Universidade Federal de Santa Catarina

Centro Tecnológico - CTC
Programa de Pós-Graduação em Ciência da Computação
Laboratório de Segurança de Redes - DMC-NS

On Self-Protection for Wireless Sensor Networks

Urian K. Bardemaker[1] **, João Bosco M. Sobral**
{uriank, bosco}@inf.ufsc.br
[1]bolsista do Programa de Ciência e Tecnologia da
Fundação Parque Tecnológico Itaipu - Brasil, PTI C&T/FPTI-BR

Abstract

Wireless sensor networks researches usually worry about things like quality of network coverage, leaving security issues beside, which eventually leave back-doors that can be exploited [1]. The problem of self-protection focuses on using its own sensors to protect themselves, the most important and critical objects in the network. In this work we will modify some algorithms for self-protection in order to apply an existing scenario with heterogeneous communication.

Self-Protection

Networks usually have a large number of distributed nodes and can be applied in monitoring, tracking, coordination and processing in different contexts. These sensors, however, can be attacked. An attack does not means that a sensor is physically removed, just a interference would work, and a smart intruder may strategically select weak sensors to amplify the effect [2].

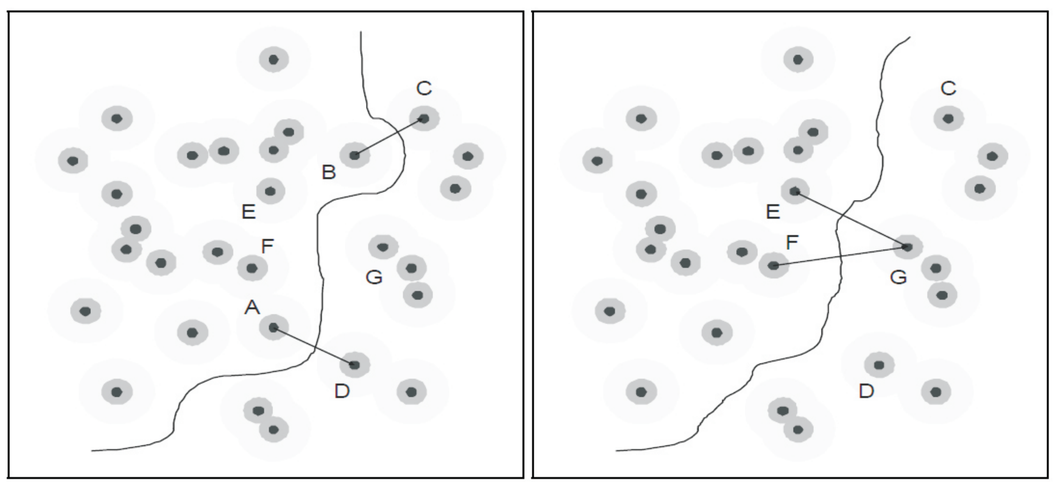

Fig. 1. (a) The maximal breach path in the network. The minimum weights are at (B, C) and (A, D). (b) By removing A and B, the weight of the maximal breach path is significantly increased. The weight of the maximum path is remarked between lines of E, G and F, G. [2]

In [2] Wang, Dan et. al. emphasize that the sensors are the most important and critical objects in the network, so they need protection. The authors believe that the sensors are the best (and often the only) candidates do protect themselves, and call it self-protection.

"In simple form, a sensor network is self-protected if all sensors are monitored/covered by at least one other active sensor." [2]

"A system that has the concept of self-protection built in, can detect possible attacks on the network and should also be able to protect itself" [4]

Scenario

We have an environment composed of a heterogeneous sensor network, which communicates via different protocols with the remote units. Remote units communicate via a link peer-to-peer with the redundant acquisition servers.

This scenario represents a system which collects the data in real time from RTUs, providing alarms and events. Additionaly identifies changes in the system state, obtained controlling the analog and digital variables.

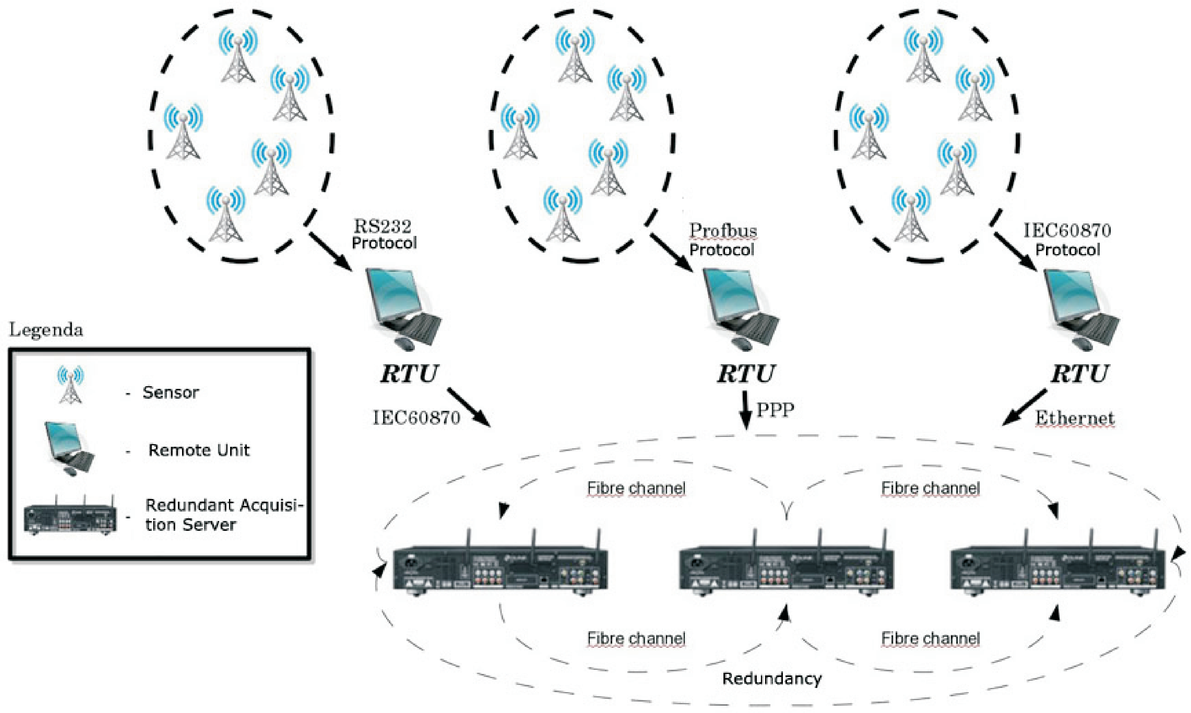

Fig. 2. Scenario: the network environment

Objectives

Develop a module for self-protection to sensor networks, applying the scenario, based on algorithms in [1] and [5], changing them according to the heterogeneous characteristics of the scenario

Create a model to be simulated, using an architecture, components and protocols, using representative sample spaces.

References

[1] W. Dan, Z. Qian, L.Jiangchuan. Self-Protection forWireless Sensor Networks
[2] Loureiro, Antonio A. F. et. al. Redes de Sensores Sem Fio
[3] D. Anirvan, B. Arijit and S. Indranil. Maximal Breach in Wireless Sensor Networks: Geometric Characterization and Algorithms
[4]White, S. et al. An architetural approach to autonomic computing
[5]C. Jibin, Z. Whenzhe, Y. Jiwen. Local Optimum Algorithms for self-protection in wireless sensor networks