Ad Hoc Networks 41 (2016) 30–46

Contents lists available at ScienceDirect

Ad Hoc Networks

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

# Resilient to shared spectrum noise scheme for protecting cognitive radio smart grid readings – BCH based steganographic approach

Alsharif Abuadbba [a,*], Ibrahim Khalil [a], Ayman Ibaida [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:*
Received 15 June 2015
Revised 31 October 2015
Accepted 2 November 2015
Available online 10 November 2015

*Keywords:*
Steganography
Wavelet
Security
Privacy preservation
Error detection and correction
BCH

ABSTRACT

Cognitive Radio smart grids have recently attracted attention because of high efficiency and throughput performance. They transmit (1) periodically collected readings (e.g. monitoring) and (2) highly sensitive data (e.g. geometric location). However, robustness, efficiency and security of the transmitted data compose an unaddressed unique challenge due to CR shared spectrum possible noise. This paper proposes the first novel hybrid model that combines advanced steganographic algorithms with error detection and correction techniques (BCH syndrome codes) in the CR smart meter context. This will allow us to (a) detect and recover any loss from the hidden confidential information without privacy disclosure, and (b) remedy the received normal readings by using the corrected version of the secret hidden data. To randomize hiding and minimize the distortion, 3D wavelet is used to decompose normal readings into a set of coefficients. To strengthen the security, a key is utilized to generate a 3D randomly selected order used in the hiding process. To accurately measure the detection and recovery capabilities, random noise levels are applied to the transmitted readings. The recovered sensitive information and stego readings are extensively measured using BER, PRD and RMS. It is obvious from the experiments that our technique has robust recovery capabilities (i.e. BER = 0, PRD < 1% and RMS < 0.01%).



## 1. Introduction

The classic power grid of the past 100 years is now regarded as ill-suited to the 21st Century requirements for many reasons such as outage management deficiency, lack of automated and real-time analysis [1,2]. Consequently, a new infrastructure called smart grid has presently emerged and can be used to automatically gather periodic readings (i.e. using smart meters) every second or minute (e.g. power consumption and environmental characteristics of the premise) and transmit them to operational centers using various techniques [3,4]. The significant benefits are improved efficiency (e.g. automated outage management), accuracy (e.g. continuous-dynamic electricity distribution) and sustainability (e.g. climate change mitigation). However, the unusual amount of the continuous transmitted data (i.e. from millions premises) and the enormous demand on the spectrum reservation results in wireless communications issues such as spectrum scarcity [5].

To solve these issues, a new wireless communication technology called Cognitive Radio (CR) has emerged [6,7]. The basic idea is that the licensed spectrum for various parties (e.g. premises) can be shared by Secondary Users (SU) whenever the Primary User (PU) is idle (i.e. white space). The main purposes are (1) improving the communication

* Corresponding author. Tel.: +61469331050.
*E-mail addresses:* alsharif.abuadbba@rmit.edu.au, shareef_6606@yahoo.com (A. Abuadbba), ibrahim.khalil@rmit.edu.au (I. Khalil), ayman.ibaida@rmit.edu.au (A. Ibaida), atiq@ou.edu (M. Atiquzzaman).

http://dx.doi.org/10.1016/j.adhoc.2015.11.002
1570-8705/

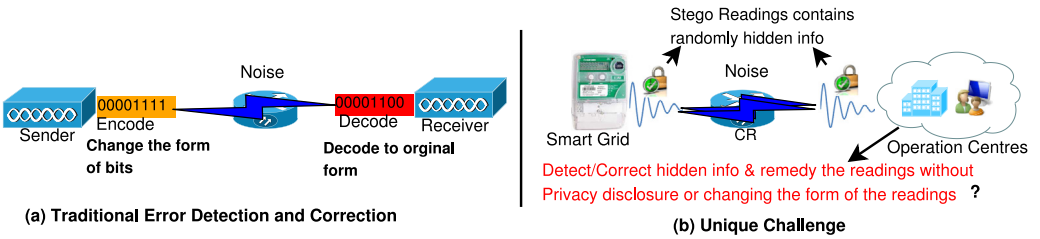


**Fig. 1.** The main unique challenges that highlight the contribution of this paper.

performance and throughput, and (2) reducing the interference between the applications that use the identical or overlapping bands (e.g. Bluetooth and ZigBee at 2.4 GHz) [8–10]. Therefore, tremendous efforts are currently made to exploit this opportunity in the smart grid context [11–15]. Despite the obvious advantages, CR smart grids cause many security and robustness issues due to sharing the transmission spectrum [16,17].

Recently, a widely-known technique in multimedia domain called steganography has been exploited to ensure the privacy without changing the form of the transmitted readings such as in models [18–20]. Steganography can protect the sensitive information where a piece of secret message is hidden inside host data and can only be retrieved by authorized users. However, due to shared spectrum characteristics in CR mechanism where PUs and SUs are sharing the same band simultaneously, the transmitted data are highly prone to an intentional (i.e. interference) and unintentional (i.e. noise) attacks rendering the existing solutions impractical [14]. This is simply because any slight change in the transmitted stego form of readings will result in (1) loss of hidden information (e.g. household sensitive data) and (2) more significantly, loss of faith in the received readings. However, (i) it may be too late to ask the source to resend especially in critical cases, (ii) the source is often configured to forget what it sends directly (i.e. due to resource constraints), and (iii) the destination has no return channel to the source. In an extreme case, this may happen to million premises the same day!.

To overcome the deficiencies of the aforementioned models, we are compelled to address the following questions (See Fig. 1).

1. How can any change in the hidden secret information be detected and recovered?
2. Can the recovered secret information be used to remedy the received collected CR smart meter readings?
3. Can both requirements be met without revealing the sensitive information (i.e. to cloud providers) or changing the form of the transmitted readings?

### 1.1. Contribution

- To the best of our knowledge, it is the first novel hybrid model that combines advanced steganographic algorithms with error detection and correction techniques (BCH syndrome codes) in the context of CR smart meter. This will allow us to (a) detect and recover any loss (i.e. due to CR shared spectrum noise) from the hidden confidential information without privacy disclosure, and (b) remedy the received normal readings by using the corrected version of the secret hidden data. Both cases have been examined carefully and highlighted in Section 5.
- To the best of our knowledge, it is the first model that strengthens the security of hiding and increases the randomization into 3D level using a fast signal processing technique called 3D Discrete Wavelet Transform (DWT).
- The integration of BCH with advanced steganographic algorithms highlighted a new finding (highlighted in Section 5), which is that by simply integrating error detection and correction techniques with most of previously proposed steganography algorithms that use the widely-known hiding positions -Least Significant Bits LSB will fail to recover the corrupted hidden bits. Therefore, the hiding positions and coefficients are chosen carefully to achieve the best BER (i.e. the recovery accuracy of the hidden secret information) and PRD/RMS (i.e. the remedy precision of the normal readings). This has been examined thoroughly and presented in Section 5 after monitoring the PRD, RMS and BER results with various ranges of hiding positions.

In our model (See Fig. 2), CR smart meters will be used to collect different normal readings from the customer premise (e.g. watts consumption, heating-index, inside/outside temperature and humidity). Customer secure information (e.g. grid ID, geometric location, name, DoB, address and total power consumption) will be then encoded (i.e. using BCH syndrome codes) and randomly hidden inside the normal readings. Finally, the stego normal readings are transmitted to the remote operational centers via CR shared spectrum. Consequently, the real-transmitted data size is only the size of the normal readings with no additional overhead, because the encoded confidential information are embedded inside them. The stego readings that contain the hidden information will be stored at operational centers. However, only authorized users can retrieve the secret encoded information from the stego normal readings (i.e. using an appropriate key), detect and recover any alteration to them (i.e. due to possible CR interference) as well as remedy the stego form of readings. On the other hand, others (including offshore cloud based servers) can only see the stego form. The second advantage is that, based on our experimental results, even the stego CR smart meter readings can be cured and so there is no need to resend the stego whenever the data is corrupted.

The rest of this paper is organized as follows. Section 2 summarizes the relevant work. Section 3 presents our algorithm and its preliminaries. Then, evaluation of different characteristics of the proposed technique is introduced in