Journal of Network and Computer Applications 78 (2017) 216–230

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

Secure key design approaches using entropy harvesting in wireless sensor network: A survey

Amrita Ghosal[a], Subir Halder[a,*], Stefano Chessa[b]

[a] Department of CSE, Dr. B. C. Roy Engineering College, Durgapur, India
[b] Department of Computer Science, University of Pisa, Pisa, Italy

ARTICLE INFO

Keywords:
Channel impulse response
Information entropy
Randomness extraction
Received signal strength
Wireless sensor network

ABSTRACT

Physical layer based security design in wireless sensor networks have gained much importance since the past decade. The various constraints associated with such networks coupled with other factors such as their deployment mainly in remote areas, nature of communication etc. are responsible for development of research works where the focus is secured key generation, extraction, and sharing. Keeping the importance of such works in mind, this survey is undertaken that provides a vivid description of the different mechanisms adopted for securely generating the key as well its randomness extraction and also sharing. This survey work not only concentrates on the more common methods, like received signal strength based but also goes on to describe other uncommon strategies such as accelerometer based. We first discuss the three fundamental steps viz. randomness extraction, key generation and sharing and their importance in physical layer based security design. We then review existing secure key generation, extraction, and sharing mechanisms and also discuss their pros and cons. In addition, we present a comprehensive comparative study of the recent advancements in secure key generation, sharing, and randomness extraction approaches on the basis of adversary, secret bit generation rate, energy efficiency etc. Finally, the survey wraps up with some promising future research directions in this area.

1. Introduction

Due to the impetuous advancement of technologies in the last years, wireless sensor networks (WSNs) have become a reliable and mature technology, widely used in several applications ranging from industry to military and home. In a typical deployment, the sensors are battery-powered microsystems that embed a variable number of transducers to monitor their surroundings. The sensors also embed a wireless radio and form a wireless network autonomously, through which they communicate their sensed data. One or more sensor(s) in WSN are also connected to the internet or to other external networks, and act as gateways for forwarding the sensed data to remote users. In some applications, WSNs need to work unattended for long periods of time, either to reduce the costs of maintenance, or because they are deployed in hardly accessible (or even hostile) places. Furthermore, some of the sensors may be deployed on mobile objects (either robots, animals, vehicles etc.) and are thus mobile.

Despite their versatility and usefulness, WSNs are vulnerable to attacks. In particular, the broadcast nature of wireless communications used by the sensors make them highly prone to attacks by adversaries, for example, confidentiality or availability of sensed data may be breached. Therefore, providing security to WSNs has become an inevitable requirement of their design. On the other hand, this requirement is difficult to achieve due to the constrained resources of sensors in most applications leading to conventional security schemes being hardly applicable. As a matter of example, the use of asymmetric cryptography and authentication is a challenging task for very low power sensors.

A prime issue in security design of WSNs is generation of secret keys and their sharing because of the restrictions posed by the sensor nodes as mentioned earlier. On the contrary, as shown by the recent developments, the generation of secret keys may take advantage of the intrinsic randomness of the physical layer or environment in which the sensors operate. One of the most notable example is given by the received signal strength (RSS), which is an indicator commonly used in sensors' radios. In this case, the combination of a strong decorrelation of the wireless channel in time and space and the variability of the environment itself (for example due to the presence of moving people or objects) makes the RSS readings vary in an unpredictable way. This fact, combined with the reciprocity properties of the wireless channel makes a pair of RSS readings collected at the same time by two communicating sensors highly related as well as opens the way for a

* Corresponding author.
E-mail addresses: ghosal_amrita@yahoo.com (A. Ghosal), subir_ece@rediffmail.com (S. Halder), stefano.chessa@unipi.it (S. Chessa).

http://dx.doi.org/10.1016/j.jnca.2016.11.019
Received 25 February 2016; Received in revised form 18 September 2016; Accepted 17 November 2016
Available online 19 November 2016

number of methods that extract randomness from the RSS readings to generate secret keys (Barsocchi et al., 2013a, 2013b; Ali et al., 2012; Liu et al., 2012). These methods leverage on the reciprocity of the wireless channel to facilitate the key's sharing, and they rely on the unpredictability of the RSS fluctuations to make the keys hardly identifiable by other sensors. The measurements of RSS are however not the only potential source of randomness from which a sensor can leverage to create keys. For example, the sensors can exploit the on board transducers to extract randomness from the measurements of the surrounding environment (Wilhelm et al., 2013, 2010; Zhang et al., 2010; Hamida et al., 2009). Also, with these methods however, the issue is how to deal with the predictability of the measurements and how to share the keys that are generated.

In the existing literatures, a number of issues relating to channel reciprocity based key establishment technique are reviewed. Shehadeh and Hogrefe (2015), reviewed existing physical layer based secret key generation techniques. In particular, they reviewed mainly two types of secret key generation techniques, namely: (i) RSS based key generation, and (ii) channel impulse response (CIR) based key generation. In addition, they reviewed few latest key generation mechanisms such as random channel hopping based mechanism. Similar to (Shehadeh and Hogrefe, 2015), Wang et al. (2015) reviewed existing physical layer based key establishment techniques for wireless networks. However, unlike (Shehadeh and Hogrefe, 2015), the authors reviewed the existing works under three categories, namely: (i) quantization methods used to form secret key from wireless channel reciprocity, (ii) reconciliation and privacy amplification methods used to handle communication errors, and (iii) the feasibility and security issues related to channel reciprocity based key establishment techniques. In contrast to (Shehadeh and Hogrefe, 2015; Wang et al., 2015), our work differs from the previous efforts in terms of emphasis and comprehensiveness. In particular, the taxonomy of physical layer based security design approaches described in this survey is depicted using Fig. 1. We summarize our main contributions as follows:

- Initially, unlike (Shehadeh and Hogrefe, 2015; Wang et al., 2015), we classified the existing physical layer based security design issue into three categories, namely, secret key generation, sharing, and extraction. We then briefly discuss about the three fundamental steps i.e., generation, sharing, and extraction and their importance in the physical layer based security design.
- Unlike (Shehadeh and Hogrefe, 2015; Wang et al., 2015), we present the latest achievements on secure key generation, sharing, and randomness extraction approaches particularly in WSNs. Most importantly, unlike (Shehadeh and Hogrefe, 2015; Wang et al., 2015), we focus especially on the methods based on RSS, frequency selectivity, and CIR not only because these methods are more mature, but also present other methods that exploit the measurements obtained by the on-board transducers. We also discuss the pros and cons of the existing secure key design approaches.
- We present a comprehensive comparative study of the recent advancements in secure key generation, sharing, and randomness extraction approaches on the basis of number of parameters like type of nodes, adversary, secret bit generation rate, secret bit mismatch rate, energy efficiency etc.
- Finally, we identify the future research trends for the benefit of both general and expert readers.

This survey work is organized as follows. In Section 2, we briefly explain each of the three fundamental steps viz. randomness extraction, key generation and sharing and their importance in designing of physical layer based security mechanisms in WSNs. In Section 3, existing physical layer based security design methods are discussed; these include RSS measurement, frequency selectivity, and CIR measurements etc. Section 4, provides a broad picture of future research directions. Finally, the survey is concluded in Section 5.

2. Overview of physical layer based security design

The design of physical layer based security mechanisms for WSN involves three primary steps, i.e., key generation, randomness extraction, and sharing. Key generation refers to the different mechanisms that are implemented for efficient on-line generation of secret keys in WSN. Traditional approaches for key generation are not suitable for

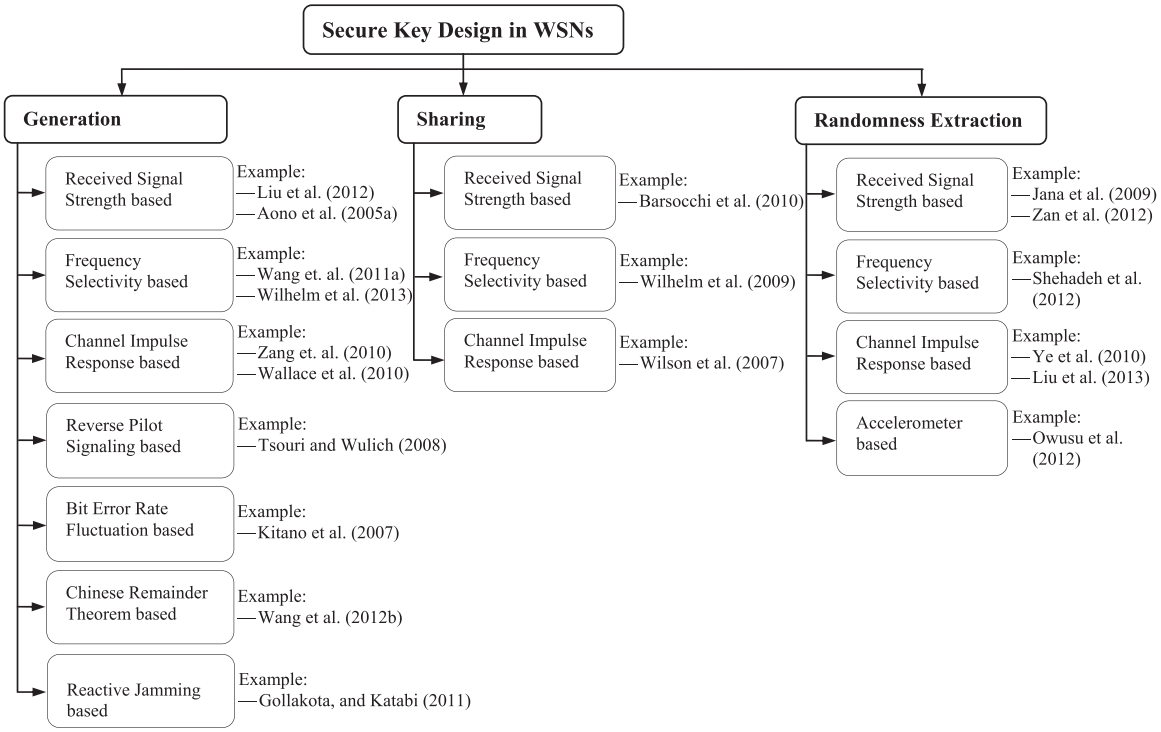

Fig. 1. Taxonomy of physical layer based security design approaches in WSNs.