
N. Anil Kumar Chowdari¹, V. Sireesha²

¹PG Scholar, Dept of CSE, Audisankara Institute of Technology, Gudur, A.P, India.
²Assoc Prof, Dept of CSE, Audisankara Institute of Technology, Gudur, A.P, India.

Abstract: Adhoc network is small power networks are an exciting research direction in sensing and persistent computing. The existing security effort in this area has paying attention mainly 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 the networks by quickly consuming node battery power. These resource depletion attacks not specific protocol any routing protocols. We find that all existing routing protocols susceptible to these attacks, which are different and difficult to detect, and are easy to carry as possible as on malicious insider exists. To address these problems in existing system, this paper proposes methods to reduce these types of attacks, and provides a new proof of concept protocol that provably bounds the damage caused by resource depletion attacks.

Keywords: Resource Depletion Attacks, No-Backtracking, Ad-Hoc Wireless Sensor Network.

I. INTRODUCTION

Ad-hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly-deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications. As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable — lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. Due to their ad-hoc organization, wireless ad-hoc networks are particularly vulnerable to denial of service (DoS) attacks, and a great deal of research has been done to enhance survivability.

We define a Vampire attack as the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. We measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e. the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Safety from Vampire attacks implies that this ratio is 1. Energy use by malicious nodes is not considered, since they can always unilaterally drain their own batteries. In this paper we stated the different types of attacks and how they are attack in the packet forwarding and path discovery phases. An adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles as shown in Figure 1(a). It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. Brief mentions of this attack can be found in other literature, but neither intuition for defense nor any evaluation is provided. In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. We call this the stretch attack, since 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, which is illustrated in Figure 1(b).

We explore numerous mitigation methods to bound the damage from Vampire attacks, and find that while the carousel attack is simple to prevent with negligible overhead, the stretch attack is far more challenging. The first protection mechanism we consider is loose source routing, where any forwarding node can reroute the packet if it knows a shorter path to the destination. In our second attempt, we modify the protocol from to guarantee that a packet makes progress through the network. We call this the no backtracking property, since it holds if and only if a packet is moving strictly closer to its destination with every hop, and it mitigates all mentioned Vampire attacks with the exception of malicious flooded discovery, which...
is significantly harder to detect or prevent. We also sketch how to further modify the protocol to detect Vampires during topology discovery and evict them after the network converges (at “dawn”).

Fig 1. Malicious route construction attacks on source routing.

A. Existing System

Existing schemes can prevent attacks on the short-term availability of a network, they do not address attacks that affect long-term availability — 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 paper we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call resource depletion attacks since they drain the life from networks nodes.

B. Proposed System

To address the above mention problems, this paper thoroughly evaluate the vulnerabilities of existing routing protocols. And then we modify the existing sensor routing protocol that provably bounds the damage from resource depletion attacks in packet forwarding phase.

II. PROPOSED WORK

In this work, we consider the a clean-slate secure sensor network routing protocol by parno, Luk, Gaustad, and Perrig (PLGP) can be modified to provably resist resource depletion attacks during the packet forwarding phase. The original version of the protocol, although designed for security, is vulnerable to resource depletion attacks. PLGP consists of a topology discovery phase, followed by a packet forwarding phase. Topology discovery 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. Node 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. 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 the nodes learn each other virtual addresses and cryptographic keys. The final address tree is verifiable after network convergence, and all forwarding decisions can be independently verified. During forwarding phase, all decisions are made independently by each node. When receiving a packet, node determines the hop by finding the most significant bit of its address that differs from the message originators address. Thus every forwarding event shortens the logical distance to the destination, since node addresses should be strictly closer to the destination function forward_packet

III. PROVABLE SECURITY AGAINST RESOURCE DEPLETION ATTACKS

Here we modify the forwarding phase of PLGP to provably avoid the above-mentioned attacks. First we introduce the no-backtracking property, satisfied for a given packet if and only if it consistently makes progress toward its destination in the logic network address space. The Definition 1 more formally:

Definition 1: No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network.

A. No-backtracking implies Resource Depletion resistance.

It is not immediately obvious why no-backtracking prevents Vampire attacks in the forwarding phase. Recall the reason for the success of the stretch attack: intermediate nodes in a source route cannot check whether...
the source-defined route is optimal, or even that it makes progress toward the destination. When nodes make independent routing decisions packets contains maliciously composed routes. This means the adversary cannot perform carousel or stretch attacks – no node may unilaterally specify a suboptimal path through the network. However the adversary cleverly may still influence packet progress. We can prevent this interference by independently checking on packet progress. If we can guarantee that a packet is closer to its destination with every hop, we can bound the potential damage from an attacker as a function of network size.

B. PLGP does not satisfy no-backtracking

In non-secure routing protocols, routes are dynamically composed of forwarding decisions made independently by each hop. PLGP differs from other protocols in that packets along the shortest route through the tree, forwarding packets along the shortest route through the tree that is allowed by the physical topology. However, this is not sufficient for no-backtracking to hold, since nodes cannot be certain of the path previously traversed by a packet and so PLGP is still vulnerable to directional antenna/wormhole attacks, which allow adversaries to divert packets to any part of the network. To preserve no-backtracking, we add a verifiable path history to every PLGP packet, similar to route authentications in path-vector signatures. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP 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. These attestations 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 in the logical address space.

Function secure_forward_packet(p)

\[\text{s} \leftarrow \text{extract_secure_address(p)};\]
\[\text{a} \leftarrow \text{extract_attestation(p)};\]
if (not verify_source_sig(p) or (empty (a) and not is_neighbor (s)) or (not saowf_verify(a))) then return ;
foreach node in a do
    pervnode \leftarrow \text{node};
    if (not are_neighbors(node,prevnode)) or (not making_progress(prevnode, node)) then return ;
\text{c} \leftarrow \text{closest_next_node (s)};
\text{p'} \leftarrow \text{saowf_append(p)};
if is_neighbor (c) then forward(p', c);
else forward(p', next_hop_to_non_neighbor(c));

C. PLGPa satisfies no-backtracking

That our modified protocol preserves the no-backtracking property, we define a network as collection of nodes, a topology, connectivity properties, and node identifies, borrowing the model. Honest nodes can also use directional antennas to transmit to any node in the network without being overhead by any other node. Honest nodes can compose, forward, accept, or drop messages, and malicious nodes can also arbitrarily transform them.

IV. SECURING THE DISCOVERY PHASE

Without fully solving the problem of malicious topology discovery, we can still reduce it by focusing synchronous discovery and ignoring discovery messages during the principal periods. This can lead to some nodes being separated from the network for a period of time, and is essentially a form of rate limiting. If a network survives the high risk discovery period, it is unlikely to suffer serious damage from resource depletion during normal packet forwarding. While PLGPa is not vulnerable to resource depletion attacks during packet forwarding phase, we cannot make the same claim about discovery. However, we can give some intuition as to how to further modify PLGPa to bound the damage from malicious discovery. The major issue is that malicious nodes can use directional antennas to masquerade neighbors to any or all nodes in the network, and therefore look like a group of size one. Since the PLGP offers the chance to detect active resource depletion attacks once the network meets, successive re-discovery periods become safer. However, the bound we can place on malicious discovery damage in PLGPa is still unknown. Moreover, if we can conclude that a single malicious node cause a factor of k energy increase during discovery, it is not clear how that value scales under collusion among multiple malicious nodes.

V. CONCLUSION

In this paper we define resource depletion attacks, a new class of resource consumption attacks that use routing protocols to permanently disable sensor networks by consuming the nodes battery power. To address these problems, we proposed defenses against some of the forwarding phase attacks and described PLGPa, the first sensor network routing protocol that provably bounds damage from resource depletion attacks by verifying that packets consistently make progress toward their destinations. In near future, we investigate the damage limitations with further modification to PLGPa.

VI. REFERENCES


Author's Profile:

N. Anil Kumar Chowdari has received his B.Tech degree in Information Technology from RSR Engineering College, Kadanuthala affiliated to JNTU, Anantapur in 2012 and pursuing M.Tech degree in Computer Science & Engineering at Audisankara Institute of Technology, Gudur affiliated to JNTU, Anantapur in (2012-2014).

V. Sireesha is working as Associate professor at Audisankara Institute of Technology affiliated to JNTU Anantapur. She received M.Tech in CSE and pursuing Ph.D in CSE.