International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Vampire Attacks: Draining Life from Wireless Ad-hoc Sensor Networks

Trupti Pawar[1], Jyoti Patil[2]

[1]M. Tech, Department of Computer Science & Engineering, Poojya Doddappa Appa College of Engineering & Technology, Gulbarga, Karnataka, India.

[2]Associate Professor, Department of Computer Science & Engineering, Poojya Doddappa Appa College of Engineering & Technology, Gulbarga, Karnataka, India.

Abstract: ***Ad-hoc low-power wireless 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 work explores resource depletion attacks, 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. Two types of vampire attacks are considered. In the carousel attack, attackers introduce some packet within a route as a sequence of loops and in the stretch attack, attackers construct falsely long routes. Whenever these two attacks are occurred the energy consumption is more as compared to the normal communication and data will reach very late to the destination. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. Mitigation method used in this work is based on time, that is time taken by carousel and stretch attacks is compared with the time of normal communication and if the time in both the attacks is greater, than the new path is formed. Results shows, that secured transmission is done in the nodes by overcoming the vampire attacks, where the data travels in the honest route by mitigating the vampire attacks.***

Keywords: Denial of service, security, routing, ad-hoc networks, sensor networks, wireless networks

1. Introduction

Ad-hoc mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access points. A wireless ad hoc network is a decentralized type of wireless network. The network is Ad-hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. 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. **Types of attacks**1.Denial of Service (DoS) attack 2. Reduction of Quality (RoQ) attacks 3.Routing Infrastructure attacks 4.Resource Depletion attack. 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 work Vampire attacks are considered, 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.

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. An Ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows, and a large Ad-hoc network quickly becomes difficult to manage. Ad-hoc networks cannot bridge to wired LANs or to the Internet without installing a special-purpose gateway. In addition to the classic routing, Ad- hoc networks can use flooding for forwarding data.

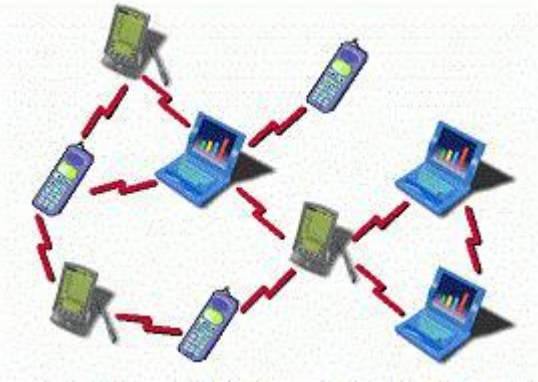

Figure 1.1: Wireless ad hoc network

This paper is organized as follows, section 1 discusses the introduction, section 2 describes related work. Section 3 details the system design and implementation. Section 4 presents the performance evaluations of our system design. Finally, section 5 presents some concluding remark.

2. 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.**GergelyAcs, LeventeButtyan, and IstvanVajdahad [2]** 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. 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.**Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly [3]** , 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. **Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig [4]**introduce a secure routing protocol authors design, implement, and evaluate a new secure routing protocol for sensor networks. The protocol presented 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. **Jae-Hwan Chang and Lindros Tassiulas [5]** had extended the maximum lifetime routing problem to include the energy consumption at the receivers during reception. In wireless sensor networks where nodes operate on limited battery energy, the efficient utilization of the energy is very important. One of the main characteristics of these networks is that the transmission power consumption is closely coupled with the route selection. **An article of computer communications [6]**, 29(2006),no 2, describes an INtrusion-tolerant routing protocol for wireless SEnsorNetworkS (INSENS). INSENS constructs forwarding tables at each node to facilitate communication between sensor nodes and a base station. It minimizes computation, communication, storage, and bandwidth requirements at the sensor nodes at the expense of increased computation, communication, storage, and bandwidth requirements at the base station. **Anthony D. Wood and John A [7],** Sensor networks hold the promise of facilitating large-scale, real-time data processing in complex environments. Their foreseeable applications will help protect and monitor critical military, environmental, safety-critical, or domestic infrastructures and resources. In these and other vital or security-sensitive deployments, keeping the network available for its intended use is essential. The stakes are high: Denial of service attacks against such networks may permit real world damage to the health and safety of people. **Jing Deng, Richard Han, and Shivakant Mishra[8],** 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 multi-hop end-to-end communication path with either replayed packets or injected spurious packets. **Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford [9],** Edge networks connected to the Internet need effective monitoring techniques to drive routing decisions and detect violations of Service Level Agreements (SLAs). Authors 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. **R.Govindan and A. Reddy [10],** The Internet routing fabric is partitioned into several domains. Each domain represents a region of the fabric administered by a single commercial entity. Over the past two years, the routing fabric has experienced significant growth.

3. Methodology

The objective of this work is to create a secure and time based mechanism which detects the vampire packets and prevents the forwarding of vampire packets and the formation of such type of packet inside the node**.**

3.1 Proposed System

This work makes four primary contributions .First, data is transferred through normal communication that is source nodes sends the route request packets and destination responds to them via shortest path. Second, during data transfer if there are routing loops between intermediate nodes then carousel attack has been detected. Third, if the route from source to destination is very long traversing many nodes in the network then the stretch attack has been detected.

Finally, the time taken to transfer the data in normal communication is compared with the time in the occurrence of both carousel and stretch attacks. If the time taken during attacks is more than time of normal communication then new path is chosen, which is free from attacks. In proposed system simulation results are shown quantifying the performance of both carousel attack and stretch attack. Then, existing route is modified to provably bound the damage from Vampire attacks during packet forwarding.

3.2 Modules

Network Creation and normal communication Module
In this Module, Network model is setup with 50 nodes namely node 1, 2, 3, 4, 5, 6 and so on. Each node will be assigned unique Identity number. Topology is discovered during an initial setup phase. 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.

Carousel Attack Module
In first attack, an adversary composes packets with purposely introduced routing loops. This is called as 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.

Stretch Attack Module
In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. This is called as 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. 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 an order of magnitude, depending on the position of the malicious node.

Energy Level Identification Module
In this module, the energy level identification is shown. A node is permanently disabled once its battery power is exhausted. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. When data is transferred through the normal path, the energy consumed by nodes is less but in case of carousel and stretch attacks it is more due to the series of loops and long paths. Hence these two attacks sends the little data with more energy.

Secured Transmission Module
In this module, results show that secured transmission is done in the nodes by overcoming the vampire attacks, where the data travels in the honest route by mitigating the vampire attacks. This module checks the delay to detect the attack.

3.3 Carousel Attack

In the carousel attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the route of communication many times. This attack increases the routing length and delay very much in the networks and also inadequate by the number of allowable entries in the resource route. This is the first type of vampires attack class in which the attacking nodes transmit the forgery report in to the network and this transmit in circled way. According to the figure it is clearly seen that source send the data packet which marked as 1to node A. Node A send it to node B. later on data packet transmitted to other nodes in the network. But instead of transmitting the data to source from node E it transmits to node F and again transmits to node A. This is done due to the corruptness nature of the data packet which is transmitting by compromised source. After three circles data send to sink after 18th round. Due to this heavy wastage of energy occur as shown in the figure 3.1.

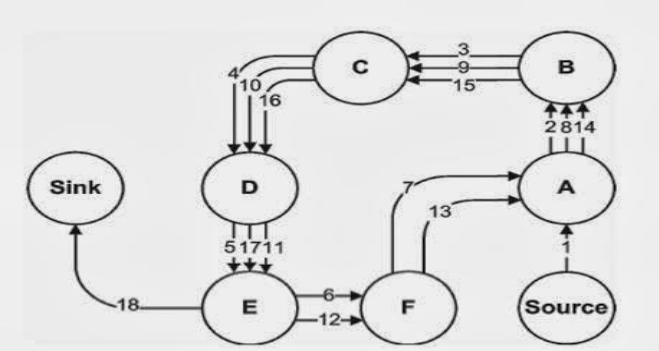

Figure 3.1: An honest route would exit the loop immediately from node E to sink, but a malicious packet makes its way around the loop twice more before exiting.

3.4 Stretch Attack

The stretch attack also targets resource steering, attackers construct falsely long routes, potentially traversing every node in the network. And also stretch attack, increases packet lane length, causing packets to be processed by a number of nodes that is self-governing of hop count down the straight path stuck between the challenger and packet target. In this type of attack, corrupt data packet chooses the longest routing path instead of shortest path. In this attack an attacker define long routes artificially, potentially lying across every node in the network. It is called as the stretch attack, since it increases data packet path lengths, causing data packets to be processed by a number of nodes that is independent of hop count along the shortest path between the source adversary and packet destination [1]. In the figure 3.2 the working of the stretch attack is illustrated by the given example. In this example it is shown that the network of eight nodes in this figure the honest route by dotted line and malicious route by dashed line, link node E to sink is same for both routing. In this attack those node waste its energy that do not belong to the honest routing path.

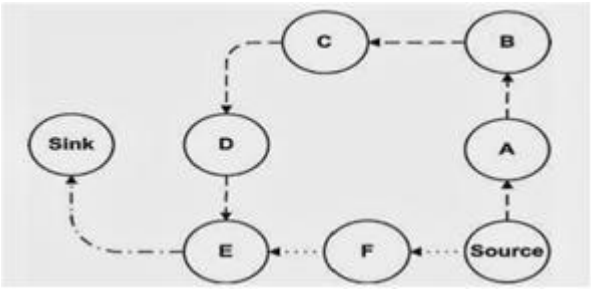

Figure 3.2: Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

3.5. Algorithm

Function forward_packet(p)
Step1:s ← extract_source_address(p);
Step 2:c ← closest_next_node(s);
Step3:if is_neighbor(c) then forward(p, c);
else
Step4:r ← next_hop_to_non_neighbor(c);
Step5:forward(p, r);
Function secure_forward_packet(p)
Step1:s ← extract_source_address(p);
Step2:a ← extract_attestation(p);
Step3:if (not verify_source_sig(p)) or
(empty(a) and not is_neighbor(s)) or
Step 4:(not saowf_verify(a)) then
return ; /* drop(p) */
foreach node in a do
Step5:prevnode ← node;
Ster 6:if (not are_neighbors(node, prevnode)) or
(not making_progress(prevnode, node)) then
Step7:return ; /* drop(p) */
c ← closest_next_node(s);
p′ ← saowf_append(p);
if is_neighbor(c) then forward(p′, c);
else forward(p′, next_hop_to_non_neighbor(c));

3.6 Flow Chart

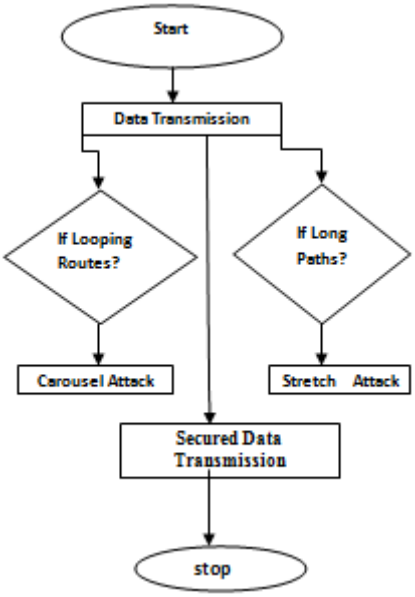

Figure 3.3: Flow diagram

4. Results

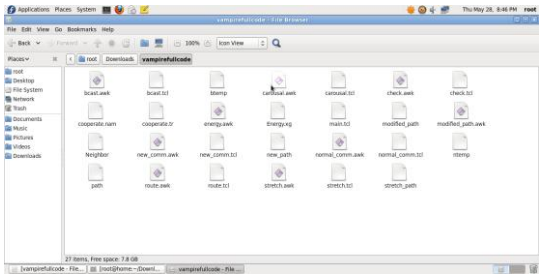

Figure 4.1: Above listed files are used to depict the results

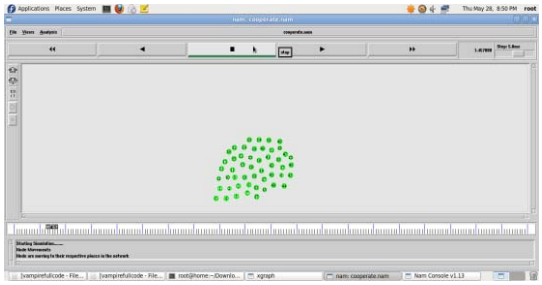

Figure 4.2: Nodes are moving to their respective places in the network

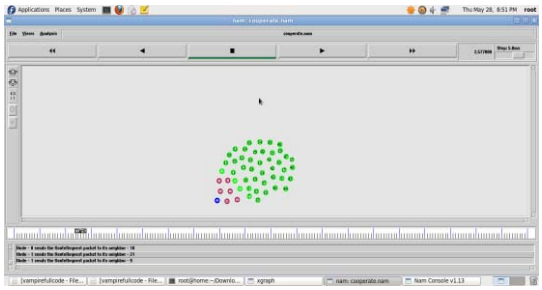

Figure 4.3: Source sends the route request packets to the neighbour.

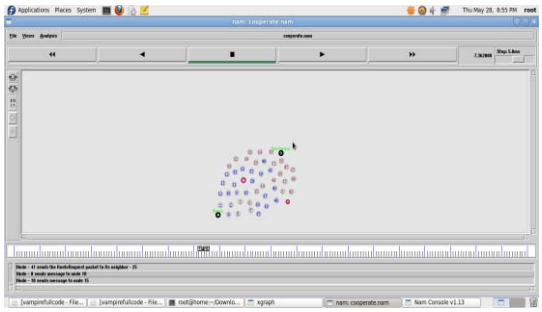

Figure 4.4: Nodes sends messages

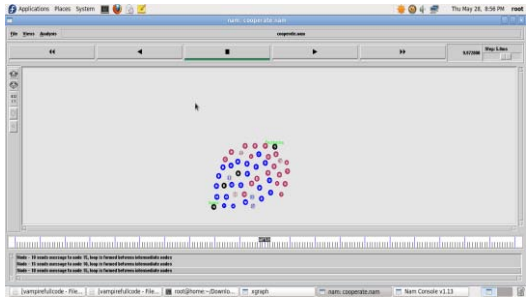

Figure 4.5: Loop is formed between intermediate nodes. (Carousel attack)

Figure 4.6: Long path is formed from source to destination. (Stretch attack)

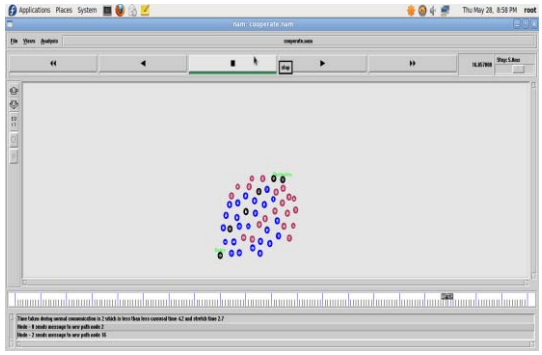

Figure 4.7: Time taken by carousel and stretch attacks is compared with the time of normal communication and if the time in both the attacks is greater, than the new path is formed.

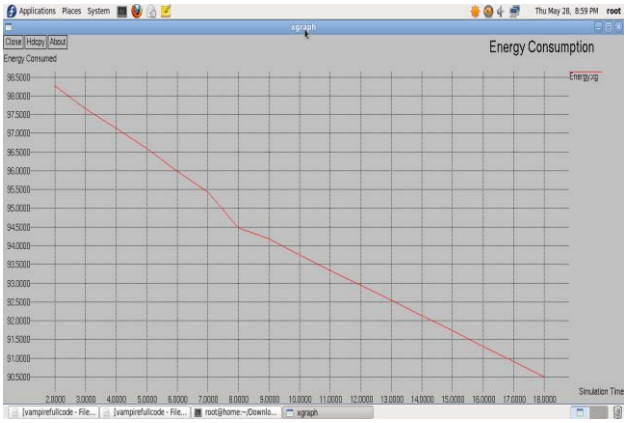

Figure 4.8: Energy consumption is more in the presence of carousel and stretch attacks

5. Conclusion

In this work Vampire attacks are defined, 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. There are many solutions and techniques that have been presented to prevent these attacks but were not effective enough which creates a need for a better solution. . Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power so the time based method is used, which gives satisfactory results as compared to previous works. In this method the time taken to transfer the data in normal communication is compared with the time in the occurrence of both carousel and stretch attacks. If the time taken during attacks is more than time of normal communication then new path is chosen, which is free from attacks.

References

[1] Eugene Y. Vasserman and Nicholas Hopper," Vampire attacks: Draining life from wireless ad-hoc sensor networks", University of Minnesota, IEEE.
[2] GergelyAcs, LeventeButtyan, and IstvanVajda, Provably secure ondemand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.
[3] ImadAad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.s
[4] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.
[5] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no. 4.
[6] INSENS: Intrusion-tolerant routing for wireless sensor networks, computer Communications 29 (2006), no. 2.
[7] Anthony D. Wood and John A. Stankovic, Denial of service in sensor networks, Computer 35 (2002), no. 10.
[8] Jing Deng, Richard Han, and Shivakant Mishra, Defending against pathbased
[9] DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.
[10] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, Path-quality monitoring in the presence of adversaries, SIGMETRICS, 2008.
[11] R.Govindan and A. Reddy, An analysis of internet inter-domain topology and route stability, INFOCOM, 1997.