April, 2012

SECURE AUTHENTICATION SCHEME PREVENTING WORMHOLE ATTACKS IN COGNITIVE RADIO NETWORKS

Fatty Salem
Maged Ibrahim, *Helwan University*
I. Ibrahim

Contents lists available at www.innovativejournal.in

Asian Journal of Computer Science and Information Technology

Journal homepage: http://www.innovativejournal.in/index.php/ajcsit

ISSN 2249 - 5126

SECURE AUTHENTICATION SCHEME PREVENTING WORMHOLE ATTACKS IN COGNITIVE RADIO NETWORKS

Fatty Mustafa Salem*, Maged Hamada Ibrahim, Ihab Abd El-wahab Ali

Helwan University, Egypt

ARTICLE INFO

Corresponding Author:
Fatty Mustafa Salem
Helwan University, Egypt
fatty4com@hotmail.com

KeyWords: Cognitive Radio Networks, link signature, Primary User Emulation, wormhole attack.

ABSTRACT

Cognitive Radio (CR) may introduce new classes of security threats and challenges where attacker could disrupt the basic functions of a CR network, cause harmful interference to primary users (PUs) or deny using licensed spectrum of PUs to other Secondary users (SUs) in CR network by emulating PUs. This attack is called the Primary User Emulation (PUE) attack. Additionally, the wormhole attack is possible even if the attacker has not compromised any user, and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and then replays them into the network from that location. A unique challenge in addressing these problems is that The Federal Communications Commission (FCC) prohibits any modification to primary users. Consequently, existing cryptographic techniques cannot be used directly. In this paper, we integrate cryptographic signatures and wireless link signatures to enable primary user detection in the presence of attackers in order to mitigate PUE attacks, and propose an efficient way to prevent wormhole attacks.

INTRODUCTION

Software Defined Radio (SDR) and Cognitive Radio (CR) technology has altered our view of opportunities in wireless communications to a great extent. The advantage of technology is to increase spectral utilization and to optimize the use of radio resources. The Federal Communications Commission (FCC) allows Secondary Users (SUs) to access licensed bands as long as they do not interfere with the transmissions of Primary Users (PUs) [9].

To avoid interfering with primary users, secondary users should detect whether a primary user is using its spectrum or not. There are two main approaches for primary user detection: energy detection and feature detection [10]. In energy detection, secondary users use energy strength of the received signal to identify the primary user's signal, whereas in feature detection, secondary users find some specific features of a signal (include pilot, synchronization word, and cyclostationarity), and use these features to identify the primary user [7, 14, 3]. However, these methods do not authenticate the PU signal.

I t is necessary to have a secure primary user detection method that can distinguish between the primary user's signal and that of the attacker. At first glance, a cryptographic signature seems to be a good solution for this problem. But CRNs face a unique constraint that prevents using such protocol. Specifically, FCC states that "no modification to the incumbent system (i.e., primary user) should be required to accommodate opportunistic use of the spectrum by secondary users" [1]. Hence, any solution that requires changes to primary users is not desirable.

Link signatures (i.e., radio channel characteristics such as channel impulse responses) have been developed recently to obtain secure and robust location distinction [8].

In this paper, we propose an approach does not require any change to primary users, and thus follows the FCC constraint properly. A key component of the approach is a helper node. Though we cannot modify any primary user due to the FCC rules, we can add necessary mechanisms on each helper node, including the use of cryptographic signatures. The helper node thus serves as a "bridge" that enables a secondary user to first verify the cryptographic signatures included in the helper node's signals, and the helper node can detect the presence of the primary user using the temporal link signature scheme [8]. Additionally, our protocol introduces an efficient way to prevent wormhole attack, a severe attack in CRNs that is particularly challenging to defend against.

PREVIOUS WORK

The problem is actually an authentication problem, i.e., when a receiver has detected signals at a particular spectrum, how can the receiver be sure that the signal is indeed sent by the primary User?

Existing spectrum sensing methods rely on physical-layer characteristics of PU transmissions are introduced. Chen et al. proposed an authentication method using received signal strength (RSS) measurements [11]. If the estimated location of a PU deviates from the known PU location by a

threshold, it is detected as the attacker's signal. But, location distinction methods based on RSS may fail if the adversary employs antenna arrays [8].

Liu et al. proposed a PU authentication approach depending on a helper node placed physically close to a primary user [17], but helper nodes are physically bound to PUs which may be TV towers with thousands of watts of transmission power, covering an area of tens of square miles [4]. Similar to the approach in [18], they are a combination of cryptographic and link signatures to authenticate PU's signal, but in [18] helper nodes need only be deployed within the area of the SUs, independent of the location of the PUs. Hence, helper nodes can be low-power. But both approaches didn't introduce an efficient solution for the problem of wormhole attack [2].

Existing cooperative sensing schemes aim to detect the anomaly in the reported sensing data and establish a mechanism to distinguish the malicious users from the authentic ones such that malicious users can be excluded from the cooperation to ensure the integrity of the sensing decisions.

In [12], a simple outlier detection is proposed for the pre-filtering of the extreme values in sensing data. The trust factor that measures the CR user's reliability is then evaluated as the weights in calculating the mean value of received sensing data. In that way, cooperative sensing can be more reliable by building trust toward CR users that report a sensing value close to the mean of all collected results at the fusion center. The method is extended in [19] to detect malicious users by the outlier factors, which are calculated based on the weighted sample mean and the standard deviation of the energy detector outputs. The outlier factors can be adjusted according to the dynamic PU activity and the observations from closest neighbours in a neighbourhood to further improve the detection of malicious users.

The approach in [20] thus proposes a secure trust-based authentication approach for CRNs. A SU's trust value is determined from its previous trust behaviour in the network and depending on this trust value, it is decided whether or not this CR node will obtain access to the Primary User's free spectrum. In [15], the authors extend the Weighted Sequential Probability Ratio Test (WSPRT) [5] by replacing the binary local report with N-bits local report to achieve a better detection performance. And many other cooperative sensing schemes are proposed in [21, 22, 23], but we can't assume a trust of secondary users as they may be any radio devices that use licensed channels for communication.

Anard et al. proposed an analytical model for detecting primary user emulation attacks [13]. In their system model, malicious devices emulating the PU signal are deployed at fixed locations, at least R0 units away from any SU. Using simplified propagation models. Whereas, Chen et al. modelled the PU emulation problem as an estimation theory problem [16].

THE MODEL

Now, we aim to describe the system and the adversary model.

1 System Model

Entities in CRs are classified into three categories:

Primary Users: The licensed users to use a fixed spectrum, which can be divided to a set of *n* orthogonal frequency bands, referred to as channels. But, following the FCC rules, no any modification to primary users to provide secure communication in CRNs.

Secondary Users: FCC allows secondary users to use a spectrum if the primary user is not using it. But, secondary users should constantly monitor the usage of the spectrum to avoid interference with the primary user.

Helper Nodes: they are trusted nodes in the network serve as "bridges" that can detect the presence of the primary user, and enable a secondary user to verify the cryptographic signatures included in their signals.

2 Adversary Model

In the adversary model, The goal of the adversary is to deny using licensed spectrum to other Secondary users in CR network by emulating Primary User Signals (PUE).

Additionally, the adversary may records packets at one location in the network, tunnels them to another location in the network, and then replays them into the network from that location without the need to compromise any node in the network.

THE PROTOCOL

We introduce a PU authentication system based on using fixed helper nodes deployed within the area of the SUs, independent of the location of the PUs. It is obvious that secondary users can't play the role of helper nodes as the secondary user may be any mobile device, and estimating the impulse response of the channel between the primary user and the secondary user is not easy due to the mobility of the secondary user.

In our system, helper nodes are responsible for authenticating the PU signal and trustworthy broadcasting spectrum status information. Initially, the helpers authenticate the PU signal using temporal link signatures in [8]. Since both the helpers and the PUs are stationary, there is no need for repeating the training process after the initial training is completed.

1 Authenticating Primary User's Signal at Helper Node

The approach presented in [8] showed that the impulse response of mutlipath fading channel between two fixed locations provides sufficient "uniqueness" to serve as a signature of the link between these locations. When PU *i* transmits a signal $s_i(t)$, helper *j* receives signal:

$$r(t) = s_i(t) * h_{i,j}(t)$$

Where * denotes the convolution operation, and the impulse response of the channel between PU *i* and helper node *j* is:

$$h_{i,j}(t) = \sum_{l=1}^{L} \alpha_l e^{j\phi_l} \delta(t - \tau_l)$$

where L is the total number of multipaths, $\delta(t)$ is the Dirac delta function, and α_l, ϕ_l and τ_l are the channel gain, phase, and time delay of the *l-th* multipath component, respectively [8].

To construct a link signature, the $s_i(t)$ must be known at the helper. Hence, link signatures can be constructed using known sequences employed by the PUs for control. For instance, digital TV transmissions consist of a sequence of segments. For every 313 segments, a Data Field Sync segment of one known 511- bit PN sequence, and three known 63-bit PN sequences is used for synchronization [6]. Hence, the impulse response of the channel can be computed. The helper can estimate the impulse response of the channel during the transmission of the known signal and stores it in the training phase, which needs to be

performed only once. it is assumed that no adversary is present.

Then, helper node can authenticate PU's signal by comparing the computed impulse response with the stored one. The helper node computes the distance between the newly measured link signature and the historical link signatures. If the distance is larger than a threshold, then a location change is detected.

Using link signatures, a helper *i* can construct *n*-bits occupancy vector V_i indicating the set of the *n* channels. The *jth* bit of V_i is set to one if channel *j* is currently used by the PU. Otherwise, it is set to zero.

2 Secure broadcasting of authentic spectrum status information:

Helper nodes are responsible for trustworthy broadcasting spectrum status information to the secondary users within its coverage area.

SU(T1) → (T2)helper : Request to helper *i*.

Helper (T3) → (T4) SU : $sig_i(m_i)$, $m_i = V_i, SN_i, T_2, T_3$

SU: verify the signature $sig_i(m_i)$, if the signature is verified, do the next steps, else abort.

: calculate end-to-end delay $d = [(T_2 - T_1) + (T_4 - T_3)]/2$

: If $d \le d_{\max}$ then accept the occupancy vector, else abort.

Here, SN_i denotes a transmission sequence number used for verifying the freshness of V_i, and $sig_i(m_i)$ denotes the cryptographic signature of helper node *i* on message m_i. While *d* represents the calculated end-to-end delay between the SU and the helper node *i*, and $d_{\max}$ is the pre-computed maximum delay which provides a distance within range R (the coverage area of helper nodes). T1, T2, T3 and T4 represent the times at either SU or the helper node as indicated.

A helper *i* responds to the secondary user with the following information:

$sig_i(m_i)$, $m_i = V_i, SN_i, T_2, T_3$

The secondary user verifies the authenticity and integrity of m_i by verifying the validity of the cryptographic signature $sig_i(m_i)$ using the public key of the helper node *i*. Message m_i that fails to be authenticated is discarded. Else, SU calculates end-to-end delay *d* between the SU and the helper node *i.* Then, SU compares the end-to-end delay with the pre-computed maximum delay $d_{\max}$ (assuming the speed of the radio channel, i.e. the speed of light) which affords a maximum distance R (the coverage area of the helper node). If $d \le d_{\max}$, SU accepts the occupancy vector, else discards the received message from helper node *i*.

SECURITY ANALYSIS:

In this section, we discuss the security of our proposed approach:

1 PUE Attacks

The attacker can emulate the primary user, and can thus convince the other secondary users that the primary user is using the spectrum when it is not. This can be achieved by mimicking characteristics of PU signal or by recording and replaying PU transmissions.

As recommended by FCC regulations, it would not be possible to place the attacker close to a PU, hence the received signal is transmitted by PU due to the unique characteristic of the radio frequency channel that are exploited in the construction of link signature.

2 Helper Impersonation Attacks

The adversary may attempt to impersonate a helper in order to provide false occupancy vectors to SUs. The use of digital signature for authenticating the broadcast of the messages m_i containing the occupancy vectors, prevents the adversary from fabricating false spectrum status information. But the adversary may choose to replay old cryptographic signature that already broadcasted by the helpers and thus will be verified correctly at SUs.

To avoid such replay attacks, the sequence number SN_i is included with the broadcast of any message m_i. Assuming that a SU under attack hears at least one legitimate helper, the SN received on a message from the legitimate helper will be larger than the SN of the replays. And hence, the received occupancy vector will be discarded as an old replay. Here, we exploit the fact that the network of helpers is loosely synchronized to the same SN.

Additionally, an attacker may record spectrum authentication messages of one remote helper node in the network, tunnel them to another location in the network, and then replay them into the network from that location.

The adversary may replay spectrum authentication messages via a wormhole tunnel between two (or more) parts of the network. The adversary deploys a fast link (i.e., wired or long-range wireless) between two locations in the network. As the sequence number is increased after period of time, a fast tunnelling and replay may contain m_i with up-to-date SN from the legitimate helper nodes. For this purpose, the algorithm includes measuring the end-to-end delay and comparing it with the pre-computed maximum delay $d_{\max}$ which affords a maximum distance R. If $d \le d_{\max}$, SU accepts the occupancy vector, else discards the received message from helper node *i*. This way ensures that the received message is transmitted from a legitimate helper node within a range of R.

CONCLUSION

In our system, we introduced an authentication scheme that provides secure verification of the spectrum status information following the FCC rule that prohibits any modification to primary users. our system can accommodate mobile SUs without need for repeating the training process with every location change. Moreover, helper nodes need only be deployed within the area of the SUs, independent of the location of the PUs. Hence, the helpers can be low-power. Additionally, our system introduces an efficient solution for replay attack and wormhole attack.

REFERENCES

[1] Federal Communications Commission. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies. ET Docket, (03-108), Dec. 2003.

[2] Y. Hu, A. Perrig, & D. Johnson, (2003) Packet leashes: a defense against wormhole attacks in wireless networks. In Proceedings of INFOCOM, 1976–1986.

[3] A. Sahai & D. Cabric, (2005) Cyclostationary feature detection. Tutorial presented at the IEEE DySPAN 2005 (Part II).

[4] B. Wild & K. Ramchandran, (2005) Detecting primary receivers for cognitive radio applications. In Proceedings of IEEE DySPAN, 124–130.

[5] E. Visotsky, S. Kuffner, & R. Peterson, (2005) On collaborative detection of TV transmissions in support of dynamic spectrum sharing. in Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 338–345.

[6] A.T.S. Committee. ATSC digital television standard (a/53) revision e, with amendments no. 1 and 2,. http://www.atsc.org/cms/, 2006.

[7] L. P. Goh, Z. Lei, & F. Chin, (2007) Dvb detector for cognitive radio networks. In Proceedings of the International Conference on Communications, 6460-6465.

[8] N. Patwari & S. Kasera, (2007) Robust location distinction using temporal link signatures. In Proceedings of MOBICOM, 122-133.

[9] FCC. Second report and order and memorandum opinion and order, FCC-08-260, 2008.

[10] H. Kim & K. G. Shin, (2008) In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?. In Proceedings of the 14th ACM international conference on Mobile computing and networking, 14-25.

[11] R. Chen, J. Park, & J. Reed, (2008) Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications **26**, 25–37.

[12] P. Kaligineedi, M. Khabbazian, & V. Bhargava, (2008) Secure cooperative sensing techniques for cognitive radio systems. in IEEE International Conference on Communications (ICC), 3406–3410.

[13] S. Anand, Z. Jin, and K. Subbalakshmi. (2008) An analytical model for primary user emulation attacks in cognitive radio networks. In Proceedings of IEEE DySPAN, 1 –6.

[14] Y. Qi, T. Peng, W. Wang, & R. Qian, (2009) Cyclostationarity-based spectrum sensing for wideband cognitive radio. In Proceedings of the 2009 WRI International Conference on Communications and Mobile Computing, 107-111.

[15] Fuping Hu, Shu Wang, & Zhuo Cheng, (2009) Secure cooperative spectrum sensing for Cognitive Radio networks. IEEE : Military Communications Conference (MILCOM), 18-21.

[16] Z. Chen, T. Cooklev, C. Chen, & C. Pomalaza-Raez. (2009) Modeling primary user emulation attacks and defenses in cognitive radio networks. In Proceedings of the 28th IEEE International Performance Computing and Communications Conference (IPCCC), 208 –215.

[17] Y. Liu, P. Ning, & H. Dai, (2010) Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, 286–301.

[18] Swathi Chandrashekar & Loukas Lazos, (2010) A Primary User Authentication System for Mobile Cognitive Radio Networks. The 3rd International Workshop on Cognitive Radio and Advanced Spectrum Management (COGART).

[19] P. Kaligineedi, M. Khabbazian, & V. Bhargava, (2010) Malicious user detection in a cognitive radio cooperative sensing system. IEEE Transactions on Wireless Communications **9**, 2488–2497.

[20] S. Parvin, Song Han, & Biming Tian,F.K Hussain, (2010) Trust-Based Authentication for Secure Communication in Cognitive Radio Networks. IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), 589 – 596.

[21] Y ali Zhu, Di Suo, & Zehua Gao, (2010) Secure Cooperative Spectrum Trading in Cognitive Radio Networks: A Reversed Stackelberg Approach. International Conference on Multimedia Communications (Mediacom), 202-205.

[22] Tengyi Zhang, Tsang, & D.H.K., (2011) Optimal Cooperative Sensing Scheduling for Energy-efficient Cognitive Radio Networks. In IEEE proceeding of INFOCOM, 2723 – 2731.

[23] Weng-Chon Ao, Shin-Ming Cheng, & Kwang-Cheng Chen, (2012) Connectivity of Multiple Cooperative Cognitive Radio Ad Hoc Networks. IEEE Journal on Selected Areas in Communications **30**, 263-270.