Pervasive and Mobile Computing 22 (2015) 58–70

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Robust privacy preservation and authenticity of the collected data in cognitive radio network—Walsh–Hadamard based steganographic approach

Alsharif Abuadbba [a,*], Ibrahim Khalil [a], Mohammed Atiquzzaman [b]

[a] School of Computer Science and IT, RMIT University, Victoria, Australia

[b] School of Computer Science, University of Oklahoma, Norman, OK 73019-6151, USA

ARTICLE INFO

Article history:
Available online 16 February 2015

Keywords:
Steganography
Walsh–Hadamard
Security
Privacy preservation
Cognitive radio

ABSTRACT

Cognitive Radio Networks have recently attracted attention because of high efficiency and throughput performance. They transmit (1) repetitively collected readings (e.g. monitoring) and (2) highly confidential data (e.g. geometric location). However, the privacy and the authenticity of the transmitted data are major challenges. This paper proposes a novel steganographic technique that guarantees (1) strong end-to-end protection of the confidential information by hiding them randomly inside the normal readings using a generated key, and (2) robust evidence of authenticity for the transported readings. To expand hiding, the Walsh–Hadamard Transformation (WHT) is used to decompose normal readings into a set of coefficients. To achieve minimum distortion, only the least featured coefficients are used. To achieve high security, a key is used to reshape the coefficients into a random 2D *M*-by-*N* matrix and to generate a randomly selected order used in the hiding process. To accurately measure the distortion after hiding and extracting the confidential data, Percentage Residual Difference (PRD) has been used. It is obvious from experiments that our technique has little effect on the original readings ($<1\%$). Also, our security evaluation proves that unauthorized retrieval of the intended confidential information within a reasonable time is highly improbable.

1. Introduction

Recently, there has been a huge interest and an increase in the amount of remotely collected data [1]. The purposes of such collections can be monitoring environmental phenomena, battlefield scenarios, surveillance, manufacturing automation, traffic screening and remote healthcare. The data is mainly collected using Wireless Sensor Networks (WSNs) which consist of large numbers of small sensors that have limited computational capabilities and low battery power [2]. Commonly, the collected data are: (1) normal readings (e.g. environmental or monitoring data), and (2) highly sensitive information (e.g. IDs, battlefield geometric location or secret nuclear facility features). This information is periodically sent via a predetermined spectrum (e.g. 2.4 GHz). However, the extraordinary amount of transmitted data (e.g. continuous military surveillance) and the massive demand on the spectrum reservation result in wireless communications issues such as "spectrum scarcity" [3].

To overcome these issues, a new wireless communication technology called Cognitive Radio (CR) has emerged [4]. It deploys a simple idea where the licensed spectrum can be shared by a Secondary User (SU) whenever the Primary User

* Corresponding author. Tel.: +61 469331050.
E-mail addresses: alsharif.abuadbba@rmit.edu.au (A. Abuadbba), ibrahim.khalil@rmit.edu.au (I. Khalil), atiq@ou.edu (M. Atiquzzaman).

http://dx.doi.org/10.1016/j.pmcj.2015.02.003
1574-1192/

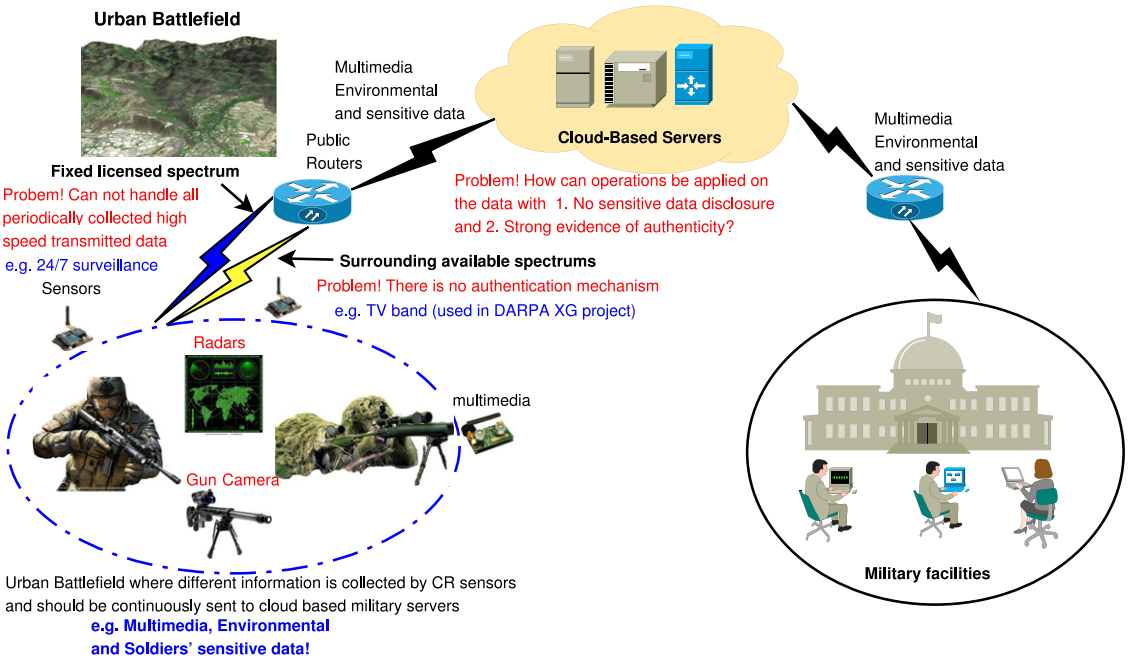

Fig. 1. Main issues faced when different information (e.g. environmental, multimedia and soldiers sensitive data) are periodically collected by CR sensors in a battlefield area and should be sent to cloud-based servers for authorized management.

(PU) is idle (i.e. white space). CR allows SU to sense the licensed bands and whenever the space is white, SUs can utilize these bands to improve the communication performance, throughput and reduce the interference between the applications that use the identical or overlapping bands such as Bluetooth and ZigBee at 2.4 GHz [5]. Therefore, tremendous efforts are currently being spent to develop various standardizations to exploit this opportunity. For example, a Defence Advanced Research Projects Agency (DARPA) project called neXt Generation (XG) is focused on how unused spectrum (e.g. TV band) technologies can be utilized for US military applications [6,7]. Also, CR technology has recently been implemented in various sets of applications such as medicine and traffic screening [8–10]. Despite the obvious advantages, CR Networks (CRNs) cause many security issues in addition to the traditional WSN troubles which can be categorized as follows.

1. The confidentiality and the privacy of the transmitted sensitive content (e.g. soldiers' sensitive and geometric locations).
2. The authenticity and the integrity of the collected normal readings because of the CR sensors' presence in hostile areas and the possible—natural or malicious interference.

Although these problems have been discussed in traditional WSNs, we are compelled to target these issues in a CRN context because: (1) they are rarely targeted in today's management model where the data is stored and processed by third parties' machines (i.e. Cloud Providers CPs), and (2) in using CRN technology, the data may be sent in a spectrum that has no authentication mechanism (e.g. TV broadcasting [11]) as in the XG project (See Fig. 1). Therefore, this paper proposes a novel solution for these issues based on the following questions:

- How can the transmitted sensitive information be protected without disrupting any possible operations at data aggregators and CPs?
- How can the authenticity and the integrity of the transmitted normal readings be checked, especially if the data are sent in a spectrum that has no authentication mechanism, such as a TV band?
- Can both requirements be met without revealing the sensitive information to CPs?

To solve these issues, most of the early solutions relied heavily on traditional cryptography techniques such as symmetric, asymmetric and digital signature [12–18]. However, they suffer from two main limitations.

- The huge delay and overhead of these approaches that result from thousands or millions of mathematical operations in order to achieve high security, which usually cannot be handled by existing CR sensors' capabilities (i.e. memory and power).
- Changing the form of all original data into a ciphertext makes applying operations on the data more difficult at aggregators (i.e. where the transmitted data may be collected and compressed) and CPs.

To solve some of traditional cryptography issues, a recent non-traditional cryptography technique called homomorphism has been used [19–21]. The advantage of this technique is that the encrypted data can be worked on at data aggregators and CPs without revealing its meaning and thus provides a strong end-to-end security. However, homomorphic techniques are still not feasible in practical applications because their computational operations are very complex [22].