Pervasive and Mobile Computing 22 (2015) 3–15

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Secure and reliable surveillance over cognitive radio sensor networks in smart grid

Uthpala Subodhani Premarathne [a,*], Ibrahim Khalil [a], Mohammed Atiquzzaman [b]

[a] National ICT for Australia (NICTA), School of Computer Science, RMIT University, Melbourne VIC 3001, Australia

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

ARTICLE INFO

Article history:
Available online 19 May 2015

Keywords:
Smart grid
Cognitive radio sensor networks
Authentication

ABSTRACT

In view of recent attacks on smart grid surveillance is of vital importance to enforce surveillance based disaster recovery management operations to ensure seamless energy generation and distribution. The reliability of disaster recovery management depends on availability and privacy preservation of surveillance data. In this paper we propose a reliable privacy preserving smart grid surveillance architecture over cognitive radio sensor networks. Cognitive radio sensor networks are capable of facilitating reliable communications through opportunistic spectrum sensing capabilities as opposed to fixed radio terminal networks based surveillance architectures. The main privacy preserving feature is a novel energy aware physical unclonable function (PUF) based cryptographic key generation method. The proposed solution determines the encryption key length depending on the remaining energy reserve to facilitate data transmission over an expected period of time with minimum channel interferences. Based on the experimental evaluation, the PUF pattern matching based key generation is viable for 32 bits pattern length over a cognitive radio sensor with optimum power utilization and with a probability of reproducibility of a bit pattern $(i - p) = 0$. We have also performed experiments to validate the reliability model using real-world data. In conclusion, our proposed cognitive radio sensor based solution provide more pragmatic insights in reliability assurances for surveillance in smart grid.

1. Introduction

A large portion of communication infrastructure of smart grid uses wireless communications. Cognitive radio (CR) networks are considered as promising solutions for efficient wireless communications in smart grid [1,2] due to several advantages: (i) to reduce radio frequency interference from power equipment and packet collisions in wireless communications links, (ii) to reduce delays in communications by employing vacant channel bandwidth and can (iii) cater to the large scale distributed communication needs of smart grid [1].

Surveillance based emergency resilience [3] is vital in smart grid in order to support self healing mechanisms [4], to facilitate seamless operations and to execute reactive or preventive measures in situation aware collaborative disaster response management [5]. In addition, due to the growing number of physical attacks on smart grid, multimedia surveillance is vital to provide adequate security to ensure reliable operations of critical smart grid components [6–9].

* Corresponding author.
E-mail addresses: uthpala.s.p@gmail.com, s3308412@student.rmit.edu.au (U.S. Premarathne).

http://dx.doi.org/10.1016/j.pmcj.2015.05.001
1574-1192/

1.1. Motivation

Motivation for this research comes from the recently reported malicious attacks on smart grid, and growing number of location-privacy violations aimed to disrupt seamless operations.

- Physical security of smart grid power generation equipment and components—Attack on Pacific Gas & Electrics (PG&E) substation in California last April raise questions about the vulnerabilities of physical security of the US power grid [6]. The assault took place in the middle of the night when at least one person entered an underground vault at PG&Es Metcalf substation and cut fiber cables. Soon after, one or more gunmen opened fire on the substation for nearly 20 min. They took out 17 transformers and then slipped away into the night before police showed up.
- Physical security of smart meters—In 2009 an electric utility in Puerto Rico asked them to help investigate widespread incidents of power thefts that it believed were related to its smart meter deployment [5]. The FBI discovered that former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash. Presumably, they hacked into the meters using an optical serial port that allowed them to connect their computers locally and change the settings for recording power consumption. They just needed a software program that could be directly downloaded from the Internet.

In addition, reliability of surveillance based disaster recovery management requires sufficient data availability to detect anomalous events, secure data generation and transmission. Therefore, to ensure the ability for a sensor to securely generate data over an expected time period is vital.

Ramifications of the above facts are to have a robust surveillance system to reduce the impact of malicious physical attacks on smart grid, reliable data communications and privacy preservation of surveillance sensor data.

1.2. Need for cognitive radio sensor networks (CRSN) for surveillance

The main objective of surveillance systems is the ability to monitor critical assets remotely without physically being present at each asset. In the context of smart grid, wireless multimedia sensor networks are of great value in providing rich surveillance information for failure detection and recovery, energy source monitoring and management as well as physical security of grid components [8]. Distributed situation awareness helps to better coordinate and strategic implementation of disaster response and emergency management in order to reduce outages and damage containment to facilitate seamless and efficient service delivery [10,11]. Reliability of decision making in disaster response and emergency management depends on the availability and privacy preservation of surveillance data.

- Ability to offer reliable communications—Existing surveillance systems are based on fixed radio access technology (RAT) [12]. However, the reliability is less in fixed RAT systems due to signal losses, power losses, hardware unavailability due to theft or damaged due to natural disasters (e.g. floods, hurricanes) [12]. Thus, CRSN can facilitate more *reliable communications* by using opportunistic spectrum sensing capabilities which are not feasible to achieve through wireless sensor networks.
- Energy-aware secure surveillance data transmission—Unlike conventional wireless sensor networks, a CRSN is composed of CR sensors which are capable of more opportunistic spectrum sensing capabilities in addition to the other computational operations such as data encryption. Energy expenditure is an important consideration for surveillance applications in order to securely transmit the surveillance data over a sufficiently long period of time. Therefore, energy-aware data encryption solutions are vital for CRSN based surveillance applications in order to guarantee data transmissions over a sufficiently long period of time.

The main objective of our research is to analyze the reliability guarantees for enforce disaster recovery management effectively in terms of (i) secure surveillance data transmission and (ii) persisted data transmission over an expected period of time.

1.3. Limitations of existing work

In applications using sensors, node identity concealment and cryptographic techniques are seen as viable solutions to preserve the location privacy of sensor nodes [13]. In cognitive radio networks, reputation (or trust) based node evaluation methods [14–16], collaborative sensing coupled with anonymity techniques or cryptographic methods [17] are proposed as viable solutions for preserving privacy of secondary users. Cryptographic techniques are more promising privacy preserving solutions. In order to reap the intended security stealth from cryptographic solutions, power consumption and computational overheads should be optimized for sensors and the cryptographic identification of sensor nodes should also be feasible with the open deployment (i.e. physically unprotected) nature in cognitive radio sensor networks [18].

Recent work propose physical unclonable functions (PUFs) based secure key generation and deployment schemes in wireless sensor networks [19,20]. PUF based keys are highly secure as these cannot be forged since the responses are generated with hardware inherent noise characteristics which are unclonable [21]. Given a challenge, a PUF generates a response. For the same challenge due to the noise characteristics of hardware, the responses may slightly vary, thus demands reliable and efficient error correction schemes. In order to account for this variability, key generations and selections for