IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 3, Mar 2014, 45-50

SECURE ROUTING PROTOCOL IN SENSOR NETWORK FOR VAMPIRE ATTACK

S. RENUKA DEVI & R. DEVI

CSE(M.E), Sri Venkateswara College of Engineering and Technology, Anna University, Tamil Nadu, India

ABSTRACT

Ad hoc low-power wireless sensor 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 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, SAODV and SEAD 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 behavior and cannot optimize out malicious action.

KEYWORDS: DSDV, DSR, MAC, OSLR, SEAD

INTRODUCTION

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.

Wireless Sensor Network

AD hoc wireless sensor networks (WSNs) 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.

While these 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 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 and resource exhaustion attacks have been discussed before 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 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, distance vector, 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.

Classification

The first challenge in addressing Vampire attacks is defining them—what actions in fact constitute an attack. DoS attacks in wired networks are frequently characterized by amplification an adversary can amplify the resources it spends on the attack, e.g., use 1 minute of its own CPU time to cause the victim to use 10 minutes. However, consider the process of routing a packet in any multi hop network: a source composes and transmits it to the next hop toward the destination, which transmits it further, until the destination is reached; consuming resources not only at the source node but also at every node the message moves through.

If we consider the cumulative energy of an entire network, amplification attacks are always possible, given that an adversary can compose and send messages which are processed by each node along the message path. So, the act of sending a message is in itself an act of amplification, leading to resource exhaustion, as long as the aggregate cost of routing a message (at the intermediate nodes) is lower than the cost to the source to compose and transmit it. So, we must drop amplification as our definition of maliciousness and instead focus on the cumulative energy consumption increase that a malicious node can cause while sending the same number of messages as an honest node.

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 batteries.

Protocols and Assumption

We consider the effect of Vampire attacks on link-state, distance-vector, source routing and geographic and beacon routing protocols, as well as a logical ID-based sensor network routing protocol proposed by Parno etal. While this is by no means an exhaustive list of routing protocols which are vulnerable to Vampire attacks, we view the covered

protocols as an important subset of the routing solution space, and stress that our attacks are likely to apply to other protocols.

All routing protocols employ at least one topology discovery period, since ad hoc deployment implies no prior position knowledge. Limiting ourselves to immutable but dynamically organized topologies, as in most wireless sensor networks, we further differentiate on-demand routing protocols, where topology discovery is done at transmission time, and static protocols, where topology is discovered during an initial setup phase, with periodic rediscovery to handle rare topology changes. Our adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Furthermore, adversary location within the network is assumed to be fixed and random, as if an adversary corrupts a number of honest nodes before the network was deployed, and cannot control their final positions.

Note that this is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. Intelligent adversary placement or dynamic node compromise would make attacks far more damaging. Discovered during an initial setup phase, with periodic rediscovery to handle rare topology changes. Our adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Furthermore, adversary location within the network is assumed to be fixed and random, as if an adversary corrupts a number of honest nodes before the network was deployed, and cannot control their final positions. Note that this is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. Intelligent adversary placement or dynamic node compromise Would make attacks far more damaging.

Clean-Slate Sensor Network Routing

We show that a clean-slate secure sensor network routing protocol by Parno et al. (“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.

Here, we present simple but previously neglected attacks on source routing protocols, such as DSR [35]. In these systems, 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. To forward a message, the intermediate node finds itself in the route (specified in the packet header) and transmits the message to the next hop. The burden is on the source to ensure that the route valid at the time of sending, and that every node in the route is a physical neighbor of the previous route hop. This approach has the advantage of requiring very little forwarding logic at intermediate nodes, and allows for entire routes to be sender authenticated using digital signatures, as in Ariadne

EXISTING SYSTEM

In source routing protocols, we show how a malicious packet source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes who forward the packet based on the included source route. An adversary composes packets with purposely introduced routing loops.

PROPOSED SYSTEM

Here we show that a clean-slate secure sensor network routing protocol by Parno, Luk, Gaustad, and Perrig ("PLGP") 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.

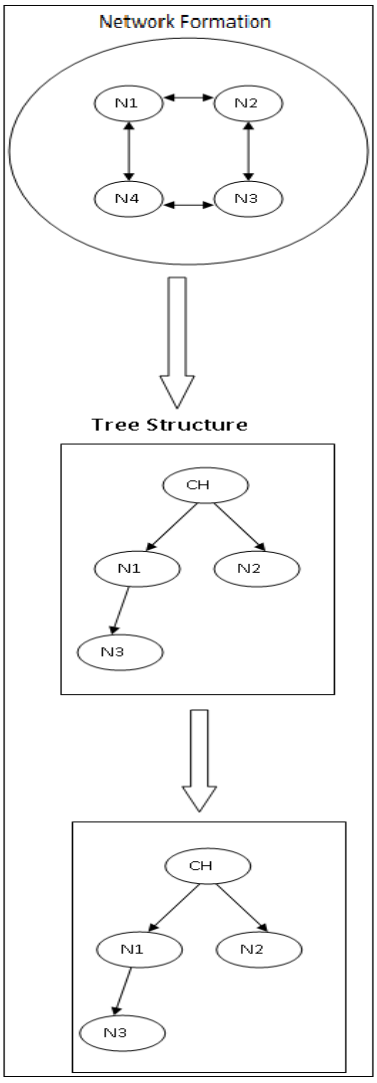

Figure 1

CONCLUSIONS

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.

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. 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.

ACKNOWLEDGEMENTS

The authors would like to thank Hal Peterson, Tian He, Yongdae Kim, Daniel Andresen, and our anonymous reviewers for their very helpful comments on earlier drafts of this paper.

REFERENCES

1. "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012.
2. I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.
3. 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.
4. T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.
5. J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
6. D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.
7. D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html, 1996.
8. I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ., 1999.
9. J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.
10. H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
11. 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.