Mitigation of vampire attacks in wireless adhoc and sensor networks during packet forwarding phase

Ghyanshyam Meena[1], Mrs. Sankuntala Sharma[2]

[1]M.Tech, Department of CSE SIETK, Noida Institute of Technology, Noida , INDIA
[2]Associate Professor, Department of CSE, Noida Institute of Technology, Noida , INDIA

Abstract— *Ad-hoc wireless networks are an exciting research direction in sensing and pervasive computing. Advance security work in this area has beenprimarily focused on denial of communication at the routing or medium access control levels. There is a common attack at routing protocol layer, i.e. resource depletion attack, which permanently disables networks by drastically draining nodes' battery power. These "Vampire" attacks are not similar to any specific protocol, but rather depend upon the properties of many popular classes of routing protocols like link state and DSR protocols. These vampire attacks are very difficult to detect, devastating and easy to carry out using as few as one malicious insider sending only protocol compliant messages. For mitigation of these kinds of attacks, some methods are explained, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.*

Keywords— Denial of service (Dos) attack; Vampire attack; Sensor network; Security; Network;

I. RELATED WORK

In wireless ad hoc networks there is a need to forward the packets from one to another. Each mode acts as a router in wireless ad hoc network. That means it must follow some routing protocols. It maintains the routing information like source address, destination address, data etc. The existing routing protocols like ARIADNE, SAODV, and SEAD do not protect against vampire attacks.ARIADNE[2] is an on-demand secure ad hoc routing protocol based on DSR that withstands node compromise and relies only on highly efficient symmetric cryptography.

ARIADNE[2] guarantees that the target node of a route discovery process can authenticate the initiator, that the initiator can authenticate each intermediate node on the path to thedestination present in the RREP message and that no intermediate nodecan delete a previous node in the node list in the RREQ or RREP messages.As for the SRP protocol, ARIADNE needs some mechanism to bootstrap authentic keys required by the protocol. In particular, each and every node needs a shared secret key (KS, D) is the shared key between a source S and a destination D) with each node it communicates with at a higher layer, an authentic TESLA key for each node in the network and an authentic "Route Discovery chain" element for each node for which this node will forward RREQ messages. There are some features like:

i. ARIADNE provides point-to-point authentication of a routing message using a message authentication code (MAC)and a shared key between the two parties.

ii. For authentication of a broadcast packet such as RREQ, ARIADNE uses the TESLA broadcast authentication protocol

iii. Selfish nodes are not taken into account.

ARIADNE copes with attacks performed by malicious nodes that modify and fabricate routing information, with attacks using impersonation and, in an advanced version; with the wormholeattack .ARIADNE is protected also from a flood of RREQ packets that could lead to the cache poisoning attack. ARIADNE is not vulnerable to the wormhole attack only in its advanced version: using an extension called TIK (TESLA with Instant Key disclosure) that requires tight clock synchronization between the nodes, it is possible to locate anomalies caused by a wormhole based on timing discrepancies.

The Secure Ad hoc On Demand distance Vector (SAODV) [3] protocol is an extension of the AODV protocol. The Secure AODV scheme is based on the premise that each node possesses certified public keys of all network nodes. The originator of the routing control packet appends its

RSA signature and the last element of a hash chain to the routing packets. A packet transverse the network, intermediate nodes cryptographically authenticates the signature and the hash value. The intermediate nodes generate the kth element of the hash chain, with k being the number of transverse hops, and place it in packet. The SAODV[3] protocol gives two alternatives for ROUTE REQUEST and ROUTE REPLY messages. In the first case when a ROUTE REQUEST is sent, the sender creates a signature and appends it to packet. Intermediate nodes authenticate the signature before creating or updating the reverse route to the host. The reverse route is stored only when the signature is verified. When the node reaches the destination, the node signs the ROUTE REPLY with its private key and sends it back. The intermediate nodes again verify the signature .The signature of the sender is again stored with the along with the route entry.

There are some features for SAODV:

i. Ownership of certified public keys enables intermediate enable intermediate nodes to authenticate all in-transit routing packets.

ii. The protocol operates mainly by using the new extension message with the AODV protocol.

iii. The SAODV can be used to protect the route discovery mechanism of the AODV by providing security features like integrity, authentication.

Hu, Perrig and Johnson presented a proactive secure routing protocol based on the Destination-Sequenced Distance Vector protocol (DSDV). In a proactive (or periodic) routing protocol nodes periodically exchange routing information with other nodes in attempt to have each node always know a current route to all destinations. SEAD [4] authenticates the sequence number and metric of a routing table update message using hash chains elements. In addition, the receiver of SEAD routing information also authenticates the sender, ensuring that the routing information originates form the correct node. The source of each routing update message in SEAD must also be authenticated, since otherwise, an attacker may be able to create routing loops through the impersonation attack. SEAD deals with attackers that modify routing information broadcasted during the update phase of the DSDV-SQ protocol: in particular routing can be disrupted if the attacker modifies the sequence number and the metric field of the routing table update message. SEAD makes use of efficient one-way hash chains rather than relying on expensive asymmetric cryptography operations. SEAD assumes some mechanism for a node to distribute an authentic element of the hash chain that can be used to authenticate all the other elements of the chain.

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.

Vampire attacks [1] are mitigated by used a new proof of protocol at the routing protocol layer during packet forwarding phase.

II. INTRODUCTION

WSN is typically an ad hoc network of nodes with sensing abilities. So many routing protocols proposed for ad hoc networks could also be used for WSNs. The characteristics of WSNs are discussed from two perspectives: from the nodes that make up the network, and from the network itself.

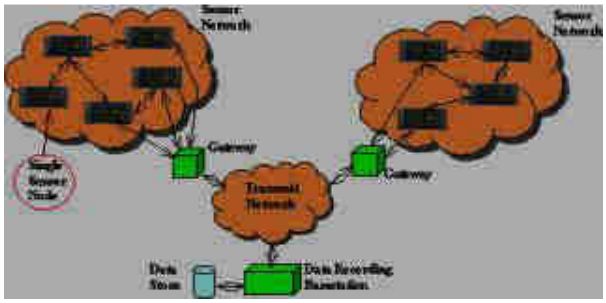

Fig:1 wireless sensor network

A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability (one or more microcontrollers, CPUs), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni-directional antenna), have a power source (e.g. batteries and solar cells), and accommodate various sensors

and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion.

A wireless ad hoc network isa decentralized type of wireless network [5]. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks.

The very idea of a wireless network introduces multiple venues for attack and penetration that are either much more difficult or completely impossible to execute with a standard, wired network. This inherent limitation makes WSNs especially sensitive to several key types of attacks. In contrast to resource-rich networks such as the Internet, a WSN is less stable, more resource-limited, subject to open wireless communication, and prone to the physical risks of in-situ deployment. These factors increase the susceptibility of WSNs to distinct types of attacks.

Although there are many factors (software and hardware bugs, environmental conditions) that could diminish the capacity of the network to provide the requisite service, there is the possibility that the service is denied as a result of being attacked by an adversary.

III. PROPOSED SYSTEM

A. PLGPa:

It adds a verifiable path history to every PLGP packet.PLGPa uses this packet history combined with PLGP's tree routing structure so every node can securely verify progress which anticipates any significant adversarial influence on the path taken by any packet which traverses at least one veracious node. These signatures form a chain attached to every packet and allows any node receiving it to proveits path. To ensure that the packet has never travelled away from its destination in the logical address space, every forwarding node verifies the attestation chain. PLGPa satisfies no-backtracking- All messages are signed by their originator. Attacker can only alter packet fields that are changed enroute, so only the route attestation field can be altered, shortened, or deleted entirely. Use one-way signature chainconstruction to prevent truncation. PLGPa never floods and its packet forwarding overhead is favorable. It exhibits more equitable routing load distribution and path diversity. Even without hardware, the cryptographic computation required for PLGPa is tractable even on 8-bit processors.

Some important things about PLGPa:

- It is PLGP with attestation
  Each packet has a verifiable path history
- It holds backtracking
- It is resistant to vampire attacks

.

IV. CONCLUSION

There are many resource depletion attacks as explained in literature survey. The most dangerous attack is vampire attack. This kind of attacks suddenly decreases the battery life of nodes and may even destroy the network permanently. These attacks are somewhat reduced by using the PLGPa method during packet forwarding phase.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks " Transactions On Mobile Computing, vol. 12,no. 2, pp.315-332 February 2013

[2] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002.

[3] Manel Guerrero Zapata and N. Asokan, Securing ad hoc routing protocols,WiSE, 2002.

[4] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, SEAD: secureefficient distance vector routing for mobile wireless ad hoc networks,IEEE workshop on mobile computing systems and applications, 2002.

[5] Chai Keong Toh Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002