ISSN 2395-1621

Clean Slate Secure Sensor Network To Prevent From Vampire Attacks

[#1]Sheetal Shete

[1]sheetaltenai@gmail.com

[#1] PG Student ,Department of Computer Engineering,
PVPIT, Bavdhan Pune.

ABSTRACT

This paper describes an Adhoc Wireless Network which is a collection of sensor nodes that does not require any pre-existing infrastructure. Adhoc networks are used in military operation , emergency disaster relief and community networking. While transmitting the data from these networks they are exposed to resource depletion attacks at routing layer protocol. These attacks creates malicious node which consumes more energy and the network gets permanently disabled. Hence, these attacks are called as vampire attacks and these are not easily identified and detected in the network. This paper explains the clean slate secure sensor network protocols which are used to eliminate the vampire attacks that bounds provably.

***Keywords*— Ad hoc sensor networks, routing, security, vampire attack, PLGPa.**

ARTICLE INFO

Article History

Received : 4th April, 2015

Received in revised form :

6th April, 2015

Accepted : 11th April, 2015

Published online :

12th April 2015

I. INTRODUCTION

Adhoc Wireless Sensor Networks are collection of multiple sensor nodes with connectionless network. These networks transmit the data with the help of sensor nodes from source to destination. The data goes through the number of intermediate nodes. The sensor nodes are dependent on the battery power. The attacks causes battery exhaustion and higher energy utilization.

The vampire attacks are resource depletion attacks which creates malicious nodes at the source node or at the routing process of the data and depletes the battery life. These vampire attacks are not protocol specific but are protocol complaint messages.There are two types of vampire attacks i.e

1. Carousel Attacks
2. Stretch Attacks

Carousel Attacks :

In this attack, the malicious node sends the packet in loops other than the honest node. Due to which the packet does not reach to the destination and consumes more energy at each and every node.

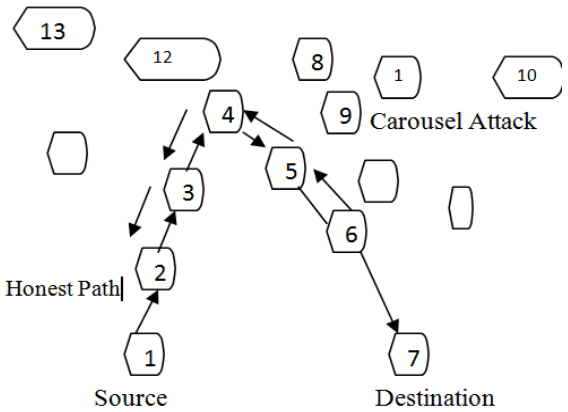

Fig 1: Carousel Attack same node in the Route Many times.

Stretch Attacks:

In this attack, the malicious node create the route other than the honest route.This attack increases the route length.

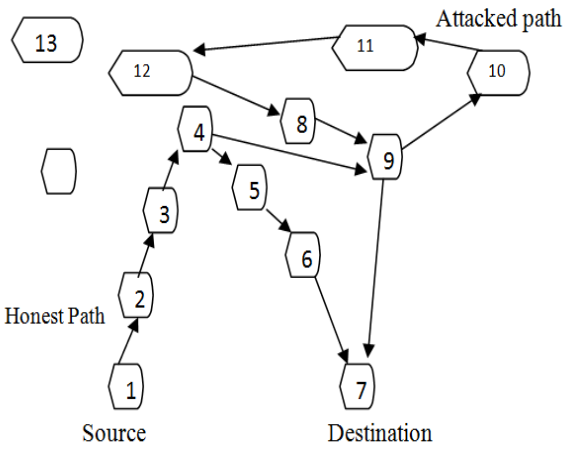

Fig 2: Stretch Attack with two different paths from source to destination(4-9-10-11-12-8-9-long Route).

II. Literature Survey

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. .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 sensor networks. There are preventive measures for these attacks in the MAC layer.

SLEEP DEPRIVATION TORTURE:

Sleep deprivation torture [2] comes in the form of sending useless control traffic and forces the node to forgo their sleep cycles so that they are completely exhausted and hence stop working. Here workload is distributed among components according to their capacity to avoid complete exhaustion of battery power. Packet transmission overhead may high in some cases and its main advantage is it enhances energy efficiency and network scalability.

RESOURCE EXHAUSTION ATTACKS:

Resource exhaustion attacks [1] can be easily performed by transmitting numerous packets from one or multiple attack terminals. All terminals reachable from the attack terminal can be the target and their batteries can be intentionally exhausted to disable further packet handling. By resource exhaustion attacks, the attacked ad hoc network may be isolated into sub-networks that cannot communicate with each other.

INTRUSION TOLERANT ROUTING PROTOCOL

INSENS [9] constructs a forwarding table at each node to facilitate communication between sensor nodes and base station. In INSENS each node shares a secret key only with the base station and not with any other nodes. This has advantage in case a node is compromised that an intruder will only have access to one secret keys rather than the secret keys of neighbors and other nodes throughout the network. It also provides multi path routing and minimize the communication, storage and computation requirements of sensor node at the expense of increased requirements at base station.

DENIAL-OF-SLEEP ATTACKS (DOS) :

Denial of sleep attacks[7] are the resource consumption attacks that make a machine or network resource unavailable to its intended users. Denying sleep effectively attacks each sensor node's critical energy resources and rapidly drains the network's lifetime so proposed a new G-MAC protocol to control the sleep awake pattern of sensor nodes. G-MAC has several energy saving features which not only show promise in extending the network lifetime, but the centralized architecture makes the network more resistant to denial of sleep attacks. This scheme performs well in all traffic situations but deals
only with MAC layer depletion attack

PATH-QUALITY MONITORING PROTOCOL

By using path-quality monitoring protocol [8], they were able to raise a reliable alarm when the packet losses or delay exceeds a threshold value. They proposed two technologies. Initially, secure sketching protocol invoked and it will identify the packet losses and delays. Finally, by invoking secure sampling protocols that makes a faster feedback and accurate round - trip delay estimates are done.

III.Existing System

Clean Slate Sensor Network:

A clean-state secure sensor network routing protocol is an efficient, highly resilient to active attacks. This protocol is introduced by Bryan Parno, Mark Luk, Evan Gaustad, Adrian Perrig(PLGP). It has two phases, they are topology discovery phase and packet forwarding phase.

Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme. When discovery begins, each node has a limited view of the network — the node knows only itself. Nodes discover their neighbors using local broadcast, and form ever-expanding "neighborhoods," stopping when the entire network is a single group. Throughout this process, nodes build a tree of neighbour relationships and group membership that will later be used for addressing and routing. At the end of discovery, each node should compute the same address tree as other nodes. All leaf nodes in the tree are physical nodes in the network, and their virtual addresses correspond to their position in the tree. All nodes learn each others' virtual addresses and cryptographic keys. The final address tree is verifiable after network convergence, and all forwarding decisions can be independently verified. Furthermore, assuming each legitimate network node has a unique certificate of membership nodes who attempt to join multiple groups, produce copy of themselves in multiple locations, or otherwise cheat during discovery can be identified and evicted.

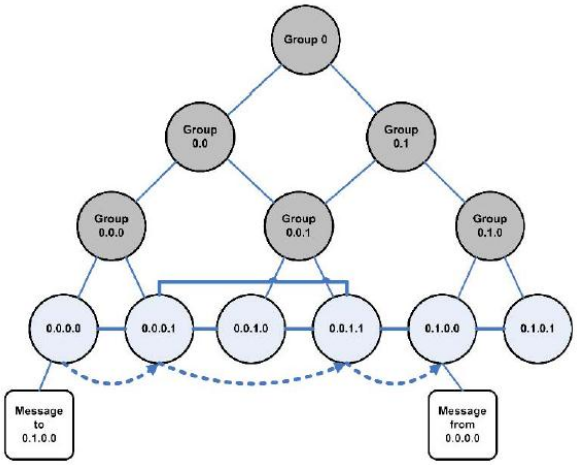

Fig 3. Topology Discovery

In PLGP protocol , it simply transmits the packet from source to destination , forwarding nodes do not know what path a packet took and it does not satisfies the No-backtracking property.

No-backtracking is satisfied if every packet traverses the same number of hops whether or not an adversary is present in the network and maintain the path history of every packet with the intermediate nodes. The PLGP protocol is again then modified as PLGP with attestation (PLGPa). Attestation are nothing but the signatures which are attached to every packet and allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination in the logical address space.

Secure_packet_forward (P) .
1) S←extract _source_add(p);
2) a← extract_attestation(p);
3) c←closest_ next_ hop(s);
4) for each node that sends packet
5) if attestation (a)verification fails
6) Drop packet (p)
7) Else //if matches
8) Retrieves next hop info to the requested node in the selected shortest path .
9) Return the c←closest next hop IP/Port number to requesting node.
10) Forward packet (p) to node (c).

The algorithm describes that the source node(s) extracts the source address of the packet and attestation(a) extracts the address of the packet and verifies that each and every packet makes progress towards its destination. The resulting protocol,PLGPa uses this packet history so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node.

IV. ADVANTAGES

1. Each packet has a verifiable path history.
2. PLGPa satisfies No-Backtracking Property
3. PLGPa never floods.
4. Even without dedicated hardware , the cryptographic computation required for PLGPa is tractable even on 8-bit processor.

V. DISADVANTAGES

1 .PLGPa includes path attestations, increasing the size of every packet, incurring penalties in terms of bandwidth use,and thus radio power.

3. Adding extra packet verification requirements for intermediate nodes also increases processor utilization, requiring time and additional power

VI. CONCLUSION

a Adhoc Wireless Sensor Networks that are affected by the vampire attacks consumes more energy and causes battery exhaustion due which the packets gets lost or is being discarded. The exixting system PLGPa keeps track of the packet which is being transmitted over the network along with the signatures but still is not vulnerable because increases size of the packet ,time and processor utilization. The **Secure_packet_forward (P)** algorithm in the network routing protocol that provably bounds the damage from vampire attack.

REFRENCES

[1] Eugene Y. Vasserman and Nicholas Hopper, " Vampire attacks: draning life from wireless ad-hoc sensor networks", IEEE Trans on mobile computing vol.12 no.2 year 2013.

[2] Tapaliana Bhattasali,Rituparna Chaki,Sugata Sanyal "Sleep Deprivation Attack Detection in Wireless Sensor Networks", International journal of computer applications(0975-8887)vol 40- No: 15,February 2012.

[3] B.Prano, M.Luk, E.Gustad, A.Perrig, "Secur Sensor Network Routing: A Clean-state Approach", CoNEXT:Proc.ACM CoNEXT Conf.,2006.

[4] Andrea J. Goldsmith and Stephen B. Wicker, Design challenges for energy-constrained ad hoc wireless networks, IEEE Wireless Communications 9 (2002), no. 4.

[5] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.

[6] INSENS: Intrusion-tolerant routing for wireless sensor networks,Computer Communications 29 (2006), no. 2.

[7] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.

[8] Sharon Goldberg, David Xiao, EranTromer, Boaz Barak, Jennifer Rexford,"Path-Quality Monitoring in the Presence of Adversaries", Proceedings of ASIACCS, 2008.

[9] Jing Deng, Richard Han, Shivakanth mishra, "INSENS: IntrusionTolerant routing in Wireless Sensor Networks", University of Colorado, Department of computer science Technical report,June 2006

