LIMITING THE ENERGY DRAIN IN WIRELESS AD HOC SENSOR NETWORKS

Bhargavi[1], Srigitha S. Nath[2], Preethi.S[3]

[1]PG Scholar, Department of ECE, Saveetha Engineering College, Tamil Nadu, India
[2]Head of Department, Department of ECE, Saveetha Engineering College, Tamil Nadu, India
[3]PG Scholar, Department of ECE, Saveetha Engineering College, Tamil Nadu, India

Abstract

Wireless Ad Hoc and Sensor networks are exciting fields of research. This paper explores resource depletion attacks where the battery of the node gets depleted excessively thereby making the node incapable of communication. The packet travels longer distances than actually required, therefore draining the energy of nodes. Stretch and Carousel attacks take place in the network which leads to looping and longer route generation in the network. To reduce such attacks, a new protocol is proposed which uses indexing number in order to reduce the energy loss due to unwanted path traversal of packet in the network.

Keywords *– Stretch attack; Carousel attack; Resource depletion attacks.*

----------***----------

1. INTRODUCTION

Wireless Ad Hoc and Sensor networks promise a wide range of applications in the near future. Sensor Networks are currently used in a large number of applications such as temperature monitoring, pressure monitoring and many more. Wireless Ad Hoc Networks have become very critical since they need to perform under heavy load and real time attacks such as Denial of Service. Resource depletion attacks on networks have become very common in the present scenario. All the real time networks need to be consistent even under such attacks. The permanent resource depletion attack is the depletion of the node's battery thereby rendering it useless for any communication. The average energy a node uses in any network is more or less constant for a particular packet size. During attacks by intruders or malicious nodes, the node's energy expenditure increases drastically thereby leading to its energy depletion making the node incapable of transmissions in future.

Resource depletion attacks that concentrate on draining the energy of nodes, calculate larger routes or loops in the network. Such attacks that deplete the nodes battery life may be called as Vampire Attacks. Stretch attacks are those that involve an adversary constructing artificially long routes, potentially traversing every node in the network [1].

Similar to Stretch attack is the Carousel attack, where an adversary composes packets with purposely introduced routing loops [1]. This increases the energy expenditure of nodes in that specific loop and thereby the node's lifetime is reduced.

In any real time application of Ad Hoc Sensor Networks, millions of nodes may be present. Computing long routes or loops in a very large network leads to unnecessary packet loss and a very large amount of energy drain. Packets might travel large number of nodes in order to reach the sink from its source in a normal environment. Therefore while considering scenarios where malicious nodes are present, the number of nodes through which the packet traverses doubles or triples in the case of stretch attacks and increases even more in case of carousel attacks. So it is highly essential to generate a network which limits the energy drain and performs well under real time traffic.

There are other attacks such as wormhole and sinkhole attacks where the packets are routed from one part of the network to another through a separate link [2]. Two malicious nodes inside a network form a link between them without other nodes being aware of it. These malicious nodes are generally placed at large distance having multiple nodes between them. Any packets that are routed into the network reach the malicious node. This node transmits the packet to the other malicious node. This way the packet travels from one part of the network to the other causing unwanted packet loss. This may be useful in certain cases where the information reaches the destination node quickly. But in general the packet details can be extracted easily since the packet is caught in the link between the two malicious nodes. Packet drop can be done at will by the malicious nodes.

2. RELATED WORK

In wireless Ad Hoc and Sensor Networks all nodes are connected to each other in a wireless manner. In Ad Hoc networks the nodes form dynamic topology depending upon the number of nodes available and the location in which the network has been deployed. The networks encounter a large number of resource depletion attacks such as denial of service (DoS), draining battery life, packet drop and many more. Denial of Service attack has become very common in present wireless networks. The entire network bandwidth gets occupied due to continuous requests sent by intruder or malicious nodes. This generates heavy traffic in the network. Multiple requests sent simultaneously create heavy traffic in the network. Authentication puzzles are used in order to check the node's honesty before they are allowed to use the entire bandwidth [5].

Draining of battery life is another resource depletion attack that leads to the failure of network. Different routing protocols are susceptible to different types of attacks. EndairA, a provably secure on-demand source routing protocol is used to avoid the routing attacks [4]. Ariadne (a clean slate routing protocol) was introduced to provide security to the transmitted data, but it consisted of a few short comings. This was rectified by EndairA but the security issues still exist. The entire network can be paralysed by a single malicious node which can change the entire routing path. Wormhole and sinkhole attacks increase the network energy usage by a large margin when compared to other attacks. Packet leashes have been introduced in order to limit this unwanted energy expenditure in the network [2]. Temporal leashes and Geographical leashes have been designed in order to minimise the energy drain due to the wormhole attacks. Temporal leashes limit the lifetime of the packet while geographical leashes limit the distance or range the packet can cover. Time synchronisation is a key feature in this method. Lack of proper time synchronisation renders the method ineffective.

Ad Hoc Networks may be mobile in nature. Since all the applications currently used are wireless in nature, Ad Hoc networks are mostly deployed in a clustering hierarchy with mobile nodes. The cluster heads may be selected based upon the energy present in them. Nodes that act as the cluster heads will require more energy than the member nodes. The energy of every node is measured while selecting a cluster head. The nodes with the optimum energy may also compete for acting as the cluster head [6]. The cluster head may be changed periodically depending upon the energy consumed. Routing protocols such as LEACH [7], Cluster-Based Energy-Efficient Routing Protocol without Location Information [8], etc., consider cluster heads to be the major part of communication and assign the clusters accordingly.

Stretch and carousel attacks have become very common in every routing protocol. The energy depletion that takes place due to these two attacks is quite high. PLGP [1], a clean slate secure sensor network routing protocol has been designed to reduce the energy drain due to these stretch and carousal attacks. The protocol is designed mainly for the packet forwarding phase and not for the topology discovery. Since networks at present are mostly Wireless, the topology is dynamic in nature. The PLGP protocol makes sure that there is always packet progress, i.e., the packet always travels towards the destination without any back tracking. The route once travelled is not back tracked since each node verifies the packet header, for the previous node's details. Even though the nodes checked the packet header details, the malicious nodes or the intruders had the capacity to edit or delete certain details. These malicious nodes may also forward packets without adding their details. Attestations were added to overcome this problem. PLGPa added attestations to the packet, which are similar to signatures, every time the packet is forwarded. This way the nodes cannot modify the previous node's details and will have to add their own signature to forward it. Attestations added to the packet header made the header size larger thereby leading to difficulty in encryption, decryption and coding.

3. PROPOSED WORK

The work proposed here is to prevent the packets from looping and stretch attacks. The energy that is depleted due to these attacks plays a very important in the life time of the node. In the existing protocol, PLGP, the packet is checked for no backtracking by ensuring that every packet makes progress in the network. Each packet that is transmitted must travel towards the destination and must not re-trace the same path it has already traversed. The major drawback here is that certain malicious nodes can alter this path information thereby again leading to stretch and carousel attacks. To overcome these drawbacks PLGPa was introduced, which uses attestations that are added to the packet header. Attestations are similar to signatures. Every node has its unique signature. Therefore this is helps in adding extra security. In scenarios where the malicious node can duplicate the signature of another node, the PLGPa protocol is rendered useless.

The main idea here is to generate a network which has very less energy depletion due to stretch and carousel attacks. A new protocol called MDSDV is proposed, which significantly reduces the energy depletion in the network due to such attacks. At first we generate a network with the required number of nodes. The nodes may be mobile or fixed in nature. The nodes are then connected using duplex links. The nodes are arranged in clusters in order to communicate efficiently. The cluster heads are elected at random. The cluster heads are changed based on LCC (Least Cluster Change). Here, the cluster head changes only when one of the following takes place; when two cluster heads are found within the same cluster or when the cluster head moves out of range of that particular cluster. The entire communication inside the cluster

is only through the cluster head. Every cluster also has a cluster gateway. Two or more clusters are connected to each other only through this gateway. When a packet needs to be transmitted from one cluster to a different cluster, the gateway node obtains the packet from the cluster head and passes to its neighbouring gateway. This is repeated until the destined cluster is reached. The Cluster head then transmits the packet to the destined member (sink) of that particular cluster.

Indexing number is added as a security to the packet header in order to avoid packet loops or stretch attacks. This is 8 bit in size therefore does not occupy much space in the header. This gets generated at random for every link therefore it cannot be duplicated. The indexing number is 0 in the beginning. Only when the link has been established the number is generated. The indexing number is changed after a particular time interval.

4. SIMULATION

NS 2 has been used to simulate the network. The simulation is shown below where the nodes are deployed as clusters. A few nodes are mobile in nature.

A main server and an intermediate server have been created which receive and process the packets. Sink nodes are present in every cluster, through which the packets are sent to the neighbouring clusters. A gateway node is present in the common region of the two clusters. The packets that are sent between these two clusters are passed through this gateway.

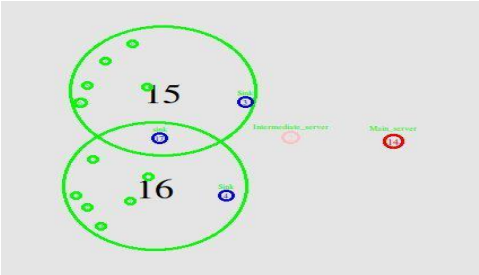

Fig.1 shows a network where the nodes are arranged in a cluster with gateway node. Intermediate server and main server are present which finally receive all the packets.

All nodes contain equal amount of energy before packet transmission starts.

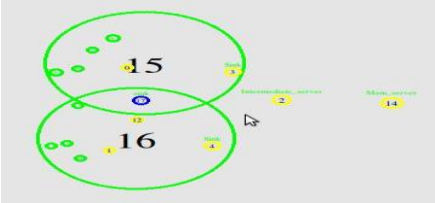

Fig 2 shows that certain nodes have lost their energy.

Only certain nodes take active participation in packet transmission. Once the packet transmission begins, the nodes that transmit the packets slowly lose their energy. The colour of the node changes depending upon the energy available in the nodes which is shown clearly in fig 2.

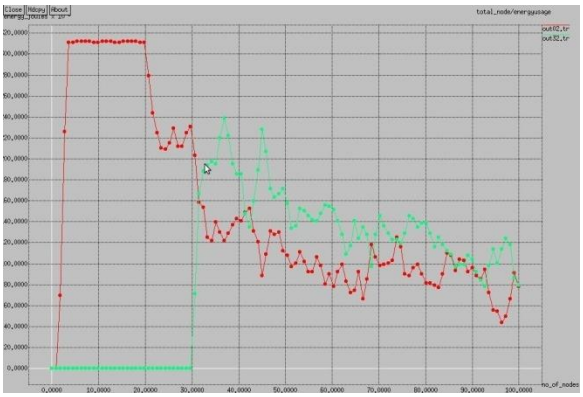

Fig 3 shows a comparison graph between PLGP and MDSDV protocol taking energy usage as the parameter.

The MDSDV protocol uses lesser energy than PLGP protocol. The energy expense for few nodes is large but as the number of node increases the energy expense reduces.

5. RESULTS AND CONCLUSIONS

The above simulation results depict that the energy used by the nodes has been significantly reduced when compared to the energy used by the nodes while implementing PLGP or PLGPa protocol. Depletion of energy due to carousal and stretch attacks has been reduced to a great extent with minimal packet overhead. The energy usage for the PLGP and MDSDV is shown as a comparison graph in fig 3. Instead of attestations indexing numbers are used which changes after a particular period of time, or when new link is established. When a link is used for quite a long time, then this indexing number is changed periodically thereby making the attacks less likely. As the indexing number occupies only 8 bits, it does not making encryption difficult.

REFERENCES

[1] E. Y. Vasserman and N. Hopper, “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks”, IEEE Transactions On Mobile Computing, Vol. 12, NO. 2, FEBRUARY 2013.

[2] Y.C. Hu, Perrig A. and Johnson D.B, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”, Twenty second Annual Joint Conference of IEEE Computer and Communications, IEEE Society, Vol. 3, pp. 1976-1986, 2003.

[3] A.D. Wood, J.A. Stankovic, “Denial of Service in Sensor Networks”, Computer, IEEE Computer Society, Vol. 35, No. 10, pp. 54-62, 2002

[4] Acs .G, Buttyan .L and Vajda .I, "Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 5, No. 11, pp. 1533-1546, 2003.

[5] Suriadi .S, Stebila .D, Clark .A and H. Liu, "Defending Web Services against Denial of Service Attacks Using Client Puzzles", IEEE International Conference on Web Services, 2011.

[6] Qu Wei-Qing, "Cluster Head Selection Approach based on Energy and Distance", International Conferenece on Computer Sciene and Network Technology, Vol. 4, 2011.

[7] L. Jun, Q. Hua and L. Yan, "A Modified LEACH algorithm In Wireless Sensor Network Based on NS2", IEEE international Conference on Computer Science and Information Processing (CSIP), 2012.

[8] G. Lee, J. Kong, M. Lee, and O. Byeon, "A Cluster-Based Energy-Efficient Routing Protocol without Location Information for Sensor Networks", International Journal of Information Processing Systems Vol.1, No.1, 2005

BIOGRAPHIES

Bhargavi.S pursuing M.E in Computer and Communication. She has presented papers in national and international conferences.

Srigitha S. Nath working as the Head of Department in Saveetha Engineering College. She has 16 years of teaching experience and has published 4 papers in international journals.

Preethi. S pursuing M.E in Computer and Communication. She has presented papers a few conferences.