A Secure and Anonymous Cooperative Sensing Protocol for Cognitive Radio Networks

Helena Rifà-Pous
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Rb. del Poble Nou, 156. 08018-Barcelona
hrifa@uoc.edu

Carles Garrigues
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Rb. del Poble Nou, 156. 08018-Barcelona
cgarrigueso@uoc.edu

ABSTRACT

Spectrum is an essential resource for the provision of mobile services. In order to control and delimit its use, governmental agencies set up regulatory policies. Unfortunately, such policies have led to a deficiency of spectrum as only few frequency bands are left unlicensed, and these are used for the majority of new emerging wireless applications. One promising way to alleviate the spectrum shortage problem is adopting a spectrum sharing paradigm in which frequency bands are used opportunistically. Cognitive radio is the key technology to enable this shift of paradigm.

Cognitive radio networks are self-organized systems in which devices cooperate to use those spectrum ranges that are not occupied by licensed users. They carry out spectrum sensing in order to detect vacant channels that can be used for communication. Even though spectrum sensing is an active area of research, an important issue remains unsolved: the secure authentication of sensing reports. Not providing security enables the input of false data in the system thus empowering false results. This paper presents a distributed protocol based on wireless physical layer security, symmetric cryptography and one-way functions that allows determining a final sensing decision from multiple sources in a quick and secure way, as well as it preserves users' privacy.

Keywords

authentication, cognitive radio, cooperative sensing, privacy, wireless physical layer security

1. INTRODUCTION

The inherent demand for wireless services has led to an increased demand for radio spectrum. The necessary sharing of this finite resource has traditionally been regulated using fixed spectrum assignment policies by governmental agencies. This means that regulatory agencies, such as the Federal Communications Commission (FCC), allocate spectrum for particular types of services on a long term basis. The problem of this assignment policy is that it has led to a considerable inefficiency in spectrum utilization. Studies conducted by the Spectrum Policy Task Force show that most of the licensed spectrum is largely under-utilized [5].

One promising way to alleviate the spectrum shortage problem is adopting a spectrum sharing paradigm in which frequency bands are used opportunistically. In this scheme, those who own the license to use the spectrum are referred to as primary users, and those who access the spectrum opportunistically are referred to as secondary users. Secondary users must not interfere with primary ones, who always have usage priority.

The enabling technology for opportunistic sharing is cognitive radio (CR) [10]. A CR is a system that senses its electromagnetic environment and can dynamically and autonomously adjust its operating parameters to access the spectrum. CR terminals form self-organizing networks capable to detect vacant spectrum bands that can be used without harmful interference with primary users. Once a vacant band is found, secondary users coordinate themselves in order to share the available spectrum.

Performing reliable spectrum sensing is a difficult task. Wireless channels can suffer fading, thus causing the hidden node problem in which a secondary user fails to detect a primary transmitter. The most important challenge for a CR is to identify the presence of primary users, and, for this reason, secondary users must be significantly more sensitive in detecting primary transmissions than primary receivers.

To increase the spectrum accuracy without increasing the hardware complexity cooperative and distributed sensing approaches (DSS) have been proposed as discussed in [9, 20]. In DSS, multiple secondary users cooperate and share their local sensing results, which are then merged together to reach a final decision. Several data fusion schemes have been proposed to merge the sensing data observed by each secondary user [1, 19, 15]. In order to correctly balance the contributions of the users and ensure a reliable data fusion, these protocols try to characterize the users, learn how they behave and at which extend they shall be trusted, using either probabilistic or reputation models.

However, in order to effectively track users, the sensing contributions that they make must be authenticated. Some proposals have been presented to authenticate users' spectrum decisions [6, 4, 13]. Yet, they introduce a notable overhead in the network since the initialization phase of the protocols is based on public key cryptography, and the sensing phase requires several cryptographic operations and/or explicit time delays. Moreover, they are not privacy sensitive. Privacy is becoming increasingly important with the dawn of the Internet and it is one of the main criticisms of the ubiquitous computing technologies, like cognitive radio networks.

Privacy can be defined as "'the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"' [17]. Network protocols should not spread information about a user without his consent, and they shall be designed so that this information is not mandatory.

Wireless networks are specially sensitive to privacy problems because of their broadcast nature. Today's secure cooperative sensing protocols require that users be authenticated using a public key and an identity certificate. This entails that both the manager of the network and the users in the near zone, know the location of the sender, her connectivity profile, with whom she tends to communicate, etc. Citizens may be concerned that they are constantly being watched, surveilled, and that their personal details and situation can get in the wrong hands and be exploited by unwanted or even criminal people.

This paper overcomes the problems of past proposals designing a cross-layer solution exclusively based on light symmetric key cryptography and providing a protocol that is robust against identity and location disclosure attacks offering privacy protection measures.

The paper is organized as follows. An overview of the goals and the structure of the protocol is provided in section 2. The steps of the secure and anonymous cooperative sensing protocol are presented in section 3. The security and cost of the protocol are analysed in section 4. The paper ends with some concluding remarks.

2. OVERVIEW

In order to perform distributed sensing securely, the cooperative system should identify the users that participate in the sensing process, authenticate their claims, and weigh up their contribution to the final decision based on their reputation or probability of successful detection. Our protocol focuses on the mechanisms required to identify the users, authenticate their sensing results, and prevent them from injecting fake sensing data into the system. The proposed protocol uses a centralized cooperation model among CR's, and it assumes that the secondary users and the fusion center can use a common control channel to exchange messages.

One of the key goals of the protocol design is to develop an efficient solution suitable for constrained devices. Therefore, the cryptography involved in our proposal is based on simple symmetric key algorithms.

The main challenge of symmetric key systems is how to distribute and manage the keys among the authorized nodes. Different processing lightweight solutions have been proposed in the scope of ad hoc sensor networks, which pre-distribute or dynamically generate the secret keys using probabilistic approaches (see a review in [18]). However, the cost of such schemes is high in terms of storage and/or communication complexities, thus limiting their applicability.

Recently, another kind of proposals has emerged that exploits the basic characteristics of the wireless physical channel to generate information-theoretic secure keys between two parties [21, 8, 11, 7, 2]. The wireless channel is assumed to be reciprocal (i.e. the channel between two antennas is symmetrical, irrespective of the propagation environment) and suffers temporal and spacial variations. The variation over time is caused by motion and multipath fading. Typically, the transmitted signal travels to the receiver along a multitude of paths. As the various paths vary in length, the signal transmitted at a particular instant will arrive at the receiver over a spread of times, causing problems with phase distortion and intersymbol, i.e. fading. If the transmitter, receptor, or any of the intermediate objects that cause multipath move, the effects of fading will vary over time. Besides, the properties of a radio channel are unique to the locations of the two endpoints of the link. Radio channels decorrelate over distances of the order of half a wavelength (λ). Hence, and eavesdropper at a third location will measure a different uncorrelated radio channel than the endpoint nodes.

Some works exploit the temporal received signal strength (RSS) variations of a radio channel to generate the secret bits [11, 2]. Some others use the spatial selectivity [21, 8] and others, use the frequency selectivity of multipath fading [7]. These last ones do not require node movement and are better suited for static networks. However they use more bandwidth (different frequency channels) to generate the key.

In our system, the need to generate or distribute symmetric keys occurs when a node decides to participate in a cooperative sensing process. This may be motivated by two circumstances: (1) the node moves into the coverage area of a fusion centre and is automatically introduced in the sensing process, or (2) the node starts the sensing on his own initiative because it must send some data. In either case, the entry of the node in the network can be tied to a certain movement: natural in the first case, or induced by the protocol in the second one. Since when a user starts the sensing on his own initiative he is aware of that, the application can asks the user to shake the terminal. Thus, we base the generation of the initial secret key required for the sensing protocol on a temporal selective wireless physical layer security protocol. In particular, we use the method proposed by Patwari et al. [11]. Their results show that high entropy bits can be quickly obtained when there is a significant movement in the environment and that the generated stream passes the randomness tests of the NIST [16]. Using this scheme, a given node and the fusion centre can initially create a secret shared key that will be used from then on to authenticate each other.

In addition to having a group of keys to establish peer to peer connections with every node in its domain, the fusion centre needs a way to authenticate its broadcast messages. To do so, we use a low-cost solution based on hash chains: the $\mu Tesla$ protocol [12]. Hash chains are composed of a sequence of values that can only be computed in one direction. A hash chain of length N is constructed by applying a one-way hash function H(.) recursively to an initial seed value v_N: $v_{N-1} = H(v_N)$, $v_{N-2} = H(v_{N-1})$, $\cdots$, $v_0 = H^N(v_N)$. In general, $v_i = H(v_{i+1}) = H^{N-i}(v_N)$. The last element of the chain v_0 is called the top value, and is indeed, a commitment to the entire chain. We can verify any element of the chain through v_0. The elements of the chain are revealed in ascending order $v_0; v_1; ..; v_N$ so that the disclosure of an element does not disclose any information of the next elements. In $\mu Tesla$ the elements of a hash chain are used as one-time keys. As we will see in section 3.3, each time a fusion centre has to send an authenticated broadcast message, it uses one of these keys.

During the sensing process, node's sensing reports are protected from forgery and manipulation using a Hash Message Authentication Code (HMAC). HMAC is a fast and simple way to perform symmetric signatures. It is based on using a hash function H over a message m and a shared secret key k:

$$H(k \oplus opad||(H((k \oplus ipad)||m))$$

where $ipad$ is the byte 0x36 repeated B times, and $opad$ is the byte 0x5C repeated B times, with B the byte length of the working data blocks of the compression function involved in the hashing process. The symbol $||$ represents the concatenation operation.

The result of an HMAC operation has the length of the hash output. Yet, in some cases, it can be truncated outputting the t leftmost bits of the HMAC computation for some parameter t, in order to obtain a shorter value and reduce the bandwidth overhead involved in its transmission. This kind of HMAC is called truncated HMAC-t. Shorter t values increase the chance that a source with no knowledge of the secret key can present a purported HMAC-t on the plaintext message that will pass the verification procedure. Therefore, t must be chosen to optimize the trade-off between security and efficiency.

2.1 Adversary Model

In our model we assume that the adversary can listen to all communications in the network. It can also measure the channels between itself and the users of the network, and between itself and the fusion centre. Further, it is free to move or stay static, and it can be anywhere in the network except next to any network members while they are extracting their shared key. To ensure that the adversary measures a different, uncorrelated radio channel than the users, it has to be located away, a few multiples of the wavelength of the radio waves being used [8]. We also assume that the adversary knows the physical layer key extraction algorithm, as well as the secure and anonymous cooperative sensing protocol.

The adversary can operate at the packet, bit, or signal levels, but cannot jam the channel; i.e., our methodology does not prevent from denial of service attacks. However, the attacker can be active and send data packets to other users and to the fusion centre.

3. SECURE AND ANONYMOUS SENSING PROTOCOL

This section presents the detailed steps of our protocol for the secure and anonymous authentication of users' sensing reports. The protocol is divided in four phases. The first phase is the registry of users; the second one is the authentication of users that want to participate in the sensing process; the third is the sensing assignment; finally, the fourth is the collection of sensing results.

3.1 Phase 1: User Registry

When a user enters in a cognitive radio domain, she contacts the fusion centre (which can be, for instance, the base station) and asks permission to join the cognitive radio network. If she is already registered at the fusion centre, the mutual authentication protocol (see section 3.2) is executed. Otherwise, she registers at the fusion centre in order to be able to use the available channels of the spectrum, and to collaborate (if required) in the sensing process. In the registration phase, the user and the fusion centre agree on a key in such a way that both influence the outcome, using a protocol based on [11]. The agreed key will be used in subsequent encounters to authenticate each other.

To agree on a shared key, the user and the fusion centre exploit the fact that a particular wireless channel between two entities is unique, varies like a stochastic process, and cannot be inferred by external parties.

1. User U and the fusion centre FC transmit known probe signals to one another. Each party can use the received signal along with the probe signal to compute an estimate of the channel: the FC estimates $\widehat{h_{FC}}$ and U estimates $\widehat{h_U}$.
2. From the channel estimations $\widehat{h_{FC}}$ and $\widehat{h_U}$ the entities derive a bit stream. The bit streams generated by FC and U are not equal due to the presence of noise and interference in the transmission, hardware limitations, manufacturing differences, and the fact that both entities do the sampling in different times (a lot of commercial transceivers are half-duplex and cannot send and receive packets at the same time). Hence, in this step FC and U must reliably reconcile channel estimations without revealing any information to an eavesdropper, since the channel characterization is the seed for a common secret. To do so, FC and U execute an iterative reconciliation protocol that divides the estimated stream in blocks and sends permutation and parity information of each block to the other party in order to find out which blocks match and which do not.
3. Upon agreeing on a channel estimation, the bit stream must be modified to amplify its secrecy. Some portions of the bit stream are removed because of the revealed information in the reconciliation step, or because subsequent bits exhibit short-term correlations. Finally, a statistically random bit stream is obtained.
4. The steps 1 to 3 are repeated iteratively until the shared key s is 20 bytes long. Note that the channel is static during its coherence time period and thus, it can only be probed once during this time. So, mobility of the end-points or environment changes are desirable in order to rapidly obtain the required bits. This can be obtained if the user simply shakes her terminal. Since this phase has to be performed only once in the lifetime of a node in a network, this issue does not negatively effect the usability of the system.
   The resulting shared key s is divided in two parts: (1) the first 8 bytes constitute a permanent value that is the user identifier: $Id_U = s_{1-8}$, (2) the last 12 bytes are a secret key k that will be periodically updated: $k = s_{9-20}$. The key will be periodically updated in order to strengthen its security. Moreover, the entities will compute a temporal index identifier for Id_U that will be used to conceal the user identity from eavesdroppers the next time the user joins the fusion centre domain. The temporal index is computed as:

   $$pid_U = H(Id_U||k)_{64}$$

   where $H(a)_t$ is the hash function over the message a truncated to t bits, and $||$ represents the concatenation function.

3.2 Phase 2: Session Authentication

When a registered user enters a cognitive radio domain, she asks permission to the fusion centre to join the network. This process requires mutual authentication using digital signatures. Besides, the fusion centre commits to a hash chain using the $\mu Tesla$ protocol [12]. The fusion centre commits to the same hash chain V with all users. V is generated from a random number, has N elements, and the top value of the chain is V_0.

The following are the detailed steps carried out during this phase.

1. When a user U wants to join a cognitive radio network where she is already registered, she sends a join request to FC. The

message contains the identity of FC Id_{FC}, an index to the identity of the user pid_U, and a challenge nonce n_U generated by U.

$$JoinReq_1 = \{Id_{FC}, pid_U, n_U\}$$

2. After verifying pid_U belongs to a registered user, FC decides whether or not to accept U into the network. This decision will be based, for example, on the reputation earned by U in previous processes. The implementation of these mechanisms is out of the scope of this paper.
   If U is accepted in the network, FC uses the session key k shared with U to sign the top value of its chain V_0, the length N and the received nonce n_U with an HMAC function. This signature is used to construct the following response:

   $$JoinResp_1 = \{V_0, N, HMAC_k(n_U, V_0, N)\}$$

3. Upon receiving $JoinResp_1$, U verifies the HMAC signature and the freshness of the hash chain V_0 (i.e. it has not been used before). The signature allows U to verify the authenticity and integrity of the received data. If the signature is correct, U signs V_0 and sends the signature to FC.

   $$JoinReq_2 = \{HMAC_k(V_0)\}$$

4. FC authenticates U by verifying the signature of $JoinReq_2$. If correct, FC updates U's temporal index identifier and the key they share as follows:

   $$k' = H(k||n_U||V_0)$$

   $$pid'_U = H(Id_U||k')_{64}$$

   k' and pid'_U will be used the next time U starts an authentication session with FC. If the authentication is successful, FC sends an acknowledge message to the user.

5. U updates her next index and shared key performing the same computations as FC.

3.3 Phase 3: Sensing Assignment

In the Sensing Assignment phase, the fusion centre requests the active users of the domain to sense a certain set of frequency bands. To do so, it sends a signed broadcast message. The signing key is an element of the hash chain it has committed to in the Session Authentication phase (see section 3.2). Users will not be able to verify the message until the fusion centre reveals the signing key, which will do after $\Delta\, t$. $\Delta\, t$ is a period of time designated by the fusion centre as the sensing interval. The fusion centre expects sensing reports from the users every $\Delta\, t$ seconds.

The following are the detailed steps carried out during the Sensing Assignment phase:

1. At time t_0, FC splits the time into equal length intervals $\Delta\, t$ and broadcasts a signed message containing the schedule they will use in the sensing process, the list of channels that have to be sensed ($ChList$), and a $mode$ parameter with detailed information about the sensing mode: hard cooperation, soft cooperation based on energy detection, soft cooperation based on cyclostationary feature detection, etc.

   $$SensReq_{t_0} = \{Id_{FC}, Id_s, ChList, mode, t_0, \Delta\, t, \\ HMAC_{V_{Id_s}}(Id_{FC}, Id_s, ChList, mode, t_0, \Delta\, t)\}$$

   where

   $$ChList = [\ Ch_0, Ch_1, \cdots Ch_k\ ]$$

   In the above expression, Id_s is a session counter; it is incremented by one unit each time the fusion centre broadcasts a sensing request. The key used to sign the message is V_{Id_s}, i.e. an element of the fusion centre hash chain. The fusion centre will reveal its value at time $t_0 + \Delta\, t$.

2. U verifies the signature of the sensing request and, if correct, starts the sensing process.

3.4 Phase 4: Collection of Local Sensing Results

Users sense the spectrum and send their results to the fusion centre using an HMAC signature. The key k used to compute the HMAC signature is the one associated with the current time frame. The following are the detailed steps carried out in this phase.

1. U senses the channels listed in $ChList$ and sends the results $SensRes$ to FC. These results can be binary decisions, long test statistics, or data captured in the sensing. This depends on whether hard or soft cooperation is employed. To enable the authentication of the sensing results, these are sent as follows:

   $$\begin{aligned} SignRes_t = \{&pid_U, SensRes_t, t, \\ &HMAC_k(pid_U, SensRes_t, t)\} \end{aligned}$$

   $SignRes_t$ includes the present time t to avoid replay attacks. The key K used to construct the HMAC signature is the one that U and FC share for the present session.

2. FC receives the sensing results and verifies their authenticity and integrity using the key shared with each user.

4. DISCUSSION

The proposed protocol allows the authentication of sensing reports with a minimum overhead. Users do not need to hold a public key certificate or some predefined shared keys in order to enter in the system. They can register at the fusion centre on-line using the intrinsic security of the wireless physical channel. In order to become members of the CRN, the disclosure of personal information to the fusion centre is not required. Users are only identified by a unique ID and they share a symmetric key with the fusion centre.

The simplicity of the registration process allows the CRN to comprise a large number of users. The only drawback of the proposed scheme is that the system is not inherently robust against Sybil attacks. This means that a user can have as many identities as she likes, and thus the tracking of malicious users (who use a different identity every time) can be difficult. To solve this problem, the reputation mechanisms of the fusion centre should be designed in such a way that a user cannot have a great weight in the final decision unless she has been a good member for a long time. The confidence in new users should always be prudent in order to keep the risk of attacks under control.

In order to protect the privacy of CRN users, they identify themselves to the system using an index that changes in every session. This index is derived from the ID of the user and the key shared with the fusion centre (which also changes in every session). Since none of these parameters is revealed during a session, an attacker eavesdropping the packets of a CRN cannot deduce the new indexes of the network members. Therefore, attackers cannot track or discover any private user information, and thus their profile and location remains protected.

The unforgeability of the keys and identities that are used in the protocol is guaranteed as we can assume that the hash functions used in the protocol are collision resistant. The initial key of the protocol is 96 bits long, which is considered long enough based on the the NIST security guidelines [3].

One of the benefit of the protocol is its efficiency. Table 1 depicts a summary of the temporal costs of the protocol in each of its stages. The cryptographic costs in the table display the time that a cognitive radio user would spend processing the cryptographic parts of the protocol. We assume clients hold an embedded ARM device at 624MHz, and their costs are based on Rifà-Pous et al. study [14]. The transmission costs in the table are computed assuming a 802.11b network at 11Mbps.

Phases	Crypto Comput.	Transmission costs
1. Registry	$5.02\mu s$	$\approx 7.28s$
2. Session Authent.	$30.12\mu s$	$697.45\mu s$
3. Sensing Assign.	$10.04\mu s$	$245.82\mu s$
4. Sensing Results	$10.04\mu s$	$245.82\mu s$

Table 1: Performance analysis of the proposed protocol

Phase 1 has to be executed only once. To generate the key we need to take measurements of the RSS (received signal strength) when this takes abnormal values due to the context variations. We assume that the generation of the secret key is produced in a fast changing environment (e.g. by the shaking of the terminal) and that two RSS measurements can be taken in each wavelength of the radio signal. The experiments carried out in [11] show that the secret bit rate in a scenario where one of the terminals is in movement is around 22 bits/s. Thus, obtaining a shared key of 20 bytes requires around 7,273s.

In phase 1, the user also has to compute a hash function to obtain her pid_U. Using a SHA-1 algorithm, the computational cost is $5.02\mu s$.

This first stage of the protocol is really costly. However, it has to be compared with the registration phases of other systems. For example, in a public key infrastructure (PKI), users need to contact to a third entity and generate a pair of keys, a resource consuming operation that may not be available in a low-end mobile device. Contrary, the generation of a shared key using the physical properties of the channel can be carried out by any device. It takes time, but it is easy to execute and convenient.

Phase 2 is executed each time a user enters the cognitive radio network. The user and the FC interchange 3 messages: $JoinReq_1$, $JoinResp_1$ and $JoinReq_2$. The packet transmission time T_{packet} over a 802.11b control channel is expressed as follows:

$$T_{packet} = T_{PhyHdr} + (M_{MacHdr} + M_{Payload})/11Mbps$$

where T_{PhyHdr} is the PLCP (Physical Layer Convergence Procedure) preamble and header. The physical control data is 24 bytes long and it is transmitted at 1Mbps, so $T_{PhyHdr} = 192\mu s$. M_{MacHdr} is the length of layer 2 headers, which for an ad-hoc connection is 24 bytes. $M_{Payload}$ is the protocol data length. Both M_{MacHdr} and $M_{Payload}$ are transmitted at 11Mbps. The length of the messages transmitted in this phase of the protocol ($JoinReq_1$, $JoinResp_1$ and $JoinReq_2$) is approximated by 30, 45, and 20 bytes respectively. Then, the total transmission time in this phase is $697.45\mu s$.

Besides, in phase 2 the user has to verify 1 HMAC signature, generate another HMAC, and compute two hashes to update its secret data. In total, 6 hash operations. Using SHA-1, the total computational cost is $30.12\mu s$.

In phase 3, a user receives a sensing assignment. The verification of the message signature costs $10.04\mu s$, and the transmission of this message (which is assumed to be 50 bytes long) takes $245.82\mu s$.

Finally, in phase 4 the user has to build the sensing reports. This phase will be repeated periodically every 2 seconds at a maximum (2 seconds is the maximum time allowed by the cognitive radio standard for Wireless Regional Area Networks -WRAN- to detect a new incumbent signal in the network) so it has to be very efficient. The user only needs to compute an HMAC for each report (so, a cost of $10.04\mu s$). Regarding the transmission, we assume the cooperative model of the network is based on soft-decision, and the sensing reports of the users have a total of 30 bytes of data. If this data is signed using a HMAC based on SHA-1, the total size of the message is 50 bytes (20 bytes of overhead). The total transmission time of the sensing report is $245.82\mu s$.

The cost analysis indicates that, except for the phase 1, both the cryptographic costs of the protocol as well as the transmission ones are very limited. Phase 1 introduces a considerable delay, but is only executed once for each cognitive radio network the users wants to join. From the other phases, the most resource consuming one is the second, which is ran once in each session.

The presented protocol can be compared with the two general purpose secure sensing protocols proposed by Jakimoski et al. [6] and Ersöz et al. [4].

Jakimoski uses a public key scheme to authenticate the users and, in the same way that in our proposal, it uses an HMAC based method to authenticate the sensing reports of the users in each round. The weak point of the protocol is that the keys used to compute the HMAC are unknown by the destination of the message (the fusion centre) and must be sent by the network some stipulated time after sending the HMAC. This feature introduces a notable delay in taking a final decision about the occupancy of a channel.

In contrast, Ersöz proposal authenticates the sensing reports using symmetric key encryption and HMACs. For each sensing report each user has to compute an encryption and an HMAC. Although the costs of the proposal are quite restricted, our scheme is even lighter (it only requires an HMAC). On the other hand, the key management structure or Ersöz proposal is based on a Logical Key Hierarchy (LKH) architecture in which users share a common key that has to be changed and re-distributed when the group of cognitive radio nodes is modified. This can present high management costs in quite dynamic networks.

5. CONCLUSION

Cooperative sensing protocols are vulnerable to malicious attacks that can result in erroneous decisions: the failure to recognize primary users signals and thus provoke inconvenient interferences; the mistake to consider a channel is occupied and can not be used for CR users; or simply making an unfair distribution of the encountered free spectrum.

In this paper, we have identified the security vulnerabilities of a cooperative sensing process and its prejudicial effects on CR networks. We have proposed a secure protocol for centralized based systems that essentially uses symmetric signatures and one-way chains. The protocol allows the fusion centre to verify the authenticity of network members and to ensure that the received sensing information was really originated from the claimed source. At the same time, the protocol guarantees the anonymity of participating nodes and is robust against location disclosure attacks. One of the main features of the proposal is the fact that is computationally efficient and introduces a small bandwidth overhead.

Acknowledgments

This work was partially supported by the Spanish Ministry of Science and Education under grants JC2010-0081, TSI2007-65406-C03-03 E-AEGIS, and CONSOLIDER CSD2007-00004 ARES.

6. REFERENCES

[1] M. J. Blasco, H. Rifà-Pous, and C. Garrigues. Review of robust cooperative spectrum sensing techniques for cognitive radio networks. *Wireless Personal Communications*, 2012.

[2] J. Croft, N. Patwari, and S. K. Kasera. Robust uncorrelated bit extraction methodologies for wireless sensors. In *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, IPSN '10, pages 70–81, New York, NY, USA, 2010. ACM.

[3] Q. Dang. Recommendation for applications using approved hash algorithms. *NIST Special Publication*, (800-107), February 2009.

[4] S. D. Ersöz, S. Bayhan, and F. Alagöz. Secure spectrum sensing and decision in cognitive radio networks. In A. Özcan, N. Chaki, and D. Nagamalai, editors, *Recent Trends in Wireless and Mobile Networks*, volume 84 of *Communications in Computer and Information Science*, pages 99–111. Springer Berlin Heidelberg, 2010. doi:10.1007/978-3-642-14171-3_9.

[5] Federal Communications Commission. Spectrum policy task force report. Technical report, ET Docket No. 02-135, 2002.

[6] G. Jakimoski and K. P. Subbalakshmi. Towards secure spectrum decision. In *IEEE International Conference on Communications*, pages 2759–2763, Piscataway, NJ, USA, 2009. IEEE Press.

[7] M. Kobayashi, M. Debbah, and S. Shamai. Secured communication over frequency-selective fading channels: a practical vandermonde precoding. *EURASIP J. Wirel. Commun. Netw.*, 2009:2:1–2:19, March 2009.

[8] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *International Conference on Mobile Computing and Networking (MobiCom)*, pages 128–139, New York, NY, USA, 2008. ACM.

[9] S. Mishra, A. Sahai, and R. Brodersen. Cooperative sensing among cognitive radios. In *IEEE International Conference on Communications*, pages 1658–1663. IEEE Computer Society, 2006.

[10] J. Mitola III and G. Maguire Jr. Cognitive radio: making software radios more personal. *IEEE personal communications*, 6(4):13–18, 1999.

[11] N. Patwari, J. Croft, S. Jana, and S. K. Kasera. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Transactions on Mobile Computing*, 9:17–30, 2010.

[12] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: security protocols for sensor networks. *Wirel. Netw.*, 8(5):521–534, 2002.

[13] H. Rifà-Pous and C. Garrigues. Authenticating hard decision sensing reports in cognitive radio networks. Technical report, Internet Interdisciplinary Institute, 2011.

[14] H. Rifà-Pous and J. Herrera-Joancomartí. Computational and energy costs of cryptographic algorithms on handheld devices. *Future Internet*, 3(1):31–48, 2011.

[15] H. Rifà-Pous, M. Jiménez-Blasco, and J. Mut-Rojas. Robust detection of incumbents in cognitive radio networks using groups. *IEICE Trans Comm*, E94-B(9), 2011.

[16] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, NIST, 2001.

[17] A. Westin. *Privacy and Freedom*. New Jork Atheneum, New York, 1967.

[18] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway. A survey of key management schemes in wireless sensor networks. *Computer Commun*, 30(11-12):2314 – 2341, 2007.

[19] T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *Communications Surveys Tutorials, IEEE*, 11(1):116–130, 2009.

[20] W. Zhang, R. Mallik, and K. Letaief. Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks. *Wireless Communications, IEEE Transactions on*, 8(12):5761 –5766, december 2009.

[21] Y. Zhang and H. Dai. A real orthogonal space-time coded uwb scheme for wireless secure communications. *EURASIP J. Wirel. Commun. Netw.*, 2009:7:3–7:3, March 2009.