University at Buffalo The State University of New York | REACHING OTHERS

Whack-a-Mote: Simulating attacks on sensor network nodes and effects of compromised nodes

Edward Poon, Advisor: Dr. Shambhu Upadhyaya
The University at Buffalo Department of Computer Science and Engineering

Abstract

There are many potential applications for sensor networks. They can be deployed to monitor natural disasters, a patient's vital signs, detect intrusion, and alert the appropriate people ahead of time. Although sensor networks have a great deal of potential applications they are limited by their security: one compromised node can lead to the failure of the sensor network. This research focuses on attacks made on individual sensor nodes that comprise the sensor network. This poster illustrates how quickly a node can be compromised, as well as the effects of a compromised node within the network. This study also illustrates how the network reconfigures itself under these attacks.

Purpose of Sensor Network

- Monitors physical or environmental conditions, e.g., tremors, changes in temperature, light, speed, etc. and upon an event, sends data through the sensor network to a base station, such as a computer.

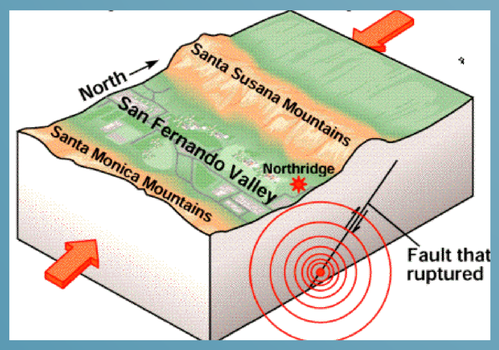
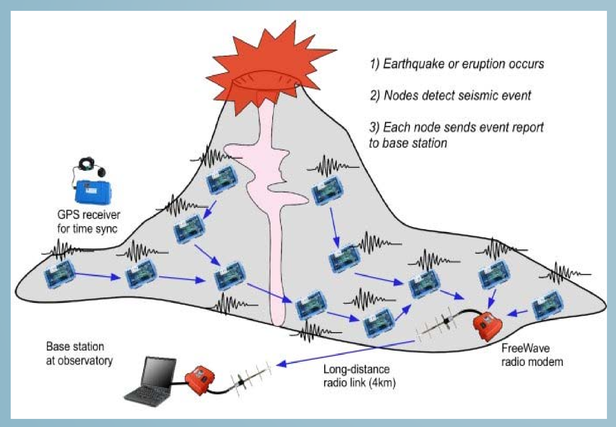


Image demonstrates tremor detection.



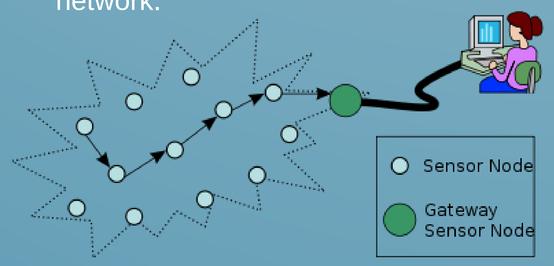
Vulnerabilities

Such vulnerabilities include but are not restricted to:

Black holes
Redundancy flooding
Exhaustion
Jamming
Tampering
Unfairness
Misdirection
Monitoring
Authorization

Motivation

- Although sensor networks can be deployed for detecting tsunamis, earthquakes, enemy encroachment, etc. they are vulnerable to attack.
- Therefore, we should analyze the vulnerabilities of the sensor network.
- We should also analyze the effects of a compromised node on the sensor network.



Objective

Whack-a-mote

- Create a network of sensor nodes to transmit a recorded message from one node to another down a line of nodes and eventually to a base station
- Use sensor boards to simulate a game similar to "whack-a-mole." We call this game "whack-a-mote." When a mote receives the packet of data it lights up, and that's when we "whack" it!
- Have sensor network reconfigure itself dynamically in order to function under these attacks.

Malicious node in the network

- This study sets up one node which acts as a malicious node and floods the network with ACK packets in a small interval of time.
- The period of flooding the network with ACK packets can be varied to find a threshold time that gives the "best" result.

Approach

Whack-a-Mote

- The network is set up in TinyOS and programmed in nesC.
- Used a distance vector routing protocol to send data packets over the network.
- Used an "event interrupt" that detected whacks and altered the network layout.
- Reconfigured the network by altering the routing table in order for the network to function under attacks.

Malicious node in the network

- The malicious node redundantly multicasts information to the network with varying amounts of data.

Expected Results

- As more and more people search for the nodes, the more likely it is for the nodes to be compromised.
- As more ACK packets are generated from the malicious node, the more detrimental it is for the network.
- The flood of ACK packets will drain the sensors' batteries as well as inhibit important messages from being sent to the base station.

Discussion

- Whack-a-mote used only one routing algorithm. Other routing algorithms should be explored and measured to determine which works best under attacks.
- For the malicious node, only a single node redundantly flooded the network. Future research should take into account other vulnerabilities such as misdirection, redundancy flooding by multiple sensor nodes, black holes, etc.

Acknowledgements

•Dr. Shambhu Upadhyaya
•Computer Science and Engineering Department.
•McNair Scholars Program

www.buffalo.edu