IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Reducing the Effect of Energy Drain Attack in Wireless Ad Hoc Sensor Network

Saneesh P S[1], Dhanya Narayan[2], Jeethumol K Joy[3]

M.Tech Scholar (Wireless Technology), ECE Department, College of Engineering, Kidangoor, India[1, 3]

Assistant Professor, ECE Department, College of Engineering, Kidangoor, India [2]

Abstract: Wireless sensor network is a network for sensed data communication across the sensor nodes. In wireless ad hoc Sensor Network each hop to hop connection of sensor nodes are in a random way, there is no fixed infrastructure and nodes are randomly deployed in the sensor field. Due to their ad hoc organization, wireless ad hoc sensor networks are affected to denial of service (DoS) attacks. The most permanent Resource depletion attacks is to entirely deplete node's batteries .One new type of attack called vampire attack. These attacks causing the impact of persistently damaging the networks by quickly draining the node's battery power. They not only affect single node but they bring down entire system battery power. So limiting the energy drain attack has very importance in sensor network. In the cause of vampire attack the packet travels longer distance than actually required this way consume more energy. To reduce such attack MDSDV protocol is used here and compare its performance with energy efficient LEACH protocol.

Keywords: Vampire Attack, Ad Hoc Network, Denial of Service Attack, Resource Depletion Attacks.

I. INTRODUCTION

An ad hoc wireless sensor network is a group of sensor nodes, where each node can communicate over multiple path without the help of any previous communication path such as base station or access points. Ad hoc wireless sensor networks (WSNs) [1] become more and more crucial to the everyday functioning of people and organizations. Due to the ad hoc nature of the wireless sensor network there is a possibility of Denial of Service attack (DoS). DoS [2] attacks that target resources can be grouped into three broad scenarios. First attack scenario targets storage, second attack targets bandwidth, the third attack scenario targets energy resource.

Denial of service attack targets batter is to entirely deplete nodes' batteries. These type of energy draining attack is also called vampire attack. Now-a-days one main issue in wireless ad hoc sensor network is draining of energy at each sensor nodes. In the cause of ad hoc sensor network energy is the important factor. Vampire attacks are the most common highly effective resource depletion attacks where the energy consumed by the network to compose and send a message is longer distance when compared to that of an ordinary network. Vampire attacks disrupt the working of a network immediately rather than work overtime to entirely disable a network.

In the cause of vampire attack the battery of the node gets depleted excessively there by making the node incapable of communication. [3] The packet forward longer distances than actually required, therefore consume the energy of nodes. Vampire attack is mainly two type carousel attack and stretch attack. In these two type of attack sending messages by malicious node which causes more energy drain by the network leading to depletion of node's battery life.

II. TYPES OF VAMPIRE ATTACK

Vampire attack constitutes of two different types of attack called Stretch attack and Carousel attack. These two mainly focuses on reducing the energy of the nodes [4].

A. Carousel Attack

In this type of attack an adversary sends a packet with a route composed as a series of loops. Carousel attack mainly targets source routing protocols by manipulating the limited verification of message headers at nodes which forward message, allowing a single packet to repeatedly travelling in the same set of nodes. Hence same node appears in the route many times. We call it the carousel attack, since it sends packets in circles. Times strategy can be used to increase the packet forwarding length and in this way the energy is lost from the nodes. Another way an adversary composes packets with purposely generates routing loops. It sends packets in circles as shown in (figure 1). It affect source routing protocols by exploiting minimum verification of message headers at forwarding source nodes , then start a single packet to traverse the same set of nodes in a number of times. This strategy can be used to increase the length of the route beyond the number of nodes in the sensor network, only limited by the number of allowed entries in the source route.

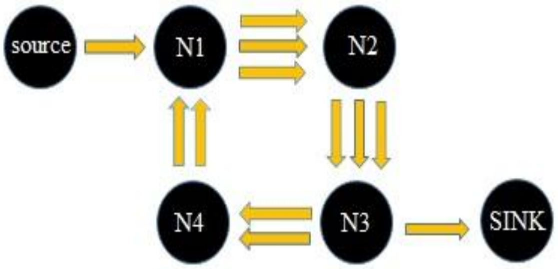

Fig. 1 Carousel attack.

DOI 10.17148/IJARCCE.2016.5644

B. Stretch Attack

In our second attack, also targeting source routing, an adversary constructs artificially long routes, this can make packet to be traverse most of the nodes in the network. This type of attack is called stretch attack, because stretch attack increases packet path lengths, such a way forwarding packets to be processed by a large number of nodes that is independent of hop count along the energy efficient shortest path between the source and destination. Increase in energy usage due to stretch attack is mainly depending up on the position of malicious node in the communication path.

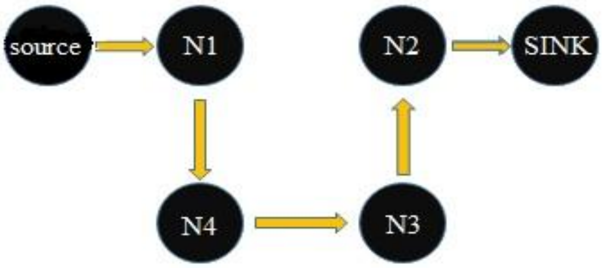

Fig. 2. Stretch attack.

In this stretch attack it principally illustrates more identical energy consumption for all the presented nodes in the network. This attack mainly increase the path length which can lead to more numbers of nodes to process the packet in the sensor network. This way stretch attack consume large energy by increasing the packet forwarding length.

III.RELATED WORKS

A. Using PLGP Protocol

A clean slate secure ad hoc sensor network routing protocol has been designed to reduce the energy drain due to vampire attack [5]. The protocol is designed mainly for the packet forwarding phase and not for the topology discovery. Because of the nature of wireless nature of ad hoc network, the topology is dynamic in nature. The original version of this protocol is mainly designed for security purpose then the protocol is vulnerable to Vampire attacks. PLGP consists of a topology discovery phase followed by a packet forwarding phase with the former optionally repeated on a fixed schedule to conform that topology data stays current. Discovery deterministically arranges nodes into a tree manner that will later be used for the purpose of addressing the nodes. When discovery process start every each node has a limited view of the network information each node known its own information only. At the initial stage of network discovery process nodes start a local broadcasting for getting neighbor information and stopping this process when getting entire network information. Throughout this process each node create a tree relationship between its neighbor nodes and this relationship is then used for the purpose of addressing and routing.

At the end of discovery process each and every node should compute the same address tree as other nodes. All children nodes in the tree are physical nodes in the ad hoc network, and position information of the each node is also present in virtual address of node. Each node in the network then capture the virtual address and cryptographic key. After network convergence final address tree of sensor network is verifiable. Then it assuming each legitimate network node has a unique certificate of membership. For joining multiple numbers of tree groups, nodes who produce clones of themselves in multiple locations, otherwise cheat during discovery can be identified and evicted.

Using PLGP protocol it is help to make sure that all of the packets forward progress. PLGP protocol conform that packet always travels towers the destination without any loop or backtracking. Each node in the sensor network verifies packet header and then forward the packet such a way the route once travelled is not back tracked. Packet header contain previous node's details, each node verifies this details. So packet always travels towards actual path without back tracking.

Drawback of PLGP protocol

The vampire node or malicious node had the capacity to change or clear details in the packet header these intruders may also make packet forwarding without adding their information.in order to overcome this drawback The malicious nodes or the intruders had the capacity to edit or delete certain details. These malicious nodes may also send packets without adding their details. Attestations were added to overcome this problem.

B. Using PLGPa Protocol

PLGPa [6] is modified form PLGP protocol for eliminating the drawback of PLGP protocol. The verifiable path history is added to every PLGP packet. The resulting protocol, PLGP with attestations (PLGPa) is used for more secure communication or packet forwarding. PLGP's tree routing scheme with packet history help to every node can securely verify progress, then preventing any significant malicious node influence on the path taken by any packet which traverses at least one honest node. Every packet is attached to a chain That is created using the signature that is attached to every packet. Each node at forwarding phase verifies the attestation chain to conform that the packet has never traveled away from its destination in the logical address space.

Drawback of PLGPa protocol

In the cause of PLGPa protocol where the malicious has capable of generating signature of another node can lead to duplicate the signature of another node, such a situation PLGPa protocol also vulnerable to vampire attack.

IV.PROPOSED WORK

In order to minimize the effect of energy drain attack Modified form of Destination Sequenced Distance Vector used here. MDSDV protocol help to prevent energy drain attack by sending packet in a longer distance than real. The main performance of this protocol is to solve routing loop problem. A table driven routing scheme is used here. For determining malicious node energy consumption of all

DOI 10.17148/IJARCCE.2016.5644

nodes are calculate. If anode consume more energy than real then this node taken as a malicious node. If vampire node determine then this protocol help to send the packet in another energy-efficient path without vampire node as the intermediate node. For efficient communication the nodes are arranged in cluster way [7]. Cluster-heads can be chosen stochastically (randomly) based on this protocol. The cluster head are changed according to satisfy any of the two condition taking place in the cluster topology. First one is when two or more cluster head with in the same cluster and second one is when cluster head move away from its own cluster communication range.in the communication process data packets from the sensor nodes with in cluster are forward through the cluster head. Some nodes with in the cluster act as a gateway node. This gateway helps to communication between two clusters.

For improving performance this protocol against energy drain attack a signature added to each node. This help to end the effect of sensor network from stretch attack. This signature is generate stochastically so malicious node does not duplicate the signature of another node.

LEACH [8] is also use cluster based communication for minimizing energy consumption. LEACH stands for Low-Energy Adaptive Clustering Hierarchy. Wireless sensor network with LEACH protocol is considered to be dynamic clustering method.

V. SIMULATION AND RESULTS

In order to check protocol performance against energy drain attack first here generate a wireless ad hoc sensor network with 50 nodes using NS2 [9] simulator. Nodes arranged in cluster manner nodes set as a mobile in nature. One node is set as a sink node. For determining cluster head and other nodes different colour used. Cluster head is act as a sink node for each cluster. A node within each cluster act as gate way node. Two clusters are communicate using this gate way node. Simulation is start with calculating energy of each node. MDSDV and LEACH protocols are used to simulating this network. MDSDV use a table driven routing scheme.

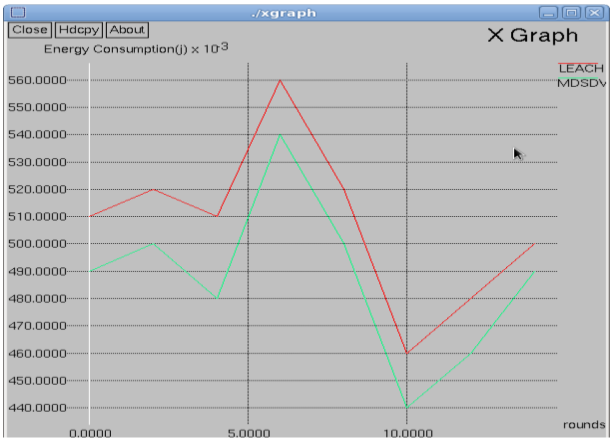

Fig. 3. Energy consumption graph of sensor MDSDV and LEACH protocol

Simulation is start with finding energy of each node. MDSDV protocol determine malicious node by determining quick decrease in energy of sensor node. Figure 3 shows the energy consumption of wireless ad hoc sensor network with energy drain attack. MDSDV protocol decrease the energy consumption of sensor node due to energy drain attack. It also shows energy consumption same network with LEACH protocol. Comparing the energy consumption of both protocol MDSDV protocol consume less energy than LEACH protocol.

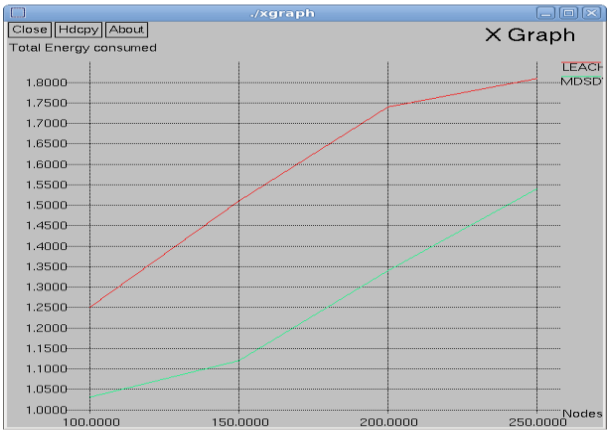

Fig.4. Total energy consumption graph of MDSDV and LEACH protocol

Figure 4 shows total energy consumption of both protocol. Compare MDSDV protocol with LEACH protocol MDSDV consume less amount of total energy than LEACH. So MDSDV protocol is more energy-efficient than LEACH.

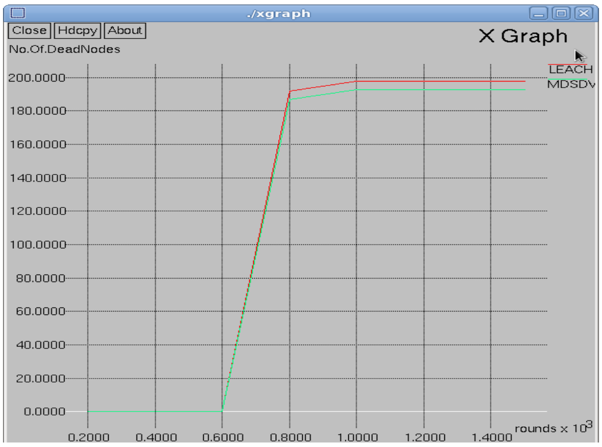

Fig.5. Number of dead nodes in LEACH and MDSDV protocol.

Comparing to the number of dead nodes MDSDV generate minimum number of dead nodes than LEACH protocol.

VI. CONCLUSION

Vampire attack is the permanent resource depletion attack in ad hoc sensor network. Reducing the effect of this type energy drain attack is the main issue in ad hoc sensor

DOI 10.17148/IJARCCE.2016.5644

network. For reducing this attack there is a number of methods such as PLGP and PLGPa protocols are present but it has not provide enough solution. Both protocol contain its own drawback. The above simulation use a new protocol called MDSDV protocol against this energy drain attack. Using this protocol malicious node determined by checking energy drain in all active nodes. Clustered communication with including signature for each node help to increase the efficiency of the protocol. Comparing its performance with energy-efficient protocol such as LEACH protocol MDSDV protocol consume less node and total energy. Number of dead nodes also less than LEACH protocol. The energy used by the nodes has been significantly reduced when compared to the energy used by the nodes while implementing LEACH protocol.

ACKNOWLEDGMENT

Authors are grateful to the TEQIP, College of Engineering Kidangoor for the financial support to complete this paper work

REFERENCES

[1] F. Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: ResearchChallenges,"; Ad Hoc Networks, vol. 2, no. 4, pp. 351-367, Oct.2014.
[2] A.D.Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer,vol. 35, no. 10, pp. 54-62, Oct. 2002.
[3] A.J. Goldsmith and S.B. Wicker, "Design Challenges for Energy-Constrained Ad Hoc Wireless Networks," IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002.
[4] H.Samuel, J.Anand ," Defending against Vampire attacks in wireless sensor networks ", International Journal of Communication Engineering Applications, Volume 5, Article C084, March 2014.
[5] B. Parno, M. Luk , E. Gaustad, and A. Perrig, " Secure Sensor NetworkRouting: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf.,2006. Volume 5, Article C084, March 2014.
[6] Eugene Y. Vassermann and Nicholas Hopper " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks " IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318-332 Feb-2013.
[7] Qu Wei-Qing, "Cluster Head Selection Approach based on Energy and Distance", International Conferenece on Computer Sciene and Network Technology, Vol. 4, 2011.
[8] 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..
[9] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012

BIOGRAPHIES

Saneesh P.S is pursuing M.Tech in Wireless Technology from College of Engineering Kidangoor. He received her B.Tech in Electronics and instrumentation Engineering from College of Engineering, Kidangoor, Kottayam, Kerala. Her primary research interest includes communication and computer networking.

Dhanya Narayan is working as Assistant Professor in Department of Electronics & Communication Engineering, College of Engineering, Kidangoor. She is currently pursuing Ph.D in Signal Processing from Division of Electronics, School of Engineering, Cochin University of Science & Technology, Kerala, India. She received her M.Tech in Wireless Technology from Department of Electronics, CUSAT and B.Tech in Electronics & Communication Engineering from Government Engineering College Palakkad. Her areas of research interest are communication and signal processing.

Jeethumol K Joy is pursuing M.Tech in Wireless Technology from College of Engineering Kidangoor. She received her B.Tech in Electronics and instrumentation Engineering from College of Engineering, Kidangoor, Kottayam, Kerala. Her primary research interest includes communication and computer networking.

DOI 10.17148/IJARCCE.2016.5644