Anomaly detection and mitigation for disaster area networks

Jordi Cucurull (PhD), Mikael Asplund (PhD Student), Simin Nadjm-Tehrani (Full Professor)
Department of Computer and Information Science, Linköping University, SE-581 83 Linköping, Sweden

Abstract:

One of the most challenging applications of wireless networking are in disaster area networks where lack of infrastructure, limited energy resources, need
for common operational picture and thereby reliable dissemination are prevalent. In this work we address anomaly detection in intermittently connected mobile ad hoc networks in which there is little or no knowledge about the actors on the scene, and opportunistic contacts together with a store-and-forward mechanism are used to overcome temporary partitions. The approach uses a statistical
method for detecting anomalies when running a manycast protocol for dissemination
of important messages to k receivers. Simulation of the random walk gossip (RWG) protocol combined with detection and mitigation mechanisms is used to illustrate that resilience can be built into a network in a fully distributed and attack-agnostic
manner, at a modest cost in terms of drop in delivery ratio and additional transmissions. The approach is evaluated with attacks by adversaries that behave in a similar manner to fair nodes when invoking protocol actions.