ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks

[I]Gowthami.M, [II]Jessy Nirmal.A.G, [III]P.S.K.Patra3
[I,II,III]Dept. of CSE, Agni College of Technology, Chennai, Tamil Nadu

Abstract
Ad-hoc sensor network and routing data in them is a most significant research area. There are lots of protocols established to protect from DOS attack, but it is not perfectly possible. One such DOS attack is Vampire attack. This vampire attack is a resource depletion attacks at the routing protocol layer, which permanently disconnect the networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather depend on the characteristics of many popular classes of routing protocols. This project illustrates a technique to tolerate the attack by employing the Cluster Head. In case of each Vampire attack, the Cluster Head employs in this situation and distributes the packet to destination without dropping the packet. Thus give a successful and reliable message delivery even in case of Vampire attack. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N is the number of network nodes.

Keywords
Denial of service, ad-hoc networks, sensor networks, stretch attack, carousel attack, routing

I. Introducion

Ad-hoc wireless sensor networks (WSNs) promise raising new applications in the upcoming future, such as continuous connectivity, ubiquitous on-demand calculating power, and immediately-deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications. Due to their ad-hoc organization, wireless ad-hoc networks are specifically vulnerable to denial of service (DoS) attacks , and a great deal of research has been done to enhance survivability. While these schemes can prevent attacks on the network in short-term availability, they do not tackle attacks that have effect on long-term availability — the most stable denial of service attack is to entirely deplete nodes' batteries. This is an occurrence of a resource depletion attack, with battery power as the resource of attention.

In this paper we consider how routing protocols, still those designed to be secure, its lack protection from these attacks, which we call as Vampire attacks, because they drain the life from networks nodes. These attacks are different from previously-studied reduction of quality(RoQ), Denail of service(DoS), and routing infrastructure attacks as they do not disturb direct availability, but somewhat work over time to entirely disconnect a network. While some of the individual attacks are simple, and resource exhaustion and power-draining attacks have been discussed before , previous work has been mostly restricted to other levels of the protocol stack, e.g. medium access control (MAC) or application layers, and to our discussion there is little discussion, and no complete analysis or mitigation, of routing-layer source exhaustion attacks.

Vampire attacks are not protocol-specific, in that they do not depend on design properties or implementation faults of specific routing protocols, but rather utilize common properties of protocol classes such as link-state, source routing, geographic, distance-vector, and beacon routing. Neither do these attacks depend on flooding the network with huge amounts of data, but somewhat try to transmit as little data as possible to attain the biggest energy drain, preventing a rate limiting solution. Because Vampires make use protocol-compliant messages, these attacks are very complicated to detect and prevent.

A. Contributions

This paper makes three main contributions. First, we completely evaluate the vulnerabilities of existing protocols to routing layer battery exhaustion attacks. We monitor that security measures to prevent Vampire attacks are orthogonal to those used to shield routing infrastructure, and so offered secure routing protocols such as SAODV ,Ariadne and SEAD do not protect against Vampire attacks. Existing work on secure routing attempts to make sure that adversaries cannot effect path discovery to come back an invalid network path, however Vampires do not disturb or change discovered paths, as a substitute using protocol compliant messages and existing valid network paths. Protocols that take advantage of power efficiency are also inappropriate, because they based on cooperative node behavior and cannot optimize out malicious action. Second, we demonstrate simulation results quantifying the performance of most representative protocols in the presence of a single Vampire (insider adversary). Third, we change an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding phase.

B. Overview

In the rest of this paper, we present a sequence of increasingly damaging Vampire attacks, calculate the vulnerability of some example protocols, and propose how to improve resilience. In source routing protocols, we illustrate how a malicious packet source can able to specify paths through the network which are far longer than optimal, wasting energy at middle nodes who further forward the packet based on the included source route.

In routing process where forwarding decisions are made independently by each node (as opposed to specified by the source), we recommend how directional antenna and wormhole attacks can be used to distribute packets to several remote network positions, forcing packet processing at nodes that would not usually receive that packet at all, and thus rising network-wide energy expenditure. Finally, we illustrate how an adversary can target not only packet forwarding but also route and topology discovery phases — if discovery messages are flooded, an adversary can, for the cost of a single packet, consume energy at each node in the network. In our first attack, 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 authentication of message headers at forwarding nodes, allowing a single packet to continually traverse the same set of nodes.

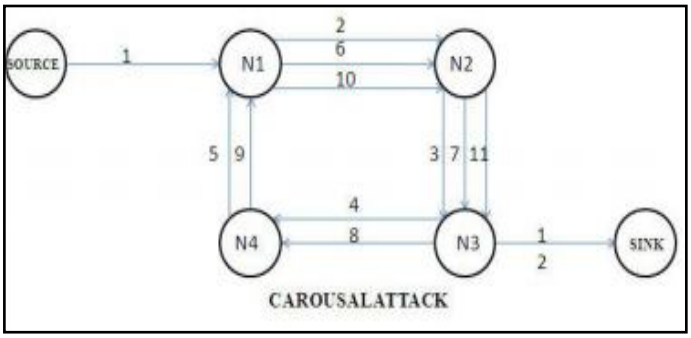

Fig. 1(a): Carousal Attack

In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. We describe this 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.

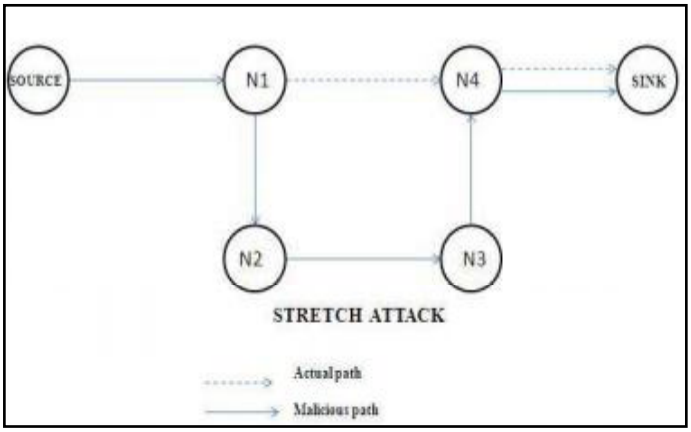

Fig. 1(b): Stretch Attack

II. Related Work

A. Jelly Fish Attack

This type of attack is used for closed loop flow such as TCP. A critical strength of the Jelly Fish Attack is that it maintains compliance with all control plane and data plane protocols in order to make detection and diagnosis costly and time consuming. The key principle that Jelly Fish attack use to facilitate is targeting end-to end congestion control.

B. Black Hole Attack

This type of attack is used for open loop control flows. Black Hole nodes participate in all routing control plane operations. However, once paths are established, Black Holes simply drop all packets.

C. Path Quality Monitoring

They design and analyze path-quality monitoring protocols that reliably raise an alarm when the packet-loss rate and delay exceed a threshold, even when an adversary tries to bias monitoring results by selectively delaying, dropping, modifying, injecting, or preferentially treating packets.

1. Stateful Protocol and their Attacks

A stateful protocol is where nodes are aware of their topology, forwarding decisions, its state. It need the server to store and record the transaction so they can be recalled or resumed. Two significant classes are link state and distance –vector. Example of link-state is OLSR and example of distance-vector is DSDV. Both these protocols are proactive, which routes to all reachable nodes in the network and minimizes the initial delay. OLSR keeps the record of up and down state of links and flood routing updates. DSDV is also known as Distributed Bellman-Ford or RIP (Routing Information Protocol). Every node maintains a routing table that contains all available destinations, the next node to reach to destination, the number of hops to reach the destination and periodically send table to all neighbors to maintain topology. Both these protocols are not vulnerable to carousel and stretch attacks.

In fact, any time adversaries cannot indicate the full path, the potential for Vampire attack is reduced. Two types of attacks in stateful protocol are directional antenna attack and malicious discovery attack. Directional antenna attack: In this the vampires have little control over the packets progress, but they still waste energy by restarting a packet in various parts of network. They will deposit the packets in arbitrary path of network due to this energy is consumed, O(d) where d is the network diameter, d/2 .It is also considered as half worm hole attack.

Packet leashes cannot prevent this kind of attack since they are not meant to protect against malicious message source but only intermediary. Malicious Discovery Attack: It is also called as spurious rote discovery. Both AODV and DSR are vulnerable to this attack since nodes may initiate discovery at any time, not just during the topology change. This type of attack becomes serious when nodes claim that long distance route has changed. This attack is trivial in open networks. Packet leashes cannot prevent this type of attack. This is similar to route flapping in BGP.

2. Stateless Protocols and their Attacks

A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. It is communication protocol that treats ach request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses. The two most common types of attacks are Carousel attack shown in Figure[1.a] and Stretch attack shown in Figure[1.b]. It is called 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. The carousel on the other hand sends packets in circles. 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.

3. Coordinate and Beacon Protocols

The two examples of coordinate and beacon protocols are GPSR and BVR. These protocols use physical coordinates or beacon distances for routing. In GPSR a packet may encounter a dead end (i.e. target separated by a wall or obstruction).The packet is then diverted until a path to the target is available .They do not take path length into account when routing around local obstructions. In BVR the packets are routed towards a node (beacon) close to the target. Each node makes independent forwarding decisions hence the vampire attacks (draining node life) is said to be limited.

III. Clean-Slate Sensor Network Routing Protocol

In this section we show that a clean-slate secure sensor network

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

routing protocol by Parno, Luk, Gaustad, and Perrig("PLGP" from here on) can be modified to provably resist Vampire attacks during the packet forwarding phase.

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. (There is no on-demand discovery.) 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. 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 (see Figure 6). All nodes learn each others' virtual addresses and cryptographic keys. The final address tree is verifiable after network convergence, and all forwarding decisions can be independently verified.

Furthermore, assuming each legitimate network node has a unique certificate of membership (assigned before 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.

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 (from now on referred to as node ID), signed by a trusted offline authority. Each node starts as its own group of size one, with a virtual address 0. Nodes who overhear presence broadcasts form groups with their neighbors. When two individual nodes (each with an initial address 0) form a group of size two, one of them takes the address 0, and the other becomes 1. Groups merge preferentially with the smallest neighboring group, which may be a single node. We may think of groups acting as individual nodes, with decisions made using secure multiparty computation. Like individual nodes, each group will initially choose a group address 0, and will choose 0 or 1 when merging with another group.

Each group member pretends the group address to their own address, e.g. node 0 in group 0 becomes 0.0, node 0 in group 1 becomes 1.0, and so on. Each time two groups merge, the address of each node is lengthened by one bit. Implicitly, this forms a binary tree of all addresses in the network, with node addresses as leaved. Note that this tree is not a virtual coordinate system, as the only information coded by the tree are neighbor relationships among nodes. Nodes 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 larger groups merge, they both broadcast their group IDs (and the IDs of all group members) to each other, and proceed with a merge protocol identical to the two-node case. 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. Each node stores the identity of one or more nodes through which it heard an announcement that another group exists. That node may have itself heard the information second-hand, so every node within a group will end up with a next-hop path to every other group, as in distance-vector. Topology discovery proceeds in this manner until all network nodes are members of a single group. By the end of topology discovery, each node learns every 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.

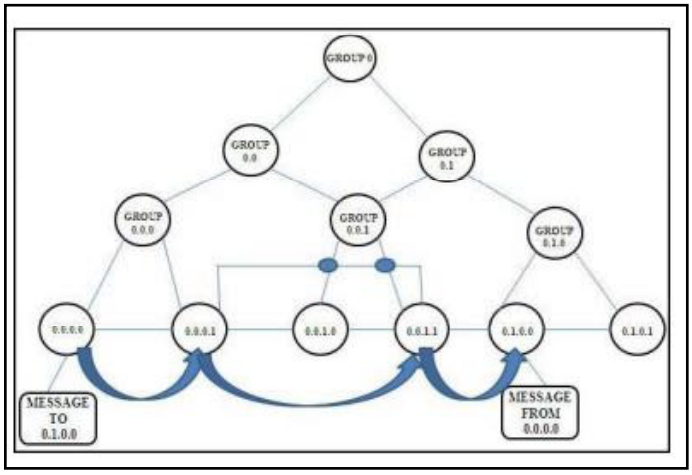

Fig. 2: The final address tree for a fully-converged 6-node network. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Note that non-leaf nodes are not physical nodes but rather logical group identifiers.

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 (see Figure 6). Thus every forwarding event (except when 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.

A. Performance Analysis

PLGP imposes increased setup cost over BVR , but compares favorably 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.

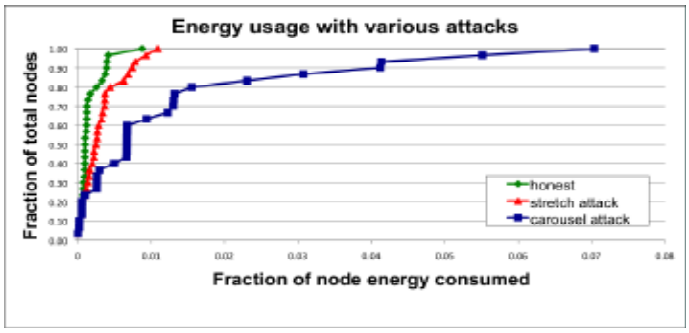

Fig. 3: Node energy distribution under various attack scenarios.

IV. Conclusion

In this paper 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. 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 mobile networks, is left for future work.

References

[1] *Eugene Y.Vasserman, Nicholas Hopper, Vampire attacks: Draining life from wireless ad-hoc sensor networks.2011*
[2] *Imad Aad, Jean-Pierre Hubaux, and Edward W.Knightly, Denail of service resilience in ad hoc networks, mobicom,2004.*
[3] *Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on demand source routing in mobile ad hoc networks, IEEE Transactions on mobile computing 05(2006),no.11.*
[4] *Tuomas Aura, Dos-resistant authentication with client puzzles, Internationalworkshop on security protocols, 2001.*
[5] *Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.*
[6] *INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.*
[7] *Daniele Raffo, C´edric Adjih, Thomas Clausen, and Paul M¨uhlethaler, An advanced signature system for OLSR, SASN, 2004.*
[8] *John R. Douceur, The Sybil attack, International workshop on peer-topeer systems, 2002.*
[9] *Computing, Lakshminarayanan Subramanian, Randy H. Katz, Volker Roth, Scott Shenker, and Ion Stoica, Reliable broadcast in unknown fixed-identity networks, Annual ACM SIGACT-SIGOPS symposium on principles of distributed 2005.*
[10] *Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002*
[11] *Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensornetwork routing: A clean-slate approach, CoNEXT, 2006.*
[12] *John R. Douceur, The Sybil attack, International workshop on peer-to peer systems, 2002.*
[13] *Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.*
[14] *Charles E. Perkins and Pravin Bhagwat, Highly dynamic desination sequenced distance-vector routing (DSDV) for mobile computers, Conference on communications architectures, protocols and applications, 1994*
[15] *Packet leashes: A defense against wormhole attacks in wireless Ad-Hoc networks, INFOCOM, 200*