R. Susan Sharon George, "Attack-Resistant Routing for Wireless A-hoc Network," Internattional Journal of Computer Science and Information Technologies, vol. 5, no. 3, pp. 420-442, 2014.

[17] I.-R. C. Fenye Bao, "Hierarchical Trust Management for Wireless Sensor Networks and its Application to Trust-Based Routing and Intrusion Detection," IEEE Transaction on Network and Service Managemnet, vol. 9, no. 2, July 2012.

[18] Y. Yuanming Wu, "Insider Threats against Trust Mechanism with Watchdog and Defending Aproaches in Wireless Sensor Networks," IEEE Symposium on Security and Privacy Workshop, pp. 134-141, 2012.

[19] K. S. Jose Anand, "Vampire Attack Detection in Wireless Sensor Network," International Journal of Engineering Science and Innovative Techonolgy, vol. 3, no. 4, July 2014.