1 Introduction

When deployed to a disaster-stricken area, first responders need to be able to efficiently communicate their location and other information to their base camp. However, communication infrastructure is often unreliable or inaccessible during these crises. To solve this problem, we design an ad-hoc wireless network of portable devices that allows responders to send messages to their base camp in a reliable, efficient, and safe way. Our rigorous design accounts for the rapid changes in network topology that occur as the responders move around, as well as the possible presence of malicious agents in the field.

1.1 Design Overview

1.2 Tradeoffs and Design Decisions

2 Design

2.1 Routing tables

Initially, and every thirty seconds onwards, the network undergoes the following update procedure that discovers changes in the network topology:

- Each node issues one scan() message to populate its neighbor table.
- The base sends a route update broadcast() message to its neighbors, notifying them they are one hop away from the base. Each of these nodes updates their routing tables.
- Each of the neighbors from step 2 repeats that step themselves, aggregating the cost metric appropriately. Each node discards every broadcast() it receives after the first. This procedure continues until all nodes have received a broadcast, and takes time proportional to the diameter of the network.

The addition of new nodes to the network is also handled by this procedure. After this procedure, each node has multiple paths to the base and can begin using the metrics to estimate which paths are best.

2.2 Cost algorithm

2.3 Security

When designing a communication system for first responders, its important that first responders are able to trust the messages they are receiving from fellow first responders. Therefore it is important to establish a mechanism by which first responders can authenticate benign messages. In Our protocol, the base will use the RSA public-key cryptosystem to generate private and public-keys that it will the distribute to the first responders.

From here on, I will use the term node and first responders interchangeably.

At the initialization phase of the Ad-hoc network, all nodes are required that they first report to the base before departing. At this step of the protocol, each of the nodes will be assigned their own private-key. Furthermore, because at this step of the protocol the total size of the network is known, every node will be able to have an initial table with every public-key assigned so far. This will be quintessential for nodes capability of verifying messages.

The system should accept messages only from first responders. Therefore it will be very important that nodes sign their messages with their private-key.

Let: $Sk_A \ : \ denote\ the\ private - key\ of\ A$

$$\sigma_{Pr_A}()$$

3 Analysis

4 Conclusion

5 References