Green Cooperative Web of Trust for Security in Cognitive Radio Networks

Vandana Milind Rohokale, Neeli Rashmi Prasad and Ramjee Prasad

Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark,
E-mail: vmr;np;prasad@es.aau.dk

Received 29 June 2013; Accepted 31 August 2013;
Publication 23 January 2014

Abstract

Spectrum is a scarce and very essential resource for the ever growing mobile communication applications. Radio networks (CRN) is the best evolved solution towards spectrum scarcity. Cooperative spectrum sensing is a well-known and proven mechanism in the CRNs. As compared to other traditional wireless networks, CRNs are more delicate and open to the wireless environments due to their heterogeneous nature. Therefore, the CRNs have more security threats than the conventional wireless networks. The spectrum sensing and sharing mechanisms are inherently vulnerable to the malicious behaviors in the wireless networks due to its openness. This paper proposes an energy efficient lightweight cryptographic Cooperative web of trust (CWoT) for the spectrum sensing in CRNs which is proved to be appropriate for the resource constrained wireless sensor networks (WSNs). Development of trust based authentication and authorization mechanism for the opportunistic large array (OLA) structured CRNs is the main objective of this paper. Received signal strength (RSS) values obtained can be utilized to avoid Primary user emulation attacks (PUEA) in CRNs.

Keywords: Cooperative Spectrum Sensing, Cognitive Radio Network (CRN), Cooperative Web of Trust (CWoT), Wireless Sensor Network (WSN), etc.

1 Introduction

Wireless communication and relative mobile computing applications is a boom in the telecom market but the available spectrum and its allocation is not

Journal of Cyber Security, Vol. 2 No. 3 & 4, 307–328.
doi: 10.13052/jcsm2245-1439.236

appropriate to satisfy the highly increasing demands by mobile applications. Cognitive radio technology is a hopeful evolution for the solution towards scarce radio spectrum [1]. Cognitive radio entities continuously sense the spectrum holes which are utilized for the opportunistic communication. CRNs provide the spectrum reuse concept. Since the CRN evolves from the hybrid combination of many heterogeneous networks, it is much more prone to the wireless open media vulnerabilities [2]. Consumer premise equipment (CPE) which has the inbuilt cognition capability, continuously monitors the spectrum, senses the white spaces in the spectrum and occupies the spectrum according to the availability and it can vacate the occupied spectrum immediately after sensing the comeback of the licensed user.

CPE is a mobile equipment with cognition capabilities which can sense radio environment eg., spectrum white spaces, information about geographic location, available wireless or wired networks around and available services. It can also analyze and get information regarding the secondary user's needs and reconfigure itself by adjusting some specific parameters to make sure that rules and regulations of CRN are strictly followed. Whenever the CPE senses spectrum holes, CRN sends Request to send (RTS) kind of packets on the network to initiate the communication [3].

Cooperation is the vital characteristic of CRNs because the secondary nodes of CRN basically cooperate with each other for finding out the spectrum white spaces in the available spectrum for the successful and timely wireless communication. With cognitive environment, it is very much essential that the information bearing secondary nodes should exchange their data through multicast communication. Safety of the secondary user's communication data from intruder is a critical issue for CRNs. Because of these reasons, Group Security is necessary for secondary users of CRN [4]. The group based security with collaborative advantages is possible with the concept of Cooperative Web of Trust (CWoT).

CRN is a multi-user environment where multiple secondary and primary users are present in the system. Spectrum sensing for such multi-user case becomes more complicated wherein the sensing of spectrum holes and the interference estimation are the complex tasks. A collaborative effort by secondary users is the attractive solution. The research work in [5] proposes a new cooperative spectrum sensing mechanism for multi-user CRNs in which each user's contribution is weighted by taking into account the parameters like received power and path loss components.

The paper is organised as follows. Related works in the security of the CRN is discussed in section II. Section III explains the proposed system

model for the green and cooperative web of trust mechanism for security in the cognitive radio networks. It explains in details how authentication, trust building and authorization are achieved in the CWoT system. Simulation results are depicted in section IV. This section shows energy efficiency of the proposed security system. Section V includes conclusions and future scope for this work.

2 Related Works

For wireless communication, a signal has to be transmitted through open media with a virtual connection. Since the CRNs are built with the numerous heterogeneous wired and wireless networks, the chances of the data being hijacked are more. Figure 1 below depicts the security threat taxonomy for CRN [6] wherein the possible security threats to CRN are mentioned.

O. Leon *et. al.* in [7], have studied various possible vulnerabilities to CRNs with classification of attacks and their impact. They have proposed security solutions to CRNs keeping in mind the FCC rules and regulations regarding primary user system and their services should remain intact irrespective of modifications in the secondary users of CRNs. In [8], cross layer (Physical plus MAC) attack strategies such as coordinated report false sensing data

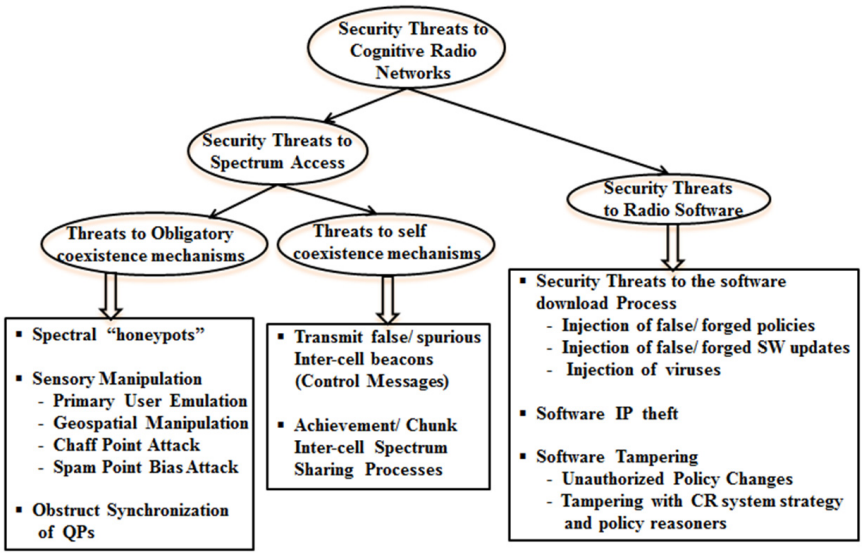

Figure 1 Security Threats Taxonomy for CRNs

attack and small back-off window attack are designed and a trust based cross layer defense framework is proposed. Due to the security provided by proposed defense mechanism, the damage percentage is shown to be reduced.

Trust based security system for community based CRNs is proposed in [9]. Here the trust value of a CR node is decided according to the history behavior of that node. Here the authors have designed trust based authentication for community based CR nodes. Paper [10] puts forth a trust based algorithm for CRNs which is based on location consciousness and estimated distance between the mobile users. Here the trust calculation is performed based on received power and trust metrics are decided by the combination of trustworthiness requirements and QoS of the radio links.

In the research work of [11], the authors have calculated trust depending on various communications attributes and it is compared with the threshold value of trust. Helena et. al. in [12] have presented a good combination of wireless physical layer security, private key cryptography and one way hash functions. They have proposed a security protocol for a centralized system where the authenticity is verified at the data fusion center which they claim as the robust mechanism against the location disclosure attacks. The research work in [13] proposes a trust methodology for secrecy in cooperative spectrum sensing (TM-SCSS) wherein the data fusion centre assigns and updates the trust value to each entity according to the sensing results. The secondary cooperating

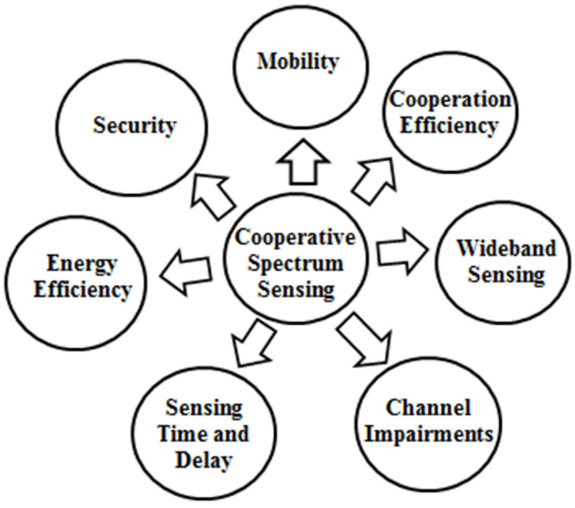

Figure 2 Gain and Overheads in Cooperative Spectrum Sensing [14]

radio nodes are classified into categories like malicious node, pending node and trusted node based on their recent trust values updated according to the data fusion center.

Cooperative spectrum sensing is a dominant technique for the detection mechanism in the CRN. It makes use of cooperative spatial diversity to exploit benefits like energy efficiency, cooperation efficiency and wideband sensing capability. But the advantages come with certain overheads like security challenges due to heterogeneous nature of CRN, sensing time and delays, mobility management and channel impairments as depicted in Figure 2. The techniques used for spectrum sensing include Energy Detector based Sensing, Cyclostationary based sensing, Radio Identification based sensing and matched filtering. For energy detection based sensing, cooperation is the best suited technique since it results into appropriate received signal strength values.

2.1 Primary User Emulation Attack (PUEA)

An attacker imitates the characteristics of a primary signal transmitter and pretends as being primary user as shown in Figure 3. Proper identification mechanisms are very much essential for the prevention of the PUEA attacks in CRN. The problems associated with the PUEA attack are security related, trust related and also performance related. So, for the prevention of the critical threat like PUEA, some kind of strong security mechanism is vital [6].

Game theoretic cooperation approaches promise to provide proper incentives for the nodes cooperating to relay the information from sender to receiver. Mainly, three types of behaviours are observed in the wireless networks like

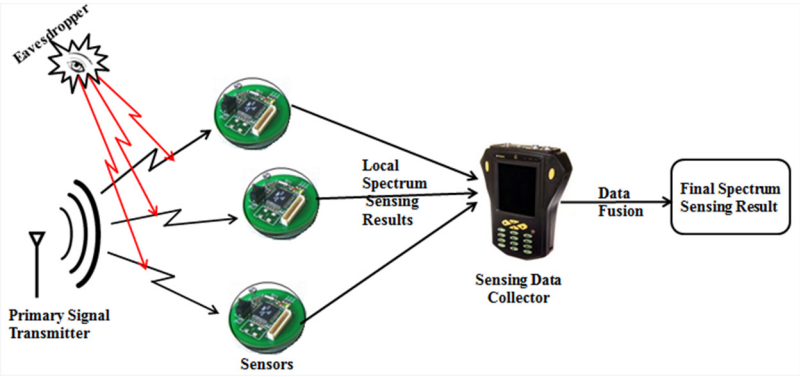

Figure 3 Primary User Emulation Attack in CRN

No Help (Egoistic Behaviour), Unidirectional Help (Supportive Behaviour) and Mutual Help (Cooperative Behaviour). For the construction of trust based security we have taken into consideration this incentive aspect in terms of increment in the trust level for good cooperation and trusted behavior. This paper proposes a lightweight CWoT for the prevention of primary user emulation attacks in the spectrum sensing technique for the heterogeneous cognitive radio networks. The facts with CWoT's considerably improved received signal strength (RSS) figures ensure the security against identity thefts of the primary users. With the CWoT mechanism, authentication and authorization techniques are proposed which are based on trust levels. The secondary user's cognitive radio equipment forms an opportunistic large array (OLA) like structure to communicate the information broadcasted by any source to its intended receiver. The CWoT mechanism is found to be efficient in terms of QoS parameters for the adhoc networks in terms of reliability, energy efficiency and delay issues.

3 Cooperative web of trust (CWoT) for cognitive radio networks

The proposed CWoT security mechanism considers following model, which is a part of the Cooperative Opportunistic Large Array (OLA), as shown in Figure 4. The model illustrates various layers. The coverage limits of the various layers of the cooperation are shown with different levels. The analytical model for cooperative opportunistic large array (OLA) approach is considered same as in the works of same authors in [14]. Accordingly, the consumer radio devices (secondary user's sensor nodes) which are half-duplex in nature are assumed to be uniformly and randomly distributed over a continuous area with average density ρ. As in [10], the deterministic model is assumed, which means that the power received at a Consumer Premise Equipment (CPE) is the sums of powers from each of the CPE. In this model, the network node transmissions are orthogonal. It is assumed that a CPE can decode and forward a message without error when it's Signal to Noise ratio (SNR) is greater than or equal to modulation-dependent threshold λ_d. Due to noise variance assumption of unity, SNR criterion is transformed into received power criteria and λ_d becomes a power threshold. Let P_s be the source transmit power and the relay transmit power be denoted by P_r, and the relay transmit power per unit area be denoted by $\overline{P_r} = \rho P_r$. Instead of infinite radius, we are considering some practical scenarios where the radius is limited.

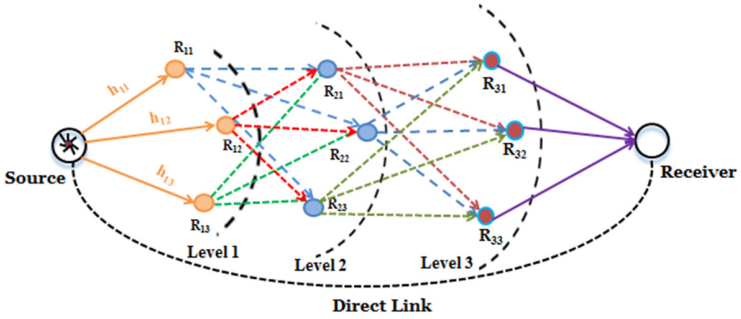

Figure 4 Proposed CWoT Model for Secondary users of CRN

Theoram: If $\mu \triangleq e^{(\lambda/\pi\rho P_R)}$ [15] and $\mu > 2$,
then

$$r_k = \sqrt{\frac{P_s(\mu-1)}{\lambda(\mu-2)}}\ (1 - \frac{1}{(\mu-1)^k}) \tag{1}$$

$$and \qquad \lim_{k\to\infty} r_k = r_\infty = \sqrt{\frac{P_s\,(\mu-1)}{\lambda\,(\mu-2)}} \tag{2}$$

For ($\mu \leq 2$), the broadcast reaches to the whole network i.e. $\lim_{k\to\infty} r_k = \infty$.

$$FES = 1 - \frac{number\ of\ active\ radio\ nodesutilized\ for\ cooperative\ transmission}{Total\ number\ of\ nodes\ in\ the\ OLA\ network}$$

For ($\mu > 2$), the total area reached by the broadcast is limited i.e. $r_k < r_{total}$ where r_k = radius of the kth level of the OLA structure.
Some preliminary assumptions for the proposed system are as below:

- All the nodes will have a unique identification, or UID, which will be utilized in the authentication of the nodes.
- All nodes are capable of transmitting and receiving information or data, if the minimum threshold for the received message is satisfied.

Taking into account the typical flow of the messages using the RTS-CTS-Message-ACK, the information about the nodes with the authentication details is transmitted cooperatively to the destination. The messages being relayed by the intermediary nodes or relays are considered on the basis of decode and forward, since the other technique amplify and forward amplifies

the noise, thus degrading the signal that is received at the other end. It is in general considered that such cooperative relay of messages may present a problem of message flooding in the network. This situation is normally avoided by restricting the transmission of messages that fall below a given criteria (received SNR threshold) for the signal-to-noise ratio (SNR) of that message, as explained by [14]. The noise variance is assumed to be unity and hence the SNR criterion in transformed into a minimum criteria for power. Hence if the power with which the message is received is less than the threshold λ_t, the corresponding secondary relay node is not eligible for further retransmission of the signal. Such node stays idle during the communication.

3.1 Authentication

Let us consider an array of n nodes, depicted by N_i for i = 1 to n. Whenever a node, say N_A wants to communicate with N_B, N_A will send a Request to send (RTS) to N_B. Depending on whether the nodes are communicating for the first time or not, two scenarios are generated as explained below.

Scenario 1: *This is the first time that N_A is communicating with N_B*: When N_A is communicating for the first time with N_B, it would require an external entity to assure the authenticity of the node. The proposed model assumes that the network nodes trust each other to some basic level at the beginning of the communication, and later verifies the credibility of each node using trust values from other nodes. The basis of web-of-trust is used. For the aforementioned scenario i.e. if the nodes are communicating for the first time, some trust is to be assumed. In such a situation there is no way for N_A to verify that the person claiming to be N_B really is N_B. Hence N_A will, for the time being, trust N_B for the communication. An Asymmetric key exchange mechanism is considered. The public key is known to all the nodes in the network, whereas individual private key is retained by the corresponding node. Newer key exchange mechanisms for 802.11ae and 802.11af, based on groups have been discussed in the research work published in [15, 16, 17].

When N_A wants to communicate with N_B, it will use the public key of N_B, $\mathrm{K_{public}}$, and will pass this, with its own UID to a one way function**,** F ($\mathrm{K_{public,}}$UID). One way function is generated as shown in Figure 5. The output of this function, **G**, will then be sent to N_B. The use of one way function is beneficial as follows: any node other than N_B, will not be able to decipher the UID of N_A because of the use of the one way function. This is then attached to the RTS frame, which is to be sent to N_B. N_B, upon receipt of this frame recognizes that this is the first time N_A, or, for that communication, someone claiming to be N_A, is communicating with him/her.

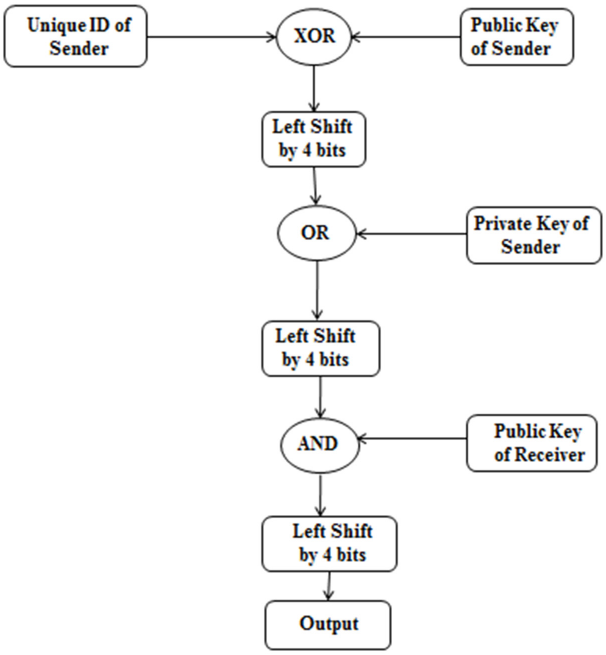

Figure 5 One Way Function Generation

Since there is no previous record of the authenticity of the identity of N_A, N_B will flag this node, and will try to confirm its identity later, as and when possible with cooperation from neighbouring nodes**.** This value G received from N_A is then given to another function F_D which will generate a corresponding value for the UID, called as K. Note that the UID itself is never disclosed to any other node. This value, K, is then stored in the memory of N_B. Based on feedback about this node from the neighbouring nodes, N_B may at a later stage delete this node, or set it to a higher priority.

In the packets that will follow, i.e. the ones containing the actual data from N_A, all N_B has to do is to extract the value of K of the sender from these packets. It may be noted that this value of K will be in encrypted format, if possible using the one way function only. N_B then extracts the K of the sender and matches it with K that it has received from the RTS packet. If the two keys match, the packet is considered as authentic and an acknowledgement is sent back to N_A. In the case that the value of $K$of the sender and the received packet do not match, the packet is discarded, with no notification being sent to the sender.

Scenario 2: N_A or someone claiming to be N_A has already communicated with N_B: In such a scenario, N_B has an idea about the identity of N_A. So all that N_B has to do is to confirm a match between the stored value of K of N_A and the value of K derived from the incoming packet. If a match occurs, the packets are processed and an acknowledgement is sent, otherwise the packet is discarded.

3.2 Trust Building

Cooperation itself has offered many of its benefits in the field of communication. The overheads of authentication can be reduced with the help of the cooperation from neighbouring nodes, i.e. by maintaining a web of trust (WoT). Consider a situation where N_A is a known party to N_B, i.e. they both trust each other. In a situation, where a third node, say Cairn, wants to contact with N_B. It is also known that N_A knows Cairn, that is, N_A trusts Cairn. This fact can be used to avoid unnecessary expenses that would be required to authenticate Cairn. As N_B trusts N_A, and N_A trusts Cairn, then a direct relation that N_B trusts Cairn can be made. Here, N_A is standing as a guarantor for Cairn.

It may be noted that this cooperation comes with its own drawbacks. Consider a situation where one of the nodes in the system is malicious. If this node stands as a guarantor for many other malicious nodes, then the security of the system can be compromised. One solution to this problem can be the use of trust-ranking of nodes. Based on the performance of nodes, ranks can be assigned to the nodes. If a node is a suspect, that is if many packets being sent via that node are not being delivered to the destination and this fact can be confirmed by some cooperation, then the node can be blacklisted, or its rank can be decreased by one. If the rank of a node reaches zero, its entry of $K$and node name is deleted and cooperatively notified to other nodes. If such a node has a guarantor, then the guarantor can be blacklisted and its priority be decreased as well. In the above example, N_A stood as a guarantor for Cairn. In the event that packets being routed through Cairn are not reaching the destination, or for that matter, if any crooked activity is suspected at Cairn then cairn can either be blacklisted or its rank can be decreased, depending upon the seriousness of the malicious nature being observed at that particular node. The message building mechanism uses the one way function as shown in Figure 6. The complete CWoT security mechanism is depicted as in the flowchart shown in Figure 7.

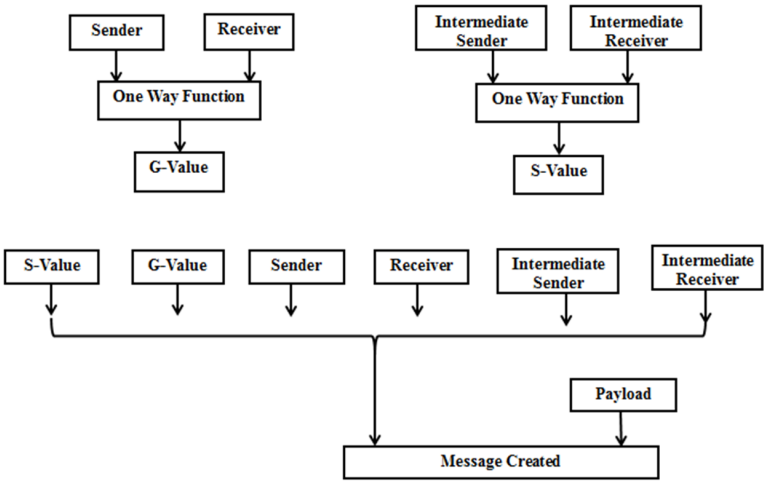

Figure 6 Message Creation Mechanism

In the event that a particular node has come up and is interacting with other nodes for the first time, the authenticity can be established based on the fact that if the new node is giving good performance with most number of neighbouring nodes, with no problems with the identity of that node, the node's rank can be increased, indicating the increased level of trust. We can do one more thing that trusted nodes can be added only at level 1, that is,

- A trusts B & B trusts C then A trusts C
- A trust B, B trusts C & C trust D then A trust D is not possible in this case.

In this scenario, we are assuming that by reducing the number of middle agents (secondary relays) will help us in improvement of security protocol.

3.3 Authorization

The role based access control technique is considered, wherein the participant radio nodes are classified according to various roles assigned to them. After the message is received, based on the reputation of that node, appropriate trust level is assigned to it. Based on the achieved trust level, the role is assigned to that particular node. Lastly, the access rights for that node are validated. The system divides the communicating nodes into three types of roles: sender, relay and receiver. Depending on the amount of information required for successful transmission of the message, appropriate access rights are assigned to these

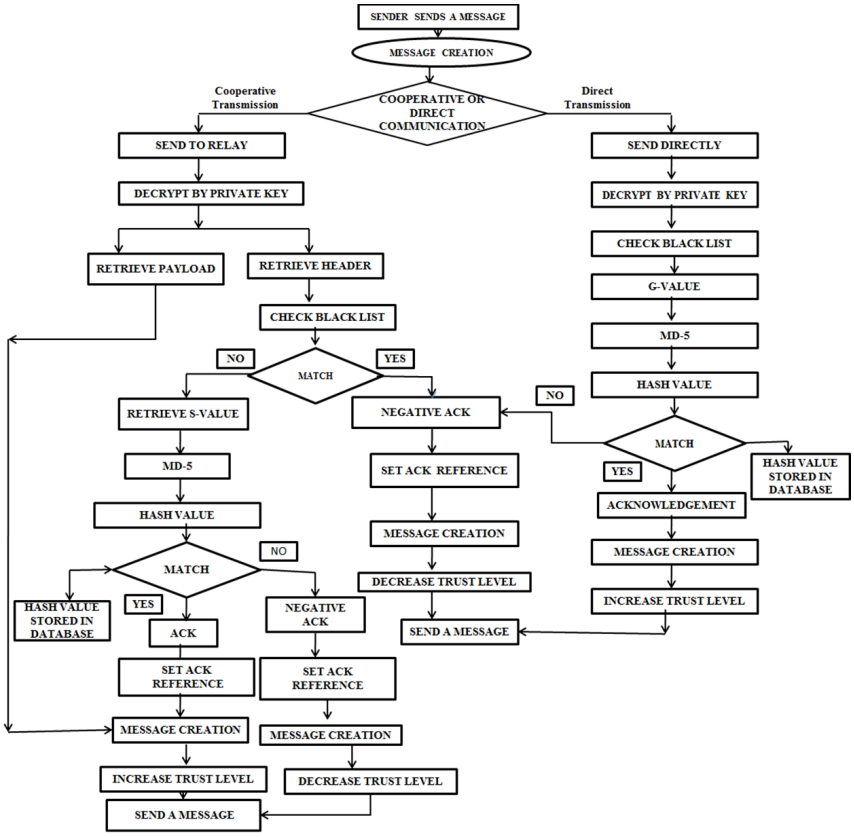

Figure 7 Flowchart for Cooperative Web of Trust (CWoT) Security Mechanism

roles. Though this scheme may look suitable for implementation, an obvious drawback of the previously implemented mechanisms is the static nature of the access roles that is provided to the participants. Therefore the roles are desired to be flexible. This can be achieved by the use of reputation based role assignment, as defined in [18]. In contrast to the multi-level approach of the technique proposed in the previous works, a decentralized approach is utilized here because of highly mobile nature of the nodes in the WSN. This gives equal priority to all the nodes, and reduces the central point of failure. On the basis of the trust level of the node that is communicating, a role is assigned to the node. It must be noted that since the role is being assigned at the necessary host, one node may have many roles assigned to it in context with different nodes. This may be thought of as a problem, but such a problem is easily eliminated

as the trust information of the nodes is shared by all communicating parties. Thus, the trust value maintains appropriate reputation of the nodes, which in turn provides the suitable role to the node.

Proposed CWoT security system works for the detection and isolation of malicious nodes, based on the distance estimation of the values generated by broadcasting nodes, and gathering information about the same signal from neighbouring nodes. It is assumed that in replayed messages if the data that is presented, i.e. distance is incorrect and if such fact is brought to the notice of the node by the neighbours, then the nodes may diagnose it as a malicious node and thus eliminate it as shown in the authorization process of Figure 8.

In case, the identity of the adversarial relay (eavesdropper) is not diagnosed, then it can be pinpointed for detection by mechanism proposed in [19]. However it may be noted that only adversarial relay can be detected using this mechanism. The method involves the inclusion of some symbols. Based on the key shared between the sender and the receiver, the key that is unknown to the relay nodes, some symbols are generated. These symbols are called as trace symbols. The function explained above for the generation of the values of K (G value) can be used, along with some pseudo random number generator to produce unique values and the location where these symbols are to be added. At the receiving end, the receiver using the shared key extracts the symbol from the location. A mathematical function corresponding to the function used for the generation of the symbols is used at the receiving end to establish the ground truth whether these symbols were indeed generated on the basis of the tracing key, and then compare it with the received values. In case, the signal is garbled, or modified by a malicious relay, such malicious behaviour can be detected. Tracing mechanisms are provided in [20] for detection of the adversarial node.

The aforementioned topics give an insight to the basic mechanism that is to be implemented for this work. As every communication is bound to change the status of the network, it can be expressed as

$$M(n') \rightarrow < \alpha > M' \tag{3}$$

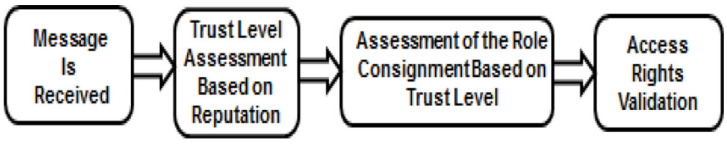

Figure 8 Authorization Process

When radio node of the network configuration transforms into another network configuration $_M$' by execution of the action/communication/message**.** M is a table maintaining the trust information of the various participating nodes in the network. Each node stores the trust information about other nodes in its vicinity. A trust handling unit keeps on updating the trust level $T(n)$ of the neighbouring nodes. The trust levels can be categorized into ***blacklisted < not trusted < acquaintance < trusted < medium < highly trusted***. During initialization, the nodes are assigned a trust value of acquaintance. Thereafter, those are the communication messages that alter the trust level $T(n)$ of the neighbours. If a communication from node A to B delivers a corrupt message or the identity of the sender cannot be verified, it takes the network to a state that invokes decrease in the trust level of that node. As a node can act as the guarantor for other nodes that are less trusted, the guarantor stands liable for any false trust that it may have stood for.

This can be expressed as:

$$M(i) \rightarrow (\alpha)M' \tag{4}$$

$$M'(T(i) - 1) \tag{5}$$

Where M'= Broadcast trust

If the step (4) results into a trust of blacklist, that is $T(i) < \theta$, the node is removed or banned from communication. θ is the minimum value below which the node is blacklisted. There may be two scenarios existing after this case: (1) If it is observed that the blacklisted node is blacklisted by a node that is still trusted, that node's trust is decreased by one. (2) If the blacklisted node is blacklisted by many other networks, its trust level is decreased as well. Based on the trust $T(i)$ for the node i, roles are assigned. The role is represented as,

$$R(I, T(i)) \tag{6}$$

Where the role R is assigned to node i at trust level $T(i)$. The participants during communication will be assessed against this role at the receiving node. If it is found that the access requested is given in the role at the trust level $T(i)$, the action is permitted, otherwise rejected. The security is ensured as below: at the time of establishing communication, a trusted node at some trust level j will never communicate with another node at a trust level below some trust level k. This trust level k may vary from one node to another depending

on the importance of the functionality of that node. In such manner, as proved by [21], malicious nodes are isolated from the communication network.

4 Simulation Results

After inclusion of security mechanisms in the communication system, it is general observation that the energy consumption of the system increases by large amount. As compared to the research work implemented in [15], the fraction of energy savings is slightly reduced with the addition of security in the system. As can be seen from the Figure 9, the energy consumption goes on increasing with the coverage area extension. It is interesting to note that for higher values of the SNR threshold (received SNR value at the secondary node), the energy consumption is observed to be reduced. The cooperative wireless communication is inherently energy efficient. By exploiting the cooperative diversity, the coverage range of the communicating nodes can be extended. Due to range extension capability, the received signal strength values are observed to be considerably better values compared to that without cooperation. This is very encouraging result for the protection against primary user emulation attack.

Received signal strength (RSS) at the secondary relay nodes is depicted in the Figure 10 below. It can be clearly seen that as compared to without cooperation, the RSS value is much better with cooperation. At the coverage radius of 30 meters, the RSS value is almost zero without cooperation whereas at the same value, the RSS value is found to be around 0.14 with cooperation. Secondary users can recognize each other's RSS signals and share a common protocol and are able to identify each other. Also due to increase or decrease in the trust levels due to the behaviour in the cooperative system, the secondary users are unable to emulate primary users. If any of the secondary user tries to misbehave and emulate primary user, its trust level gradually decreases and at the last, the node is blacklisted from the total communicating network entities.

The RSS value with cooperation is promising figure for the secondary entities in the cognitive radio networks. As in [6], the fraction of energy saving (FES) is given by,

$$FES = 1 - \frac{\begin{array}{c} number\ of\ active\ radio\ nodes\ utilized \\ for\ cooperative\ transmission \end{array}}{\begin{array}{c} Total\ number\ of\ nodes \\ in\ the\ OLA\ network \end{array}} \tag{5}$$

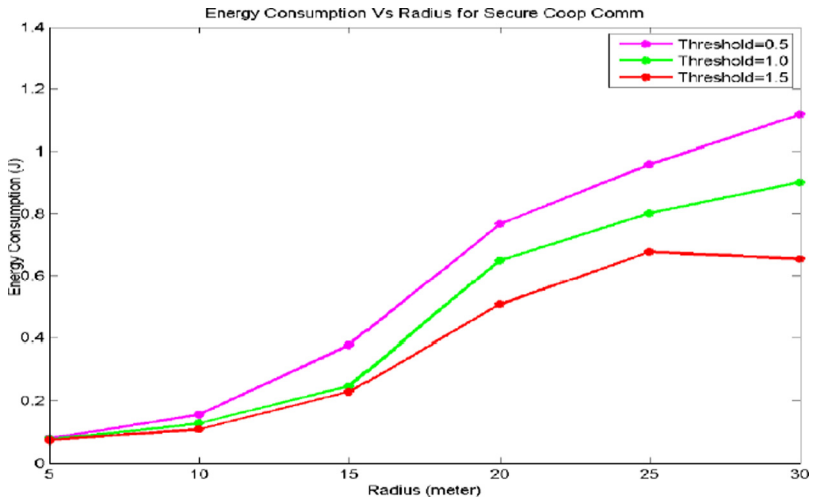

Figure 9 Energy Consumption Vs Coverage Radius for Secure Cooperative CRN

It is clearly observed from the figure that the FES value with security mechanism differs from the Cooperative system without security by almost 10%. Since the proposed system makes use of light weight cryptography and cooperative web of trust, the cost for the cooperative web of trust mechanism inclusion is less almost 10% as shown in Figure 11. Security inclusion cost of 10% is the promising result. Because the traditional cryptographic

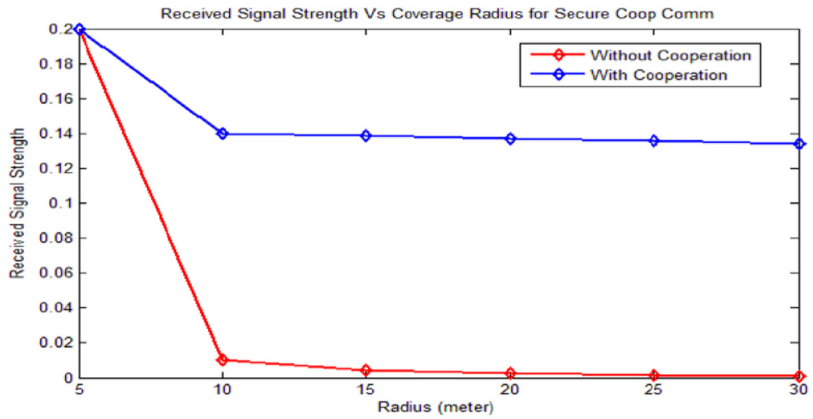

Figure 10 Received Signal Strength vs. Coverage Radius for Secure Web of Trust with and without Cooperation

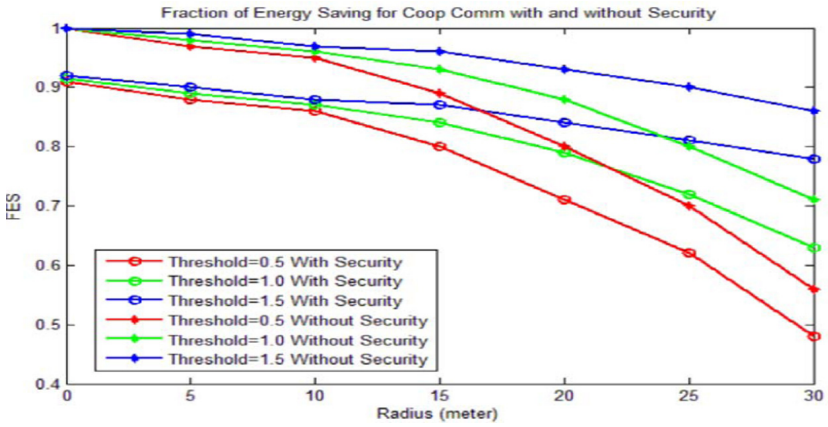

Figure 11 Fraction of Energy Savings Vs Coverage Radius with and without application of Secure Web of Trust

techniques are very much costly in terms of energy and computing power. Also, it is interesting to note that for higher values of threshold, the fraction of energy savings is considerably higher as compared to the low threshold situations.

5 Conclusions and Future Scope

The cooperative web of trust seems to provide promising energy efficient security solution for the spectrum sensing technique in cognitive radio networks. Also, the RSS values obtained are observed to be the effective result in the direction of the energy detection mechanism for spectrum sensing. Due to web of trust mechanism with cooperative diversity provides appropriate security solution for the primary user emulation attacks. Depending on the trust levels acquired through reputation in the system, the nodes immediately get either rewards for good behaviour or get blacklisted due to extreme misbehaviour. However, some improvements are needed in the present system. The storage of hash values is also a resource consuming prospect. Using proper function by light weight cryptography, the hash values can be computed at the run time, without consuming much time, thus eliminating the overheads of space and time requirements. Also since each broadcast consumes some energy, only relevant acknowledgements should be propagated, so that the system assumes the presence of an end-to-end logical channel, without having to bother about the intermediaries and the overhead such as acknowledgement

sending to them. The authorization implemented assigns the role dynamically on the basis of reputation of the node.

References

[1] J. Mitola. Cognitive radio architecture evolution, Proceedings of IEEE Journals and Magazines, vol. 97, Issue 4, pp. 626–641, Apr. 2009.

[2] J. L. Burbank. Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network, 3rd International conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008, pp. 1–7.

[3] K-C Chen et al. Cognitive radio network architecture: part I—general structure, In the Proceedings of the 2nd international conference on ubiquitous information management and communication, Suwon, Korea, 2008a, pp.114–119.

[4] S. Parvin, F. Khadeer Hussain, O. K. Hussain, S. Han, B. Tian, E. Chang. Cognitive radio network security: A survey, Journal of Network and Computer Applications, Vol.35, Issue. 06, November 2012, pp. 1691–1708.

[5] MIB Shahid, J. Kamruzzaman. Weighted soft decision for cooperative sensing in cognitive radio networks", 16th IEEE international conference on networks (ICON), New Delhi, 2008, pp. 1–6.

[6] A. M. Wyglinski, M. Nekovee, Y. T. Hou. Cognitive Radio Communications and Networks: Principles and Practice", Elsevier, Dec 2009.

[7] O. Leon, J. Hernandez-Serrano and M. Soriano. Securing Cognitive Radio Networks, International Journal of Communication Systems, Wiley InterScience, vol. 23, pp. 633–652, 2010.

[8] W. Wang, Y. (L.) Sun, H. Li and Z. Han. Cross-Layer Attack and Defense in Cognitive Radio Networks, IEEE Global Telecommunications Conference (GLOBECOM 2010), pp. 1–6, 2010.

[9] S. Parvin and F. K. Hussain. Trust-Based Security for Community Based Cognitive Radio Networks, 26th IEEE Conference on Advanced Information Networking and Applications, pp. 518–525, 2012.

[10] R. Dubey, S. Sharma, and L. Chouhan. Secure and Trusted Algorithm for Cognitive Radio Networks, Ninth International Conference on Wireless and Optical Communication Networks (WOCN), pp. 1–7, 2012.

[11] S. Parvin, S. Han, F. K. Hussain, Md. A. A. Faruque. Trust Based Security for Cognitive Radio Networks, Proceedings of the 12th International

Conference on Information Integration and Web-based Applications & Services, pp 743–748, 2010.

[12] H. Rifà-Pous, C. Garrigues. A Secure and Anonymous Cooperative Sensing Protocol For Cognitive Radio Networks, ACMSIN'11, Proceedings of the 4th international conference on Security of information and networks, pp 127–132.

[13] I. F. Akyildiz, Brandon F. Lo, Ravikumar Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: A survey", Elsevier Science Direct Physical Communication 4, 2011, pp. 40–62.

[14] V. Rohokale, N. Kulkarni, N. Prasad, H. Cornean. Cooperative Opportunistic Large Array Approach for Cognitive Radio Networks, 8th International conference on communications, COMM 2010, pp. 513–516.

[15] W. Guo-feng, Z. Shi-lei, H. Xiao-ning and H. Han-Ying. A Trust Mechanism-based Secure Cooperative Spectrum Sensing Scheme in Cognitive Radio Networks", ESEP 2011: 9–10 December 2011, Singapore.

[16] J. Hong, Y. Qing-song, L. Hui. Simulation and Analysis of MAC Security Based on NS2, IEEE International Conference on Multimedia Information Networking and Security, vol.2, pp. 502–505, 2009.

[17] S. Misra, A. Vaish. Reputation-based role assignment for role based access control in wireless sensor networks, Computer Communications 34 (2011), pp.281–294, 2011.

[18] J. U. Duncombe. Infrared navigation—Part I: An assessment of feasibility (Periodical style), IEEE Tranactions on Electron Devices, vol.11, pp. 34–39, Jan. 1959.

[19] D. Liu, P. Ning. Security for Wireless Sensor Networks, Book Series in Advances in Information Security, Springer, ISBN 978-0-387-46781-8, vol.28, 2007.

[20] Y. Mao, M. Wu. Tracing Malicious Relays in Cooperative Wireless Communications, IEEE Transactions on Information Forensics and Security, Vol. 2, No. 2, pp. 198–212, June 2009.

[21] M. Merro and E. Sibilio. A Caluculus of Trustworthy Ad-hoc Networks", Springer-Verlag Berlin Heidelberg, pp. 157–172, 2010.

Biographies

Vandana Milind Rohokale received her B.E. degree in Electronics Engineering in 1997 from Pune University, Maharashtra, India. She received her Masters degree in Electronics in 2007 from Shivaji University, Kolhapur, Maharashtra, India. She is presently working as Assistant Professor in Sinhgad Institute of Technology, Lonavala, Maharashtra, India. She is currently pursuing her Ph.D. degree in CTIF, Aalborg University, Denmark. Her research interests include Cooperative Wireless Communications, AdHoc Networks and Cognitive Networks, Physical Layer Security, Information Theory and its Applications.

Dr. Neeli Prasad is leading a global team of 20+ researchers across multiple technical areas and projects in Japan, India, throughout Europe and USA. She has a Master of Science degree from Delft University, Netherlands and a PhD degree in electrical and electronic engineering from University of Rome Tor Vergata, Italy. She has been involved in projects totaling more than $120 million – many of which she has been the principal investigator. Her notable accomplishments include enhancing the technology of multinational players including Cisco, HUAWEI, NIKSUN, Nokia-Siemens and NICT as well as defining the reference framework for Future Internet Assembly and being one of the early key contributors to Internet of Things. She is also an advisor to the European Commission and expert member of governmental working groups and cross-continental forums. Previously, she has served as chief architect on large-scale projects from both the network operator and

vendor side looking across the entire product and solution portfolio covering wireless, mobility, security, Internet of Things, Machine-to-Machine, eHealth, smart cities and cloud technologies. She has more than 250 publications and published two of the first books on WLAN. She is an IEEE senior member and an IEEE Communications Society Distinguished Lecturer.

Prof. Dr. Ramjee Prasad is the Director of the Center for TeleInfrastruktur (CTIF) and Professor Chair of Wireless Information Multimedia Communication at Aalborg University (AAU), Denmark. He is a Fellow of the Institute of Electrical and Electronic Engineers (IEEE), USA, the Institution of Electronics and Telecommunications Engineers (IETE), India; the Institution of Engineering and Technology (IET), UK; and a member of the Netherlands Electronics and Radio Society (NERG), and the Danish Engineering Society (IDA). He is recipient of several international academic, industrial and governmental awards of which the most recent is the Ridder in the Order of Dannebrog (2010), a distinguishment awarded by the Queen of Denmark.

Ramjee Prasad is the Founding Chairman of the Global ICT Standardisation Forum for India (GISFI: www.gisfi.org) established in 2009. GISFI has the purpose of increasing the collaboration between Indian, Japanese, European, North-American, Chinese, Korean and other worldwide standardization activities in the area of Information and Communication Technology (ICT) and related application areas. He is also the Founding Chairman of the HERMES Partnership (www.hermes-europe.net) a network of leading independent European research centres established in 1997, of which he is now the Honorary Chair.

Ramjee Prasad is the founding editor-in-chief of the Springer International Journal on Wireless Personal Communications. He is member of the editorial board of several other renowned international journals and is the series editor of the Artech House Universal Personal Communications Series. Ramjee Prasad is a member of the Steering, Advisory, and Technical Program committees of many renowned annual international conferences, e.g.,

Wireless Personal Multimedia Communications Symposium (WPMC); Wireless VITAE, etc. He has published more than 25 books, 750 plus journals and conferences publications, more than 15 patents, a sizeable amount of graduated Ph.D. students (over 60) and an even larger number of graduated M.Sc. students (over 200). Several of his students are today worldwide telecommunication leaders themselves.