IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. III (May-Jun. 2014), PP 08-13
www.iosrjournals.org

Vampire Attacks: Wearing Out Life of Wireless Adhoc Sensor Networks

Aruna M.G , Nivedita G Y
Associate Professor Department Of CSE M.S.Engineering College Bangalore
Department Of CSE M.S.Engineering College Bangalore

Abstract: *Ad-hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. More security work in this area has focused mainly on denial of service attack at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly decreasing nodes' battery power.These "Vampire" attacks are not specific to any particular protocol, We evaluate in this paper the protocols are Vulnerable 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. In proposed framework we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.*

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.

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 trust 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.

II. Objective

The projects main objective and 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.

Second,we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

III Realted work

Jing Deng, Richard Han, and Shivakant Mishra, Defending against Path-based DoS Attacks in Wireless Sensor Networks.

In this paper Denial of service (DoS) attacks can cause serious damage in resource constrained, wireless sensor networks (WSNs). This paper addresses an especially damaging form of DoS attack, called PDoS(Path-based Denial of Service). In a PDoS attack, an adversary overwhelms sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replayed packets or injected spurious packets. This paper proposes a solution using one-way hash chains to protect end-to-end communications in WSNs against PDoS attacks. The proposed solution is lightweight, tolerates bursty packet losses, and can easily be implemented in modern WSNs. The paper reports on performance measured from a prototype implementation.
While this strategy may protect against traditional DoS, where the malefactor overwhelms honest nodes with large amounts of data, it does not protect against "intelligent" adversaries who use a small number of packets or do not originate packets at all.

David R. Raymond and Scott F. Midkiff, Denial-of-service in wireless sensor networks:Attacks and defenses.

This survey of denial-of-service threats and countermeasures considers wireless sensor platforms' resource constraints as well as the denial-of-sleep attack, which targets a battery-powered device's energy supply. Here, we update the survey of denial-of-service threats with current threats and countermeasures.In particular, we more thoroughly explore the denial-of-sleep attack, which specifically targets the energy-efficient protocols unique to sensor network deployments. We start by exploring such networks' characteristics and then discuss how researchers have adapted general security mechanisms to account for these characteristics.

IV System Analysis

4.1 Existing System

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.

4.2 Limitation Of Existing System

- Power outages
- Due to Environmental disasters, loss in the information
- Lost productivity
- Various DOS attacks
- Secure level is low

4.3 Proposed System

In proposed system we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

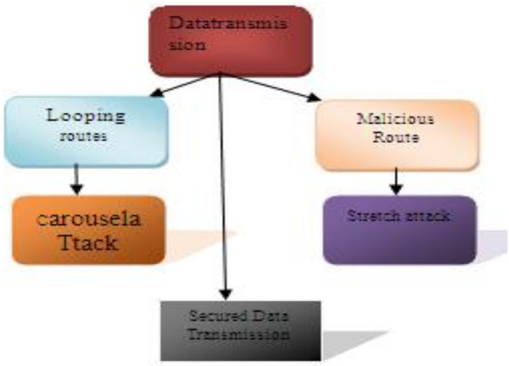
4.4 Advantages Of Proposed System

- Protect from the vampire attacks
- Secure level is high
- Boost up the Battery power

V System Design

In the below fig 5.1

- We have three modules i.e carousel,stretch,secure transmission.
- **Carousel Attack**:The packet will go in louping routes.
- **Stretch attack**:The packets will go in malicious route i.e long route path.
- **Secure Data Transmission**:The packets will go in shortest path.



VI Implementation

6.1 Network Creation Module

In this Module, we setup our Network model with Sink, Source and with Six nodes namely Node A, B, C, D, E, F. Each node will be assigned unique Identity number. And also 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 accss 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.

.

6.2 Carousel Attack Module

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. 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. In this attack, an adversary sends a packet with a route composed as a series of loops, such that 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

6.3 Stretch Attack

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. Results show that in a randomly generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage by up to asn order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overheard packets, we assume that only messages originated by adversaries may have maliciously composed routes.

6.4 Energy Level Identification Module

In this module, we show the energy level identification of each nodes to show the vampire attack reactions. A node is permanently disabled once its battery power is exhausted, let us briefly consider nodes that recharge their batteries in the field, using either continuous charging or switching between active and recharge cycles. In the continuous charging case, power-draining attacks would be effective only if the adversary is able to consume power at least as fast as nodes can recharge. Assuming that packet processing drains at least as much energy from the victims as from the attacker, a continuously recharging adversary can keep at least one node permanently disabled at the cost of its own functionality. However, recall that sending any packet automatically constitutes amplification, allowing few Vampires to attack many honest nodes.

6.5 Secured Transmission Module

In this module, we show the secured transmission done in the nodes by overcoming the vampire attacks. Where the data travels in the honest route and mitigating the vampire attacks

VII Results

7.1 Source Side:

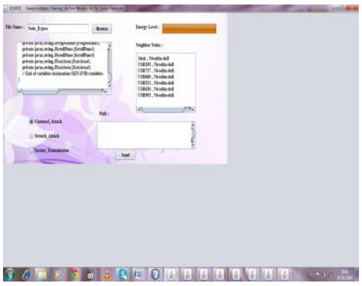


Fig 7.1: Source side frame

- The file which has to be sent.
- The neighbour nodes address
- At the start we can view that the energy level is full.

And the methods of transmission we can select,here we have selected the carousel attack

7.2 Simulation:

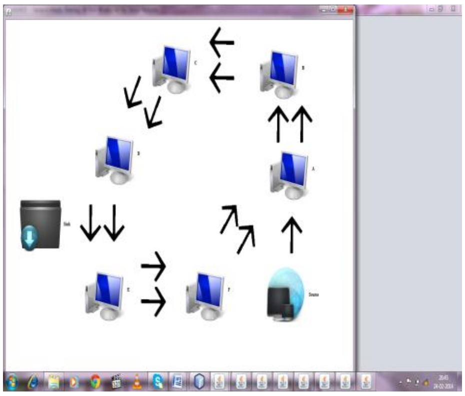


Fig 7.2:simulation

- It consists of a source and a sink.

It is simulating about the Carousel attack where in the packet is moving along loops.

7.3 Node D:

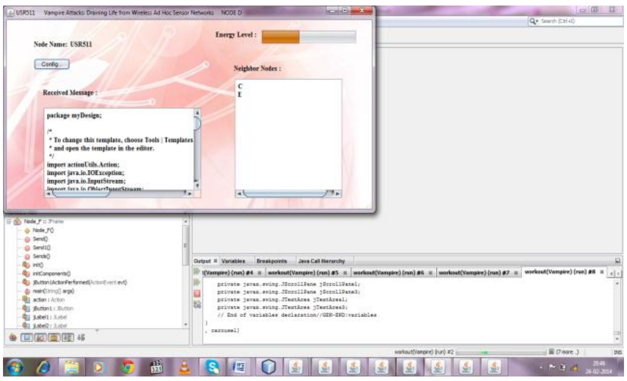


fig 7.3: Node D

- Node which contains the node name.
- We can see the file being transfered .
- The neighbouring nodes also are available when we click the configure button.
- The energylevel reduction due to carousel attack we can see here,the same is the case with all ather nodes.

7.4 Sink:

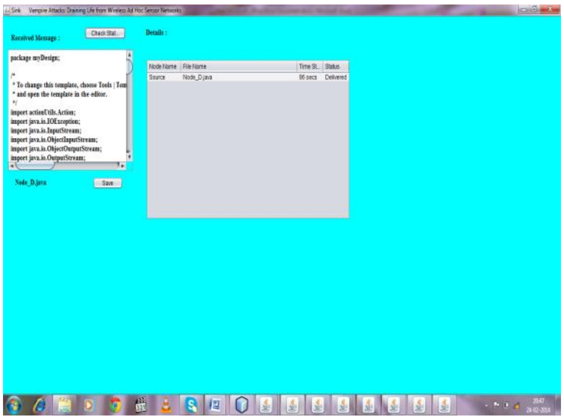


Fig 7.4 sink

- The message or the file being received.
- If we want we can also save the particular file.
- We can check the status in which the time taken by the source to send to the sink is given and along with that acknowledgement whether the file is delivered or not.

7.5 Performance Evaluation:

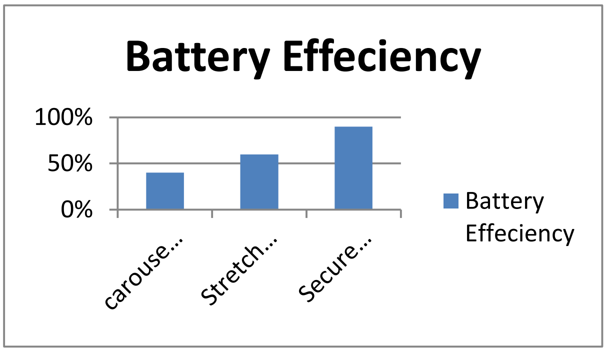


Fig 7.5 Battery efficiency

- The figure shows the battery efficiency of secure transmission around 95% efficient compared with carousel and stretch attacks

VIII Conclusion

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

References

[1] Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on security protocols, 1999.
[2] 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, IEEE Transactions on Vehicular Technology 58 (2009), no. 1.
[3] Jing Deng, Richard Han, and Shivakant Mishra, Defending against pathbased Dos attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.
[4] ImadAad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004. GergelyAcs, LeventeButtyan, and IstvanVajda, Provably secure ondemand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.
[5] Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.
[6] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.
[7] Daniel Bernstein and Peter Schwabe, New AES software speed records,INDOCRYPT, 2008.
[8] Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.
[9] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography,Vol. 265, Cambridge University Press, 1999.
[10] Joppe W. Bos, Dag Arne Osvik, and Deian Stefan, Fast implementations of AES on various platforms, 2009.
[11] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks,Computer 36 (2003), no. 10.

[12] Jae-Hwan Chang and LeandrosTassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12(2004), no. 4.
[13] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.
[14] Jing Deng, Richard Han, and Shivakant Mishra, Defending against pathbased DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.
[15] INSENS: Intrusion-tolerant routing for wireless sensor networks,Computer Communications 29 (2006), no. 2.
[16] SheetalkumarDoshi, ShwetaBhandare, and Timothy X. Brown, An ondemandminimum energy routing protocol for a wireless ad hoc network.
[17] David R. Raymond and Scott F. Midkiff, Denial-of-service in wireless sensor networks:Attacks and defenses, IEEE Pervasive Computing 7 (2008), no. 1.