Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Alleviation of Energy Draining attacks in Wireless Ad hoc Sensor Networks

Mr. Chandrashekhar Goswami
Asst. Professor
Department of Computer Science & Engg.
PRMITR Badnera Maharashtra, India

Abstract— Network survivability is the major concern to the design and design interpretation of wireless ad hoc sensor networks. This paper explores energy draining attacks at the routing protocol layer, which drains battery power. A innovative approach for routing protocols, affect from attack even those devised to be protected which is short of protection from these attacks, which we call energy draining attacks, which permanently disable networks by quickly draining battery power of nodes. These energy depletion attacks are not protocol specific but are disturbing and hard to notice, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages.

Keyword—Denial of service, security, routing, ad hoc networks, sensor networks, wireless networks.

I. INTRODUCTION

A wireless sensor network (WSN) is a computer network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations [1]. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control [1][2].

An ad hoc wireless sensor network is a decentralized, collection of wireless mobile sensor nodes forming ad hoc network without aid of any established infrastructure. Each node in a sensor network is equipped with a radio transceiver, a small microcontroller, and a battery. Wireless Ad hoc Sensor networks are emerging as a new technology with evidence of their deployment in space, educational, agricultural, domestic, commercial, military environments [1]. The sensors are generally utilized in particular geographic areas and these sensors self-configure to form an ad-hoc wireless network to gather data from environment. Because of Ad hoc nature these sensor networks promise exciting new applications in the forthcoming future, such as on-demand computing power, continuous connectivity, and instantly deployable communication for military and other application area. Such networks monitor environmental conditions, factory performance, agricultural growth and security deployment at borders [2].

Routing and data forwarding is a vital service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. For example, an attacker might launch denial of-service attacks on the routing protocol, preventing communication in WSN [2] [3]. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are vulnerable to replay by the attacker of legitimate routing messages. The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones [3].

Extensive researches have been done on power draining and resource exhaustion scenarios [6], [8]. But these focused more on the other layers of protocol stack. Resource exhaustion attacks at the routing layer are left untouched. Energy draining attacks are also called as Vampire attacks. Vampire attacks differ from DoS attacks because they do not immediate interrupt service availability. Rather it works over time, entirely draining out the nodes' battery power, leading to the permanent disabling of the network. Moreover, Vampire attacks exploit general properties of protocol classes such as link-state, distance vector, source routing and geographic routing. Vampire attacks are very difficult to detect and prevent, since they use protocol-compliant messages.

Consider the process of routing a packet in an ad hoc wireless network. A source composes and transmits the packet to the next hop node, which in turn relays the packet further, until the packet reaches to its destination. However, this multi hop relaying can consume the energy resources at each node. So, the process of routing a packet itself leads to resource exhaustion. Further, a malicious node within the path traced by the packet can cause an increase in the energy consumption while sending the same number of messages as an honest node. Hence, Vampire attacks is the composition and transmission of a message that causes an increase in the energy consumption by a network than if an honest node transmitted a message of identical size to the same destination.

II. RELATED WORK

Eugene Y. Vasserman and Nicholas Hopper [1] introduced a definition for vampire attacks in February 2013. Vampire attacks are clearly defined in their study. The study makes three primary contributions. First evaluates the vulnerabilities of existing protocols to routing layer battery depletion attacks. The 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. The authors 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. They 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. They concentrated only in the network layer but not considered about the application layer where the malicious packet actually originates.

Gergely Acs, Levente Buttyan, and Istvan Vajda [5] had introduced a new attack on Ariadne, a previously published "secure" routing protocol. These attacks clearly demonstrate that flaws can be very subtle, and therefore, hard to discover by informal reasoning. Hence, they advocate a more systematic approach to analyzing ad hoc routing protocols, which is based on a rigorous mathematical model, in which precise definitions of security can be given, and sound proof techniques can be developed.

Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly[4], mainly focuses on the design and study DoS attacks in order to assess the damage that difficult-to-detect attackers can cause. The authors presented a novel DoS attack perpetrated by JellyFish: relay nodes that stealthily disorder, delay, or periodically drop packets that they are expected to forward, in a way that leads astray end-to-end congestion control protocols. This attack is protocol- compliant and yet has a devastating impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows. For completeness, they have also considered a well known attack, the Black Hole attack, as its impact on open-loop flows is similar to the effect of JellyFish on closed-loop flows. They studied these attacks in a variety of settings and have provided a quantification of the damage they can inflict. It is showed that, such attacks can actually increase the capacity of ad hoc networks as they will starve all multi hop flows and provide all resources to one-hop flows that cannot be intercepted by JellyFish or Black Holes.

Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig [2] introduce a secure routing protocol for Ad-hoc wireless networks. The deployment of sensor networks in security-and safety-critical environments requires secure communication primitives. In this study, the authors design, implement, and evaluate a new secure routing protocol for sensor networks. The protocol presented in this paper requires no special hardware and provides message delivery even in an environment with active adversaries. They adopt a clean-slate approach and design a new sensor network routing protocol with security and efficiency as central design parameters. The protocol is efficient yet highly resilient to active attacks.

III. ENERGY DRAINING ATTACKS (Vampire Attacks) : AN OVERVIEW

This section analyses two types of Vampire attacks:

1) Carousel attacks
2) Stretch attacks.

In WSN, there are several protocol classes such as source routing, distance vector, link-state, geographic routing and so on. In source routing, to send a packet to another host, the sender constructs a source route in the packet's header, giving the address of each host in the network so that the packet is forwarded in order to the destination host. In this case, a malicious source can specify a source route through the network that traverses more hops than optimal, results draining of energy from the intermediate nodes who forward the packet based on the source route.

Our first attack, called the carousel attack, targets source routing protocols, exploiting the limited verification of message headers at each forwarding node. A malicious node composes and transmits packets with knowingly routing loops. It sends packets in circles. Carousel attack causes a single packet to repeatedly traverse the same set of nodes, depleting the nodes' battery power. As Fig. 1 shows, a malicious packet introduces routing loops, makes its way twice around the loop before delivering it to the sink. This makes the packet repeatedly traverse the same set of nodes, while a honest loop passes the packet directly from E to sink.

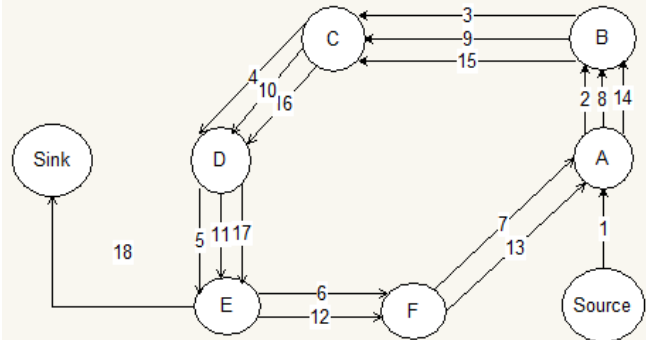

Fig. 1. Carousel attack

The second attack, Stretch attack, the malicious packet traverses all parts of the network. It also targets source routing. Here, an adversary constructs artificially long route, making the packet traverse all nodes of the network. We call this stretch attack, since it increases the packet length. So that the packets are to be processed by a number of nodes, regardless of the hop count along the shortest path between the adversary and packet destination.

Fig. 2 shows an example of stretch attack. Honest route is made solid. The last link to the sink is shared.

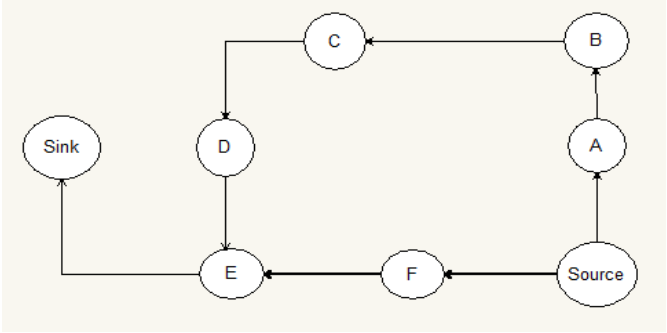

Fig. 2. Stretch attack

IV. MITIGATION METHODS FOR ENERGY ATTACKS

The carousel attack can be prevented entirely by having forwarding nodes check source routes for loops. But this adds extra forwarding logic and thus more overhead. The ns2 AODV protocol does implement loop detection, but does not use detection to check routes while forwarding packets. When a loop is detected, the source route can corrected and the packet moves further towards its destination, but one of the good features of source routing is that the route can itself be signed by the source node and destination node while sending Route Request Message (RREQ) and Route Reply (RREP). Hence, it is better to just drop the packet, considering that the sending node is likely malevolent i.e. honest node will not likely to introduce loops.

The other solution is to make some changes to show how intermediate nodes process the source route. To forward a message from source to destination, a node must determine the next hop and the id of the node can be attached with the packet, so that it can locate itself in the source route. Consider, if a node wants to search for itself from the destination but from backward instead from the source forward, any loop that includes the present (current) node will be automatically reduced. Therefore no further processing is required for this strategy. The stretch attack is more difficult to prevent as longest route for sending packets is way to drain energy from the sensor nodes. Its triumph rate relies on the forwarding node as no checking for optimality of the route is carried out. Some changes as specified in the header, Further; some loose source routing methods are defined, where intermediary nodes can replace some part or the entire route in the packet header if a better route to the destination so known.

This makes it necessary for nodes to notice and store optimal routes to at least some portion of other nodes, moderately defeating the as-needed discovery gain. Moreover, storing must be done carefully lest a maliciously suboptimal route be introduced. There are some algorithms proposed [16, 17], but there has been very little work on whether they could yield satisfactory results in the presence of adversaries. Alternatively bounding the damage of carousel and stretch attackers by limiting the allowed source route length based on the expected maximum path length in the network. But a way is needed to determine the network length. If the number of nodes is known ahead of time which are going to join the network, graph-theoretic techniques can be used to calculate approximately the diameter.

V. 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

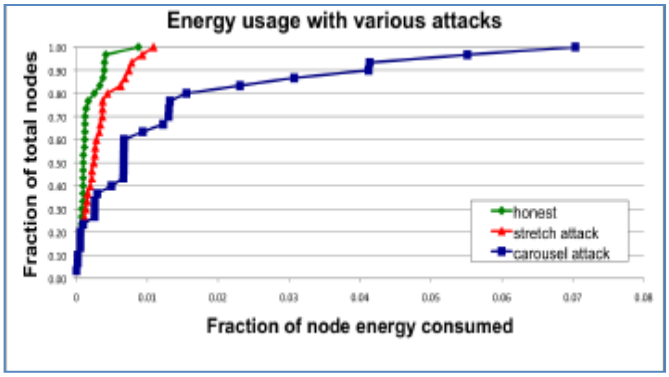

Fig. 3. Node energy distribution under various attack scenarios

VI. CONCLUSION AND FUTURE WORK

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.

ACKNOWLEDGMENT

The author would like to thank Dr. M. A. Pund for his valuable guidance and anonymous reviewers for their helpful comments on earlier draft of the work.

REFERENCES

[1] E Y Vasserman , N Hopper ,Vampire Attacks: Draining life from wireless Ad hoc sensor networks, IEEE Transactions on Mobile Computing, volume 12, issue 2 , Feb 2013.
[2] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.
[3] INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications2006.
[4] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.
[5] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on demand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 2006.
[6] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 2004.
[7] Sheetalkumar Doshi, Shweta Bhandare, and Timothy X. Brown, An on demand minimum energy routing protocol for a wireless ad hoc network, ACM SIGMOBILE Mobile Computing and Communications Review 2002.
[8] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.
[9] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003
[10] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, andScott F. Midkiff, Effects of denial-of-service attacks on wireless sensor network MAC protocols, IEEE Transactions on Vehicular Technology 2009.
[11] David R. Raymond and Scott F. Midkiff, Denial-of-service in wireless sensor networks: Attacks and defenses, IEEE Pervasive Computing 2008.
[12] Volkan Rodoplu and Teresa H. Meng, Minimum energy mobile wireless networks, IEEE Journal on Selected Areas in Communications 1999.
[13] 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. [14] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.
[15] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, Path-quality monitoring in the presence of adversaries, SIGMETRICS, 2008.
[16] Andrea J. Goldsmith and Stephen B. Wicker, Design challenges for energy-constrained ad hoc wireless networks, IEEE Wireless Communications 2002.
[17] R. Govindan and A. Reddy, An analysis of internet inter-domain topology and route stability, INFOCOM, 1997.
[18] Mina Guirguis, Azer Bestavros, Ibrahim Matta, and Yuting Zhang, Reduction of quality (RoQ) attacks on Internet end-systems, INFOCOM, 2005.
[19] J.L. Hill and D.E. Culler, Mica: a wireless platform for deeply embedded networks, IEEE Micro 2002.
[20] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, IEEE workshop on mobile computing systems and applications, 2002.

