ijecs
open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume - 3 Issue -9 *September*, 2014 Page No. 8143-8146

Switching attacks in wireless networks using denial of service phenomenon

Srinivas Kolli, B. V. Srikanth, Dr.P.Venkateswarlu
,m.tech(cse) college-nagole institute of technology and science,yderabad
mail-kollisreenivas@gmail.com
-associate professor college-nagole institute of technology and science,yderabad
head of the dept. cse college-nagole institute of technolog and science,yderabad

Abstract:

sensor networks offer eco- nomically viable solutions for a variety of applications. for example, current implemen- tations monitor factory instrumentation, pollution levels, free- way traffic, and the structural integrity of buildings. other applications include climate sensing and control in office buildings and home environ- mental sensing systems for tempera- ture, light, moisture, and motion. 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.

Index Terms—measurement, security.denial of service.

1 Introduction

edge networks connected to the internet need effective mon- itoring techniques to drive routing decisions and detect vi- olations of service level agreements (slas). however, ex- isting measurement tools, like ping, traceroute, and trajec- tory sampling, are vulnerable to attacks that can make a path look better than it really is. in this paper, we 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, inject- ing, or preferentially treating packets.application possibilities for miniature wire- less sensing devices include inventory asset tracking, roadside traffic pattern and open parking spot detection, individual plant monitoring for precision agriculture, habitat mon- itoring in nature preserves, and advanced building security and automation. the mili- tary could blanket fields with sensors to detect troop movement. sensors might enable civil engineers to gauge the structural integrity of buildings and bridges after earthquakes or fires. integrating hundreds of thousands of sensing and control points could provide new insights into the state of the world.

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.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 bound the damage from vampire attacks during packet forwarding

2 Workflows

A workflow is a depiction of a sequence of operations, declared as work of a person, work of a simple or complex mechanism, work of a group of persons, work of an organization of staff, or machines. Workflow may be seen as any abstraction of real work, segregated in workshare, work split or whatever types of ordering. For control purposes, workflow may be a view on real work under a chosen aspect, thus serving as a virtual representation of actual work. The flow being described often refers to a document that is being transferred from one step to another .

in our model, a source alice sends packets to a destination bob over a path through the internet. fixing a particular time period, which we call an interval, we define a packet delivery failure to be any instance where a packet that was sent by alice during the interval fails to arrive unmodified at bob before the the interval ends. an adversary eve can sit anywhere on the path between alice and bob, and we empower eve to drop, modify, or delay every packet or add her own packets. a path quality monitoring (pqm) proto- col is a protocol that alice and bob run to detect whether the number of failures during the interval exceeds a certain fraction of total packets transmitted. that masks packet loss by injecting an equal number of non- sense packets onto the data path.

while for the rest of this paper we will assume that 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.

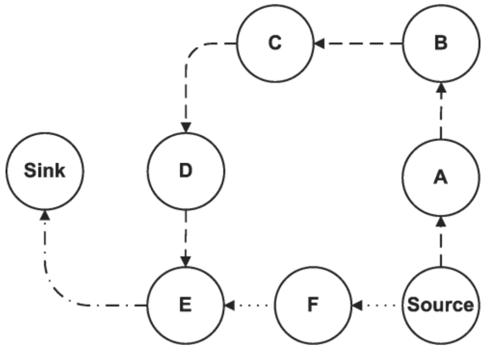
in this paper we consider the effect of vampire attacks on link-state, distance-vector, source routing, and geographic and beacon routing protocols, as well as a logical id-based sensor network routing protocol proposed by parno et al. [53]. while this is by no means an exhaustive list of routing protocols 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.

4 Related Works

the literature on path-quality monitoring typically deals only with the benign setting; most approaches either have the destination return a count of the number packets he receives from the source, or are based on active probing (ping, traceroute, [17,27,28] and others). however, both ap- proaches fail to satisfy our security definition. the counter approach is vulnerable to attack by an adversary who hides packet loss by adding new, nonsense packets to the data path. active probing fails when an adversary preferentially treats probe packets while degrading performance for reg- ular traffic, or when an adversary sends forged reports or acknowledgments to mask packet loss. even known pas- sive measurement techniques, where normal data packets are marked as probes, either explicitly as in ippm [17] or im- plicitly as in trajectory sampling [12] and psamp [16], are vulnerable to the same attacks as active probing techniques if the adversary can distinguish the probe packets from the non-probe packets (e.g., □ee [13] for attacks on psamp).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.

6 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 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 is 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 [29].



(b) Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

7. IMPLEMENTATION:

Implementation is the stage of the project wh theoretical design is turned out into a working s Thus it can be considered to be the most critical st achieving a successful new system and in givi user, confidence that the new system will work a effective.

The implementation stage involves careful pla investigation of the existing system and it's cons on implementation, designing of methods to a changeover and evaluation of changeover methods

Main Modules:-

data-verification

in data verification module, receiver verifies the path. suppose data come with malicious node means placed in malicious packet. otherwise data placed in honest packet. this way user verifies the data's.

denial of service

in computing, a denial-of-service attack or distributed denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users. although the means to carry out, motives for, and targets of a dos attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet.

user module

in user module, verify user and any time create a new path. in security purpose user give the wrong details means display wrong node path otherwise display correct node path.

8 Conclusions

Our system for private stream searching allows a range of applications not previously practical. In particular, 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.

10.References

1. tuomas aura, dos-resistant authentication with client puzzles, interna- tional workshop on security protocols, 2001.

2. john bellardo and stefan savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, usenix security, 2003.

3. thomas h. clausen and philippe jacquet, optimized link state routing protocol (olsr), 2003.

4. john r. douceur, the sybil attack, international workshop on peer-to- peer systems, 2002.

5. laura m. feeney, an energy consumption model for performance anal- ysis of routing protocols for mobile ad hoc networks, mobile networks and applications 6 (2001), no. 3