Ad Hoc Networks xxx (2012) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Survey Paper

Survey and comparison of message authentication solutions on wireless sensor networks

Marcos A. Simplicio Jr [a,*], Bruno T. de Oliveira [a], Cintia B. Margi [a], Paulo S.L.M. Barreto [a], Tereza C.M.B. Carvalho [a], Mats Näslund [b]

[a] Escola Politécnica – University of São Paulo, São Paulo, Brazil
[b] Ericsson Research, Stockholm, Sweden

ARTICLE INFO

Article history:
Received 3 February 2012
Received in revised form 29 April 2012
Accepted 31 August 2012
Available online xxxx

Keywords:
Survey
Benchmark
Message authentication
Security
Wireless sensor networks

ABSTRACT

Security is an important concern in any modern network. This also applies to Wireless Sensor Networks (WSNs), especially those used in applications that monitor sensitive information (e.g., health care applications). However, the highly constrained nature of sensors imposes a difficult challenge: their reduced availability of memory, processing power and energy hinders the deployment of many modern cryptographic algorithms considered secure. For this reason, the choice of the most memory-, processing- and energy-efficient security solutions is of vital importance in WSNs. To date, a number of extensive analyses comparing different encryption algorithms and key management schemes have been developed, while very little attention has been given to message authentication solutions. In this paper, aiming to close this gap, we identify cipher-based Message Authentication Codes (MACs) and Authenticated Encryption with Associated Data (AEAD) schemes suitable for WSNs and then evaluate their features and performance on a real platform (TelosB). As a result of this analysis, we identify the recommended choices depending on the characteristics of the target network and available hardware.

1. Introduction

Wireless Sensor Network (WSNs) can be seen as a especial type of ad hoc network composed by a large number of tiny, cheap and highly resource constrained sensor nodes, known as motes [1,2]. The sensors are distributed in the area of interest, and can then gather and process data from the environment (e.g., mechanical, thermal, biological, chemical, and optical readings). In this manner, they enable applications for environment and habitat monitoring, support for logistics, health care, emergency response, as well as military operations [3].

Sensors used in WSNs are typically battery-powered, which has motivated considerable research efforts on the development of energy-aware protocols, such as data link layer protocols (for a survey, see [4]). In general, one of the main goals driving the design of these schemes is to optimize network communications in order to save energy, and thus extend the network's lifetime. On the other hand, security is often (and sadly) considered at the very last step in the design of WSNs. Actually, most WSN deployments do not even consider security among their requirements because the execution and energy overheads it adds to the system is seen as an undesirable "extra cost" in such constrained environments. However, in WSN-based applications that monitor sensitive information, it is essential to prevent eavesdropping, which is typically obtained by means of encryption algorithms (e.g., symmetric ciphers). Even when the information acquired is not confidential, it is still necessary to ensure data integrity and authenticity

* Corresponding author.
E-mail addresses: mjunior@larc.usp.br (M.A. Simplicio Jr), btrevizan@larc.usp.br (B.T. de Oliveira), cbmargi@larc.usp.br (C.B. Margi), pbarreto@larc.usp.br (P.S.L.M. Barreto), carvalho@larc.usp.br (T.C.M.B. Carvalho), mats.naslund@ericsson.com (M. Näslund).

1570-8705/$ - see front matter © 2012 Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.adhoc.2012.08.011

Table 1
Hardware specification of some motes.

	Processor (MHz)	Code memory (KiB)	RAM (KiB)	Bandwidth (Kbps)
MICAz [13]	7.3	128	4	250
Mica2 [14]	7.3	128	4	38.4
FireFly [15]	7.3	128	8	250
TelosB [16]	8	48	10	250

by means of message authentication mechanisms. This happens because the acceptance of invalid data (generated either by natural causes or with malicious purposes) could lead to mistaken actions and severe consequences. Finally, given that such algorithms depend on the existence of secret keys for their functioning, applications need also to deal with the distribution of these keys.

To date, many security-oriented architectures have been proposed for WSNs. One of the most popular is TinySec [5], which provides link layer security in TinyOS [6], arguably the *de facto* standard operating system (OS) for sensor networks. TinySec provides two modes of operation: while TinySec-Auth provides only authentication, TinySec-AE also provides encryption functionalities. Another solution is SNEP (Secure Network Encryption Protocol), the component of SPINS (Security Protocols for Sensor Networks) [7] responsible for data confidentiality, two-party data authentication, and data freshness. There are also some more recent proposals such as the SenSec [8], MiniSec [9] and ContikiSec [10] architectures, which claim to provide similar security services with a lower energy consumption.

In spite of these advances, a main challenge in the security field is that the low resource availability inherent to WSNs still imposes several limitations on the type of cryptographic algorithms that can be effectively deployed in such environments. As shown in Table 1, motes usually have 48–128 KiB of code memory, 4–10 KiB of data memory (RAM) and are equipped with 8- or 16-bit processors operating at 7–8 MHz; the transmission bandwidth is also small, ranging from 38 to 250 Kbps. Moreover, messages exchanged between nodes are frequently small, a typical packet being between 30 and 60 bytes in length [11]. Finally, a mote constantly operating in active mode is expected to run out of batteries in about 72 h [12].

It is a well-known fact that transmission in WSNs consumes more energy than computation—1 bit transmitted may require the power equivalent to executing 800–1000 instructions [5]. Nonetheless, once the communication is already fully optimized, identifying and optimizing resource consuming tasks becomes the next natural step, and cryptographic algorithms usually play a crucial role in this context due to their expected complexity. Indeed, this is the motivation behind many extensive analyses available in the literature. Most of these studies have been concentrated on the efficiency of symmetric ciphers [17–22], hash functions [17,23] and asymmetric algorithms [24–27] on constrained platforms. However, and despite the fact that most security architectures rely on message authentication algorithms, only recently some attention has been given to another challenging subject [28]: message authentication. Specifically, Bauer et al. [29] evaluated the suitability of some AEAD (Authenticated-Encryption with Associated Data) schemes—solutions used in scenarios requiring both confidentiality and message authentication—in a MICAz [13] sensor node simulated using Atmel's *AVR Studio*. The conclusion of this study is that CCFB+H [30] is the best choice in scenarios where a solution such as TinySec-AE would be typically adopted. Aiming to provide a broader analysis, in [31] we presented a similar-purpose survey of AEAD schemes in a wider range of WSNs scenarios, showing that CCFB+H is actually not the optimal choice for applications with high security requirements.

In this paper we extend and complement our analysis in [31], considering not only AEAD solutions but also Message Authentication Codes (MACs).[1] The interest of analyzing the latter is that they are the most logical choice for applications where only authentication and integrity are required, while the former is the preferable when encryption is also required for data secrecy. Indeed, most security architectures for WSNs (e.g., TinySec, SenSec, Minisec and ContikiSec) give support for both types of scenarios. We develop both a theoretical analysis, comparing the design characteristics of each algorithm and its expected performance, and an experimental evaluation, considering their energy consumption, execution time, code size and RAM occupation. Our goal is not to propose a new authentication scheme but rather to identify the most prominent algorithms for different application scenarios, as done in previous WSN-oriented works for ciphers [17–22], hash functions [17,23] asymmetric algorithms [24–27] and AEAD schemes [29]. The results obtained should be useful for designers of security-sensitive sensor applications who wish to create more efficient solutions, and also for the creation of more efficient sensor-oriented security frameworks.

The remainder of this document is organized as follows. Section 2 discusses the usage of MAC and AEAD algorithms in the context of WSNs, further motivating our research. Sections 3 and 4 describe and analyze the features of the MAC and AEAD algorithms covered in this document, respectively. Our benchmark methodology is covered in Section 5, and the results obtained are discussed in Section 6. Based on these results, Section 7 presents some recommendations depending on the characteristics of the target application and platform. Finally, Section 8 presents our final conclusions.

2. Message authentication and sensor networks

Message authentication mechanisms ensure data integrity and authenticity by means of a key-dependent authentication tag of length τ. The presence of a secret key assures that only authorized users are able to create and verify those tags. The security of such algorithms is related to their resistance against forgery – the generation of a valid message-tag pair without knowledge of the secret key K, which is similar to generating collisions in hash-functions – and key-recovery attacks. Specifically, forgery attacks against a secure algorithms are expected to succeed after approximately $2^{\tau-1}$ attempts, while there should be no

[1] Not to be confused with the Media Access Control layer, also commonly abbreviated as MAC but not mentioned in this paper.