Conquer Vampire Attacks in Wireless Sensor Network

S.Vedha Nayaki[1] Dr. G. Ravi[2]
[1]Research Scholar [2]Associate Professor & Head of the Department
[1,2]Department of Computer Science
[1,2]Jamal Mohamed College, Trichirapalli, Tamil Nadu, India

Abstract— Ad hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of OðNÞ, where N in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

Key words: Conquer Vampire Attacks, Wireless Sensor Network, reduction of quality, MAC

I. INTRODUCTION

While these schemes can prevent attacks on the shortterm availability of a network, they do not address attacks that affect long-term availability—the most permanentdenial of service attack is to entirely deplete nodes'batteries. This is an instance of a resource depletion attack,with battery power as the resource of interest. In this paper,we consider how routing protocols, even those designed tobe secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes. These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network. While some of the individual attacks are simple, and power draining andresource exhaustion attacks have been discussed before [53], [59], [68] prior work has been mostly confined to other levels of the protocol stack, e.g., medium access control (MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks.Vampire attacks are not protocol-specific, in that they donot rely on design properties or implementation faults ofparticular routing protocols, but rather exploit general properties of protocol classes such as link-state, distancevector,source routing, and geographic and beacon routing.Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain,preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

II. SYSTEM ANALYSIS

A. *Existing System*

- In Wireless Ad-hoc Sensor network the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest.
- In this project, we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes. These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network.
- Vampire attacks (**Carousel,Stretch**)are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distancevector, source routing, and geographic and beacon routing.
- Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest **energy drain**, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.
- Adversary can deposit a packet in arbitrary parts of the network.
- Adversary targets not only packet forwarding but also route and topology discovery.

B. *Proposed System*

- We proposed defenses against some of the forwarding-phase attacks and described **PLGPa**, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations.
- **PLGP** consists of a topology discovery phase, followed by a packet forwarding phase, with the former optionally repeated on a fixed schedule to ensure that topology information stays current.
- 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 neighbor relationships and group membership that will later be used for addressing and routing.
- PLGP offers secure Packet forwarding and provably resist the attacks by secure rules followed in topology discovery and packet forwarding phase.

C. *Advantages*

- In Discovery phase each node learn each others' virtual addresses and cryptographic keys.
- Each node has a unique certificate of membership before a network deployment.
- Nodes who attempt to join multiple groups, produce clones of themselves in multiple locations, or otherwise cheat during discovery can be identified and evicted.
- Every node must announce its presence by broadcasting a certificate of identity(ID), including its public key signed by a trusted offline authority.
- A Node determines the next hop by finding the most significant bit of its address that differs from the message originator's address.
- Every node select a shortest path to the destination.

III. Requirement Specification

A. *User Interfaces*

User-friendly look, feel menus and screens are provided. Java swing is used for creating GUI.

B. *Hardware Interfaces*

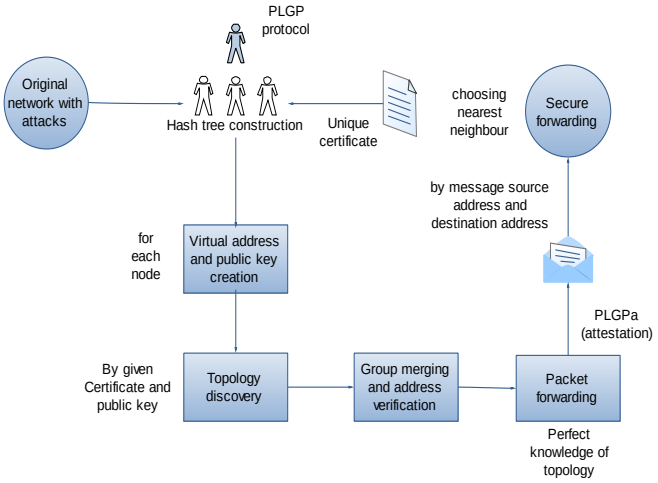
Processor	: Any Processor above 500 MHz.
Ram	: 128Mb.
Hard Disk	: 40 GB.
Compact Disk	: 650 Mb.
Input device	: Standard Keyboard and Mouse.
Output device	: VGA and High Resolution Monitor.

C. *Software Interfaces*

Operating System	: Windows XP and above.
Language	: JAVA1.6
Front End	: Java
Back End	: MySQL

IV. System Design

A. *Architecture diagram:*



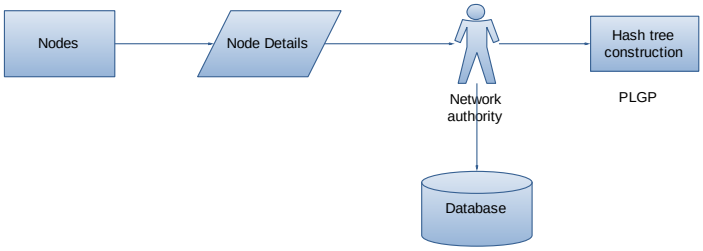
V. System Implementation

System Implementation is the stage in the project where the theoretical design is turned into a working system. The most critical stage is achieving a successful system and in giving confidence on the new system for the user that it will work efficiently and effectively. The existing system was long time process. The proposed system was developed using Java Swing. The existing system caused long time transmission process but the system developed now has a very good user-friendly tool, which has a menu-based interface, graphical interface for the end user. After coding and testing, the project is to be installed on the necessary system. The executable file is to be created and loaded in the system. Again the code is tested in the installed system. Installing the developed code in system in the form of executable file is implementation.

A. *Modules and explanation*

- Node Activation in Hash Tree.
- Topology Discovery.
- Address and Routing setup.
- Secure Packet Forwarding.

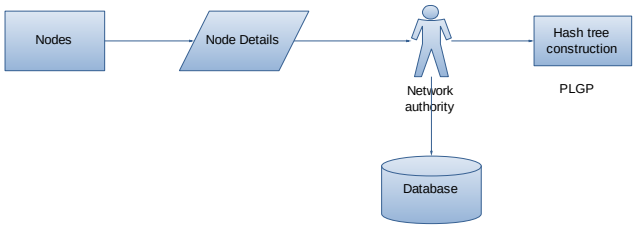
B. *Node Activation in Hash Tree.*



In this module we first register the nodes detail such as ip address, port number, energy level, etc. Trees are formed as nodes form group.Nodes details are stored and maintained in our database.After that Nodes enter the ip and port number to activate themselves in the tree. Its a clean slate approach routing protocol for secure packet forwarding and vulnerable to adversaries.

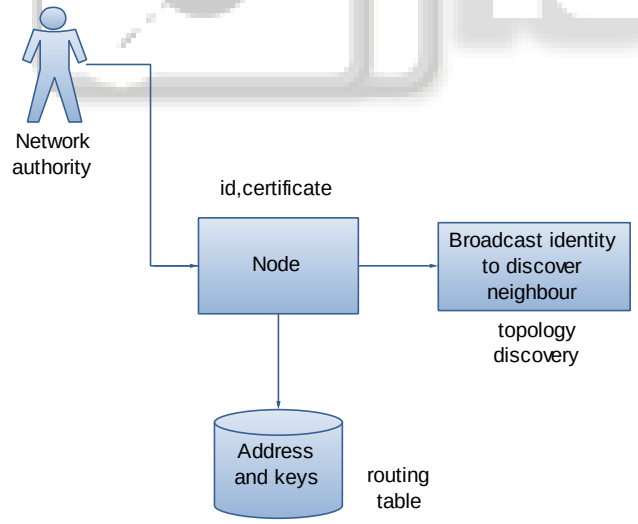
C. Topology discovery

In this model we assume the Network Authority signed the node's unique Id and certificate. And Network Authority uses the signature scheme to efficiently send the packet. Discovery begins with a time limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key, signed by a trusted Network authority. All nodes compute the sameaddress as the other nodes they also learn each other's virtual address as well as their cryptographic keys.



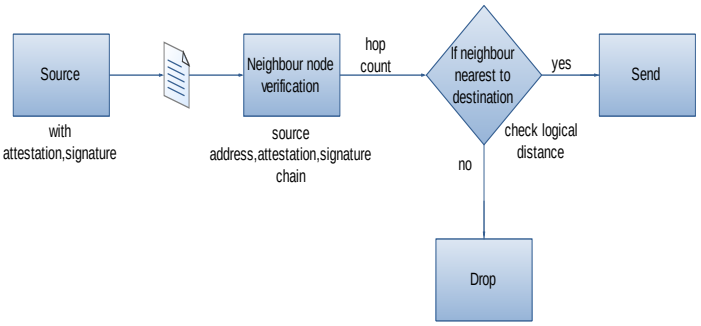
D. Address and Routing Setup

In this module every node in the tree will request to join with the smallest group in their vicinity, with ties broken by group IDs, which are computed cooperatively by the entire group as a deterministic function of individual member IDs. When largergroups merge, they both broadcast their group IDs to each other.Groups mostly communicate other nodes within their radio range. Some members are not within radio range of other groups will communicate through "gateway nodes," which are within range of both groups. By the end of topology discovery, each node learnsevery other node's virtual address, public key, and certificate, since every group members knows the identities of all other group members and the network converges to a single group.



E. Secure Packet Forwarding

During this phase each node is independent of other node and hence the decision made by them is also independent. Every neighbor node verifies the signature chain, source address, extract attestation. If it is not correct and the neighbor is not nearest to destination it will drop the packet.And every node verify the hop count to avoid attacks. Every node send packets by checking the node's mobility,energy, distance and check the node address should be strictly closer to destination or not.In this way we securely forwarding the packets in the network.



VI. CONCLUSION

We defined 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. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly generated topology of 30 nodes. Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase increases from between 50 to 1,000 percent. Theoretical worst case energy usage can increase by as much as a factor of OðNÞ per adversary per packet, where N is the network size. We proposed defenses against some of the forwarding-phase attacks and described PLGPa, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations.

VII. FUTURE ENHANCEMENT

We proposed defenses against some of the forwarding-phase attacks and described PLGPa, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. We have not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGPa. Derivation of damage bounds and defenses for topology discovery, as well as handling mobilenetworks, is left for future work.

REFERENCE

[1] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.

[2] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[3] 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.
[4] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.
[5] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.

