Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 171 (2007) 71–81
www.elsevier.com/locate/entcs

Rijndael for Sensor Networks: Is Speed the Main Issue?[1]

Andrea Vitaletti[2]

Dipartimento di Informatica e Sistemistica
University "La Sapienza"
Rome, Italy

Gianni Palombizio[3]

Dipartimento di Informatica e Sistemistica
University "La Sapienza"
Rome, Italy

Abstract

We present an implementation of Rijndael for wireless sensor networks running on Eyes sensor nodes. In previous works, Rijndael has not been considered a suitable encryption algorithm for sensor nodes because it is too slow and requires a large space in memory, a precious resource in this environment. Our implementation of Rijndael is smaller, from about 1/3 to 1/5 of the size of previous implementations. Furthermore, we observe that nowadays MAC and routing protocols for wireless sensor networks, exhibit latencies up to few seconds, and thus the few milliseconds required by Rijndael to encrypt a TinyOS message are negligible if compared to these latencies. For this reason, in our opinion the main focus on the implementation of encryption algorithms for wireless sensor networks should move from speed, to memory occupation and energy efficiency.

Keywords: AES implementation, wireless sensor networks, performance evaluation

[1] Supported by EU Integrated Project AEOLUS (FET-15964) and MIUR-FIRB project VICOM.
[2] Email: Andrea.Vitaletti@dis.uniroma1.it
[3] Email: gpalombizio@etnoteam.it

1571-0661 © 2007 Elsevier B.V. Open access under CC BY-NC-ND license.
doi:10.1016/j.entcs.2006.11.010

1 Introduction

A wireless sensor network (WSN) is an ad-hoc wireless network made of sensor nodes which are able to monitor events (e.g. seismic activity, animals moving in a forest, enemies or intruders entering a monitored area, chemical agents), to process the sensed data and to communicate these data to a central node, the *sink*. The sink is a powerful base station which gathers data sensed in the network and either processes them or acts as gateway to other networks.

Sensor nodes are typically battery powered, making sensor networks highly energy constrained. Replacing batteries on hundreds or thousands of nodes, often deployed in inaccessible environments, is infeasible or too costly. Therefore, a key challenge in a wireless sensor networks is the reduction of energy consumption. For this reason most of the research in this field is focused on the development of energy efficient media access control (MAC) and routing algorithms.

Nevertheless sensor networks are becoming a cost-effective solution to a range of applications in critical domains. For example, after the recent terroristic events, there is a pressing need for the deployment of efficient and low-cost infrastructures for the detection of chemical or biological agents. When sensor networks are used in these security domains, besides energy efficiency, security become a strong and important requirement. Indeed these applications should not only timely detect a potential risk, but should also be protected from malicious attacks such as for example fake messages (i.e. an attacker injects malicious data which are erroneously interpreted by the system) or corrupted data (i.e. the attacker manipulate data in order to disguise the real information).

Motivation. Sensors are still some time away from actual mass fabrication and use.

Most of the current nodes, such as the Eyes node (`http://www.eyes.eu.org/`) or the TMote (`http://www.moteiv.com/`), typically run the TinyOS operating system, and are equipped with temperature and humidity sensors. They also support the installation of more advanced sensors such as microphones, accelerometers and motion sensors. However sensors for detecting biomedical data [12], explosives, radiation, chemical and biological toxins are becoming available. This paves the way for new and interesting applications. In [1] the authors study the environmental problems involving water quality and security. Clean waterways, and secure water supply are our best protection from communicable disease and the effects of chemical and biological contaminants either accidentally or intentionally released to our environment. Wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT) systems [2]. All the above applications have important security requirements.

Security features such as authentication, authorization and confidentiality (see [8] for an extensive discussion of the unique security challenges in Wireless Sensor Networks) can be implemented at two distinct network layers: *link layer* and *ap-*

Download English Version:

https://daneshyari.com/en/article/424157

Download Persian Version:

https://daneshyari.com/article/424157

Daneshyari.com