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/© 2015 Elsevier B.V. All rights reserved.

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 identification and authentication applications has to be carefully designed to preserve the uniqueness of keys [22]. PUF based cryptographic device identification applications have been proposed for wireless sensor networks [20], RFID systems [23,24], secure storage applications [25]. However, PUF based authentications with energy expenditure awareness have not been explored in CR sensors for surveillance applications in smart grid.

Based on the above discussion, existing privacy preserving mechanisms do not suffice on their own to address the privacy requirements for reliable cognitive radio sensor based surveillance in smart grid. Therefore, more robust energy-aware privacy schemes are required.

1.4. Contributions

Reliability of decision making in situation-aware disaster response and emergency management depend how secure is the transmitted surveillance data and whether sufficient amount of data is available to make reliable decisions. The data should be transmitted securely so as to ensure its confidentiality. Therefore, encryption schemes are of vital importance. However, in order to maintain an efficient power consumption in the cognitive radio sensors, the encryption method should not demand heavy computational demands on CR sensors.

In this paper we propose an energy-aware key generation method with reliability guarantees. The main focus of our research is how to realize highly reliable smart grid surveillance system over cognitive radio networks by improving the privacy preservation of sensor data. The main contributions are,

- Robust surveillance architecture based on CRSN for smart grid—Cognitive radio sensor networks is more appropriate to facilitate surveillance in smart grid. We propose a reliable surveillance architecture based on CRSN. The proposed architecture provides reliability in terms of communications, energy-aware PUF-based encryption to ensure data availability using secure data transmissions over an expected period of time.
- Novel energy-aware PUF based key generation model for CR sensors—Our key generation model uses a novel approach of being energy-aware. This approach is more suitable for a CR sensor based critical applications such as for surveillance in smart grid in order to ensure reliable data generation and for secure transmission for an expected length of time. We have developed a constraint based model to derive the optimal key size based on channel availability and minimum interferences in a CRSN.
- Novel reliability model—The proposed reliability model is based on the energy-aware key size, channel availability and surveillance application specific constraints. Our approach is more suitable to analyze the impact of reliable data generation and data availability with known quality-of-service constraints in a CRSN. The proposed reliability analysis model proves to be more expressive than the existing security analysis models which only focus on specific attacks for specific components in the smart grid.

Rest of the article is organized as follows. In Section 2, we discuss the existing privacy attacks on cognitive radio sensor network applications and sensor node identification attributes. In Section 3, we present the cognitive radio sensor network based privacy preserving surveillance architecture for smart grid. In Section 3.3 we present the reliability model. Section 4 we present our results and the effectiveness of the proposed solutions through a case study. Finally, Section 5 concludes.

2. Existing work

Existing work on privacy preservation mainly focus on wireless sensor networks and cognitive radio networks. Both these research areas are of paramount importance in realizing the potential privacy threats in cognitive radio sensor networks.

2.1. Privacy issues in cognitive radio sensor networks

In cognitive radio sensor networks, significant privacy concerns exist with the identity of sensors and the privacy of the data generated. In cognitive radio sensor networks spectrum sensing reports are valuable sources of information to malicious adversaries to identify the location of the primary users, to launch privacy violation attacks on primary users, service disruptions. Location privacy mechanisms have been proposed to prevent malicious adversaries from gaining control over the sensor node capabilities to send erroneous data or to completely tamper with sensor functionalities. Various defense mechanisms aimed at preserving location privacy and confidentiality of sensor data can be categorized as: schemes based on (i) reputation and trust of the CR sensor nodes, (ii) robust authentication schemes using cryptographic algorithms, (iii) obfuscation techniques to preserve confidentiality of sensor data, (iv) point-of origin verification techniques. Table 1 provides overview of the privacy issues and the existing measures to mitigate or minimize the impact of potential privacy violations in cognitive radio sensor networks.

In order to reduce the breeches location privacy of sensor nodes, cryptographic measures, anonymity of sensing data reports, reputation and trust based validation methods as well as emulated geo-location techniques have been proposed. The main objective of reputation based spectrum sensing methods are to *quantify the trust or the reliability* of a sensor node to validate the data by using qualitative or evidence-based quantitative measures. The initial selection of trusted sensor nodes helps to (i) collect correct data, (ii) aggregate data with high accuracy, (iii) reliability of the integrity of the sensor data as well

Table 1
Threats and mitigation strategies for different elements of a cognitive radio sensor.

Elements that require security	Vulnerabilities	Mitigation strategies
Location	Geo-location estimation.	Geo-location countermeasures such as emulated geolocation [26]
	Primary user emulation attacks—transmit high power signals to falsify the presence of primary users [27,15]	Cryptographic countermeasures [27], point of origination verification [15]
	Inferring location and time from sensor data in participatory sensing [28]	Obfuscation methods
	Intercepting spectrum sensing reports [29]	Transmit dummy sensing reports [29]
Data	Eavesdropping	Cryptographic randomization [17] where all n number of sensing reports from n nodes should be there to decrypt the data and each independent report cannot be decrypted on its own.
	Impersonation or mimicry attacks	Authentication of the received signal and the sensing reports [29]
	Traffic analysis to infer context of data	Information flooding such as probabilistic flooding [30]
	Sensor data falsification attack [31]	
Operations	Erroneous spectrum sensing information injection.	Authentication of the received signal and the sensing reports [29]
	Excuse attack which exploits the over-riding of explicit authentications in events of damage to sensor nodes [32].	Trust and reputation based node authenticity verification [14–16].
	Newbie picking attack which exploits the possibility to move from one newbie node to another to avoid mandatory requirements to provide network based information [32].	Trust and reputation based node authenticity verification [14–16].

as (iv) to reduce the potential vulnerabilities in making wrong decisions in transmission allocations. For example, in [14], sensing information from trusted nodes is only considered reliable and used in the decision making. The use of reputation system increases the robustness of cooperative sensing scheme. In order to reduce the disclosure of sensor data as a measure of preserving confidentiality, anonymity schemes have been proposed. In addition information flooding as well as sending dummy data are also proposed to reduce the likelihood of disclosure of sensor data. These methods ensure privacy but with processing overheads and reduced data utility.

2.2. Identification attributes of sensors

Recently, secret key pre-distribution techniques have been proposed for wireless sensor networks [33,34]. When new sensor nodes are added on to the network, keys have to be update and revoked. Thus, increase the complexity of these key pre-distribution systems. Random key pre-distribution schemes with the assumption that a sensor node is able to verify the identity of a sender, make them rather weak security enforcement. So in order to successfully receive the message content, unless the sensors are able to identify the sender, the key pre-distribution is of little use. One feasible identification parameter is the RF fingerprint [33].

Radio fingerprinting can be used as an identity of a sensor [35,34]. RF fingerprints allow wireless signals to be identified based on their physical characteristics. Therefore, the RF fingerprint can be used as an equivalent biometric feature in authentication processes. However, the radio fingerprint is not unique for every sensor. If the application carefully selects a set of sensors, then the identity of each of the sensors can be established as an identity to distinguish its RF operations [35]. Moreover, the identification accuracy depends on the accuracy of the classification technique employed [34]. Proximity based sensor identification techniques have also been proposed as potential identifications of the sensors. However, since the proximity is an estimation which is not collusion resistant, it is not a highly reliable identification technique. Since location privacy is vital in CRSN applications, accurate location information being used as sensor identity form is conflicting.

In sensors, photo-response non-uniformity (PRNU) is a multiplicative noise caused by imperfections in the manufacturing process and non-homogeneous properties of silicone [36]. PRNU is unique to each sensor and therefore is used for forensic applications (e.g. point of origin of digital image identification). However, the raw sensor output should be measured in order to capture the PRNU signature to be used for identification purposes. Its applicability in wireless sensor network applications are limited due to the complex signal processing to extract the identification features in the presence of noise in wireless links.

More 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]. However, the PUF-based key should be sufficiently large enough to provide security as well as not to computationally over-burden the sensor node.

3. Reliable energy-aware cognitive radio sensor data generation model

In this section, we explain the energy-aware key generation and reliability model. We explain the energy-aware optimal key generation in a CR sensor. Then, we describe the reliability model to analyze the effectiveness of the proposed solutions.

3.1. Overview

Based on the recent literature on CRSN applications [37–39], we infer the following requirements to provide reliable surveillance in smart grid using CRSN: (i) prioritize spectrum access based on traffic type (e.g. high priority assigned to real-time control and monitoring and event reporting traffic), (ii) authenticity of CR sensors, (iii) confidentiality of sensing data. In this paper will not consider the spectrum access and priority based traffic management, rather we will only focus on the latter two requirements.

Fig. 1 illustratesthe CRSN smart grid surveillance architecture using home area network (HAN), field area network (FAN) and wide area network (WAN) terms familiar in smart grid. In HAN, surveillance is required for advanced metering infrastructure (AMI). We assume that the CR sensors are installed within the smart meters and the data communications are performed over CR network. The CR sensors of smart meters communicate to FAN via a gateway. The spectrum access is determined by the gateway in consultation with the spectrum database. In WAN, over a large distributed area, actor nodes perform spectrum access decision making in consultation with the spectrum database.

In smart grid surveillance, CR sensors exchange different types of data. Examples of different types of data include event readings, control data for group formation as well as for spectrum allocation and hand-off management [38]. Application of CRSN on smart grid surveillance requires CR sensors to forward critical information pertaining to different operational aspects of smart grid. Essentially, the surveillance sensor data from CR sensors are used in collaborative situation-aware disaster recovery management, which is a decision making process. Examples include distributed feeder switching control data, emergency response data, transmission line monitoring data, event data from intelligent electronic devices in order to detect faults and malfunctions [37]. Secure transmission of surveillance data demands to have strong resilience against malicious information leakage or misuse by eavesdropping and traffic analysis based attacks. Therefore, authenticity of CR sensors and confidentiality of sensing data are essential requirements for reliable surveillance for smart grid.

CR sensor has to perform multiple functions including spectrum sensing using the RF transponder, monitoring and sensing, data encryption, data transmission, receiving information from neighborhood sensors as well as control messages from base stations. Secure data transmission is of vital importance to ensure the reliability of the surveillance sensor data.

3.2. Energy-aware PUF based key generation

PUF based key generation essentially requires the keys to be generated so as to preserve the uniqueness among the keys. Recent work on this area use pattern matching approaches using Hamming distance metric to preserve the uniqueness of PUF based cryptographic keys [22]. However, there is no formal approach to define the key generation and error corrected key selection so as to maximize the uniqueness among the keys. We select the key generation method using pattern matching [22]. Pattern matching method proposed in [22] is a more efficient and less complex technique suitable for smart grid surveillance applications which involves real-time decision making.

When PUF is used to generate secret keys, a fixed number of secret bits are required to be generated from the PUF. The challenge is kept public and the seed bots are selected differently to generate different keys. These bits are then used to generate the public/private keys in a separate secure processor. However, noise introduced should be error corrected using helper bits to ensure reliable key management. Robust error correction mechanisms such as index based syndrome coding [40] have been proposed. However, the robust error correction schemes demand high computational resources which are stringent in cognitive radio sensors. Pattern matching based key deployment using a trusted server is more viable for CRSN surveillance application. In this approach, there are more than one challenge and these are kept in secret while response bits are kept public.

In PUF-based pattern matching key generation technique requires multiple streams to be selected in m number of rounds to generate the key as a composition. The index for each round is combined to form the full-length key. For encrypting the data, CR sensors use the PUF-based secret key by *KeyGen* and the raw sensor data. The encryption function is bit-wise XOR operation over the blocks of size n bits 2. This approach is cryptographically strong, since a one-way compression function is a function that transforms two fixed-length inputs into a fixed-length output, which makes it difficult, given a particular output, to compute inputs which compress to that output. However, the stealth of the encryption depends on the secrecy of the key. Since the key is generated by PUF streams, which are near-perfect random sources, selected based on an access structure, it is theoretically impossible to hack the ciphertext.

3.2.1. Impact of key size on pattern reproducibility

It is evident, when the key size is large, the security offered is high as the reproducibility of the key reduces. However, in application on cognitive radio sensors, large key sizes demand more processing power from the sensors in encrypting

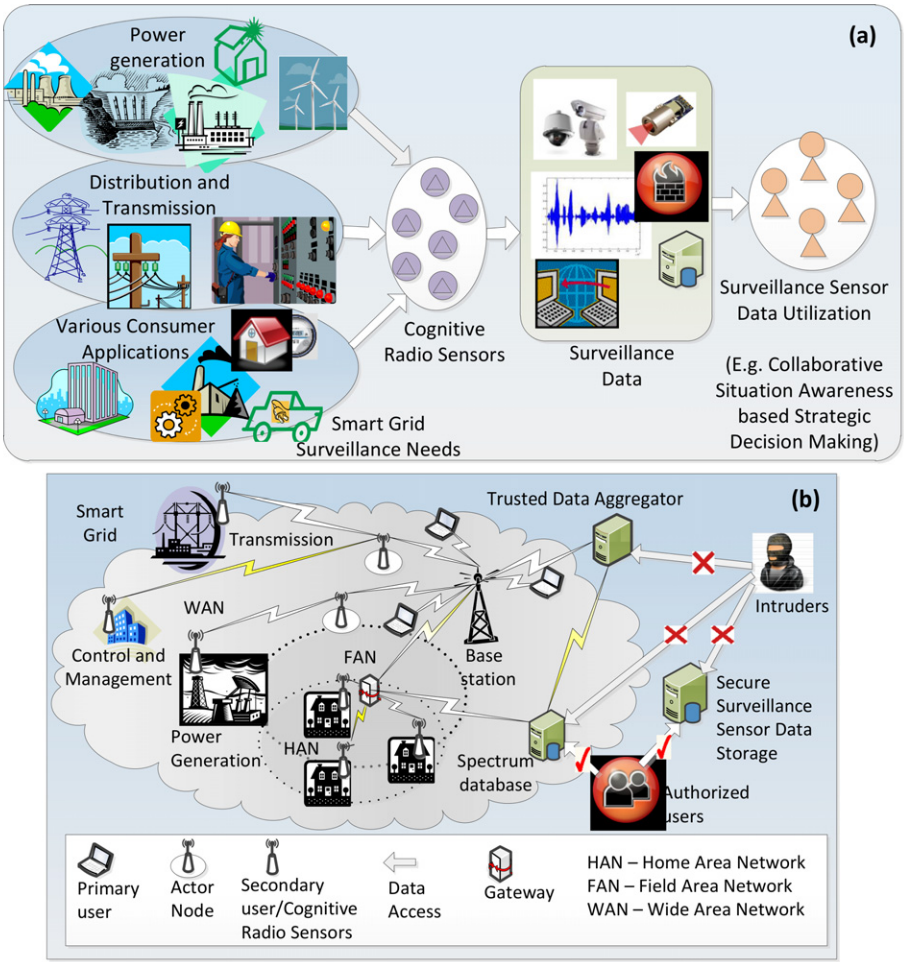

Fig. 1. Privacy preserving cognitive radio sensor network based surveillance architecture for smart grid.

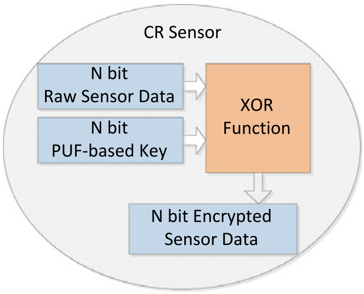

Fig. 2. Block-cipher encryption function in a cognitive radio (CR) sensor. The encryption is equivalent to a one-way function with XOR operation over n-bit data block with n-bit PUF-based secret key to output a n-bit ciphertext.

and decrypting the data. Therefore, it is necessary to find the optimal trade-off between the key size and the computational demand on cognitive radio sensors to sustain a minimum required level of security.

Consider a pattern w_i which is likely to be reproduced. The ability to predict the whole pattern w_i depends on the ability to guess the bit values based on observed sub-strings $s_{i,j}$. This approach is more realistic than to assume independent guessing of each bit. The security objective is to reduce the likelihood of reproducibility of the patterns so as to minimize the misuse of PUF-based key generation. To address this requirement we assume the events of guessing the sub-strings of the pattern is not limited but the dependency of these events are limited. Such a dependency structure can be well represented by using the Lovasz local lemma.

We define the probability that an event of reproducing a sub-string bit pattern as $P(E_i) \leq p$ and the probability of not existing a dependency for reproducing a sub-string pattern is $P(E *_i) \geq 0$. The aim is to prove that, the average event dependency probability ($P(\cup_{j=1}^{n} E *_j)$) is $P(E_i | \cup_{j \in S} E *_j) \leq P(E_i)$. In orderto prove this result we make use of the event dependency graph structure. Event dependency graph structure $G = (E, V)$ such that $v = 1, \ldots, m$ and $E = E_1, \ldots, E_m$ where an event E_j is mutually independent of the events if $E_j|(i, j) \notin E$. If the degree of the dependency graph is bounded by d and $4 \cdot d \cdot P(E_i) \leq 1$, then it is proved that the average event dependency probability is non-zero $P(\cup_{j=1}^{n} E *_j) \geq 0$. Consider the dependent events occur very rarely, then we can assume these event to be represented by Poisson trials,

$$P([E_i]k) = \frac{e^{-\mu}\mu^k}{k!} \tag{1}$$

for a set of k events. Using $k = 0$ we have $P(E *_i) \approx e^{-\mu} \leq P([E_i]k)$. Therefore, wehave $P(E_i | \cup_{j \in S} E *_j) \leq P(E_i)$.

In order to limit the degree of nodes to d, we have to restrict the number of dependent events. To do this, we define a confidence level which limits the choice of the possible sub-strings. Consider $E* \in E$ as the possible range of sub-string patterns which limits the match probability of θ. So θ is the event probability that a sub-string pattern s_i is within the range of w_i for a population size of k out of K i.e. $P(E \in E*) \geq \theta$ for $i = 1, 2, \ldots, k$.

In order to derive the relation between θ and P_{E_i} as follows. Assume that $\bar{rp}$ is the average estimate of the reproducibility P_{E_i} such that $P_{miss} \notin [\bar{P}_{E*} - \delta, \bar{P}_{E*} + \delta]$. Then, we have the following propositions,

- if $P_{E_i} < \bar{P}_{E*} - \delta$ then $X = k\bar{P}_{E*} > k(P_{E_i} + \delta) = E[X](1 + \frac{\delta}{P_{E_i}})$
- if $P_{E_i} > \bar{P}_{E*} + \delta$ then $X = k\bar{P}_{E*} > k(P_{E_i} - \delta) = E[X](1 - \frac{\delta}{P_{E_i}})$.

Applying the Chernoff bounds, we have,

$$P(X \geq (1 + \delta)\mu) < e^{-\frac{\mu\delta^2}{3}} \tag{2}$$

$$P(X \leq (1 - \delta)\mu) \leq e^{-\frac{\mu\delta^2}{2}}. \tag{3}$$

Assume that $\delta < \bar{P}_{miss}$ we have,

$$\begin{aligned} P(P_{miss} \notin [\bar{P}_{miss} - \delta, \bar{P}_{miss} + \delta]) &= P\left(X < k \cdot P_{miss}\left(1 - \frac{\delta}{P_{miss}}\right)\right) + P\left(X > k \cdot P_{miss}\left(1 + \frac{\delta}{P_{miss}}\right)\right) \\ &< e^{-\frac{k \cdot P_{miss}\left(\frac{\delta}{P_{miss}}\right)^2}{2}} \\ &= e^{-\frac{k \cdot \delta^2}{2 \cdot P_{miss}}} + e^{-\frac{k \cdot \delta^2}{3 \cdot P_{miss}}}. \end{aligned}$$

Since $P(P_{miss} \notin [\bar{P}_{miss} - \delta, \bar{P}_{miss} + \delta]) = 1 - \theta$, the above result reduces to,

$$\theta = 1 - e^{-\frac{k \cdot \delta^2}{2 \cdot P_{miss}}} - e^{-\frac{k \cdot \delta^2}{3 \cdot P_{miss}}}. \tag{4}$$

3.2.2. Energy-aware key size selection

In order to determine the possible values of θ, we define the probability of reproducibility of a bit and the bit-pattern of length w. We use the l, w and t of the pattern based PUF based key generation introduced in [22]. We define the bit reproducibility as rp. The probability for a bit to be successfully estimated or to miss it completely depends on the value of $rp \in [0, 1]$. In order to derive the relationship of rp and the probability of missing estimating a bit successfully $P_{miss-bit}$, we state the following rationale. The worst-case when $rp = 1$, it is impossible to miss accurate bit estimation, so $P_{miss-bit} = 0$ and when $rp = 0$, it is impossible to estimate the bit, so $P_{miss-bit} = 1$. Therefore, we have,

$$P_{miss-bit} = \frac{1}{2} - \left(rp - \frac{1}{2}\right). \tag{5}$$

For a bit-pattern of length w indexed with t, we assume Binomial trials ($X = k \cdot \bar{rp}$) to assume the bit estimation for the whole pattern. We can modify the above formulation as follows.

$$p = P_{miss} = 1 - \sum_{t=0}^{T} (wt) P_{miss-bit}^{t} (1 - P_{miss-bit})^{w-t}. \tag{6}$$

In this section, we optimize this key size to retain a viable power constraint on the cognitive radio sensor so to minimize the impact on its necessary processing capabilities (e.g. spectrum sensing). We assume that the main power consumption determinants are spectrum sensing and data encryption functionalities. And the other potential computational capabilities incur relatively low power consumption demands in a cognitive radio sensor.

We define a throughput metric (TM) to find the relative energy expenditure with respect to the key size as follows.

$$TM(n) = \frac{z_{tr}(n)}{z_{tr}(n) + z_{pr}(n)} \tag{7}$$

where $z_{tr}(n)$, $z_{pr}(n)$ denote the energy consumption in transmitting an encrypted packet and the fraction of energy consumed in encrypting the data using n bit key respectively.

$$z_{tr} = E^1_{total} \cdot P_{success} \cdot n \cdot t_1. \tag{8}$$

E^1_{total} denotes the energy consumed during transmission of one bit, t_1 is the transmission time and $P_{success}$ denotes the probability of the channel state without any interruptions offered by the PUs and collisions from SUs [41]. This is the most desirable transmission state, so we term this scenario as the best case. It is reasonable approximation to use $P_{success} \approx e^{-\frac{n}{R v_p}}$ where R is the datarate of a CR sensor and v_p is the channel idle time modeled as an exponential random variable [41]. The worst possible channel state will then have $P_{fail} = 1 - P_{success} = 1 - (e^{-\frac{n}{R v_p}})$ implies that there exists no transmissions. We assume that E^1_{total} is constant over t_1.

$$z_{pr} = E^2_{total} \cdot e(n) \cdot t_2 \tag{9}$$

where E^2_{total} denotes the energy consumed during encryption of one bit, t_2 is the processing time to perform encryption for n bits and $e(n)$ denotes the encryption function. The total energy expenditure should be less than $E_{total} < E^1_{total} + E^2_{total}$ where E_{total} denotes the total energy available for consumption. We assume that E^2_{total} is constant over t_2.

Since our proposed scheme is a symmetric encryption technique, we approximate the encryption function, $e(n)$, as a one-way block cipher computation with the transformation function as XOR 2. Based on the efficiency of a hash function stated in [42], we can approximate the average computational efficiency of the encryption function for n bit blocks in the CR sensor as follows.

$$e(n) = \frac{\sum_{i=1}^{n} \frac{m_i}{s \cdot n}}{n} \tag{10}$$

where m_i is the processed number of bits at the ith iteration, n is the total number of output bits and s is the number of operations to process $n - m_i$ bits.

3.3. Reliability model

In this section, we formally present the reliability model and analyze its properties using failure criteria.

3.3.1. Reliability requirements

Surveillance data (D) should be available for decision making. We define $D = \{d_1, d_2, d_3 \ldots d_{n-1}, d_n\}$ as the data required to make a decision E_i at the ith instance, where d_j (where $j = 1, 2, \ldots, n$) is the data required by the jth CR sensor. In order to analyze this reliability requirement we use queuing theory. Consider the arrival of surveillance data should be available with minimum uncertainty. This implies that if the data availability is less than that of the required amount of data, then uncertainty is claimed to be high. This is not desirable as a reliable decision making will have a significant risk. Suppose the uncertainty caused due to absence of ΔD amount of data is computed using a utility function $U_{\Delta D}$.

We assume that the n CR sensors experience homogeneous channel conditions in transmission and also assume the channel is available and the channel conditions do not vary significantly over time. With this assumption we define another channel availability based utility function $U_{channel} \in [0, 1]$. Fig. 3 shows both the utility functions $U_{channel}$ and $U_{\Delta D}$. We have considered the possible utility variation of a channel depending on the interference $U_{channelInt}$ (inferred the utility bounds based on the results published in [41]).

By using a particular surveillance data D is required to formulate a decision E_i to perform a specific disaster recovery and emergency management operation O_i. The reliability of decision $R(E_i)$ to select to perform the operation O_i, depends on the reliability of surveillance data $R(D)$ and the relative importance of performing that operation at the ith time instance. We can formally state this as follows.

Reliable decision, to perform an operation is define as $R(E_i) = p(O_i) \in [0, 1]$. The decision to select to perform the operation O_i is denoted by 1 and not being successful denoted by 0. We calculate $p(O_i)$ as a conditional probability ($R(D)$) based on the reliability of D_i.

$$R(E_i) \propto \frac{R(D_i)}{R(D_i) + A(D_i)} \tag{11}$$

$$R(E_i) = \alpha \cdot \frac{R(D_i)}{R(D_i) + A(D_i)} \tag{12}$$

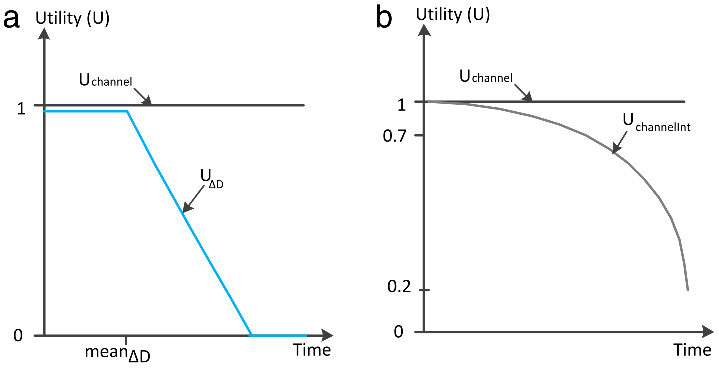

Fig. 3. Utility functions (a) $U_{channel}$ and $U_{\Delta D}$ and (b) variation of channel utility depending on the interferences $U_{channel}$ and $U_{channelInt}$.

where, α is the relative importance of the operation O_i.

As defined before, suppose we have a sequence of event data generated by n CR sensors $D_i = d_1, d_2, \ldots, d_n$. t_{exp} is the expected time of surveillance by that particular CR sensor. $P_{success}$ is defined in Section 3.2.2 as the reliability of the wireless channel with minimum interference for communication. Then, reliability $R(D)$ is defined as follows.

$$R(D) \propto n \cdot P_{success} \cdot t_{exp} \cdot TM(n) \tag{13}$$

$$R(D) = \beta \cdot n \cdot P_{success} \cdot t_{exp} \cdot TM(n) \tag{14}$$

where, β is the relative importance of D_i at the ith time instance.

3.3.2. Failure criteria

If any sensor drains its battery power to a level E_v that encryption function cannot be performed for bit size v of the key but for a smaller bit size v' (where $v > v'$). For a conventional sensor node secure transmission does not occur at $TM(v')$ as $E_{av} < TM(v)$ and $TM(v) > TM(v')$. We assume that the channel availability is guaranteed. The impact of data unavailability $(UA(D_j))$ of k CR sensors at the jth time instance can be stated as follows.

$$UA(D_j) = \beta \cdot U_{\Delta D} \cdot t_{rem} \cdot P_{success} \cdot TM(v') \tag{15}$$

where t_{rem} is the remaining time that a CR sensor is expected to transmit the required data. If the channel conditions vary, then $P_{success}$ gets replaced by $U_{channel}$.

Suppose there is a minimum key size $v*$ such that minimum security against a possible interception of the transmitted data can be prevented, then a minimum reliability $(R_{\min}(D))$ can be guaranteed so as to preserve the data transmission over a period of t_{exp}.

$$R_{\min}(D) = \beta \cdot U_{\Delta D} \cdot n \cdot P_{success} \cdot t_{exp} \cdot TM(v*). \tag{16}$$

When there is a fixed width key (i.e. of v bits) for encryption the CR sensor will not be able to transmit data securely and thus there will be an uncertainty in the data D' (where $D < D'$ and $\Delta D = D - D'$) that is required to make the decision E_i at the ith time instance. Based on the above formulation, it is evident that in order to maintain a minimum reliability in decision making it is evident to have minimum key size to encrypt data in a CR sensor so as to ensure required data availability with minimum uncertainty.

4. Evaluation

In this section we describe the theoretical validation of the energy-aware pattern size computation. Then, we experimentally evaluate the effectiveness of the proposed solutions using the reliability model described in Section 3.3 with real-life sensor data for smart grid surveillance application.

4.1. Optimum energy-aware pattern size computation

When $\frac{\delta^2}{P_{miss}} < 1$, variation of θ with k is shown in Fig. 4.

We have used Eqs. (5) and (6) to compute the p values with different n values. We use Eqs. (10) and (9) to compute thevariation of $e(n)$ with different n values. As mentioned in Section 3.2.2, based on our assumption that the main processing functions are encryption and spectrum sensing we have,

$$z_{pr} < 0.5 \tag{17}$$

$$\text{since} z_{pr} + z_{tr} < 1. \tag{18}$$

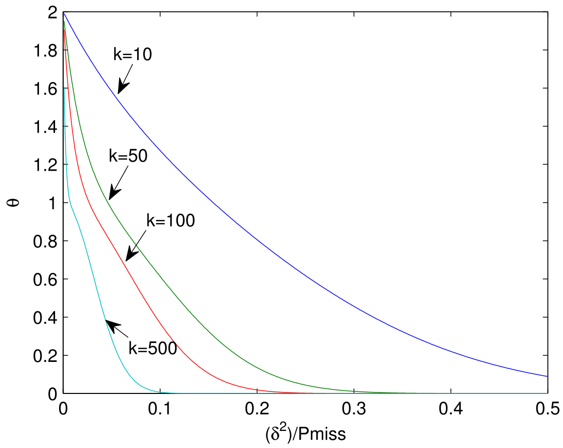

Fig. 4. Variation of θ with k when $\frac{\delta^2}{P_{miss}} < 1$.

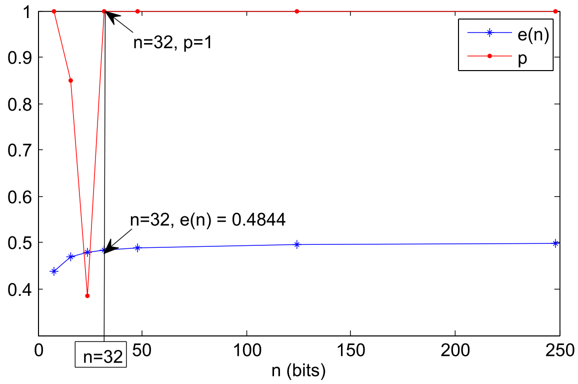

Fig. 5. Optimum pattern size computation. Variations with pattern miss detection probability (p) and the energy consumption for encryption $(e(n))$ for n bits.

Based on Eq. (9) and the above relation we have,

$$e(n) \propto z_{pr} \rightarrow e(n) < 0.5 \tag{19}$$

$$\frac{\sum_{i=1}^{n} \frac{m_i}{s \cdot n}}{n} < 0.5. \tag{20}$$

Then, in order to determine the bit pattern size in order to minimize the bit-pattern reproducibility we use the Eqs. (5) and (6).

The results shown in Fig. 5, we have the optimal solution at $w = 32$ with $e(n) = 0.4844$ and a probability of the not reproducing the bit pattern $p = p_{miss} = 1$. The results also indicate that depending on the capabilities of the cognitive radio sensor, larger key sizes can also be accommodated with lower probability to reproduce the bit pattern however, with an increased cost of battery power consumption.

4.2. Experimental scenario: reliability for fire detection in cables in smart grid using temperature measurements communicated over CRSN

Temperature sensing of cables, ducts and chases is a vital DRM pro-active measure in smart grid to ensure seamless power delivery [43]. For example, in October 2014, in Calgary in Canada the city had to experience a power outage due to an underground electric fire effecting over 5000 residents and 1200 businesses [44]. Existing approaches for distributed real-time temperature sensing of electrical cables include use of fiber optic cables [45] and sensor networks [43]. Due to limitation of providing reliable communications wireless multimedia sensor networks, CRSN is ore useful for surveillance applications in smart grid [46]. Therefore, the reliability of accurate decision making in DRM for smart grid essentially need to have the communication channel reliability as a pre-requisite to facilitate secure data transmission over a channel. Therefore, the *main objective of this experimental scenario* it is to demonstrate why we need to have an energy-aware sensor data encryption

Table 2
Number of samples analyzed for four sensor nodes.

	Sensor 01	Sensor 02	Sensor 03	Sensor 04
Normal operating conditions [48]				
Maximum	30.38	30.59	27.92	27.96
Minimum	26.29	26.41	25.69	25.97
No. of samples	4632	4690	4590	4690
Possible fire events				
Maximum	65	58	64	50
Minimum	50	54	60	50
No. of samples	500	500	500	500

Table 3
$R_{\min}$ variations with ΔD for fire event data (when $P_{success}$ does not vary depending on $U_{channelInt}$ and for a constant key size υ).

ΔD	10%	20%	30%	40%
Mean variation	84	92	93	97
$U_{\Delta D}$	0.73	0.62	0.54	0.47
$P_{success}$	1	1	1	1
$TM(\upsilon)$	0.5	0.5	0.5	0.5
$R_{\min}(\Delta D)$	0.73	0.62	0.54	0.47

Table 4
Classification error to declare a fire event with respect to ΔD using neural network classifier.

ΔD	10%	20%	30%	40%	50%
Error	5%	12%	24%	33.8%	53%

method in CR sensors to securely transmit temperature sensing data, provided that the communication channel is reliable over the CRSN in order to perform reliable DRM to handle cable fire disasters in smart grid.

We use two data sets (D_1 and D_2) for four (04) sensors. For D_1 we have used the public data set on temperature measurements for four (04) sensors [47,48]. We have considered D_1 to indicate normal operating conditions over a day. However, in the multihop temperature sensor data set of [48], the introduced events indicated by $'1'$ had a range of maximum 48.24 and a minimum of 26.97. According to the published results in [45] this range was too narrow to declare a potential fire event. Therefore, we have generated the second data set (D_2) with a higher temperatures to indicate anomalous data. The anomalous data are considered as fire event trigger points which has to be detected to take a DRM action O_i. Table 2 shows the summary of the number samples that were used in the analyses.

We consider the decision E_i to be to declare a fire. The accuracy of this decision depends on the availability of data by k CR sensor. We also define the current energy profile for each CR sensor and calculate the likelihood of each sensor to encrypt the data using an l bit key. We assume that 50% of the k CR sensors experience a exponential energy expenditure over the next time instance. Then, there is an uncertainty (see the $U_{\Delta D}$ in Fig. 3) due to the missing data from $\frac{k}{2}$ sensors. So there is an uncertainty to distinguish between normal operating condition and a fire event. Then, we compare the reliability of this scenario against a situation when the CR sensors can generate data with a key l' (where $l > l'$) such that over m more time instances can encrypt data to be transmitted securely. Furthermore, if $P_{success}$ vary due to channel conditions. Then, $UA(D_j)$ (see Eq. (15) in Section 3.3.2), depends on the utility of the channel (i.e. based on the utility variation shown in Fig. 3). We performed our experiment in Matlab. In our evaluation, we used fuzzy numbers to represent the utility functions, energy profile and the time variation [49,50]. The main reason for selecting fuzzy numbers to represent each of these variables are due to several reasons. We need to associate the uncertainty of lack of available data as an estimate. This is not possible when we use crisp values. Therefore, we use fuzzy numbers for the variables to calculate the extent of information unavailability. We compute $U_{\Delta D}$ based on the mean variation of the data.

Interpretation of results: As shown in Table 3, $U_{\Delta D}$ degrades to a relatively low level. On the other hand, when ΔD reduces more than 40%, it is difficult to detect the fire event accurately using a neural network classifier (Table 4). Therefore, we conclude that $U_{\Delta D}$ should be at least 40% to identify a fire event with minimum uncertainty. When $P_{success}$ is not a constant, Table 5 shows the variation of $R_{\min}$. Based on the results it is evident that it is more suitable to have energy-aware key size to encrypt surveillance sensor data in CR sensors in order to provide reasonable reliability guarantees in terms of transmitting over a t_{exp} time, provided channel availability by CRSN.

5. Conclusion

Cognitive radio sensor networks are more useful communication facilities for smart grid to facilitate reliable communications for reliable surveillance and situation-specific disaster recovery and emergency management. In view of recent attacks on smart grid surveillance is of vital importance to ensure seamless energy generation and distribution. In order

Table 5
$R_{\min}$ variations with ΔD for fire event data (when $U_{channelInt}$ varies over time for a constant key size υ).

ΔD	10%	20%	30%	40%
Mean variation	84	92	93	97
$U_{\Delta D}$	0.73	0.62	0.54	0.47
$U_{channelInt}$	0.2	0.3	0.4	0.5
$TM(\upsilon)$	0.5	0.5	0.5	0.5
$R_{\min}(\Delta D)$	0.146	0.219	0.292	0.365

to perform reliable disaster recovery mechanisms, authenticity of cognitive radio sensors and sensor data is vital. In this paper we propose a privacy preserving smart grid surveillance architecture over cognitive radio sensor networks. The main privacy preserving feature is a novel energy-aware key generation method for secure surveillance data transmission. We analyze its usefulness using a reliability model. Our contributions mainly solves the question of how reliability of surveillance can be assured with known energy constraints, channel availability with minimum security guarantees using the energy-aware key generation for encryption. We have performed theoretical analysis as well as simulation based analysis to experimentally validate the proposed model. Based on the results it can be concluded that the proposed security guarantees can ensure reliable decision making in situation-specific disaster recovery and emergency management operations in smart grid surveillance.

Acknowledgments

We wish to acknowledge NICTA as the main funding source for the research studentship. NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Center of Excellence program.

References

[1] V.C. Gungor, D. Sahin, Cognitive radio networks for smart grid applications: A promising technology to overcome spectrum inefficiency, IEEE Veh. Technol. Mag. 7 (2) (2012) 41–46.
[2] H. Wang, Y. Qian, H. Sharif, Multimedia communications over cognitive radio networks for smart grid applications, IEEE Wirel. Commun. 20 (4) (2013) 125–132.
[3] M. Amin, Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid, in: Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, 2008, pp. 1–5.
[4] X. Fang, S. Misra, G. Xue, D. Yang, Smart grid—the new and improved power grid: A survey, IEEE Commun. Surv. Tutor. 14 (4) (2012) 944–980.
[5] Smart grid security—annex ii security aspects of the smart grid, 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf.
[6] K. Tweed, Attack on california substation fuels grid security debate, February 2014. http://spectrum.ieee.org/energywise/energy/the-smarter-grid/attack-on-california-substation-fuels-grid-security-debate.
[7] R. Puri, A. Majumdar, P. Ishwar, K. Ramchandran, Distributed video coding in wireless sensor networks, IEEE Signal Process. Mag. 23 (4) (2006) 94–106.
[8] M. Erol-Kantarci, H.T. Mouftah, Wireless multimedia sensor and actor networks for the next generation power grid, Ad Hoc Networks 9 (4) (2011) 542–551. multimedia Ad Hoc and Sensor Networks.
[9] J. Huang, H. Wang, Y. Qian, C. Wang, Priority-based traffic scheduling and utility optimization for cognitive radio communication infrastructure-based smart grid, IEEE Trans. Smart Grids 4 (1) (2013) 78–86.
[10] F. Greitzer, A. Schur, M. Paget, R. Guttromson, A sensemaking perspective on situation awareness in power grid operations, in: IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, 2008, pp. 1–6.
[11] G. Gelston, A. Dalton, L. Tate, Multi-organizational distributed decision making in the power grid industry, in: IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA, 2012, pp. 158–161.
[12] F. Riaz, R. Akhter, B. Zulfiqar, A. Ahmed, S. Shah, J. Ahmad, Surveillance system using cognitive radio approach, in: International Conference on Computer Networks and Information Technology, ICCNIT, 2011, pp. 217–221.
[13] R. Rios, J. Lopez, Analysis of location privacy solutions in wireless sensor networks, IET Commun. 5 (17) (2011) 2518–2532.
[14] K. Zeng, P. Paweczak, D. Čabrić, Reputation-based cooperative spectrum sensing with trusted nodes assistance, IEEE Commun. Lett. 14 (3) (2010) 226–228.
[15] R. Chen, J.-M. Park, K. Bian, Robust distributed spectrum sensing in cognitive radio networks, in: INFOCOM 2008. The 27th Conference on Computer Communications, IEEE, 2008.
[16] J. Wang, S. Feng, Q. Wu, X. Zheng, Y. Xu, G. Ding, A robust cooperative spectrum sensing scheme based on dempster-shafer theory and trustworthiness degree calculation in cognitive radio networks, EURASIP J. Adv. Signal Process. (1) (2014).
[17] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, X. Shen, Location privacy preservation in collaborative spectrum sensing, in: Proceedings IEEE INFOCOM, IEEE, 2012, pp. 729–737.
[18] M. Rostami, J.B. Wendt, M. Potkonjak, F. Koushanfar, Quo vadis, puf?: Trends and challenges of emerging physical-disorder based security, in: Proceedings of the Conference on Design, Automation & Test in Europe, DATE'14, European Design and Automation Association, 2014, pp. 352:1–352:6.
[19] G. Selimis, M. Konijnenburg, M. Ashouei, J. Huisken, H. de Groot, V. van der Leest, G.-J. Schrijen, M. van Hulst, P. Tuyls, Evaluation of 90nm 6t-sram as physical unclonable function for secure key generation in wireless sensor nodes, in: IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2011, pp. 567–570.
[20] J. Guajardo, S.S. Kumar, P. Tuyls, Key distribution for wireless sensor networks and physical unclonable functions, Printed handout of Secure Component and System Identification—SECSI, 2008, pp. 17–18.
[21] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber, Modeling attacks on physical unclonable functions, in: Proceedings of the 17th ACM Conference on Computer and Communications Security, ACM, 2010, pp. 237–249.
[22] Z. Paral, S. Devadas, Reliable and efficient puf-based key generation using pattern matching, in: IEEE International Symposium on Hardware-Oriented Security and Trust, HOST, 2011, pp. 128–133.

[23] L. Bolotnyy, G. Robins, Physically unclonable function-based security and privacy in RFID systems, in: Fifth Annual IEEE International Conference on Pervasive Computing and Communications, PerCom'07, IEEE, 2007, pp. 211–220.
[24] J. Guajardo, B. Škorić, P. Tuyls, S.S. Kumar, T. Bel, A.H. Blom, G.-J. Schrijen, Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions, Inf. Syst. Front. 11 (1) (2009) 19–41.
[25] K. Kursawe, A. Sadeghi, D. Schellekens, B. Skoric, P. Tuyls, Reconfigurable physical unclonable functions-enabling technology for tamper-resistant storage, in: IEEE International Workshop on Hardware-Oriented Security and Trust, 2009, HOST'09, IEEE, 2009, pp. 22–29.
[26] Z. Jin, S. Anand, K.P. Subbalakshmi, Detecting primary user emulation attacks in dynamic spectrum access networks, in: IEEE International Conference on Communications, 2009, pp. 1–5.
[27] A. Alahmadi, M. Abdelhakim, J. Ren, T. Li, Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard, IEEE Trans. Inf. Forensics Secur. 9 (5) (2014) 772–781.
[28] J.A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M.B. Srivastava, Participatory sensing, Center for Embedded Network Sensing, 2006.
[29] Z. Gao, H. Zhu, S. Li, S. Du, X. Li, Security and privacy of collaborative spectrum sensing in cognitive radio networks, IEEE Wirel. Commun. 19 (6) (2012) 106–112.
[30] C. Ozturk, Y. Zhang, W. Trappe, Source-location privacy in energy-constrained sensor network routing, in: Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN'04, 2004, pp. 88–93.
[31] R. Chen, J.-M. Park, Y. Hou, J. Reed, Toward secure distributed spectrum sensing in cognitive radio networks, IEEE Commun. Mag. 46 (4) (2008) 50–55.
[32] A. Araujo, J. Blesa, E. Romero, D. Villanueva, Security in cognitive wireless sensor networks. Challenges and open problems, EURASIP J. Wirel. Comm. Netw. (1) (2012).
[33] K. Henry, D. Stinson, Secure network discovery in wireless sensor networks using combinatorial key pre-distribution, in: Workshop on Lightweight Security Privacy: Devices, Protocols and Applications, LightSec, 2011, pp. 34–43.
[34] D.A. Knox, T. Kunz, Practical RF fingerprints for wireless sensor network authentication, in: 8th International Wireless Communications and Mobile Computing Conference, IWCMC, 2012, pp. 531–536.
[35] K. Bonne Rasmussen, S. Capkun, Implications of radio fingerprinting on the security of sensor networks, in: Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007, pp. 331–340.
[36] J. Lukas, J. Fridrich, M. Goljan, Digital camera identification from sensor pattern noise, IEEE Trans. Inf. Forensics Secur. 1 (2) (2006) 205–214.
[37] G. Shah, V. Gungor, O. Akan, A cross-layer QoS-aware communication framework in cognitive radio sensor networks for smart grid applications, IEEE Trans. Ind. Inf. 9 (3) (2013) 1477–1485.
[38] O. Akan, O. Karli, O. Ergul, Cognitive radio sensor networks, IEEE Netw. 23 (4) (2009) 34–40.
[39] J. Wang, M. Ghosh, K. Challapali, Emerging cognitive radio applications: A survey, IEEE Commun. Mag. 49 (3) (2011) 74–81.
[40] S. Devadas, M. Yu, Secure and robust error correction for physical unclonable functions, 2013.
[41] M. Oto, O. Akan, Energy-efficient packet size optimization for cognitive radio sensor networks, IEEE Trans. Wireless Commun. 11 (4) (2012) 1544–1553.
[42] http://www.emsec.rub.de/media/crypto/attachments/files/2011/03/bartkewitz.pdf.
[43] http://www.sensortran.com/applications_smartgrid.php (accessed on 16.01.15).
[44] Power restored to downtown calgary five days after outage, 2014. http://live.calgaryherald.com/Event/Part_of_downtown_Calgary_in_darkness_after_underground_electrical_fire?Page=0 (accessed on 16.01.15).
[45] M.-H. Luton, J.A. Downes, G. Anders, J. Braun, N. Fujimoto, S. Rizzeto, Real time monitoring of power cables by fibre optic technologies tests, applications and outlook, in: International Conference on Insulated Power Cables, 2003.
[46] M. Erol-Kantarci, H.T. Mouftah, Wireless multimedia sensor and actor networks for the next generation power grid, Ad Hoc Networks 9 (4) (2011) 542–551.
[47] S. Suthaharan, M. Alzahrani, S. Rajasegarar, C. Leckie, M. Palaniswami, Labelled data collection for anomaly detection in wireless sensor networks, in: Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), IEEE, 2010, pp. 269–274.
[48] http://www.uncg.edu/cmp/downloads/.
[49] G.J. Klir, U.S. Clair, B. Yuan, Fuzzy Set Theory: Foundations and Applications, Prentice Hall, Upper Saddle River, NJ, 1997.
[50] P. Dutta, H. Boruah, T. Ali, Fuzzy arithmetic with and without using α-cut method: A comparative study, Int. J. Latest Trends Comput. 2 (2011) 99–107.