Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

Research Paper

Vampire Attack : Detection and Elimination in WSN

Computer Science

KEYWORDS : Ad hoc networks, wireless networks, sensor networks, vampire attack, resource consumption attack, security.

Ambili M. A — Department of Computer Science, Nehru Institute of Technology, Coimbatore

Biju Balakrishnan — Deprtment of Computer Science, Nehru Institute of Technology, Coimbatore

ABSTRACT

Network survivability is the ability of a network keeping connected under failures and attacks, which is the most important issue in the design and performance of wireless ad hoc sensor networks. The motivation of a large portion of research efforts has been to maximize the network lifetime, where the lifetime of network is measured from the instant of deployment to the point when one of the nodes has exhausted its limited power source and becomes in-operational – commonly referred as first node failure. But there is a class of resource consumption attack called vampire attack which permanently disables the whole network by quickly draining nodes battery. The paper projects its focus on the way in which the attack can be overcome in the best possible manner. The proposed system describes some methods and alternative routing protocols solution that help to detect and eliminate vampire attack and thus make the network live.

INTRODUCTION

Wireless ad-hoc Sensor Networks provide one of the missing connections between the Internet and the physical world. One of the main problems in sensor networks is the limited power of nodes. Wireless ad hoc sensor networks do not require any predefined infrastructure like access points, base stations etc. for communication purposes. This makes ad hoc networks suitable for easy deployment with low cost and minimal configuration, commercial uses and emergency situations like natural disasters or military conflicts. WSN is characterized with low power, low computational capabilities and limited memory nodes. Battery power is an important resource regarding ad hoc networks. One of the main issues that should be studied in WSNs the limited energy of the nodes.

Wireless ad hoc networks suffer from four different kinds of attacks i) Denial of Service (DoS) attacks ii) Reduction of Quality (RoQ) attacks iii) Routing infrastructure attacks and iv) Resource Depletion attacks. Of these, the resource depletion attack affects long-term availability of the network by entirely depleting node's battery power. Most of these attacks (attacks which reduce the quantity of a particular resource like battery power, storage capacity, memory etc.) have preventive measures at the MAC layers but not at the routing layer [1].Vampire attacks are the most common resource depletion attacks where the energy consumed by the network to compose and transmit a message is greater 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 [1].

In this paper, the actions of the vampire attacks in the wireless ad hoc networks are discussed. These types of attacks not directly link with the protocols; it links with the properties of the routing protocols in the communication networks. This attack affects the properties such as relation state between the nodes, remoteness vectors between the nodes, resource and location based routing. The vampire attack in the WSN is not easy to discover and to predict. Due to the solitary vampire attack in the networks, total force goes down and leads to the complete systems to the collapse. In order to overcome the above attacks in the wireless ad hoc networks we proposed a protocol for secured transmission in the networks. In order to overcome the above attacks, an efficient intrusion detection system based on energy of nodes.

The remainder of this paper is organized as three sections. The first section gives an idea about resource depletion attack and how it will drain the battery power of nodes. The second section will discuss the related work which familiarizes the earlier security measures on wireless sensor network. After that the proposed method is explained. The result and simulation result is discussed in next section and lastly we conclude our paper.

RESOURCE DRAINING ATTACKS

Vampire attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node's battery life. The vampire attacks can be classified has two types. There are: one is Carousel attack and other is Stretch attack.

CAROUSAL ATTACK

In the Carousel attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the route of communication many times. This attack increases the routing length and delay very much in the networks and also inadequate by the number of allowable entries in the resource route.

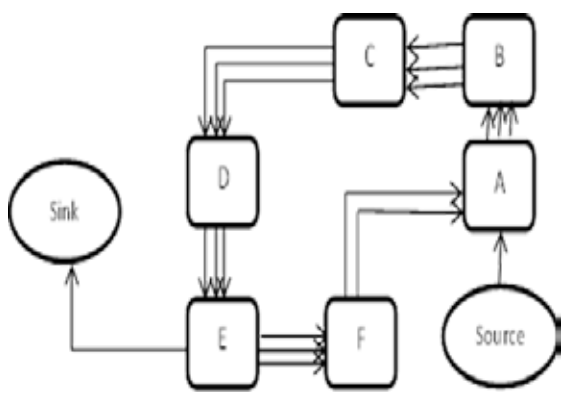


Fig. 1. Shows the carousel attack same node appears in the route many times

STRETCH ATTACK

And the other attack also targeting resource steering, attackers construct falsely long routes, potentially traversing every node in the network. And also stretch attack, increases packet lane length, causing packets to be processed by a number of nodes that is self-governing of hop count down the straight path stuck between the challenger and packet target.

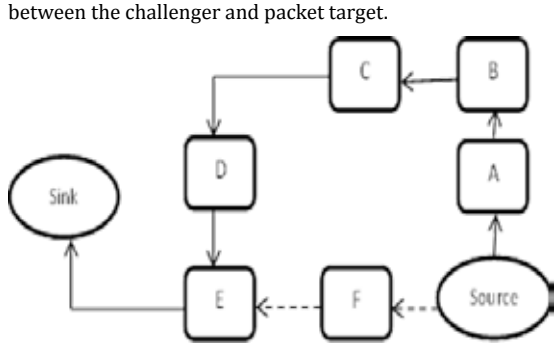


Fig .2 Shows Stretch attack with two different paths from source to destination.(Source-A-B-C-D-E-Sink—long route).

Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

RELATED WORKS

There are several challenges pose by the resource limitations in the wireless sensor networks due to the vulnerabilities that may occur due to dynamic behaviour of networks. . Due to some of hardware constraints the algorithm must be framed with the parameters like bandwidth, computational complexity and memory. Since the cost occurred is very high when we equate communication in terms of power, it may not be a trivial task. So energy efficient wireless sensor networks must be given at most priority.

The problem of security has received considerable attention by researchers in ad hoc networks. Vulnerabilities in WSN could occur based on certain dimensions in accordance with the characteristics of dynamic topology and lack of central base station. There are many different kinds of attacks that occur in wireless ad hoc sensor networks. There are preventive measures for these attacks in the MAC layer. Some of the techniques are described below:

A. Path- based attacks

These attacks are common in wireless ad hoc sensor networks. They are commonly referred as path-based DoS (Denial of Service) attacks. One-way hash chains can prevent these attacks by limiting the rate at which nodes transmit packets. But one-way hash chains cannot be used for all kinds of path- based attacks. Specific methods are used to eliminate specific kinds of path-based attacks.

B. Rushing attack

Rushing attack occurs in on-demand routing protocols like DSR, Ad hoc On-Demand Distance Vector routing (AODV) where route discovery is done by forwarding REQUEST messages to the neighboring nodes. In rushing attack, the malicious node sends the REQUEST message much faster when compared to the legitimate node. This results in wrong route discovery and the packet is not sent to the destination. To prevent this attack trust oriented secured AODV protocol is used where a trust threshold value is incorporated on the misbehaving node and based on the trust value, the misbehaving node can be isolated. Another method is to use Rushing Attack Prevention (RAP) protocol.

C. Wormhole attack

In wormhole attack, the malicious node constructs a tunnel (path) to the destination in such a way that all the packets from the source are transferred via the attacker which can modify contents of the packet before sending it to the destination. To prevent this attack, packet leashes technique is used. A leash is information added to the packet inorder to restrict the packet's travelling distance. A Packet leash is of two types: i) Geographical leash is based on the distance and the position of the receiver ii) Temporal leash is based on the lifetime of the receiver.

D. Routing infrastructure attacks

Routing infrastructure focuses on minimal-energy routing, which aims to use minimal energy to transmit and receive packets and by using minimal energy paths to transmit packets. However using such schemes may reduce the network connectivity and lifetime of the network. To avoid such problems, an energy aware routing protocol, which uses sub- optimal paths, was introduced. Many routing paths are present where the protocol chooses one based on probabilistic values. In this case, every routing path is given a chance to transfer packets thus enhancing the network lifetime.

E. Resource depletion attacks

Resource depletion attacks focus on reducing the quantity of resources used by nodes like battery power, storage, memory etc thus reducing the overall capacity of the network. There are many kinds of attacks like carousel attack, stretch attack, directional antenna attack, and malicious discovery attack. Many methods such as loose source routing, secure protocols or checking the path for any loops can be used to prevent such attacks.

Many schemes proposed in the literature deal with the detection and /or prevention from resource exhaustion attack mostly confined to other levels of protocol stack eg., Medium Access Control layer(MAC) and application layer. A very little research is done on the resource draining attack routing layer.

METHODOLOGY

In the proposed system, mainly two methods are used to detect and eliminate the important class of resource consumption attack called vampire attack which drains the battery power of nodes in the network abnormally. The two methods are:

1. Energy constrained Intrusion Detection System
2. Path tracking technique

ENERGY BASED INTRUSION DETECTION SYSTEM

During the deployment of the network almost all nodes have same energy. The energy or power of nodes is used for the processing of packet and transmission or forwarding of data packets. Thus there will be a small variation in energy level of nodes.

In the presence of vampire attack, it causes more energy to be consumed than a network with normal node does for the same processing and forwarding. Thus it makes the energy of whole network very much low.

Energy constrained intrusion detection is based on the concept of energy level. It works on the fact that the malicious nodes will have abnormally high energy than legitimate nodes. Thus in this energy of all nodes are measured and the node with abnormally high energy is detected as malicious node.

The network authority(NA) will eliminate the detected node by informing all other nodes about this detection. The nodes will eliminate the malicious node from its list and wont forward packet to that detected nodes.

PATH TRACKING TECHNIQUE

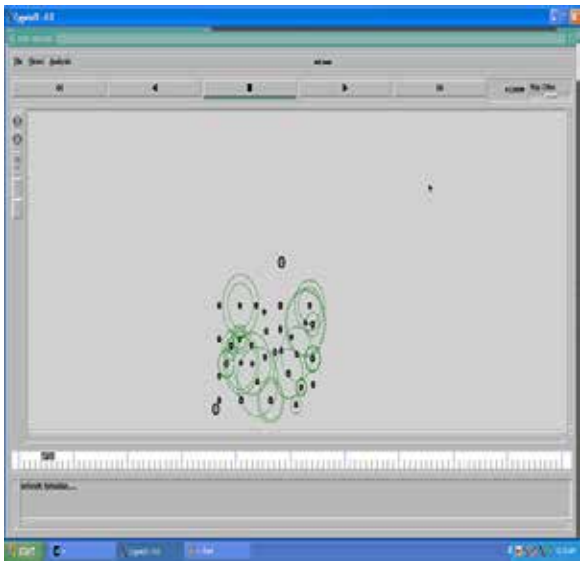
The vampire attack drains energy by introducing routing loops and stretching the normal route.

Routing loops happens because nodes are not aware of whether they are processing the same packet that it processed previously. To avoid this, in the proposed system, each node maintains a log-file. The log- file contains the source, destination and packet id. Whenever a packet arrives each node check the log file for the source- destination pair of packet. If present it verifies that it is not processing the same packet by comparing the packet id. The energy spent for this checking is less compared to the energy drained during infinite looping of a single packet.

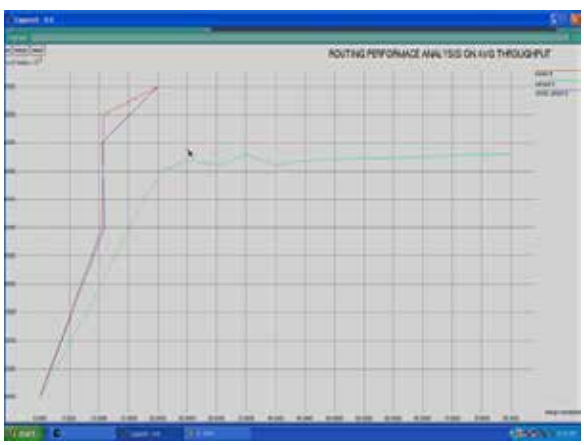
Stretching of route happens because nodes are not aware of whether they are forwarding the packet towards destination or making a path that takes packet away from destination. This stretching occurs when source itself become malicious and intermediate node forward the packet according to source route without any further checking. This can be avoided by tracking the path. In this, a path history is maintained along with packet. Each node makes an attestation to each packet by adding its id to the end of packet. On receiving, the node checks the path history to verify that the packet is actually moving forward to the destination and not backtracking. Thus stretching of routes can be avoided.

SIMULATION RESULT

The proposed system is implemented using NS2. For this I am using ns allinone 2.35. NS2 is mainly used for the simulation purposes where we can configure all the protocols such as aodv etc. and simulate the project. 34 nodes is considered to form the system. The nodes are configured. The nodes will find its neighbours that is nodes within its transmission range.



The graph below shows the performance of network in presence of carousal attack, stretch attack and network without any attacker. The graph clearly gives an idea of how much energy is drained by a single carousal attacker and stretch attacker.



The performance analysis of the two proposed methods energy based intrusion detection system and path tracking technique can be clearly understood using the graph shown below.

CONCLUSION

In this paper, we define Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. An energy constraint intrusion detection scheme is introduced along with clean state secure routing protocol

REFERENCE

[1] Eugene Y. Vasserman , Nicholas Hopper, Vampire attacks: Draining life from wireless ad-hoc sensor networks.2011 | | [2] Imad Aad, Jean-Pierre Hubaux, and Edward W.Knightly, Denail of service resilience in ad hoc networks, mobicom,2004. | | [3] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on demand source routing in mobile ad hoc networks, IEEE Transactions on mobile computing 05(2006),no.11. | | [4] H. Chan and A. Perrig, "Security and Privacy in | Sensor Networks," computer, vol. 36, no. 10, pp. | 103-105, Oct. 2003. | | [5] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion- Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29,no. 2, pp. 216-230, 2006. | | [6] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006. | | [7] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002. | | [8] M.G. Zapata and N. Asokan, "Securing Ad Hoc RoutingProtocols," Proc. First ACM Workshop Wireless Security (WiSE), 2002. | | [9] 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. | | [10] 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 | | [11] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003. | | [12] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54- 62, Oct. 2002. |