RAHIM: Robust Adaptive Approach Based on Hierarchical Monitoring Providing Trust Aggregation for Wireless Sensor Networks

Nabila Labraoui
(STIC University of Tlemcen, Tlemcen, Algeria
labraouinabila@yahoo.fr)

Mourad Gueroui
(PRISM University of Versailles, Versailles, France
mourad.gueroui@prism.uvsq.fr)

Makhlouf Aliouat
(University of Setif, Setif, Algeria
m_aliouat@yahoo.fr)

Jonathan Petit
(University of Twente, Enschede, The Netherlands
j.petit@utwente.nl)

Abstract: In-network data aggregation has a great impact on the energy consumption in large-scale wireless sensor networks. However, the resource constraints and vulnerable deployment environments challenge the application of this technique in terms of security and efficiency. A compromised node may forge arbitrary aggregation value and mislead the base station into trusting a false reading. In this paper, we present RAHIM, a *reactive defense* to secure data aggregation scheme in cluster-based wireless sensor networks. The proposed scheme is based on a novel application of adaptive hierarchical level of monitoring providing accuracy of data aggregation result in lightweight manner, even if all aggregator nodes and a part of sensors are compromised in the network.

Keywords: Accuracy, Availability, Data aggregation, Monitoring mechanism, Wireless sensor networks, Security
Categories: C.2, C.2.3

1 Introduction

Wireless sensor networks (WSN) are rapidly emerging technologies with potentials for many different distributed applications, such as detection of chemical or biological agents, fire detection or tracking of enemy vehicles, which renders them a hot research topic over the past few years. However, sensor network has extremely constrained resources like energy, bandwidth and capabilities of processing and storing data. The current version of sensors such as mica2 [Corporation, 07] uses a 16 bits, 8 MHz Texas Instruments MSP430 microcontroller with only 10 KB RAM, 48 KB Program space, 1024 KB External flash, and is powered by two AA batteries.