BAFFLE TECHNIQUE TO AVOID VAMPIRE ATTACKS USING ROUTE TRACKING IN WIRELESS AD HOC NETWORK

[1]SUSHMA N. THAKUR, [2]SANDEEP RASKAR

[1]Student, M.E. Computer Engineering, Pillai's HOC college of Engineering and Technology, Rasayani.,
[2]Guide, Department of Computer Engineering, Pillai's HOC college of Engineering and Technology, Rasayani.
E-mail: [1]s.thk2411@gmail.com, [2]sandeepraskar@gmail.com

Abstract - The Ad hoc wireless network contains a number of small wireless devices which has the wireless communication capability, signal processing intelligence and transferring of the data. Communications are vulnerable to various kinds of attacks due to insecure wireless channels. The objective of this paper is to examine energy depletion attack which attempts to permanently disable nodes by draining their battery power which is known as vampire attack. These attacks rely on the properties of many popular classes of routing protocol. In this paper, the proposed prevention technique is used to reduce vampire attack using new protocol and route recovery technique to decrease the energy loss due to packet transmission over the unwanted route in the network.

Index Terms - carousal attack, energy depletion attack, path recovery technique,routing,stretch attack, vampire attack, wireless Ad hoc network.

I. INTRODUCTION

Wireless ad hoc network is composed of a multiple nodes which use ad hoc networking to communicate observed information. A node measures a physical quantity and converts it into a signal, destined for an observing instrument. The purpose of wireless networking is to interconnect computational nodes for information exchange. In Network each node participates in the routing of packets, deciding dynamically, based on connectivity to neighbor nodes. The principle behind ad hoc networking is multi-hop relaying in which messages are sent from the source to the destination by relaying through the intermediate hops (nodes).

The basic components of a node are sensor and actuator, Controller, Memory, Communication, Power Supply. Power Supply is the supply of energy for smooth operation of a node like a battery. A main security issue that has been identified in the network is an energy depletion attack in routing layer protocol.

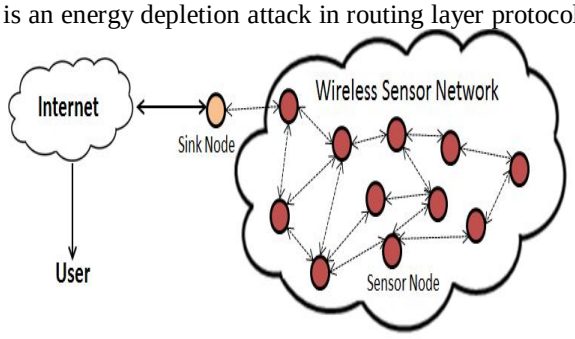

Fig. 1 Wireless Ad hoc Network

II. OVERVIEW

Vampire attack is responsible for creating and sending messages by the malicious node which causes more energy consumption by the network leading to slow depletion of node's battery life so that network get disabled permanently.

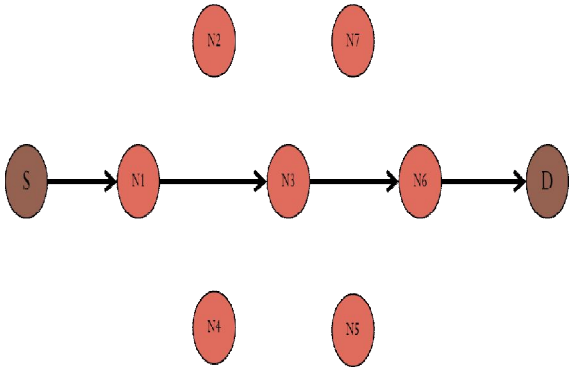

Fig. 2 Honest path

Vampire attack Includes stretch attack and carousal attack. Figure 2. Shows the honest path from source to destination which includes Node S-N1-N3-N6-D.

Stretch Attack

In stretch attack an adversary (malicious node) constructs artificially long route so that packet traversing almost every node in the network. This attack increases the packet lane length so that the packet is processed by maximum number of nodes which is independent of hop count along shortest path between the malicious node and packet destination. Figure 3. Shows the path during a stretch attack from source to destination which includes Node S-N1-N3-N4-N5-N6-N2-N7-D.

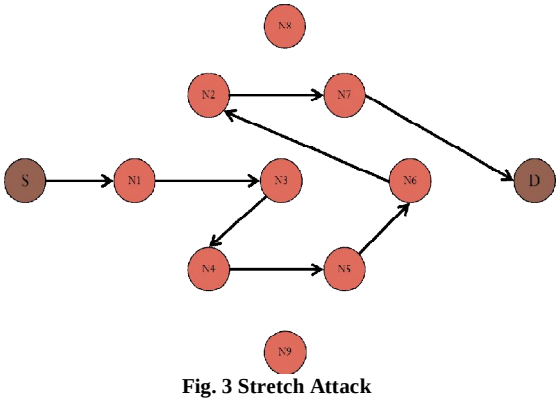

Fig. 3 Stretch Attack

Carousel Attack

In Carousal attack an adversary (malicious node) sends a packet on route composed as a sequence of loops. So that the same node appears multiple times in route of communication.

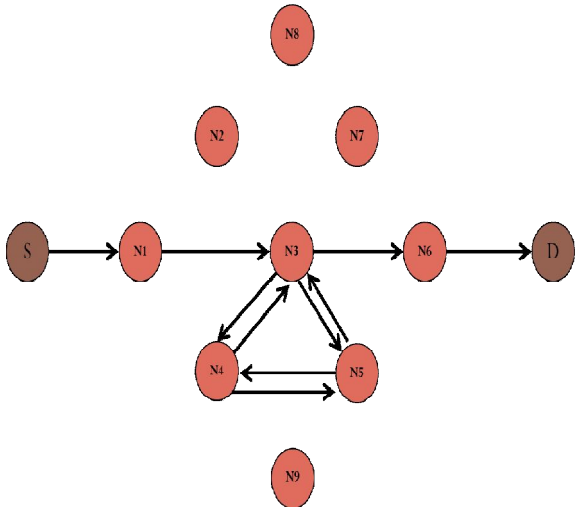

Fig. 3 Stretch Attack

In this adversary increases route length and delay in the network. It introduces multiple loop in the path of the packet traversal to purposely deplete the energy of honest nodes. Figure 4. Shows the path with carousal attack from source to destination which includes Node S-N1-N3-N4-N5-N3-N5-N4-N3-N6-D.

III. EXISTING SYSTEM

In routing layer, the resource depletion attacks are not thoroughly analyzed. An attacker may interact with a node in an otherwise legitimate way, but the only purpose to consume its battery energy. For many portable devices Battery life is a very critical parameter. Existing system for secure routing attempts to ensure that a malicious node cannot cause route discovery to return an invalid network path.

Clean-slate network routing is known as PLGP because it's developed by the scientist piano, Luk, Gaustad and Perrig. Original version of PLGP is open to vampire attack and it modified to prevent vampire attack.It consists of two phases:

1. Topology Discovery Phase
2. Packet Forwarding phase

Topology discovery organizes nodes to trees as shown in Figure 5. Initially, each node knows only itself and at the end of discovery each node should compute the same address tree as other nodes. All leaf nodes are physical nodes in network and virtual address corresponds to their position in the network. Topology discovery Phase In this phase, every node broadcast certificate of identity including public key. Each node starts as its own group size one, having a virtual address zero. Groups are merging with the smallest neighboring group and each group chooses 0 or 1 when merge with another group. Each member prepends group address to their own address gateway nodes. At the end each node knows every node virtual address, public key and certificate and then network converges to a single group.

Packet forwarding Phase In this phase, all decisions are made independently by each node. When a node receives a packet determines the next hop by finding the most significant bit of its address that varies from the message originator's address. Every forwarding event shortens the logical distance to destination.

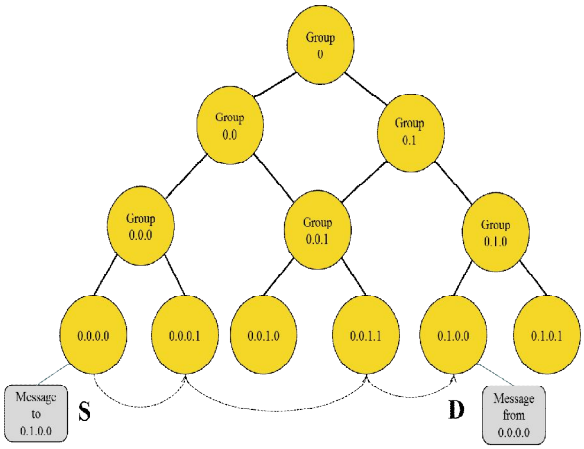

Fig.5PLGP's Tree Routing Structure

IV. PROBLEM STATEMENT

PLGPa is a protocol that bounds damage from a vampire attack, but this has several drawbacks.It includes Path attestation which increasing size of every packet. Incurring penalties in terms of bandwidth use, thus radio power. It addsan extra packet verification requirement for intermediate nodes,which increases processor utilization, time and additional power.PLGPa is not providinga satisfactory solution during the topology discovery phase.

V. PROPOSED SYSTEM

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 weight detection algorithm
2. Route Tracking Technique

Energy Weight Detection Algorithm:

This section focuses on the design details of our proposed protocol EWDA. Where the battery power of a node gets to the threshold level, it plays a crucial role by performing energy intensive tasks, thereby bringing out the energy efficiency of the nodes. EWDA contains two phases:

1. Network configuration Phase
2. Communication phase

Network configuration Phase is used to establish optimal routing path from source to destination in the

network. The key factors considered are balancing the load of the nodes and minimization of energy consumption for data communication. It is used to prevent from a stretch attack in which we set No. of hop count initially and if it exceed the no. of hop count then reroute the path.
Communication phase avoids the same data packets transmitting through the same node repeatedly to deplete the batteries fast and leads to network death because of vampire attacks. Data aggregation is achieved. This phase is used to avoid the carousal attack in which we avoid the repeating nodes and reroute the path.

Route Tracking Technique
To enhance more security in the routing phase, we can include the trust factor in the routing path, i.e. the routing can be taken considering node's trust factor. For example, the trust level is denoted as T. Trust value is assigned to each and every node, the numeric value such as 0 or 1 is assigned, whereas 0 is considered to be malicious node and trust value 1 is considered to be normal node. Based upon the assigned trust value, the routing path is constructed. The node, which has trusted value 1, will be included in the route rather than the node having trust level 0.

Routing loops happen because the 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 using infinite looping of a single packet.

CONCLUSION

Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless networks by depleting nodes battery power. These attacks do not depend on any protocol or implementation, but rather expose vulnerabilities in a number of popular protocol classes.
To avoid these types of attackthis paper introducing a number of proofs of concepts against existing routing protocols. By using the Energy weight detection algorithm and Route tracking algorithm to overcome resource depletion attack.

REFERENCES

[1]. Vasserman, E.Y.; Hopper, N., "Vampire Attacks: Draining Life from Wireless Ad Hoc Networks," Mobile Computing, IEEE Transactions on , vol.12, no.2, pp.318,332, Feb. 2013
[2]. J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Networks," Proc. ACM Workshop Security of Ad Hoc and Networks, 2005.
[3]. K.Vanitha,V.Dhivya, ''A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Vidya M, SHARNEE KAUL and our anonymous reviewers Networks", 2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14) On 21st & 22nd March Organized by K.L.N. College of Engineering , Madurai, Tamil Nadu, India.
[4]. Ambili M.A, Biju Balakrishnan, ''Vampitr attack: Detection and elimination in WSN", IJSR Vol-3April ,2014
[5]. Vidya.M, Reshmi.S, ''Alleviating Energy Depletion Attacks in Wireless Networks", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014

★★★