ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Packet Forwarding Method by Clustering Approach to Prevent Vampire Attacks in Wireless Sensor Networks

Vijimol Vincent K[1], D.Prabakar[2]

PG scholar, Dept of Computer Science and Engineering, SNS College of Technology, Coimbatore-35, Tamilnadu, India [1]

Assistant Professor, Dept of Computer Science and Engineering, SNS College of Technology, Coimbatore-35, Tamilnadu, India [2]

ABSTRACT – Wireless ad hoc sensor networks and transmission of data in them is a significant research area. Security is established in sensor networks using different types of protocols. But it is not completely possible. One such DOS attack is Vampire attack, which makes permanent unavailability of the networks by draining the power of each node in the networks. This paper presents a method to bound the damage caused by vampire attack by using the Cluster Head. If any Vampire attack is present in the network, the Cluster Head engages in the situation and delivers the packet to sink without dropping the packet. Thus it provides a successful and reliable message delivery even in the presence of Vampire attack.

Keywords: Wireless sensor networks, security, denial of service attack, vampire attacks

I. INTRODUCTION

Wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Wireless Sensor Networks (WSN) provides different methods for sensing and disseminating information from various environments which provide the potential to serve many different applications. Each sensor has a wireless communication capability and some level of intelligence for signal processing and networking of the data. It provides a capable network infrastructure for many applications like environmental monitoring, medical care, military surveillance etc.

WSN consists of sensor nodes that are deployed in designated area. The security in the communication has become a major concern. Hence securing each node in the network becomes a major issue. There are many types of attacks are present which makes short term unavailability of the networks, but a great deal of research has been done to enhance the survivability. But these schemes cannot address the attacks that affect long term availability of the networks. One such attack is Vampire attack. Vampire attacks are a type of resource depletion attack that makes nodes battery power as a resource of interest [1]. Vampire attacks are different from other types of DoS reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely deplete the network power [2]. Vampire attacks are not protocol specific, since they do not depend on the design properties and implementation faults of particular routing protocols. Vampire attacks will exploit general properties of protocol classes such as link-state, geographic and beacon routing, source routing, and distance vector.

Vampire attacks do not rely on flooding the network with large amount of data, rather they try to transmit as little data possible to drain maximum energy from the network. This kind of attack is very much difficult to find out since it uses protocol-compliant messages. The most difficult challenge is to detect the vampire attacks in the network since it is not protocol specific and they do not depend on the design properties or the other scenarios of the network. It uses only little transmission of data to drain maximum energy of the nodes in the network. Vampire attacks will cause more energy to be consumed by the network rather than the honest node that transmit message of identical size to the same destination. It is not necessary that the message should be transmitted through the same number of hopes.

1.1 Classification

In the process of routing a packet to the destination, the source node composes and transmits the packet into the next hop through the network to reach its destination that has been specified by the route. Thus energy consumption is done not only by the source and destination, but also all the nodes that take part in the process of routing. According to wired networks resources can be characterized by amplification [12],[13].The adversaries can amplify the resource it has been used. Hence amplification attack is possible in the network since the adversary an compose and transmit the message that will process by each node that is specified by the route [1].

1.2 Protocols and Assumptions

In this paper, we are mainly considering two kinds of protocols such as on-demand routing protocols and static protocols[10]. On-Demand routing protocol is the one in which the topology discovery is done at the time of transmission of packets whereas in static routing protocol topology discovery is done at the initial set up phase. Periodic rediscovery of the topology will be done here in order to handle rare topology changes in the network.

The location of adversaries within the network is considered to be fixed and random, since it will corrupt some of the honest node before the network was deployed and cannot control their final position. Sensor networks are having limited battery power [3]. A node will permanently disable from the network once its battery power has been exhausted. A single vampire can attack every node in the network. Hence continuous recharging of the node will prevent from vampire attacks if and only if the vampire attacks are more resource constraint than honest node.

1.3 Overview

In this paper we present a number of increasingly damaging vampire attacks that may affect different types of routing protocol. There are mainly two types of attacks have been discussed here. Carousal attack and stretch attack. By doing so, we are evaluating the vulnerability of the existing protocols.

Carousal attacks are the one in which the adversary packet will create a route to the destination that consists of a number of loops thereby increasing the energy consumption by the networks.

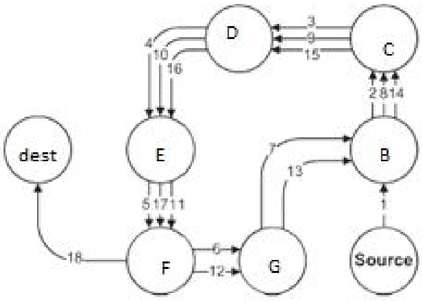

Fig 1: carousal attack

Figure shows carousal attack in which the source sends a packet to the sink [4],[5]. The packet from the source will reach to the destination only after the traversal of packet more than once through the same nodes. Here the length of the route will be greater than the number of nodes of the network. Hence the maximum power will be drained from each node that is participating in the routing of packets. Stretch attacks constitute the process of making the packet to be traversed through almost every node in the networks. It is called stretch attack since it lengthens the packet path causing the packet to be traversed through a number of nodes in the network. Hence it diverts the packet to be transferred from the optimal path.

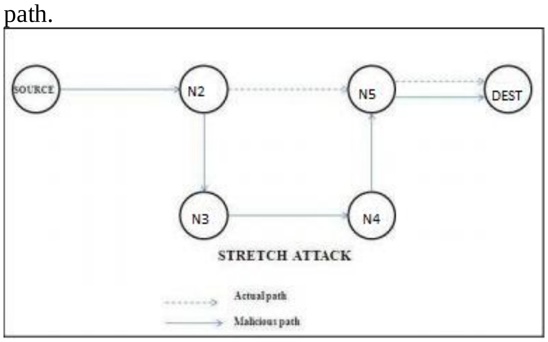

Fig 2: Stretch Attack

Figure shows an example of stretch attack in which the packet is diverted from the optimal path. Here instead of traversing the packet from the node N2 to node N5, it makes the route to the node N3 thereby making the nodes N3 and N4 to take part in the routing process. Hence the powers of these nodes get wasted. In this way stretch attack causes the drainage of the power from the nodes that are not necessary to take part in the routing. The energy consumption in case of carousal attack is higher than that of the stretch attack as it makes same node to be appears in the route more than once.

Compared to carousal attack, stretch attack consumes less energy of the network. Carousal attack can be prevented by making the forwarding node to check source route for loops. Stretch attack can be reduced by making the intermediate node to replace the part or the entire route if they know a better path to the destination.

II. RELATED WORKS

There are many types of power drained attacks are present in the network. One such attack has been defined in [8], which is "sleep deprivation torture". It blocks the node to enter into low power sleep state thus making its power to be drained faster. Another type of attack is denial of sleep attack, which will attack at the MAC layer [9]. Routing loops are discussed in [10] but it does not provide any defenses against it. It discuss only about the underlying MAC and routing protocol. Other than power constrained attacks there are many types of resource depletion attacks are present in the network. Depletion of other resources such as memory, CPU time etc may also cause problems. Example of such attack is SYN flood attack [14].

There consists of a past study about the attacks and defense against quality of service (QoS) degradation that produce long term degradation of the network performance [11],[15],[16],[17],[18],[19]. But this work has been focused on transport layer rather than the routing layer. Current work is mainly concentrates on the minimal energy routing protocol, which tries to increase the network life time. This has been done by using minimum energy for the transmission and reception of packets [6]. Vampire attacks will cause more energy to be consumed even in the minimal-energy routing protocol, as the attacker will produce a route that will make the packet to be traversed through more number of nodes than necessary [7].

III. KEY AREAS

The entire work is divided into 3 phases. First phase include discovery of the topology and selection of the cluster head. Second phase include the identification of neighbor nodes and the third phase includes packet forwarding.

3.1 Selection of Cluster Head and Topology Discovery

Topology discovery includes the implementation of connection across the network. Here we are using mesh topology in which every neighboring node is connected to each other. Mesh network is established by each sending a message to every other node in the network. A node that receives the message will store the information about the node in its record. After the construction of mesh topology in the network, cluster head is selected. Selection of cluster head is mainly based on mobility, range and battery power. Cluster head will be changed periodically in order to distribute the power consumption across the entire network.

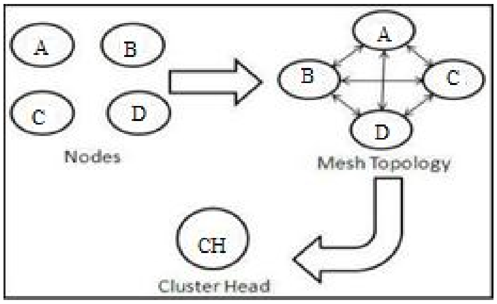

Fig 3: Topology Discovery and Cluster Head Selection

Figure shows the construction of mesh topology. It consists of 4 nodes which are connected to each other.

3.2 Identification of Neighbor Nodes for Packet Transmission

This phase includes the identification of neighbor nodes of each node in the network. This has been done with the help of tree formation[1]. Trees are formed as nodes combine together to form a group. Each node starts as a group that consists of size as1 and virtual address as 0. When two groups that consist of one node combines then its size will become 2 and virtual address will be 0 and 1.

Each group will have their own group address. That is node 0 of group 0 will have an address as 0.0 and node 0 of group 1 becomes 1.0. Whenever two groups are merged to form a new group, the address of the group is lengthened by one bit. Hence tree structure is formed with all the addresses in the network. Hence the neighbor node of each node can be determined.

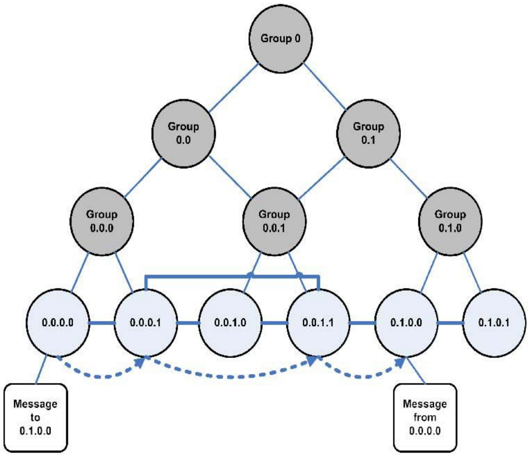

Fig 4: Identifying the Neighbor Nodes.

Figure shows the formation of tree in order to identify the neighbor node. Each node will advertise its presence by broadcasting its ID, and public key signed by its online authority. A tree is formed like this way until all the nodes of the network forms a single group. Hence each node will know about the id, virtual address and public key. Hence it shows the maximum number of connection that can be established between the nodes.

3.3 Packet Forwarding

This phase determine how the packets are forwarding in the network. Each node in the network is independent of every other node. Hence when a packet reaches to a node, the node can take a decision about the next hop by finding the Most Significant Bit (MSB) of its virtual address. MSB of virtual address of next hop will be different than that of the originators address. Hence every forwarding decision should reduce the virtual address length as it becomes closer to the destination.

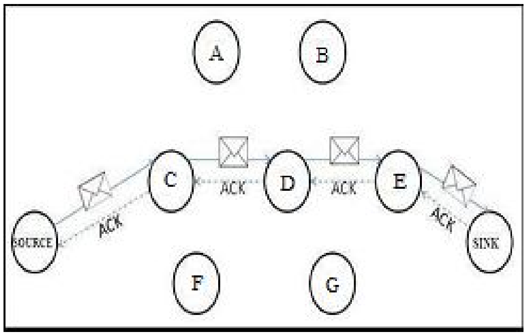

Fig 5: Message Traversal In Normal Situation

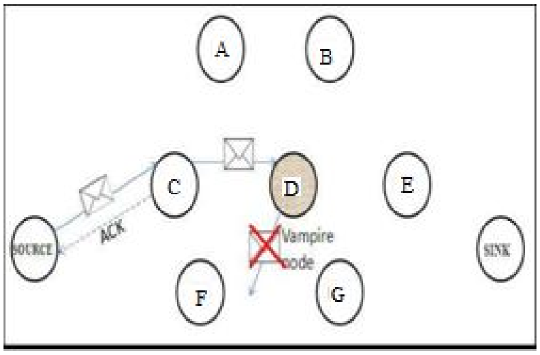

Fig 6: Vampire Attack Leading Top Packet Drop

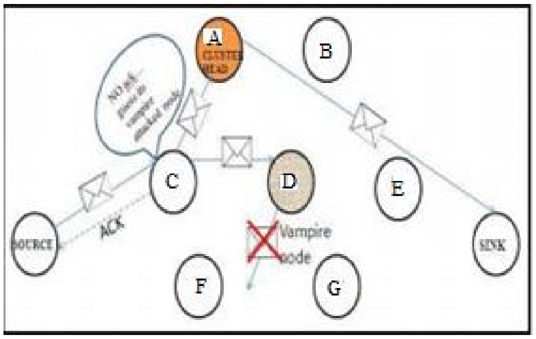

Fig 7: after N trials node N3 forward the packet to the Cluster Head which sends the packet to the sink.

Figure 6,7 and 8 shows the process of forwarding the packet in the network in the presence of vampire. The adversary will prevent the packet from reaching to the destination. Hence dropping of packet will occur as shown in figure 8. In such situation the node tries to resend the packet through the same path more than once. When it fails it will decide to send the packet to the Cluster Head.

The cluster head is chosen based upon the range, mobility and battery power. The node which has the highest battery power and range will be taken as the Cluster Head. The Cluster Head will transmit the packet to the sink directly if it is within the range or else it will send it to the next hop based on the information in its record.

IV. CONCLUSION

In this paper we discussed about Vampire attack, a new type of resource consumption attack which makes the permanent unavailability of the sensor network by depleting the node's battery power. It mainly concentrates on the routing protocol. We discussed about how to preserve the energy by efficient utilization of node's battery power. We showed how to overcome vampire attack thus increasing the network energy by a factor of O (N) per adversary per packet, where N is the number of nodes in the network. Whenever a vampire attack is detected, the cluster head engages the situation and deliver the packet to the destination without any modification of the packet. Handling the mobile network is left for future work.

REFERENCES

[1] Eugene Y.Vasserman , Nicholas Hopper, "Vampire attacks: Draining life from wireless ad- hoc sensor networks".2013

[2] Yun Zhou , Yuguang Fang And Yanchao Zhang "Securingwireless Sensor Networks: A Survey" IEEE Communications,2008.

[3] Eiko Yoneki, Jean Bacon "A survey of Wireless Sensor Network technologies: research trends and middleware's role" 2005.

[4] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[5] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev.,vol. 6, no. 3, pp. 50-66, 2002.

[6] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12,no. 4, pp. 609-619, Aug. 2004

[7] L. Xiaojun, N.B. Shroff, and R. Srikant, "A Tutorial on Cross-Layer Optimization in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 8, pp. 1452-1463, Aug. 2006.

[8] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks," Proc. Int'l Workshop Security Protocols, 1999.

[9] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1,pp. 367-380, Jan. 2009

[10] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.

[11] S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "Path- Quality Monitoring in the Presence of Adversaries," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of Computer Systems, 2008.

[12] K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack," Proc. IEEE INFOCOM, 2001.

[13] V. Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks," SIGCOMM Computing Comm. Rev.vol. 31, no. 3, pp. 38-47, 2001.

[14] D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html,1996.

[15] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems," Proc. IEEE INFOCOM, 2005.

[16] Y.-K. Kwok, R. Tripathi, Y. Chen, and K. Hwang, "HAWK: Halting Anomalies with Weighted Choking to Rescue Well-Behaved TCP Sessions from Shrew DDoS Attacks," Proc. Int'l Conf.Networking and Mobile Computing, 2005.

[17] X. Luo and R.K.C. Chang, "On a New Class of Pulsing Denial-of-Service Attacks and the Defense," Proc. Network and Distributed System Security Symp. (NDSS), 2005.

[18] H. Sun, J.C.S. Lui, and D.K.Y. Yau, "Defending against Low-Rate TCP Attacks: Dynamic Detection and Protection," Proc. IEEE 12th Int'l Conf. Network Protocols (ICNP), 2004.

[19]G. Yang, M. Gerla, and M.Y. Sanadidi, "Defense Against Low-Rate TCP-Targeted Denial-of-Service Attacks," Proc. Ninth Int'l Symp.Computers and Comm. (ISCC), 2004.

[20] R.C. Shah and J.M. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," Proc. IEEE Wireless Comm. and Network Conf. (WCNC), 2002.