**Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks**

**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 paper explores 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. 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. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

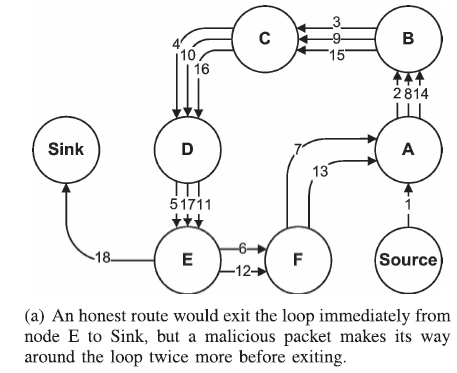
**Introduction**

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 shortterm 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’

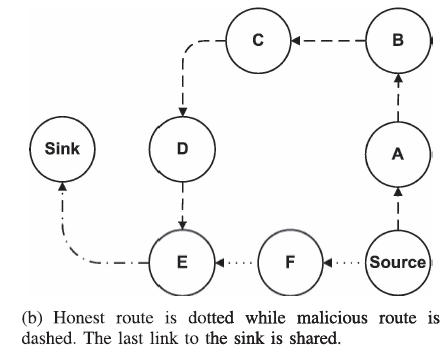
batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper, we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes.

we present a series of increasingly damaging Vampire attacks, evaluate the vulnerability of several example protocols, and suggest how to improve resilience. 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.

1. In our first attack, an adversary composes packets with purposely introduced routing loops. We call it the carousel attack



1. 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.



**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. 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. There are two types of attacks are occur carousel attack and stretch attack. 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. Brief mentions of this attack can be found in other literature but neither intuition for defense nor any evaluation is provided. 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.

**Disadvantages of Existing System:**

* Power outages
* Due to Environmental disasters, loss in the information
* Lost productivity
* Various DOS attacks
* Secure level is low
* They do not address attacks that affect long-term availability.

**PROPOSED SYSTEM:**

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

**Advantages of Proposed System:**

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

**System Requirement:**

**Hardware requirements:**

* Processor : Any Processor above 500 MHz
* Ram : 128Mb.
* Hard Disk : 10 GB.
* Compact Disk : 650 Mb.
* Input device : Standard Keyboard and Mouse.
* Output device : VGA and High Resolution Monitor

**Software requirements:**

* Operating System : Windows Family.
* Language : JDK 1.5
* Data Bases : Microsoft SQL Server
* Front End : Java Swing