Maintaining Lifetime of Wireless Adhoc Sensor Networks by Mitigating Vampire Attacks

A.Anto Jenifer
PG Student
Department of Computer Engineering
Govt. College of Engineering, Tirunelveli, Tamilnadu, India

V.Thangam
PG Student
Department of Computer Engineering
Govt. College of Engineering, Tirunelveli, Tamilnadu, India

N.Jeenath Laila
Assistant Professor
Department of Computer Engineering
Govt. College of Engineering, Tirunelveli, Tamilnadu, India

Abstract

Wireless sensor network is a communication network across the sensors nodes. Sensor nodes collect information about the physical environment. Now-a-days one main issue in wireless adhoc sensor network is wastage of energy at each sensor nodes. Energy is the one most important factor while considering sensor nodes. Wireless sensor networks require solution for conserving energy level. One new type of attack called vampire attack, which occurring at network layer. It leads to resource depletion (energy) at each sensor nodes, by destroying battery power of any node. It transmits a small complaint messages to disable a whole network, hence it is very difficult to detect and prevent. Existing protocols are not focusing on this vampire attack happening on routing layer, hence there exist two types of attacks namely, carousel and stretch attack. Hence there is a large of energy loss. New protocol called PLGP, a valuable and secure protocol is proposed along with one-way signature chaining algorithm to avoid this vampire attack. By using this, existing problems can be overcome.

Keywords: security, routing, one-way signature chaining, ad hoc networks, sensor networks, wireless networks

I. INTRODUCTION

A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. Sensors are spread in an environment without any predetermined infrastructure and cooperate to execute common monitoring tasks which usually consist in sensing environmental data from the surrounding environment.

Wireless sensor networks provide unique opportunities of interaction between computer systems and their environment. Their deployment can be described at high level as follows: The sensor nodes measure environmental characteristics which are then processed in order to detect events. Upon event detection, some actions are triggered. This very general description applies to extremely security critical military applications as well as to such kind ones.

One of the main design issues for a sensor network is conservation of the energy available at each sensor node. The energy efficiency of a node is defined as the ratio of the amount of data delivered by the node to the total energy expended. Higher energy efficiency implies that a greater number of packets can be transmitted by the node with a given amount of energy reserve.

Adversary injecting malicious information or altering legitimate routing setup messages, or can prevent the routing protocol from functioning correctly. For example, an attacker can forge messages to convince legitimate nodes to route packets in a way from the correct destination. Vampire attack is one of the resource depletion attacks. The resource depletion attack focuses the node's batteries life. Vampire attacks affect any protocol and utilize the properties of routing protocols classes such as source routing, distance vector and link state and geographic and beacon routing.

Dynamic Source Routing (DSR) Protocol is a stateless protocol do not store or maintain any routing information at the nodes. The source node specifies the entire route to a destination within the packet header, so intermediaries do not make independent forwarding decisions, relying rather on a route specified by the source. An adversary arranges packets with knowingly establish routing loops sends packets in circles targets source routing protocols by take advantage of the limited verification of message headers at forwarding nodes, allowing a single packet to repetitively traverse the same set of nodes that is called Carousel attack. In stretch attack, an adversary develops the long route between the source and destination. Both attacks perform on stateless protocol.

Stateful protocol store and maintain the routing information at the nodes. In Directional antenna attack, an adversary have modest control over packet progress when forwarding decisions are made independently by each node, but they can still waste energy by restarting a packet in various parts of the network. In the malicious discovery attack, the adversaries induce a supposed

topology. Both attacks perform on stateful protocol such as Optimized Link State Routing Protocol (link state) and Destination-Sequenced Distance Vector (DSDV).

II. RELATED WORK

David R.Raymond, Randy C.Marchany, Michael I.Brownfield and Scott F.Midkiff, discussed denial-of-sleep attack[13], in which a sensor node's power supply is targeted. Attacks of this type can reduce the sensor lifetime from years to days and have a disturbing impact on a sensor network. This paper proposed three contributions for sensor network security.

First, it classifies denial-of-sleep attacks on WSN MAC protocols based on an attacker's knowledge of the MAC protocol and ability to penetrate the network. Second, it explores potential attacks from each attack classification, both modeling their impacts on sensor networks running four leading WSN MAC protocols and analyzing the efficiency of implementations of these attacks on three of the protocols. Finally, it proposed a framework for defending against denial- of-sleep attacks and provides specific techniques that can be used against each denial-of sleep vulnerability.

Bryan Parno, Mark Luk, Evan Gaustad and Adrian Perring[17] have introduced a new secure routing protocol for sensor networks. Our protocol requires no special hardware and provides message delivery even in an environment with active adversaries. Design a new sensor network routing protocol with security and efficient yet highly resilient to active attacks our protocol assigns a network address to each node and establishes routing tables using a recursive grouping algorithm.
For a given topology, the algorithm proceeds entirely deterministically, preventing attacks on routing information and limiting a subverted node's ability to perform malicious actions. The existing secure routing protocols introduced either an unacceptable level of complexity or an excessive performance penalty.

Jing Deng, Richard Han, Shivakant Mishra[16], had proposed an Intrusion tolerant routing protocol for wireless sensor networks (INSENS). INSENS constructs forwarding tables at each node to facilitate communication between sensor nodes and a base station. It minimizes computation, communication, storage, and bandwidth requirements at the sensor nodes at the expense of increased computation, communication, storage, and bandwidth requirements at the base station. The scope of damage inflicted by intruders is further limited by restricting flooding to the base station and by having the base station order its packets using one-way sequence numbers.

Jing Deng, Richard Han and Shivakant Mishra, have discussed Denial of service (DoS)[18] attacks can cause severe damage in resource constrained, wireless sensor networks. In WSNs, an adversary can launch with little effort a path based denial of service (PDoS) attack that will have a severe widespread effect on the WSN, disabling nodes on all branches downstream of the path, due to the tree-structured topology of WSNs. To defend against a PDoS attack, an intermediate node must be able to detect spurious packets or replayed packets, and then reject them.

Rahul C.Shah and Jan M.Rabaey[19] have discussed sensor networks has led to a number of routing schemes that use the limited resources available at sensor nodes more efficiently. These schemes typically try to find the minimum energy path to optimize energy usage at a node. In this paper addressed lowest energy paths may not be optimal from the point of view of network lifetime and long term connectivity.

To optimize these measures, proposed a new scheme called energy aware routing that uses sub optimal paths occasionally to provide substantial gains. This paper proposed new protocol named energy aware routing. This protocol to increase the survivability of networks, it may be necessary to use sub-optimal paths occasionally.

To achieve this, multiple paths are found between source and destinations, and each path is assigned a probability of being chosen, depending on the energy metric. Every time data is to be sent from the source to destination, one of the paths is randomly chosen depending on the probabilities. Also different paths make an effort continuously, improving tolerance to nodes moving around the network. Using probabilistic forwarding to send traffic on different routes provides an easy way to use multiple paths without adding much complexity or state at a node.

Jae-Hwan Chang and Lindros Tassiulas[5] had extended the maximum lifetime routing problem to include the energy consumption at the receivers during reception. In wireless sensor networks where nodes operate on limited battery energy, the efficient utilization of the energy is very important. One of the main characteristics of these networks is that the transmission power consumption is closely coupled with the route selection. The energy efficiency has been considered in wireless adhoc network routing, but the conventional routing objective was to minimize the total consumed energy in reaching the destination.

III. ENERGY DRAINING ATTACKS

Vampire attacks are nothing but a new class of resource consumption attacks (denial of service attack) that use routing protocols to permanently disable ad hoc wireless sensor networks by decreasing node's battery power. A discussion about the carousel attack and stretch attack are given below.

A. Carousel Attack:

In this type of attack, a malicious node sends a packet with a route composed as a series of loops with the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route.

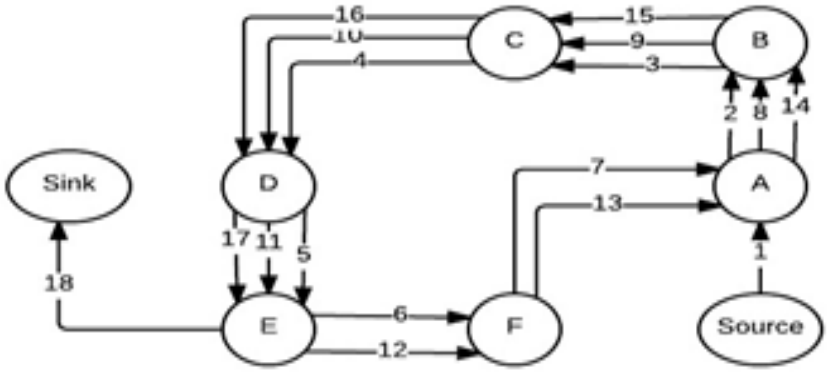

Fig. 3.1: An honest route would exit the loop immediately from node E to sink, but a malicious packet makes its way around the loop twice more before exiting.

B. Stretch Attack:

In this type of attack, a malicious node constructs artificially long routes from the source in spite of shorter routes being available. It increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. This attack causes the packets to be travelled a long route in the network.

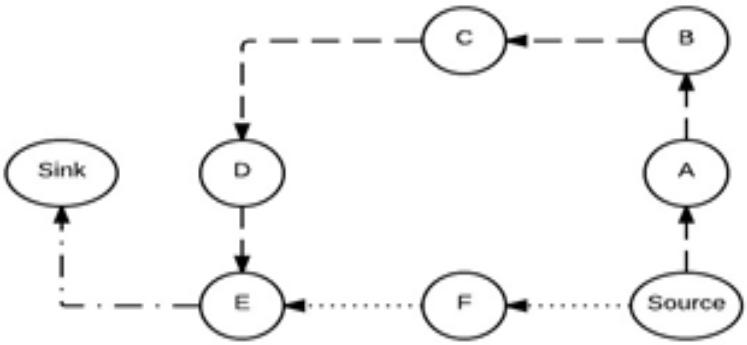

Fig. 3.2: Honest route is dotted while malicious route is dashed. The last link to the sink is shared

This attack is not specific to any protocol. Few kinds of attacks are the needed to reach the destination leading to energy wastage. Thus both lead to consumption of energy unnecessarily. 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. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols. We also saw how to overcome vampire attacks thus increasing the energy of the node by a factor of O(N) per adversary per packet, where N is the network size. We defined about PLGP the first sensor network routing protocol that provably bounds damage from vampire attacks by verifying the packets towards the destination.

IV. A BASIC CONSTRUCTION

This paper makes three primary contributions. First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing infrastructure, and so existing secure routing protocols such as Ariadne [11], SAODV [7], and SEAD [10] do not protect against Vampire attacks. Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but Vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol-compliant messages. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behaviour and cannot optimize out malicious action. Second, we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary). Third, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

V. SYSTEM MODEL

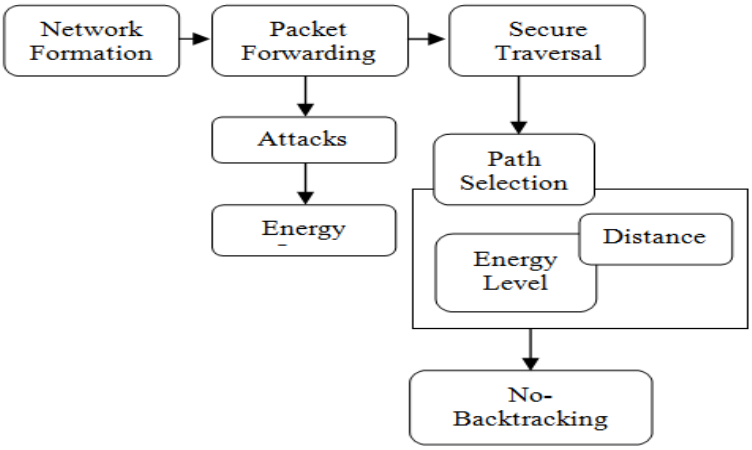

Fig. 5.1: System Model

In the block diagram describes the system model, first create network formation with wireless nodes in which each node has the initial energy value. An adversary perform the attacks during the packet forwarding, this causes the loss of energy in wireless networks. Using the secure packet traversal algorithm, to protect malicious action and achieving the node's battery life.

The major components of the system architecture are network formation, attacks on protocol, security against vampire attacks. The various systems are briefed below:

A. Network Formation:

A network describes a collection of nodes and the links between them. Source node wish send the packet to destination through intermediate nodes. Packet contains the control information and user data. Network creation is the process of create the N number of nodes within the network. Each and every node has node id and initial energy value by its creation time. The nodes are wished to transfer the data in one node to another. Select the source and destination node and also maintain the neighbor list.

B. Attacks on Protocol:

Resource depletion attacks focus on sinking the quantity of resources used by nodes like battery power, storage, memory etc, thus reducing the overall capacity of the network. Existing schemes can prevent attacks on the short term availability of a network, but do not address attacks that affect long-term availability. The most permanent denial of service attack is to entirely deplete node's batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest.

During the forwarding phase the clean slate sensor routing protocol is used (PLGP). All decisions are made independently by each node. Forwarding nodes do not know what path a packet took, allowing adversaries to divert packets to any part of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks.

C. Secure Packet Traversal:

PLGP refers clean-slate secure sensor network routing protocol by Parno, Luk, Gaustad, and Perrig. 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 neighbors using local broadcast, and form ever expanding neighborhoods stopping when the entire network is a single group. All over this process, nodes build a tree of neighbor 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.

The original version of the protocol is vulnerable to Vampire attacks. PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure 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 and also achieve the highest battery life in order to avoid the avoid the unconditional overhearing.

The Floyd-Warshall Algorithm is an efficient algorithm to find all-pairs shortest paths. That is, it is guaranteed to find the shortest path between every pair of nodes For example, if node i is a source and k is a sink. This algorithm first finds the distance between i and k. i.e) d(i,k).Then it finds the distance through any intermediate nodes. If j is an intermediate node, then the distance is calculated as d(i,k)=d(i,j)+d(j,k). Filally it finds the minimum distance by comparing these two distances.d(i,k)=min{d(i,k),d(i,j)+(d(j,k)}After j=*n* iterations, we have the shortest distance between *i* and *k*.

D. No-Backtracking:

To preserve no-backtracking, verifiable path history is added to every packet. Whenever node n forwards packet p, every ode attaching non-replayable attestation (signature). These signatures form a chain attached to every packet, 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. When any node receives a message, it checks that every node in the path attestation 1) has a corresponding entry in the signature chain, and 2) is logically closer to the destination than the previous hop in the chain This way, forwarding nodes can enforce the forward progress of a message, preserving no-backtracking. If no attestation is present, the node checks to see if the originator of the message is a physical neighbor. Since messages are signed with the originator's key, malicious nodes cannot falsely claim to be the origin of a message, and therefore do not benefit by removing attestations.

Signature chaining is essentially a method of generating a chain of signatures on the same message by different users. Each signature acts as a "link" of the chain. The one-way-ness implies that the chaining process is one-way in the sense that more links can be easily added to the chain. Every forwarding node verifies the attestation chain to ensure that the packet has never traveled away from its destination.

Anomalies are handled based on the category in which the anomaly belongs to. If the vampire is from the network, then that should be prevented from entering in to the node and from forwarding to another node. We cannot delete that packet because the packet is created by some other node in the network .If any vampire is found inside the node that should be deleted immediately and should prevent from forwarding. For avoiding the entry of anomalies from the network to any packet, all the packets should satisfy no backtracking property [1]. The algorithm is explained below

1) *Algorithm (PLGPa)[1]:*

```
Function secure_forward_packet (p)
s ← extract_source_address(p);
a ← extract_attestation(p);
if (not verify_source_sig(p)) or
(empty(a) and not is_neighbor(s)) or
(not saowf_verify(a)) then
return ; /* drop(p) */
foreach node in a do
prevnode ← node;
if (not are_neighbors(node, prevnode)) or
(not making_progress(prevnode, node)) then
return ; /* drop(p) */
c ← closest_next_node(s);
p′ ← saowf_append(p);
if is_neighbor(c) then forward(p′, c);
else
forward (p′,next_hop_to_non_neighbor(c));
```

VI. PERFORMANCE ANALYSIS

PLGP imposes increased setup cost over BVR , but compares favourably to in terms of packet forwarding overhead. While path stretch increases by a factor of 1.5–2, message delivery success without resorting to localized flooding is improved: PLGP never floods, while BVR must flood 5–10% of packets depending on network size and topology. PLGP also demonstrates more equitable routing load distribution and path diversity than BVR. Since the forwarding phase should last considerably longer than setup, PLGP offers performance comparable to BVR in the average case.

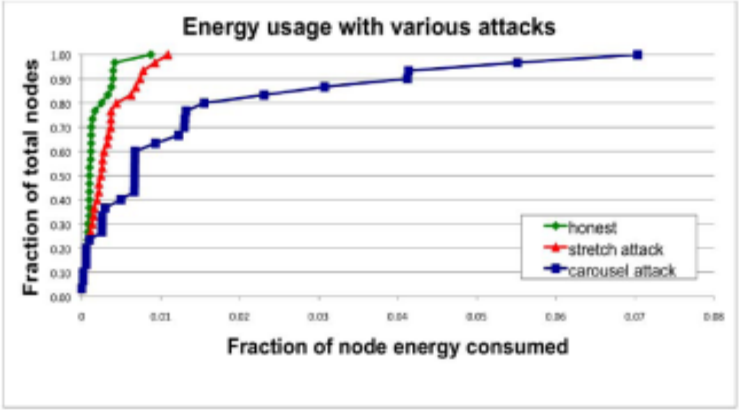

Fig. 3: Node energy distribution under various attack scenarios.

VII. CONCLUSION

Vampire attacks has been 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. Defenses against some of the forwarding-phase attacks has been proposed and PLGP-a, the first sensor network routing protocol that reduces the damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. The routing protocol has been used at the time of routing to make efficient energy utilization during the packet forwarding phase.

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, February 2013.
[2] 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.
[3] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009
[4] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2008.
[5] Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp.609–619, Aug. 2004.
[6] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.
[7] 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.
[8] A. Kroller, S.P. Fekete, D. Pfisterer, and S. Fischer, "Deterministic Boundary Recognition and Topology Extraction for Large Sensor Networks," Proc. Ann. ACM-SIAM Symp. Discrete Algorithms, 2006.
[9] Y.-C. Hu, D.B. Johnson, and A. Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc. IEEE INFOCOM, 2003.
[10] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications, 2002.
[11] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002.
[12] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols"(2009).
[13] David R. Raymond and Scott F.Midkiff,"Denial-of-service in wireless sensor networks: Attacks and defenses," (2008).
[14] Yangcheng Huang and Saleem Bhatti,"Fast converging distance vector routing for wireless mesh networks" ICDCS, (2008)
[15] Jing Deng, Richard Han, Shivakant Mishra,"INSENS: Intrusiontolerant routing for wireless sensor networks" (2006).
[16] Jing Deng, Richard Han, and Shivakant Mishra, "Defending against path based DoS attacks in wireless sensor networks" ACM workshop on security of ad hoc and sensor networks, (2005).
[17] Rahul C. Shah and Jan M.Rabaey,"Energy aware routing for low energy ad hoc sensor networks"(2002).