A Device-Based Secure Scheme Against PUEA Attacks in Cognitive Radio Sensor Networks

SHIH-CHANG LIN
Department of Electrical Engineering
National Chung Hsing University
250 Kuo-Kuang Rd., Taichung 402, Taiwan
d099064004@mail.nchu.edu.tw

CHIH-YU WEN
Department of Electrical Engineering
National Chung Hsing University
250 Kuo-Kuang Rd., Taichung 402, Taiwan
cwen@dragon.nchu.edu.tw

Abstract: Due to the resource-constrained sensor motes and critical security concerns, feasible wireless sensor-based systems require more breakthroughs in terms of network architecture, system design, and data processing techniques. In this paper, we incorporate the strengths of cognitive radio and the physical property of a device to improve the performance of a cognitive radio sensor network (CRSN) and resolve the security problem, considering one of the most destructive attacks in CRSNs called the primary user emulation attack (PUEA). Accordingly, we aim to develop a fully distributed method against PUEA attacks from two perspectives: (1) spectrum management with separate sensing and (2) device-based node identification, in order to explore the trade-off between spectrum management and the successful detection rate of malicious nodes. The proposed distributed secure algorithm with the knowledge of separate sensing allows the sensing sensors and the tasking nodes to perform a detection and identification mechanism such that dynamic spectrum management and correct spectrum decision can be achieved. The experimental results show that the proposed secure system provides a feasible way against the PUEA attacks.

Key–Words: primary user emulation attack, cognitive radio sensor networks, separate sensing, node identification.

1 Introduction

In general, a cognitive radio sensor network (CRSN) has two unique characteristics: (i) Cognitive Capability and (ii) Reconfigurability, which may make CRSNs vulnerable to a number of novel attacks during the cognitive cycle [1]. One of the most destructive attacks in CRSNs is called the primary user emulation attack (PUEA), which mimics a primary user (PU) by transmitting fake signals [2]. Therefore, considering the PUEA attack, effective secure operations should be carried out in order to obtain awareness about the spectrum usage and the possible presence of primary users [3]. Since the centralized spectrum analysis scheme may not be feasible under certain circumstances, such as the sink is far away from the majority of the sensors, in this paper, we present a distributed device-based secure scheme (DBSS) with separate sensing against PUEA attacks in hierarchical CRSNs.

Figure 1 shows that a tasking group in a hierarchical CRSN may consist of (1) sensors for separate sensing (SS) and (2) cognitive nodes (e.g. the clusterheads and cluster members) for sensor tasking. Denote the target (e.g. patients or habitat monitoring) and the cognitive node as the primary user (PU) and the secondary user (SU), respectively. Accordingly, in order to maintain network operation and defend PUEA attacks, a fully distributed secure method in CRSNs is developed from two perspectives: (1) Spectrum management with separate sensing and (2) Device-based node identification. The first perspec-

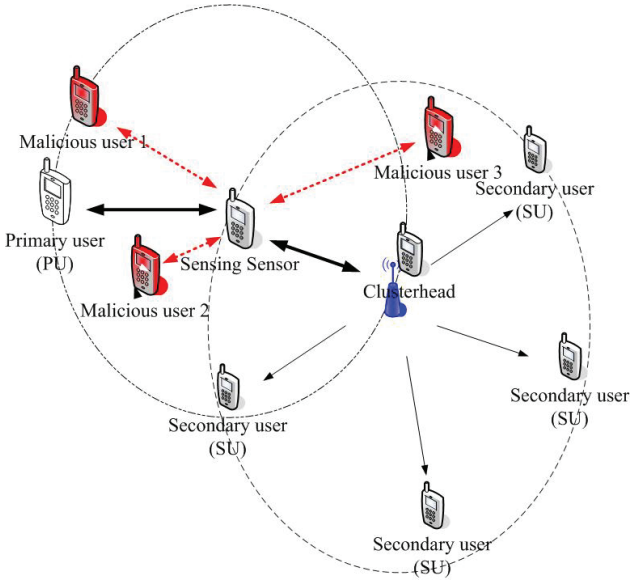

Figure 1: Spectrum sensing using sensing sensors (SSs).

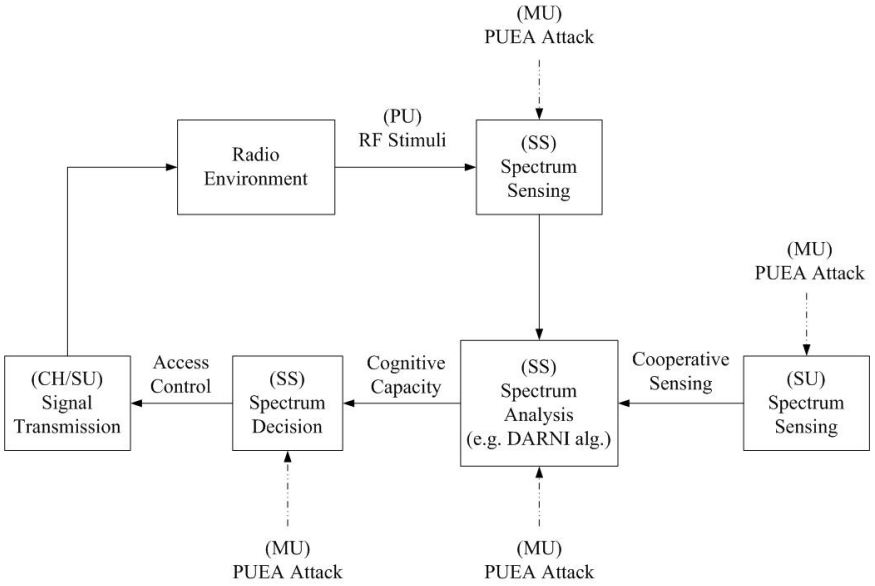

Figure 2: The cognitive cycle against PUEA attacks (modified and reproduced from [1]).

tive is to select sensing sensors and develop a detection and notification mechanism, considering information exchange and the handshaking protocol between the sensing sensors and the tasking nodes (i.e. cognitive nodes). The second perspective is to apply the physical property of a device, the communication delay (e.g. internal component delay, difference of the clocks, and the response delay) between two wireless sensors such that the malicious nodes which mimic the PU can be identified. The conceptual cognitive cycle against PUEA attacks is shown in Figure 2, including the operations of spectrum sensing, spectrum analysis, and spectrum decision.

This paper is organized as follows: In Section 2, we review related works about PUEA attacks and spectrum sensing in CRSNs. Section 3 describes the network architecture for separate sensing. Section 4 presents a device-based secure scheme against PUEA attacks. In Section 5, we evaluate the system performance and present the performance comparison between the proposed DBSS and the belief propagation-based scheme [4]. Finally, Section 6 draws conclusions and shows future research directions.

2 Literature Review

This section summarizes the most relevant existing research on three problems: separate sensing, cluster-based CRSNs, and security issues about PUEA attacks.

2.1 Spectrum Sensing Using Sensing Sensors

Instead of using the resources of the tasking nodes (SUs) for spectrum sensing, sensing sensors may be used specifically for spectrum sensing. Referring to Figure 1, the sensing results can be forwarded to the SU to make a decision on spectrum access, which reduces the sensing overheads and improves the sensing performance in noisy environments. In [5], a spectrum sensor network is proposed to detect a passive PU based on the local oscillator (LO) leakage power, which can be applied as an indicator to detect the presence of a PU. The authors in [6] propose a network structure to separate the sensing task from the SUs with placing sensing devices in the network of PUs. Therefore, the sensing devices sense PUs' activity and then decide whether to allow a SU's transmission.

With constraints on the detection performance, several protocols [7]-[9] have been proposed for choosing the sleeping and censoring design parameters of sensing sensors in order to minimize energy consumption and determine the desired number of sensing sensors. However, no information about the sensing node selection is provided. Authors in [10] address the problem of sensor selection for energy efficient spectrum sensing in CRSNs, considering energy consumption minimization and spectrum sensing performance simultaneously. Nonetheless, the solution in [10] is not a event-driven/application-driven scheme.

Notice that the above works focus on the detection of the PU's activity and PUEA attacks, not carefully considering the impacts of network topol-

ogy and the collaboration between the cognitive nodes (SUs) on the system performance. Therefore, instead of just considering energy consumption minimization and spectrum sensing performance, in this paper we plan to tackle the sensing node selection problem and the malicious node identification problem such that the tradeoffs among the energy efficiency, spectrum sensing performance, and the impact of malicious node behaviors on system performance can be clarified.

2.2 Cluster-Based Cognitive Radio Networks/CRSNs

In [11], a CogMesh framework is proposed for cluster-based ad-hoc cognitive networks. By exploiting the spectrum opportunities, the SUs group into clusters on available channels in the network. Based on the detection of a beacon message, the SU can determine whether to become a clusterhead or join the cluster in the context of open spectrum sharing. Since existing clustering approaches for sensor networks are not applicable in CRSNs and existing solutions for cognitive radio networks may not be suitable for sensor networks, in [12], a cluster-based CRSN MAC protocol (KoN-MAC) for the multi-hop cognitive radio wireless sensor networks is described. A medium access scheme for nodes in every cluster and a channel-sensing scheme are designed to perform a channel-sensing scheme and a contention free communication.

In the context of CRSNs, a distributed spectrum-aware clustering (DSAC) scheme [13] is proposed, which aims at forming energy efficient clusters in a self-organized fashion for intra-cluster aggregation and inter-cluster relaying. In [14], an event-driven clustering protocol is presented to select eligible nodes for clustering and form temporal cluster for each event in CRSNs.

2.3 Primary User Emulation Attack (PUEA)

PUEA in cognitive radio networks was studied in [2, 15, 16]. In [2], Chen *et al* discuss defense against PUEA by localization of primary transmitters using the angle of arrival, the time of arrival, and the received signal strength of the primary signal. In [15], Chen and Park propose two mechanisms, which use the ratio and the difference of the distances of the primary and malicious transmitters from the secondary user to detect a PUEA. In [16], the authors use a hypothesis testing method to detect a primary transmission with spectrum sensing. Regarding the detection of the PUEAs, received power measurements of the SUs can be applied to detect the attack [4, 17, 18]. Note that the above studies assume that the locations of the primary transmitters are known a priori. In non-location-based algorithms, a helper node (HN) with cryptographic signatures by HN's signals [19], a public key cryptography mechanism [20], or a AES-assisted scheme [21] can be used to verify the integrated signatures in order to characterize the signal.

In contrast to the conventional hardware/software authentication solutions, in this work, we incorporate the strengths of cognitive radio and the physical property of a device to improve the performance of a CRSN and resolve the security problem.

3 Network Architecture for Separate Sensing

By exploiting the information about coverage, connectivity, and sensing spatial redundancy, we may use the Clustering Algorithm via Waiting Timer (CAWT) [22] to form a 2-hop cluster-based network topology and then apply the Distributed Adaptive Scheduling Algorithm (DASA) [23] to determine the sensing sensors (SS) in each cluster such that the SSs can monitor channel spectrum, effectively control the spectrum access of the sensors, and further mitigate the PUEA attack. The DASA method operates much like the CAWT in utilizing a random timer. As the clusterhead broadcasts a message to start the sensing assignment, sensor *i* initializes a random waiting timer with a value

$$WT_i^{(0)} = \frac{1}{N_{hop}} \cdot T_i \cdot \beta^{N_b^{(i)}}, \qquad (1)$$

which is related to the cluster topology and the neighbor information. Note that T_i is a sample from the distribution $C+\lambda \cdot U(0,1)$, where C and λ are positive numbers for specifying the sampling range of the waiting time, and $U(0,1)$ is a uniform distribution. N_{hop} is the number of hops from the clusterhead to the cluster member, $N_b^{(i)}$ is the number of neighboring cluster members of sensor *i*, β is a positive number with $1 < \beta$.

The rationale for the settings in equation (1) is that, due to the overlap of sensing area in a cluster, the coverage overlap of a 1-hop cluster member is usually larger than that of a 2-hop cluster member. This suggests that a 2-hop cluster member may be a good candidate to initialize a round group. On the other hand, a 1-hop cluster member may choose to wait and join the round group later. Furthermore, a cluster member with more neighbors may have a lower priority to execute the sensing task since its sensing area may be covered by the nearby cluster members. If the random waiting timer expires (i.e. $WT_i = 0$), then sensor *i* broadcasts a message proclaiming that it is a

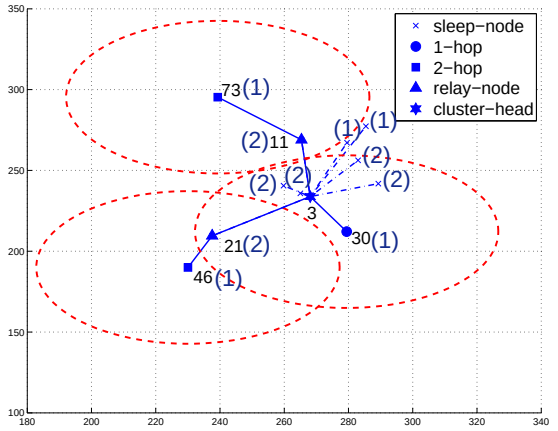

Figure 3: An example of the selection process of sensing sensors for spectrum management in a cluster.

good candidate to be a sensing sensor (SS), which also serves to notify its neighbors that it has a higher priority for the sensing task. Figure 3 illustrates an example of the selection process of sensing sensors, which shows that sensor 73, sensor 30, and sensor 46 are candidates for being sensing sensors. By following the above procedures, the sensing sensors for spectrum management can be determined in each cluster.

4 Distributed Device-Based Secure Scheme Against PUEA Attacks

This section describes the proposed distributed secure method for cooperative spectrum control against PUEA attacks in a cluster-based network topology, which is based on the framework of our previous work [24]. The characteristics of sensing sensors and the tasking nodes are applied to achieve spectrum management and node identification. In contrast to our previous work considering homogeneous device characteristics [24], in this work, the authentication process may be fulfilled by applying heterogeneous device information. We assume: (1) The sensor nodes may have different internal device delay characteristics, (2) a pair of sensors A and B are equipped with clocks (oscillators) that are assumed to be asynchronous in time, and (3) there is no malicious node in the network during the network initialization phase. Thus, the characteristics of asynchronization between sensors and device delay are applied to achieve distributed node identification. Consequently, the proposed scheme can restrict the impact of the attacker on the basis of synchronization precision and device

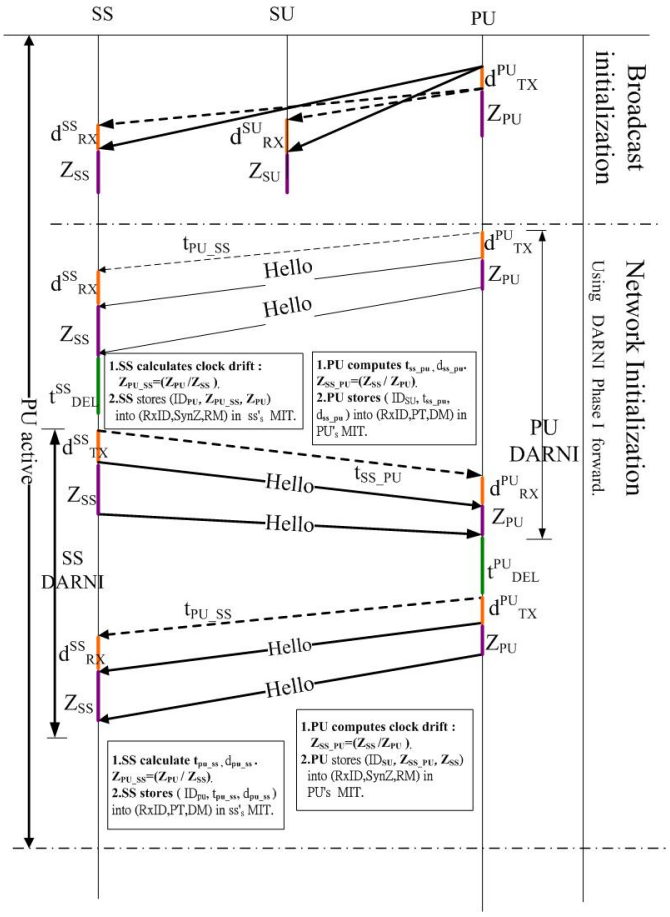

Figure 4: A conceptual handshaking/communication procedure of the proposed secure scheme.

delay. Note that these assumptions may be applied to health-care scenarios, habitat monitoring applications, and the network architecture of internet of things applications, such as locating patients or animals and performing intruder detection.

4.1 Network Initialization and Communication Protocols

Since the PU, the sensing sensors (SSs) and the cluster members (i.e. cognitive radio users, SUs) play different roles, it is necessary to design a handshaking mechanism among the PU, SSs and SUs. Figure 4 describes a conceptual communication protocol to address the above operations. Referring to Figure 4, after the sensors are deployed, each sensor broadcasts a *Hello* message for information exchange. A *Hello* message consists of: (1) RxID - the sensor ID of the receiving sensor, (2) TxID - the sensor ID of the sending sensor and (3) time stamps of the message transmission. Based on the *Hello* message, the

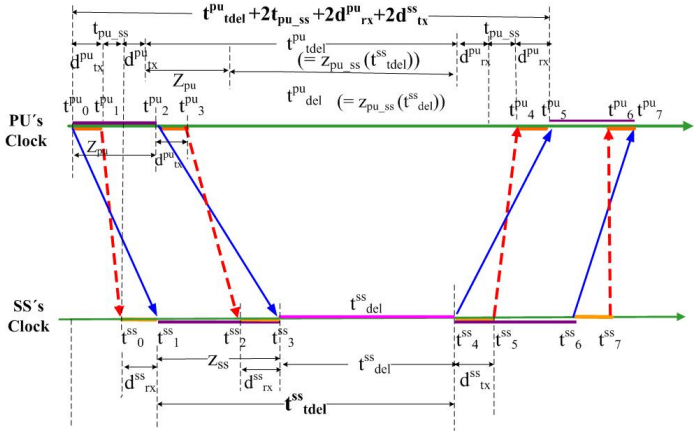

Figure 5: The procedure of the DBSS scheme.

measurement information table (MIT) is established, which consists of: (1) TxID - the sensor ID of the sending sensor, (2) RxID - the sensor ID of the receiving sensor, (3) SynZ - the scale factor of a clock due to time asynchronization between a pair of sensors, (4) RM - the length of received message, (5) PT - the estimated propagation time, and (6) DM - the distance measurement. Assume sensor A and sensor B perform the handshaking procedure, which is initiated by sensor A. Notice that in Table 1 the values in roman font represent the measurements via two-way communication (i.e. A $\rightarrow$ B $\rightarrow$ A) and the values in bold font represent the measurements via three-way communication (i.e. A $\rightarrow$ B $\rightarrow$ A $\rightarrow$ B).

Table 1: Measurement Information Table (MIT)

Sensor A	TxID	RxID	SynZ	RM	PT	DM
	ID_a	ID_b	$\mathbf{Z_{ba}}$	$\mathbf{Z_a}$	t_{ab}	d_{ab}
Sensor B	**TxID**	**RxID**	**SynZ**	**RM**	**PT**	**DM**
	ID_b	ID_a	Z_{ab}	Z_b	$\mathbf{t_{ba}}$	$\mathbf{d_{ba}}$

4.1.1 Forward Communication

Before describing the forward and backward communication procedures between a PU and a SS, denote t_i^{ss} as the time stamp in a SS; denote d_{tx}^{ss} and d_{rx}^{ss} as the delay times of internal device for transmission and reception in a SS, respectively; let t_{del}^{ss} be the response delay in a SS; t_{ss_pu} is the signal propagation time between a SS and a PU. Note that the above notations apply to all nodes in the network. On the basis of conceptual communication protocol (Figure 4), Figure 5 details the procedures of the forward and backward communication between a PU and a SS.

For forward communication (i.e. from a PU to a SS), the operation procedures yield:

1. A PU sends a message (ID_{ss},ID_{pu},t_0^{pu},t_2^{pu}) to a SS. Note that t_0^{pu} is the time of sending the first bit of the message from a sender, $t_2^{pu}$is the time of sending the last bit of the message from a sender. Thus, the message length is $z_{pu} = t_2^{pu} - t_0^{pu}$.

2. Due to the device delay, the actual message sending time stamps of the PU are $t_1^{pu} = t_0^{pu} + d_{tx}^{pu}$ and $t_3^{pu} = t_2^{pu} + d_{tx}^{pu}$.

3. Similarly, the message receiving time stamps of the SS are $t_1^{ss} = t_0^{ss} + d_{rx}^{ss}$ and $t_3^{ss} = t_2^{ss} + d_{rx}^{ss}$. Therefore, the time interval of receiving the message is $z_{ss} = t_3^{ss} - t_1^{ss}$.

4.1.2 Backward Communication

For backward communication (i.e. from a SS to a PU), the procedures are described as follows:

1. After the response delay time t_{del}^{ss}, the SS transmits a message back to the PU along with the time stamp t_4^{ss} (the time on SS's clock when it transmits). Thus, the delay time of the PU is $t_{tdel}^{pu} = z_{pu\_ss} \cdot (z_{ss} + t_{del}^{ss})$, where the scale factor $z_{pu\_ss} = (t_2^{pu} - t_0^{pu})/(t_3^{ss} - t_1^{ss})$.

2. The propagation time t_{pu_ss} can be calculated as

$$\begin{aligned} t_{pu\_ss} &= \frac{[t_5^{pu} - t_0^{pu} - d_{\mathrm{de}}^{pu} - t_{tdel}^{pu} - z_{pu\_ss} \cdot d_{\mathrm{de}}^{ss}]}{2} \\ &\approx \frac{[t_5^{pu} - t_0^{pu} - 2d_{\mathrm{de}}^{pu} - t_{tdel}^{pu}]}{2}, \end{aligned}$$

where $d_{\mathrm{de}}^{pu} = d_{tx}^{pu} + d_{rx}^{pu}$, $d_{\mathrm{de}}^{ss} = d_{tx}^{ss} + d_{rx}^{ss}$, and $d_{\mathrm{de}}^{pu} \approx z_{pu\_ss} \cdot d_{\mathrm{de}}^{ss}$ due to the clock and device characteristics. Thus, the distance is $d_{pu\_ss} = c \cdot t_{pu\_ss}$ with the speed of the signal c.

3. The PU and SS store ($\mathrm{ID}_{ss}, t_{pu\_ss}, d_{pu\_ss}$) and ($\mathrm{ID}_{pu}, z_{pu\_ss}, z_{ss}$) into (RxID,PT,DM) fields in their MITs, respectively (Table 2).

Consequently, Figures 4 and 5 depict the communication protocol and operation procedures for distance estimation and the information processing between a PU and a SS. Note that the same operations can be applied to the communication between a SS and a SU or between a PU and a SU during the network initialization phase. Table 3 illustrates the detailed MIT for a SS.

Table 2: MIT: PU ↔ SS

PU	TxID	RxID	SynZ	RM	PT	DM
	ID_{pu}	ID_{ss}	Z_{ss_pu}	Z_{pu}	$\mathbf{t_{pu\_ss}}$	$\mathbf{d_{pu\_ss}}$
SS	TxID	RxID	SynZ	RM	PT	DM
	ID_{ss}	ID_{pu}	$\mathbf{Z_{pu\_ss}}$	$\mathbf{Z_{ss}}$	t_{ss_pu}	d_{ss_pu}

Table 3: MIT: Network Initialization

PU	TxID	RxID	SynZ	RM	PT	DM
	ID_{pu}	ID_{ss}	Z_{ss_pu}	Z_{pu}	$\mathbf{t_{pu\_ss}}$	$\mathbf{d_{pu\_ss}}$
	ID_{pu}	ID_{su}	Z_{su_pu}	Z_{pu}	$\mathbf{t_{pu\_su}}$	$\mathbf{d_{pu\_su}}$
SS	TxID	RxID	SynZ	RM	PT	DM
	ID_{ss}	ID_{pu}	$\mathbf{Z_{pu\_ss}}$	$\mathbf{Z_{ss}}$	t_{ss_pu}	d_{ss_pu}
	ID_{ss}	ID_{su}	$\mathbf{Z_{su\_ss}}$	$\mathbf{Z_{ss}}$	t_{ss_su}	d_{ss_su}
	ID_{ss}	ID_{ch}	$\mathbf{Z_{ch\_ss}}$	$\mathbf{Z_{ss}}$	t_{ss_ch}	d_{ss_ch}
SU	TxID	RxID	SynZ	RM	PT	DM
	ID_{su}	ID_{pu}	$\mathbf{Z_{pu\_su}}$	$\mathbf{Z_{su}}$	t_{su_pu}	d_{su_pu}
	ID_{su}	ID_{ss}	$\mathbf{Z_{ss\_su}}$	$\mathbf{Z_{su}}$	t_{su_ss}	d_{su_ss}
	ID_{su}	ID_{ch}	$\mathbf{Z_{ch\_su}}$	$\mathbf{Z_{su}}$	t_{su_sh}	d_{su_ch}

4.2 Malicious Node Identification

Figure 6 describes the communication mechanism of the DBSS method for establishing the MIT and performing the detection for a PUEA attack. Assume the spectrum decision of PU is inactive and a MU claims to be a PU. Then node identification is initiated by sensor SS. Here two node identification schemes are considered: (1) Non-Cooperative Node Identification and (2) Cooperative Node Identification.

4.2.1 Non-Cooperative Node Identification

Referring to Figure 6 (i.e. SS ↔ MU), the procedures of node identification are depicted as follows:

1. A SS transmits a sequence with length $z_{ss}^{'} = t_2^{ss'} - t_0^{ss}$, which is n times of the sequence length of the SS (z_{ss}) during the network initialization phase. At the same time, the SS sends a message $(\mathrm{ID}_{pu}, \mathrm{ID}_{ss}, t_0^{ss}, t_2^{ss})$ to a MU with a wrong message sending time stamp of the SS, t_2^{ss}, where $z_{ss} = t_2^{ss} - t_0^{ss}$. That is, $z_{ss}^{'} = n \cdot z_{ss}$ with a real number n, which depends on the SS's clock. Note that the purpose of using a variable message length with parameter n is to confuse the anti-node and against the masquerade attack.

2. Assume the time interval of receiving the message of the MU is $z_{mu}^{'}$. The delay t_{tdel}^{mu} is given by
$$t_{tdel}^{mu} = z_{mu}^{'} + t_{del}^{mu}, \quad (2)$$

3. Accordingly, the MU calculates $z_{ss\_mu}^{(n)} = z_{ss}/z_{mu}^{'}$. Note that z_{ss_mu} should be $z_{ss}^{'}/z_{mu}^{'}$ (i.e. $z_{ss\_mu}^{(n)} = z_{ss\_mu}/n$). Afterwards, the MU replies the message $(\mathrm{ID}_b, \mathrm{ID}_a, t_4^{mu}, t_{del}^{mu})$ to the SS at the time t_4^{mu} with
$$\begin{aligned} t_{tdel}^{ss} &= z_{ss\_mu}^{(n)} \cdot t_{tdel}^{mu} = \frac{z_{ss}}{z_{mu}^{'}} \cdot (z_{mu}^{'} + t_{del}^{mu}) \\ &= \frac{z_{ss}^{'}}{n}(1 + \frac{t_{del}^{mu}}{z_{mu}^{'}}). \end{aligned}$$

4. Thus, referring to (2), the estimated device delay for transmission and reception of the SS yields
$$\hat{d_{\mathrm{de}}^{ss}} = t_5^{ss} - t_0^{ss} - t_{tdel}^{ss} - 2 \cdot t_{ss\_pu} - d_{\mathrm{spec}}^{ss}, \quad (3)$$
where $d_{\mathrm{spec}}^{ss} = d_{tx(\mathrm{spec})}^{ss} + d_{rx(\mathrm{spec})}^{ss}$ and $d_{tx(\mathrm{spec})}^{ss}$ and $d_{rx(\mathrm{spec})}^{ss}$ are the true device delays for transmission and reception of a SS, respectively. Note

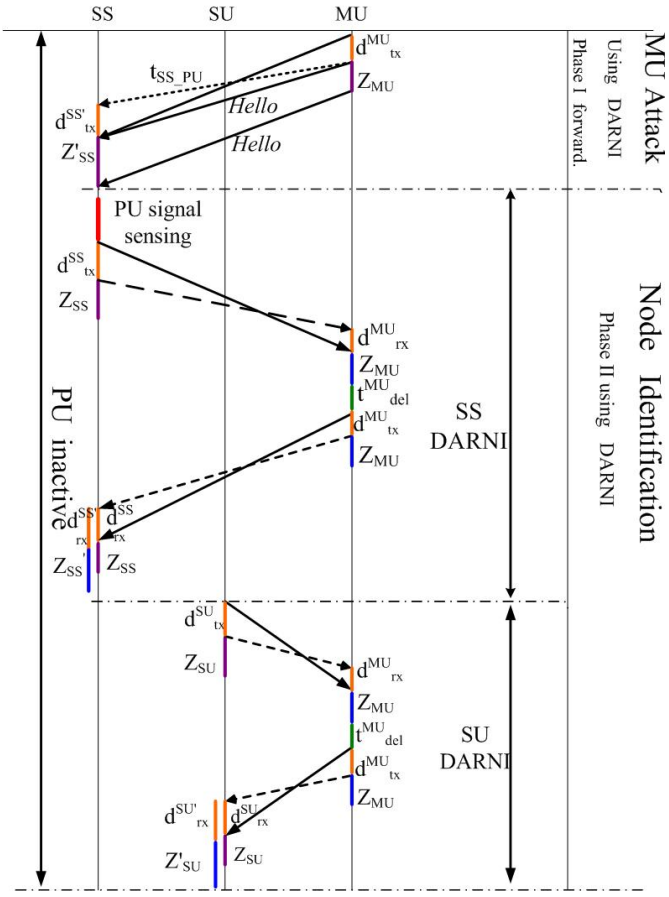

Figure 6: The operating procedures defending against the PUEA attack in a non-cooperative/cooperative manner.

that the time stamp t_5^{ss} is based on the reception time of the message sent from sensor MU and t_{ss_pu} is known from the SS's MIT table.

5. Decision criterion:

   - If $\eta_{ss} \leq \eta_r$, then the MU passes the node identification test.
   - Otherwise, the MU is regarded as an anti-node.

η_{ss} is defined as:

$$\eta_{ss} = |(\hat{d}_{\text{de}}^{ss} - d_{\text{spec}}^{ss})/d_{\text{spec}}^{ss}|, \tag{4}$$

where η_r is a given threshold trust value for node identification. In the general case, $\eta_r \leq 1$.

4.2.2 Cooperative Node Identification

When detecting a PUEA attack, a SS and SUs may work as a group and follow Steps $1 \sim 4$ depicted in Section 4.2.1 to verify a MU. Assume M is the number of SUs to perform cooperative identification. The decision criterion with majority voting for the MU to pass the node identification test is

$$\left(A_{ss} + \sum_{i=1}^{M} B_{su}^{(i)}\right) > \frac{M+1}{2}, \tag{5}$$

where A_{ss} and $B_{su}^{(i)}$ are indicator variables, which are

$$A_{ss} = \mathbf{1}_{\{\eta_{ss} \leq \eta_r\}} \tag{6}$$

$$B_{su}^{(i)} = \mathbf{1}_{\{\eta_{su}^{(i)} \leq \eta_r\}}. \tag{7}$$

Similarly, η_{su} is given by $\eta_{su} = |(\hat{d}_{\text{de}}^{su} - d_{\text{spec}}^{su})/d_{\text{spec}}^{su}|$. Thus, the MU nodes may be cooperatively verified by the node group, a SS and SUs.

5 Simulation Results

The DBSS scheme is evaluated via simulations and numerical examples, considering measurement errors from several sources such as timing resolution, response delay, device delay, and clock calibration. The system performance under masquerade attack is investigated. Suppose that N_s normal sensor nodes in the two-dimensional space are deployed according to the uniform distribution in a square with the side length $l = 100$ meters. For the anti-nodes, we assume that network instances comprise $N_A = 20$, 30, 40, 50, 60, 70, 80, 90 and 100 anti-nodes, respectively, which are with random uniform deployment. Assume

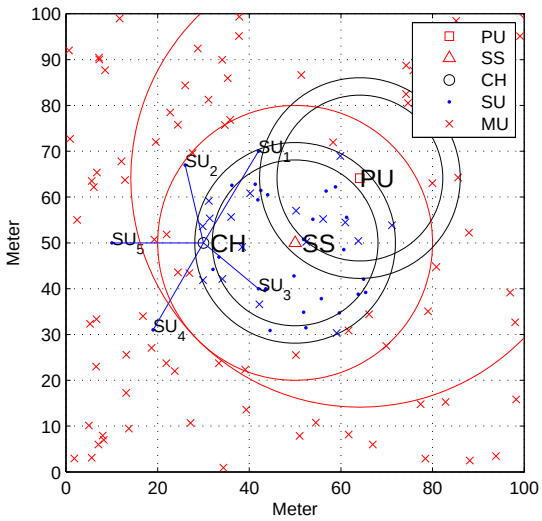

Figure 7: An attack scenario for sensor SS and sensor PU. Note that in our case, sensors SS, PU, SU can be normal devices and sensors MU can be anti-nodes.

the device delay of an anti-node MU, d_{spec}^{mu}, is referenced to d_{spec}^{ss}, which yields $d_{\text{spec}}^{mu} = \alpha_{mu} \cdot d_{\text{spec}}^{ss}$, where $\alpha_{mu} > 0$. Referring to the node deployment in Figure 7 and the parameter settings in Section V of [24], we investigate the typical system performance in a local network.

5.1 The Impact of Device Delay and Time Synchronization

Figure 8 (top) shows the successful detection rate for varying the value of device delay and the number of malicious nodes. Referring to (4), given a threshold trust value $\eta_r = 0.4$, a smaller value of d_{spec} allows a smaller deviation range $|\hat{d}_{\text{de}} - d_{\text{spec}}|$, which increases the successful detection rate. Observe that due to the random uniform deployment of the anti-nodes, the successful detection rate maintains with a small variation even with an increase in density of malicious nodes. Considering an anti-node with synchronous clocking and the same device characteristic ($\alpha_{mu} = 1$), the performance of the proposed secure scheme ($\approx 85\%$) is comparable to that of the belief propagation-based (BP) system in [4] ($\approx 85\%$). In contrast, considering an anti-node with different device characteristic ($\alpha_{mu} \neq 1$), the performance of the proposed secure scheme ($\approx 90\%$ for $\alpha_{mu} = 1.5$) is superior to that of the BP detection system.

With the settings in Figure 8 (top), Figure 8 (bottom) shows the successful detection rate with varying the the time asynchronization of an anti-node. Observe that with varying the value of N_A, the device

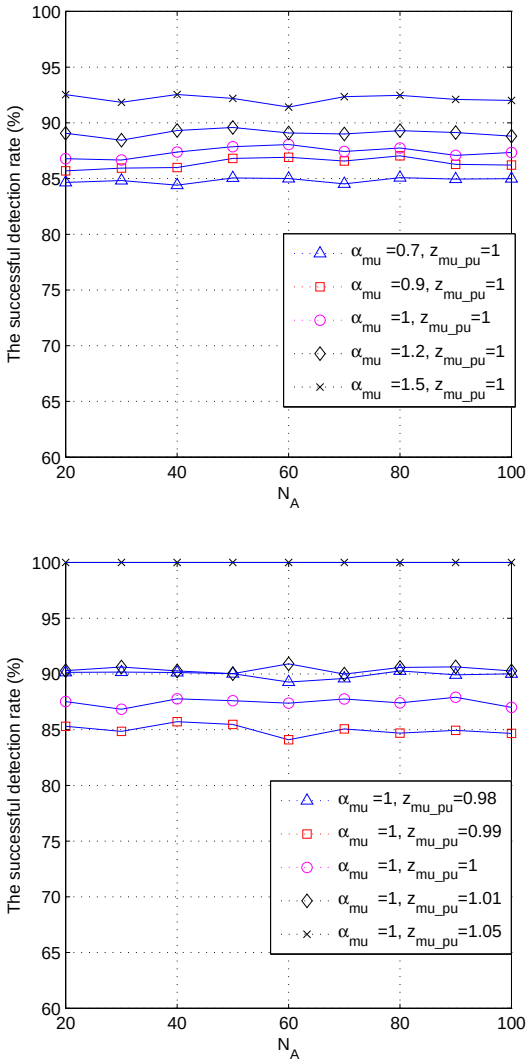

Figure 8: The successful detection rate with varying N_A: given the device delay of anti-nodes (top); given the scale factor of anti-nodes (bottom).

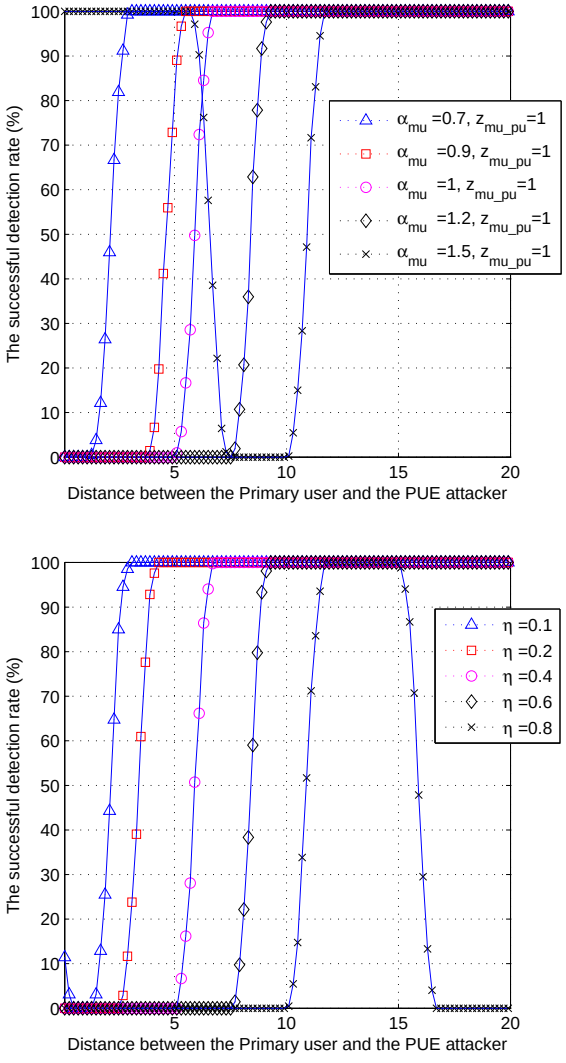

Figure 9: The successful detection rate with varying distance between the primary user and the PUE attacker: given the device delay of anti-nodes (top) and given a threshold trust value η_r (bottom).

characteristic ($z_{mu\_pu} = 0.99$) and and ($z_{mu\_pu} = 1.01$) lead to the detection rate of the proposed secure scheme $\approx 85\%$ and $\approx 100\%$, respectively.

5.2 The Impact of the Distance d_{pu_mu}

Given the threshold trust value ($\eta_r = 0.5$) and with synchronous clocking ($z_{mu\_pu} = 1$), Figure 9 (top) explores the impact of device characteristic on system performance. As shown in Figure 9 (top), given $\alpha_{mu} = 0.7$, as the distance between the primary user and the PUE attacker increases (e.g., $d_{pu_mu} \geq 2$m), the successful detection rate is larger, which represents a higher probability of being a PUE attacker. Observe that there exists a potential undetectable area (e.g., $d_{pu_mu} < 2$m) due to the decision criterion in (4). Accordingly, with $\alpha_{mu} = 1.5$, we have an undetectable area about 10m $> d_{pu\_mu} >$ 7m. Similarly, given the device information ($\alpha_{mu} = 1$) and with synchronous clocking ($z_{mu\_pu} = 1$), Figure 9 (bottom) explores the impact of the threshold trust value on node identification performance. As expected, a lower threshold trust value leads to a smaller undetectable area due to an increased strictness in the decision criterion (4).

5.3 The Impact of Threshold Value η_r

Based on the settings in Figure 8, Figure 10 (top) considers the successful detection rate with varying the threshold η, the device delay of an anti-node α_{mu}, and the time asynchronization of an anti-node z_{mu_pu}. Observe that given $\eta_r = 0.5$ and with varying the value of α_{mu}, the successful detection rate of the proposed system achieves about 83% and 88% for the system with $\alpha_{mu} = 0.9$ and $\alpha_{mu} = 1.2$, respectively.

Figure 10 (bottom) shows the performance improvement with the cooperative identification scheme. Observe that given a device delay, a smaller threshold trust value of η_r leads to a higher successful detection rate. This is attributed to the fact that a smaller η_r contributes to a smaller estimation range, which yields $(1-\eta_r)\cdot d_{\text{spec}} \le \hat{d}_{\text{de}} \le (1+\eta_r)\cdot d_{\text{spec}}$. Given the number of anti-nodes $N_A = 30$, $n = 1$, $\eta_r = 0.5$, and considering anti-nodes with the same device characteristic (i.e. $\alpha_{mu} = 1$) and synchronous clocking with respect to sensor SS, the successful detection rate improves from 85% with the non-cooperative scheme in Figure 10 (top) to 95% with the cooperative scheme associated applying the node group, a SS and a SU, in Figure 10 (bottom).

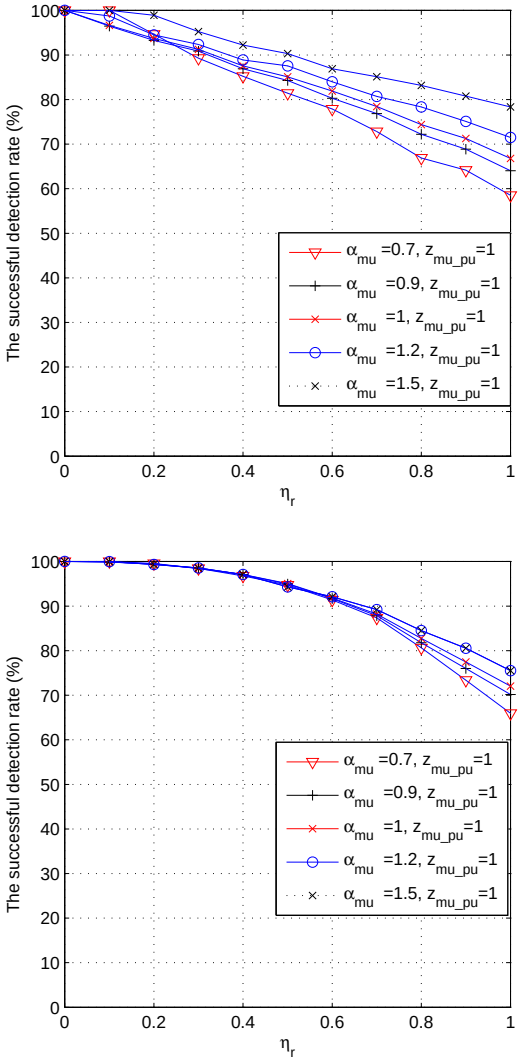

Figure 10: The successful detection rate with varying η_r given the device delay of anti-nodes: non-cooperative method (top); cooperative method with a SU (bottom).

6 Conclusion

This paper develops a new scheme for sensor tasking (e.g., a novel scheme for sensing decision and selecting sensing sensors) in CRSNs, provides the conceptual principle of the proposed scheme against the PUEA attack, and details its implementation. With the development of joint spectrum allocation and topology control algorithms, performance of real-time sensing applications may be further improved. That is, controlling channel access and end-to-end delay for real-time surveillance applications are achievable.

Although the proposed strategy may achieve effective attack detection, further experimental and theoretical extensions are possible. In our future work, we plan to involve more efficient mechanisms to make the protocol faultless and practical, such as developing a feasible algorithm for sensor scheduling and power management, searching for appropriate cooperative schemes, and exploring intelligent physical layer security mechanisms.

Acknowledgements: This research is supported by the Ministry of Science and Technology of Taiwan under Grant MOST-104-2221-E-005-034.

References:

[1] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys and Tutorials*, vol. 15, pp. 428-445, 2013.

[2] R. Chen, J. Park, and J. H. Reed, "Defense against primary user emulation attacks in Cognitive Radio networks," *IEEE JSAC*, vol. 26, no. 1, pp. 25-37, 2008.

[3] T. Yucek and H. Arslan, "A survey of spectrum

sensing algorithms for cognitive radio applications," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, pp. 116-130, 2009.

[4] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1850-1860, Nov. 2012.

[5] B. Wild and K. Ramchandran, "Detecting Primary Receivers for Cognitive Radio Applications," in *Proc. of IEEE DySPAN*, pp. 124-130, Nov. 2005.

[6] Z. Han and H. Jiang, "Replacement of Spectrum Sensing and Avoidance of Hidden Terminal for Cognitive Radio," in *Proc. of IEEE WCNC*, pp. 1448-1452, Mar. 2008.

[7] C. Sun, W. Zhang, and K. B. Letaief, "Cooperative spectrum sensing for cognitive radios under bandwidth constraints," in *Proc. IEEE WCNC*, Mar. 2007, pp. 1-5.

[8] S. Appadwedula, V. V. Veeravalli, and D. L. Jones, "Decentralized detection with censoring sensors," *IEEE Trans. Signal Process.*, vol. 56, no. 4, pp. 1362-1373, Apr. 2008.

[9] S. Maleki, A. Pandharipande, and G. Leus, "Energy-efficient distributed spectrum sensing for cognitive sensor networks," *IEEE Sensors J.*, vol. 11, no. 3, pp. 565-573, Mar. 2011.

[10] M. Najimi, et al., "A Novel Sensing Nodes and Decision Node Selection Method for Energy Efficiency of Cooperative Spectrum Sensing in Cognitive Sensor Networks," *IEEE Sensors J.*, vol. 13, no. 5, pp. 1610-1621, May 2013.

[11] T. Chen, et al., "CogMesh: A Cluster-based Cognitive Radio Network," 2nd *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 168-178, 2007.

[12] Yanchao Xu, et al., "A Cluster-based Energy Efficient MAC Protocol for Multi-hop Cognitive Radio Sensor Networks," *IEEE GLOBECOM*, 2012.

[13] Huazi Zhang, et al., "Distributed Spectrum-Aware Clustering in Cognitive Radio Sensor Networks," *IEEE GLOBECOM*, 2011.

[14] Ozger, M. and Akan, O.B., "Event-driven Spectrum-Aware Clustering in Cognitive Radio Sensor Networks," *IEEE INFOCOM*, 2013.

[15] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. of IEEE Workshop on Networking Technol. for Software Defined Radio Networks* (SDR) 2006, pp. 110-119, Sep. 2006.

[16] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. of IEEE Conference on Computer Communications* (INFOCOM) 2008 mini-conference, Apr. 2008.

[17] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. of the IEEE International Conference on Communications* (ICC'09), June 2009.

[18] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proc. of the 28th IPCCC*, pp. 208-215, Dec. 2009.

[19] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. of the 31st IEEE Symposium on Security and Privacy* (SP'10), pp. 286-301, May 2010.

[20] C. N. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Proc. of the 4th Annual IEEE CCNC*, pp. 1037-1041, Jan. 2007.

[21] A. Alahmadi et al., "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard," *IEEE Trans. Inf. Forensic Secur.*, vol. 9, no. 5, pp. 772-781, May 2014.

[22] Wen, C. Y.; Sethares, W. A. "Automatic decentralized clustering for wireless sensor networks," *EURASIP JWCN* 2005, *5*, 686-697.

[23] Chih-Yu Wen and Ying-Chih Chen, "Dynamic Hierarchical Sleep Scheduling for Wireless Ad-Hoc Sensor Networks," *Sensors*, vol. 9, no. 5, pp. 3908-3941, May 2009.

[24] Shih-Chang Lin and Chih-Yu Wen, "Device-Based Asynchronous Ranging and Node Identification for Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 14, no. 10, pp. 3648-3661, Oct. 2014.