International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Secure Packet Forwarding Over Resource Depletion Attacks in Wireless Sensor Networks

Saranya. S
M.E CSE II Year
Srinivasan Engineering College
Perambalur, India

Jaya. K
M.E CSE II Year
Srinivasan Engineering College
Perambalur, India

Saravanan. S
Assistant Professor/IT
Srinivasan Engineering College
Perambalur, India

***Abstract*— The deployment of sensor networks in security and safety critical environments requires secure communication primitives. Ad-hoc sensor network and routing data in them is a significant research area. Lot of protocols have been developed to protect from DOS attack, but it is not completely possible. In this paper, a new secure routing protocol for sensor networks is designed, implemented, and evaluated. This protocol requires no special hardware and provides message delivery even in an environment with active adversaries. A clean-slate approach is adopted and a new sensor network routing protocol is designed with security and efficiency as central design parameters. Protocol used here is efficient yet highly resilient to active attacks.**

I. INTRODUCTION

Ad hoc wireless sensor networks (WSNs) [2] promise exciting new applications for the upcoming future, like ubiquitous on-demand computing power, instantly deployable communication for military and first responders, and continuous connectivity. Wireless Sensor Networks become more and more crucial. Fault availability becomes less tolerable. This lack of availability can make the difference between businesses as usual and lost productivity, power outages, and even lost lives. Hence high availability of these networks is a critical one, they must hold even under malicious conditions.

When they can prevent attacks when the availability of a network is short term, they do not address attacks which affect the long-term availability. These attacks are distinct from previously studied DoS,[3] reduction of quality (RoQ), and routing infrastructure attack instead of disrupting immediate availability, it work over time to disable a network fully. At this case some of the individual attacks becomes simple, and draining the power and discussion of resource exhaustion attacks has been before prior work has been mostly confined to other levels of the protocol stack, and there is little discussion upto knowledge there is no thorough analysis or mitigation of those routing-layer resource exhaustion attacks.

This paper makes three primary contributions. First, thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. Then observe the security measures to prevent.

Existing work on secure routing attempts to ensure adversaries cannot cause path discovery to return an invalid network path, but Vampires do not disrupt or alter discovered paths, but rather they use protocol-compliant messages and existing valid network paths. Inappropriate protocols are used to maximize power efficiency since they rely on cooperative node behaviour and cannot optimize out malicious action.

Second, simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary) is shown. Third, an existing sensor network routing protocol to provably bind the damage from Vampire attacks [1] during packet forwarding is modified.

II. RELATED WORK

In Existing, the permanent denial of service attack [3] [4] entirely deplete nodes batteries. When battery power is the resource of interest it is an instance of a resource depletion attack. Routing protocols have been designed to be secure, but they lack protection from these attacks, these attacks are called as Vampire attacks.

These attacks drain the life from networks nodes. These attacks are distinct from previously studied DoS,[3] reduction of quality (RoQ), and routing infrastructure attack instead of disrupting immediate availability, it work over time to disable a network fully.

Vampire attacks (**Carousal, Stretch**) are not protocol-specific. They do not rely on design properties or implementation faults of particular routing protocols; they also exploit general properties of protocol classes which includes link-state, source routing, distance vector and beacon routing.

These attacks do not rely on flooding the network with large amounts of data; instead they try to transmit as little data as possible to prevent a rate limiting solution and to achieve the largest energy drain.

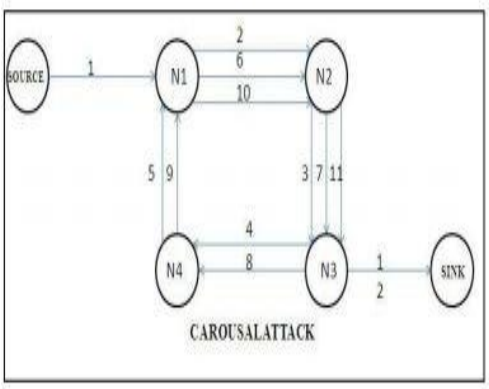

Figure 1. Carousal Attack

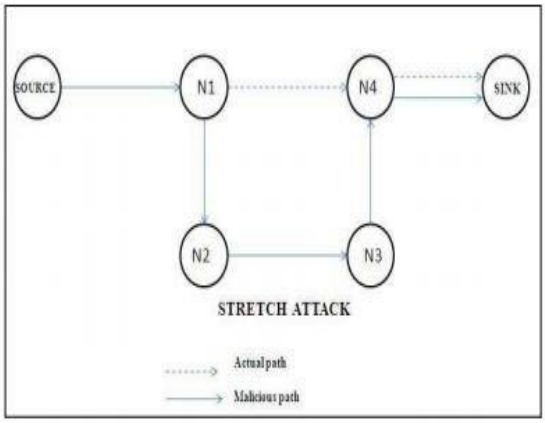

Figure 2. Stretch Attack

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.

In existing **Continuous charging** system, adversary can able to recharge as fast as honest nodes. **Duty Cycling** is only effective when duty cycle groups outnumber Vampires, because only one Vampire per group is taken into consideration to carry out the attack. Drain the life of a honest node by selecting the longest path to the destination. Adversary can deposit a packet in arbitrary parts of the network.

III. CLEAN STATE SECURE ROUTING PROTOCOL

In proposed defences against some of the forwarding-phase attacks are taken into account and **PLGPa**, the first sensor network routing protocol is described which provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations.

PLGP [1] consists of a topology discovery phase, and also packet forwarding phase, including the optional 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 neighbours using local broadcast, and form ever expanding "neighbourhoods", is stopped only when there is a single group for the entire network. Throughout this process, nodes build a tree of neighbour 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.

In Discovery phase, each node learns each other's virtual addresses and cryptographic keys. Each node has a unique certificate of membership before a network deployment. Nodes, who join multiple groups, produce duplicates in multiple locations, else they may also 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 selects a shortest path to the destination.

The original version of the protocol, although designed for security, is vulnerable to Vampire attacks. 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.

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 neighbours using local broadcast, and form ever expanding "neighbourhoods", 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.

A. Topology Discovery

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 offline authority. Groups merge preferentially with the smallest neighbouring group, which may be a single node. Groups that have grown large enough that some members are not within radio range of other groups will communicate through "gateway nodes", which are within range of both groups.

B. Packet Forwarding

During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originator's address. Thus, every forwarding event (except then a packet is moving within a group in order to reach a gateway node to proceed to the next group) shortens the logical distance to the destination, since node addresses should be strictly closer to the destination.

IV. MODULES

A. Node Activation and Topology Discovery

First the nodes detail such as ip address, port number, energy level, etc are registered. Trees are formed as nodes form group. Nodes details are stored and maintained in the database. After that Nodes enter the ip and port number to activate themselves in the tree.

Then 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 same address as the other nodes they also learn each other's virtual address as well as their cryptographic keys.

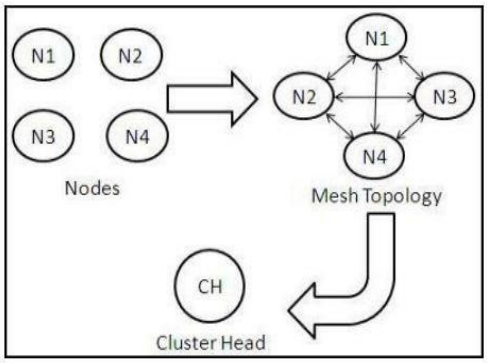

Figure 3. Topology Discovery

B. *Address and Routing Setup*

Every node in the tree will request to join with the smallest group, with ties broken by group IDs, and then it is computed cooperatively by the entire group as a deterministic function of individual member IDs.

When forming larger groups, they both group IDs are broadcasted to each other. Some members that are not within radio range of other groups will communicate through "gateway nodes," that is in the range of both groups.

By the end of topology discovery, each node knows about several other node's virtual address, public key, and certificate, every group members knows the identities of all other group members.

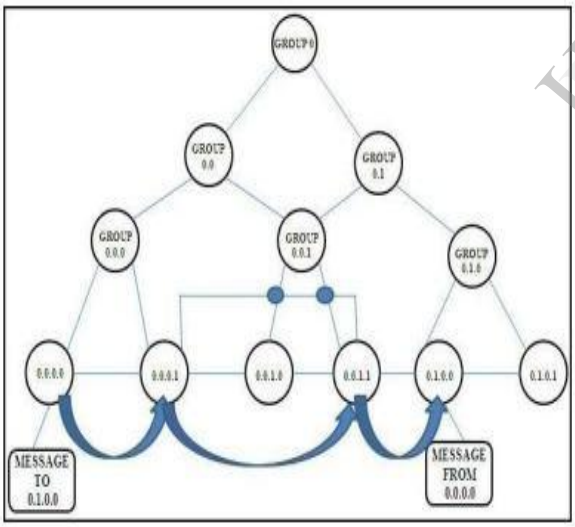

Figure 4. Group Identification

C. *Secure Packet Forwarding*

During this phase each node is independent of other node and hence the decision made by them is also independent. Every neighbour node verifies the signature chain, source address, extract attestation.

If it is not correct and the neighbour is not nearest to destination it will drop the packet. And every node verifies 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 the packets in the network is forwarded securely. To send the packet more secure MD5 Algorithm is used, so that the packet can be viewed only by the source and the sink.

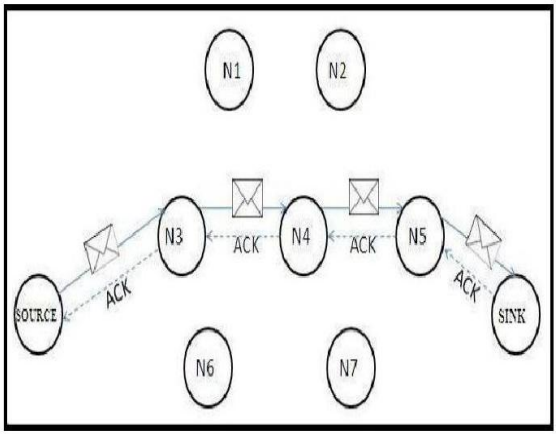

Figure 5. Message traversal in normal situation

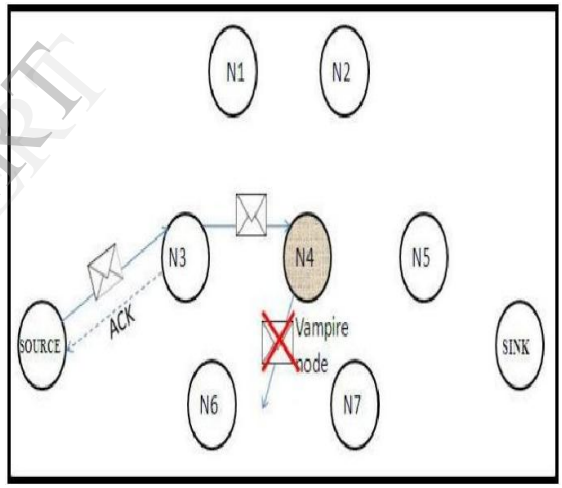

Figure 6. Vampire Attack leading to message drop

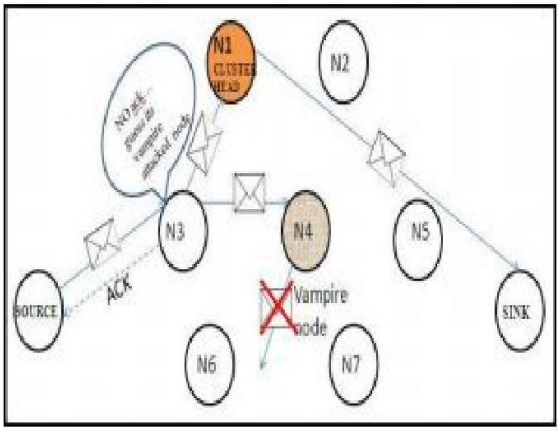

Figure 7. N3 sends data to Sink

V. CONCLUSION

Vampire attacks are defined as a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes battery power. Attacks do not depend on particular protocols or implementations; rather they expose vulnerabilities of popular protocol classes which are many in number.

It showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured the attack success topology of 30 nodes which are randomly generated.

Simulation results show that depending on the location of the adversary, network energy expenditure increases from between 50 to 1,000 per cent during the forwarding phase.

Theoretical worst case energy usage can increase by as much as a factor of OONP per adversary per packet, where N is the network size. Defences against some of the forwarding-phase attacks is being proposed and described PLGPa, provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations, which is the first sensor network routing protocol.

ACKNOWLEDGMENT

We would like to thank our college Srinivasan Engineering College, PRINCIPAL, Mr. B. Karthikeyan, our HOD, Mrs. S. Jayanthi, my guide, Mr. S. Saravanan and other staff members for their continuous support and for their helpful comments on the earlier drafts of this paper.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" *IEEE Transactions on Mobile Computing*, vol.12, no.2, Feb 2013.

[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] T.Aura, "DOS-Resistant Authentication with Client Puzzles," *Proc. Int'l Workshop Security Protocols*, 2001.

[4] J. Bellardo and S. Savage, "802.11 Denial–of-Service Attacks: Real Vulnerabilities and Practical Solutions," *Proc 12th Conf. USENIX Security*, 2003.

[5] H.Chan and A.Perrig, "Security and Privacy in Sensor Networks," Computer, vol.36, no.10, pp. 103-105, Oct 2003.

[6] J. H. Changand L. Tassiulas "Maximum Life Time Routing in Wireless Sensor Networks," *IEEE/ACM Trans. Networking*, vol.12, no.4, pp. 609-619, Aug 2004.

[7] Jennifer Rexford, J.Wang, Z.Xiao and Y.Zhang "BGP Routing Stability of Popular Destinations," *Proc. Second ACM SIGCOMM Workshop Internet Measurement* (IMW) 2002.

[8] Jun Yuan, Zongpeng Li, Wei Yu and Baochun Li "A Cross-Layer Optimization framework for Multihop Multicast in Wireless Mesh Network"*IEEE J.Selected areas in Comm.*, vol..24, no.11,pp. 2092-2103, Nov 2006.

[9] C. Karlofand D. Wagner, "Secure Routing in Wireless Sensor Networks: attacks and Counter measures," in Proc. *IEEE Int'l workshop Sensor Network Protocols and Applications*, 2003.

[10] H.Sun, J.C.S.Lui and D.K.Y. Yau, "Defending against Low – Rate TCP Attacks: Dynamic Detection and Protection," Proc. *IEEE 12th Int'l Conf. Network Protocols (ICNP).*, 2004.

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