A Trust Model Based Energy Detection for Cognitive Radio Networks

Fan Jin
Department of Computing
Macquarie University
Sydney NSW 2109
fan.jin@students.mq.edu.au

Vijay Varadharajan
Department of Computing
Macquarie University
Sydney NSW 2109
vijay.varadharajan@mq.edu.au

Udaya Tupakula
Department of Computing
Macquarie University
Sydney NSW 2109
udaya.tupakula@mq.edu.au

ABSTRACT

In a cognitive radio network (CRN), energy detection is one of the most efficient spectrum sensing techniques for the protection of legacy spectrum users, with which the presence of primary users (PUs) can be detected promptly, allowing secondary users (SUs) to vacate the channels immediately. In this paper, we design a novel trust based energy detection model for CRNs. This model extends the widely used energy detection and employs the idea of a trust model to perform spectrum sensing in the CRN. In this model, trust among SUs is represented by *opinion*, which is an item derived from subjective logic. The opinions are dynamic and updated frequently: If one SU makes a correct decision, its opinion from other SUs' point of view can be increased. Otherwise, if an SU exhibits malicious behavior, it will be ultimately denied by the whole network. A trust recommendation is also designed to exchange trust information among SUs. The salient feature of our trust based energy detection model is that using trust relationships among SUs, this guarantees only reliable SUs will participate in generating a final result. This greatly reduces the computation overheads. Meanwhile, with neighbors' trust recommendations, a SU can make objective judgment about another SU's trustworthiness to maintain the whole system at a certain reliable level.

Keywords

Cognitive radio network; trust model; subjective logic; energy detection

1. INTRODUCTION

With the rapid increase in the number of mobile devices and their requirements for the spectrum, the limited available spectrum becomes a constrained resource. To remedy this spectrum scarcity issue, cognitive radio (CR) was proposed as an efficient and opportunistic use of the frequency spectrum in order to increase spectral efficiency. A cognitive radio network (CRN) is an intelligent network that contains both licensed users and unlicensed wireless users who have CR capabilities. These users are referred to as primary users (PUs) and secondary users (SUs) respectively. The CRNs help to address the problem of spectrum shortage by adapting to dynamic changes in their environment to make efficient use of the radio spectrum. CRN enables SUs to use the spectrum without interference to the PUs. This has to be achieved without any modifications or interactions with the PUs.

For maximal protection of PUs, spectrum sensing becomes one of the most important components for the establishment of cognitive radio. Spectrum sensing is the task of obtaining awareness about the spectrum usage and existence of PUs in a geographical area. That is, spectrum sensing discovers spectrum opportunities or holes by monitoring out-of-band channels and detecting spectrum holes. When discovered opportunities are utilized by SUs, in-band spectrum sensing must promptly detect return of PUs to an in band channel so that SUs can vacate the channel immediately upon detection of returning PUs.

Energy detector based spectrum sensing, also known as radiometry or periodogram, is the most common way of spectrum sensing because of its low computational and implementation complexities [27, 21, 28]. In addition, it is more generic (as compared to other spectrum methods) as receivers do not need any knowledge on the PUs' signal. The signal is detected by comparing the output of the energy detector with a threshold which depends on the noise floor [24]. Some of the challenges with energy detection include selection of the threshold for detecting PUs, inability to differentiate interference from PUs and noise, and poor performance under low signal-to-noise ratio (SNR) values [22]. Moreover, energy detection does not work efficiently for detecting spread spectrum signals [3, 27] and hidden primary user problem [6, 4].

In this paper, we apply a trust model into the energy detection to make it become a reliable spectrum sensing method in CRN. Our trust model is derived and modified from subjective logic [9, 10, 11], which qualitatively defines the representation, calculation, and combination of trust. Trust models have been found in security applications in e-commerce, peer-to-peer networks, and some other distributed systems [12, 2, 26, 1, 23]. In recent years, some research work is conducted to apply trust models into the security solutions of CRNs [19, 17, 16]. However, there are

ACSW '17, January 31-February 03, 2017, Geelong, Australia
© 2017 ACM. ISBN 978-1-4503-4768-6/17/01...$15.00
DOI: http://dx.doi.org/10.1145/3014812.3014882

no concrete and applicable designs proposed for the energy detection in CRNs, to the best of our knowledge.

We design our trust based energy detection system without modifying existing PUs. The new system has several salient features: (1) SUs perform trusted energy detection mainly according to the trust relationships among them; (2) A SU who performs malicious behaviors will eventually be detected and denied to the whole network; (3) System performance and detection accuracy are improved by avoiding malicious nodes at every detection step. The idea of the trust model can also be applied into other spectrum sensing methods such as cyclostationary feature detection, matched filter and so on.

The remaining of this paper is organized as follows. Some background overviews about existing energy detection and subjective logic are introduced in section 2. In section 4, we present the framework and network assumptions for the trusted energy detection system. Our trust model are described in section 3. We illustrate our trust based energy detection system details including collaborative energy detection and trust maintenance, as well as trust recommendation and updating algorithms in section 5. Performance and accuracy analyses are presented in Section 6. Finally, we conclude the paper in Section 7.

2. BACKGROUND

2.1 Energy Detection

Energy detection is the simplest technique for local spectrum sensing. An energy detector infers the existence of an PU based on the measured signal energy level. To measure the signal energy level in a band, the received signal is first processed using a bandpass filter and then the output signal is squared and integrated over an observation interval. The output of the integrator is compared with a predefined threshold to decide whether the band is being used or not. When a receiver has no sufficient information about the primary signal, such as the characteristics of the primary signal or the power of the random Gaussian noise, an energy detector is optimal [7].

In energy detection, let $x(n)$ and $w(n)$ denote the transmitted signal and the additive white Gaussian noise (AWGN) sample, of the channel between the transmitted signal and the receiver respectively, and n is the sample index. Moreover, let $s(n)$ denote a real PU signal. Then the transmitted signal $x(n) = s(n)$ for the real PU signal and $x(n) = 0$ when only SUs are transmitting or there is no signal in the channel. The two possible received signals can be described as follow:

$$y(n) = \begin{cases} w(n) & \text{SU only or none} \\ s(n) + w(n) & \text{PU} \end{cases} \tag{1}$$

The decision metric for the energy detection can be written as:

$$M = \sum_{n=0}^{N} |y(n)^2| \tag{2}$$

where N is the size of the observation vector. The decision on the occupancy of a band can be obtained by comparing the decision metric M against a fixed threshold λ_E, which is equivalent to distinguish between the following two hypohesis:

$$\begin{array}{lcl} H_0 & : & y(n) = w(n) \\ H_1 & : & y(n) = s(n) + w(n) \end{array} \tag{3}$$

The performance of the detection algorithm can be summarized with two probabilities: probability of detection P_D and probability of false alarm P_F. P_D is the probability of detecting a signal on the considered frequency when it truly is present. Thus, a large detection probability is desired. It can be formulated as:

$$P_D = P_r(M > \lambda_E | H_1) \tag{4}$$

P_F is the probability that the test incorrectly decides that the considered frequency is occupied when it actually is not, and it can be written as:

$$P_F = P_r(M > \lambda_E | H_0) \tag{5}$$

P_F should be kept as small as possible in order to prevent underutilization of transmission opportunities. However, The decision threshold λ_E to be selected for finding an optimum balance between P_D and P_F requires knowledge of noise and detected signal powers. The noise power can be estimated, but the signal power is difficult to estimate as it changes depending on ongoing transmission characteristics and the distance between the SU and PU. In practice, the threshold is chosen to obtain a certain false alarm rate [13]. Hence, knowledge of noise variance is sufficient for selection of a threshold.

Since the threshold used in energy detection depends on the noise variance. As a consequence, a small noise power estimation error causes significant performance loss [7]. As a solution to this problem, noise level is estimated dynamically by separating the noise and signal subspaces using multiple signal classification (MUSIC) algorithm [15]. Noise variance is obtained as the smallest eigenvalue of the incoming signal's autocorrelation. Then, the estimated value is used to choose the threshold for satisfying a constant false alarm rate. An iterative algorithm is also proposed to find the decision threshold in [25]. The threshold is found iteratively to satisfy a given confidence level, i.e. probability of false alarm.

2.2 Subjective Logic

Subjective logic is a kind of trust model which was proposed by A. Josang [9, 10, 11]. It is "a logic which operates on subjective beliefs about the world, and uses the term opinion to denote the representation of a subjective belief" [9]. The trust between two entities is then represented by opinion. An opinion can be interpreted as a probability measure containing secondary uncertainty.

In CRNs, SUs move with high mobility and may experience long distance in space among each other. A SU may be uncertain about another SU's trustworthiness because it does not collect enough evidence. This uncertainty is a common phenomenon, therefore we need a model to represent such uncertainty accordingly. Traditional probability model, which is also used in some trust models, cannot express uncertainty. While in subjective logic, an opinion consists of belief, disbelief and also uncertainty, which gracefully meets our demands. Subjective logic also provides a mapping method to transform trust representation between the evidence space and the opinion space [14].

Our trust model used in energy detection is then derived and modified from the subjective logic and is more applicable for the CRN. In our trust model, we substantiate the definition of the opinion by changing opinions about the 'TRUE' or 'FALSE' state of a proposition to opinions about a real SU entity's trustworthiness. The evidences we use in our trust model are collected through the correct or incorrect times when SUs perform collaborative energy detections with other SUs.

3. TRUST MODEL

3.1 Trust Representation

Our trust model is an extension of the original trust model in subjective logic which is introduced in Section 2. In our trust model, opinion is a 3-dimensional metric and is defined as follows:

Definition 1 (Opinion):

Let $O_b^a = (b_B^A, d_B^A, u_B^A)$ denote any SU A's opinion about any SU B's trustworthiness in a CRN, where the first, second and third component correspond to belief, disbelief and uncertainty, respectively. These three elements satisfy:

$$b_B^A + d_B^A + u_B^A = 1 \tag{6}$$

In this definition, belief means the probability of a SU B can be trusted by a SU A, and disbelief means the probability of B cannot be trusted by A. Then uncertainty u_B^A fills the void in the absence of both belief and disbelief, and sum of these three elements is 1.

3.2 Mapping between the Evidence and Opinion Spaces

A SU in CRN will collect and record all the positive and negative evidences about its neighboring SUs' trustworthiness, which will be explained in detail in Section 4. With these evidences we can obtain the opinion value by applying the following mapping equation which is derived from [11].

Definition 2 (Mapping):

Let $O_b^a = (b_B^A, d_B^A, u_B^A)$ be SU A's opinion about SU B's trustworthiness in a CRN, and let p and n respectively be the positive and negative evidences collected by SU A about SU B's trustworthiness, then O_b^a can be expressed as a function of p and n according to:

$$\begin{cases} b_B^A = \frac{p}{p+n+2} \\ d_B^A = \frac{n}{p+n+2} \qquad \text{where } u_A^B \neq 0 \\ u_B^A = \frac{2}{p+n+2} \end{cases} \tag{7}$$

3.3 Trust Combination

In our trust model, a SU will collect all its neighbors' opinions about another SU and combine them together using combination operations. In this way, the SU can make a relatively objective judgment about another SU's trustworthiness even in case several SUs are lying. The followings are two combination operations SUs may adopt: Discounting Combination and Consensus Combination.

3.4 Discounting Combination:

Let's consider such a situation: SU A wants to know Cs trustworthiness, then SU B gives its opinion about C. Assuming A already has an opinion about B.

Then A will combine the two opinions: A to B, B to C to obtain a recommendation opinion A to C. Discounting combination is for this purpose.

Definition 3 (Discounting Combination): *Let A, B and C be three SUs where $O_b^a = (b_B^A, d_B^A, u_B^A)$ is SU A's opinion about SU B's trustworthiness, and $O_c^b = (b_C^B, d_C^B, u_C^B)$ is SU B's opinion about SU C's trustworthiness. Let $O_c^{ab} = (b_C^{AB}, d_C^{AB}, u_C^{AB})$ be the opinion such that:*

$$\begin{cases} b_C^{AB} = b_B^A b_C^B \\ d_C^{AB} = b_B^A d_C^B \\ u_C^{AB} = d_B^A + u_B^A + b_B^A u_C^B \end{cases} \tag{8}$$

$O_C^{A,B}$ is called the disconnecting of O_C^B by O_C^A, which expresses A's opinion about C as a result of B's advice to A. By using the symbol '$\otimes$' to designate this operator, we define $O_C^{AB} \equiv O_B^A \otimes O_C^B$.

The discounting combination can be used for a mobile SU just moved from one location to a new one and becomes a new neighbor to some SUs in the new location.

3.5 Consensus Combination:

Different SUs may have different, even contrary opinions about one SU. To combine these opinions together to get a relative objective evaluation about that SU's trustworthiness, we may use Consensus combination.

Definition 4 (Consensus Combination): *Let $O_C^A = (b_C^A, d_C^A, u_C^A)$ and $O_C^B = (b_C^B, d_C^B, u_C^B)$ be opinions respectively held by SUs A and B about SU C's trustworthiness. Let $O_C^{A,B} = (b_C^{A,B}, d_C^{A,B}, u_C^{A,B})$ be the opinion such that:*

$$\begin{cases} b_C^{A,B} = (b_C^A u_C^B + b_C^B u_C^A)/k \\ d_C^{A,B} = (d_C^A u_C^B + d_C^B u_C^A)/k \\ u_C^{A,B} = (u_C^A u_C^B)/k \end{cases} \tag{9}$$

where $k = u_C^A + u_C^B - 2uA_C uB_C$ such that $k \neq 0$. Then $O_C^{A,B}$ is called the consensus between O_C^A and O_C^B, representing an imaginary SU $[A, B]$'s opinion about C's trustworthiness, as if it represented both A and B. By using the symbol '$\otimes$' to designate this operator, we define $O_C^{A,B} \equiv O_C^A \otimes O_C^B$.

The consensus combination can reduce the uncertainty of one's opinion.

4. OVERVIEW OF THE TRUSTED ENERGY DETECTION IN CRN

In this section, we first make some assumptions about our trusted energy detection system in CRN. We also describe the framework design of the system.

4.1 Network Model and Assumptions

SUs in CRNs often communicate with one another through an error-prone, bandwidth-limited, and insecure wireless channel. We do not concern the security problem introduced by the instability of physical layer or link layer. We only assume that: (1) Each SU in the CRN has the ability to recover all of its neighbors; (2) Each SU in the CRN can exchange some essential messages to its neighbors with high reliability; (3) Each SU in the network possesses a unique ID, the physical network interface address for example, that can be distinguished from others.

Moreover, SUs in the CRN can be either fixed or mobile devices with CR and energy detection capabilities, and can be either legal or malicious. Furthermore, we assume the transmitted signal power is much higher than that of the SU or the environmental noise level in the system while PU transmitting and only one PU is transmitting in the network at any given time.

Finally, we assume each SU has few neighboring SUs can communicate with, and each of them maintains a trust table to store its opinion about other SUs' trustworthiness.

4.2 Framework of trusted energy detection system in CRN

There are mainly three types of nodes in the CRN: PU, legal SUs and malicious SUs. All SUs are distributed in a certain area that within the transmitting range of the PU. Legal SUs will start collaborative energy detection with its neighbors and hence the trustworthiness of its neighbors will be changed according to their energy detecting results every time. The SUs always generate wrong results will then be discarded from next collaborative energy detecting process. On the contrary, SUs always give correct detecting results will be regarded as trusted and hence stay in next collaborative detecting process.

Let us first imagine the beginning of the CRN which contains a PU and a few SUs. Each node's opinion towards one another initially is $(0, 0, 1)$, which means that the SU does not trust or distrust another node but it is only uncertain about another SU's trustworthiness. Suppose SU A just joined a CRN, because the uncertainty element in A's opinion towards others is larger than or equal to 0.5, which means that A is not sure whether it should believe or disbelieve any other SUs, A will need to perform some collaborative energy detections with other SUs to build up its trust table. After some detection loops, A will change its opinions about other SUs gradually using the trust updating algorithm. The uncertainty elements in its opinions about other SUs will be mostly less than after a period of time. By means of this procedure, each SU in this CRN will form more certain opinions towards other SUs eventually after this period of initial time.

Once the trust relationship is established among most of the SUs in this CRN, these SUs can use the collaborative energy detection again which is based our trust model to perform a more efficient and accurate energy detecting. Note that the trust relationships among SUs are not symmetric. That is, if SU A totally trust SU B, B may not have the same opinion about A's trustworthiness. As a result, SU A will be excluded from B's collaborative energy detecting process.

In this framework, the establishment of trust relationships among SUs and the discovery of primary signals are all performed in a self-organized way, which is achieved by the cooperation of different SUs to exchange information and to obtain agreements without any third-party's interventions.

5. TRUST BASED ENERGY DETECTION IN CRN

In this section, we first discuss a collaborative energy detection used in CRN. We then combine this energy detection method with the trust model we mentioned in section 3. Details of our trust based collaborative energy detection such as trust judging rules and trust updating policies will be elaborated in this section, as well as the framework of the whole system.

5.1 Collaborative Energy Detection:

As being discussed in 2.1, energy detection is the most common way of spectrum sensing because of its low computational and implementation complexities [28, 20, 27]. However, energy detection has poor performance under low signal-to-noise ratio (SNR) values [22]. Moreover, energy detection does not work efficiently for detecting spread spectrum signals [3, 27] and hidden primary user problem [6, 4].

To improve the detection accuracy, a collaborative energy detection is proposed in [8]. Assuming there are M SUs and the local decision for each SU is 1 if it decides a PU's signal is present and 0 otherwise. Denoting D_i as the every local decision and D_M as the aggregated results observed by M SUs, $D_M = \sum_1^M D_i$. For an unknown signal, the global decision can be described as:

$$r_{global} = \begin{cases} 1 & D_M >= \frac{M}{2} \\ 0 & D_M < \frac{M}{2} \end{cases}$$

where r_{global} is the global result concluded by all SUs.

Introducing local decision and global decision is based on the following principle. It is difficult for the attacker to fabricate a signal so that all of the SUs receive the signal with the power level similar to that of the real PU. In other words, if the majority of the SUs decide the signal is from a potential attacker, then the global decision that the attacker is present will be made. However, it is still possible that multiple attackers maybe present and around a SU, hence the SU will make an invalid detection result. Therefore, by assigning the SU and all its (M) neighbors to measure the received signal power, letting these SUs know the signal power of the real PUs and exchanging the local decisions made by them for generating a global decision, a trust table can be build and the trustworthiness to its neighbors can be updated in the SU. After the trust table is properly built, untrusted neighboring SUs will be excluded from the collaborative energy detection and the detecting result can be achieved in a high reliability.

5.2 SU Model

We add three new fields into each SU's original trust table: positive events, negative events and opinion. Positive events are the correct energy detection times between two SUs. Similarly negative events are the incorrect detection ones. Opinion means this SU's belief towards another SU's trustworthiness as defined before. The value of opinion can be calculated according to Formula 7. These three fields are the main factors when performing trusted energy detection.

5.3 Trust Judging Rules

Before describing the process of trusted energy detection system in detail, we predefine some trust judging rules here and in Table 1.

- In SU A's opinion towards SU B's trustworthiness, if

Table 1: Criteria for Judging Trustworthiness.

Belief	Disbelief	Uncertainty	Actions
		> 0.5	A request trustworthiness towards B from its neighbors, the SU will still be included in the collaborative energy detection for B's neighbors to build their trust table. However, B's detection will not be counted in global detection result
	> 0.5		Distrust a SU for an expire time
> 0.5			Trust a SU and include it in collaborative energy detection to generate a global result
≤ 0.5	≤ 0.5	≤ 0.5	A request trustworthiness towards B from its neighbors, the SU will still be included in the collaborative energy detection for B's neighbors to build their trust table. However, B's detection will not be counted in global detection result

the first component *belief* of opinion O_B^A is larger than 0.5, A will trust B and include B in collaborative energy detection to make a final decision with A.

- In SU A's opinion towards SU B's trustworthiness, if the second component *disbelief* of opinion O_B^A is larger than 0.5, A will not trust B and A will refuse B to participate in collaborative energy detection with A. Accordingly the trustworthiness for B in A's trust table will be disabled and deleted after an expire time.

- In SU A's opinion towards SU B's trustworthiness, if the third component *uncertainty* of opinion O_B^A is larger than 0.5, A will request B's trustworthiness from other neighboring SUs if it is possible. And then decide whether B is trusted. If no neighbor of A can provide trustworthiness recommendation to B, B will still be included in the collaborative for other SUs to build up their own trust tables, but B's detection will not be counted in global detection result as it is not trusted yet.

- In SU A's opinion towards SU B's trustworthiness, if the three components of opinion O_B^A are all less than 0.5 or equal to 0.5, A will request B's trustworthiness from other neighboring SUs if it is possible. And then decide whether B will be included in the collaborative energy detection. If no neighbor of A can provide trustworthiness recommendation to B, B will still be included in the collaborative for other SUs to build up their own trust, but B's detection will not be counted in global detection result as it is not trusted yet. Otherwise, B is trusted and it will be included to make a final decision with A.

- If SU B has no trust entry in A's trust table, A's opinion about B is initialized as $(0, 0, 1)$.

5.4 Trust Updating Policies

Opinions among SUs change dynamically with the increase of correct or incorrect detection times. When and how to update trust opinions among SUs will follow some policies. We derive as follows:

- Each time a SU A has performed a collaborative energy detection with another SU B and B gets the same detection result as the global result. B's correct events in A's trust table is increased by 1.

- Each time a SU A has performed a collaborative energy detection with another SU B and B gets a different detection result from the global result. B's incorrect events in A's trust table will be increased by 1.

- Each time when the field of the correct or incorrect events changes, the corresponding value of opinion will be recalculated using formula 7 from the evidence space to opinion space.

- If SU B's trust entry has been deleted from SU A's trust table because of expiry, or there is no B's trust entry from the beginning, the opinion O_B^A will be set to $0, 0, 1$.

5.5 Trust Recommendation

Existing trust models seldom concern the exchange of trust information. However, it is necessary to design an information exchange mechanism when applying the trust models into CRN. In our trust recommendation protocol, there are three types of messages: Trust Request Message (TREQ), Trust Reply Message (TREP), and Trust Warning Message (TWARN). SUs who issue TREQ messages are called *Requestor*. Those who reply TREP messages are called *Recommender*. The recommendation target nodes are called *Recommendee*. Any node may be a *Requestor*, a *Recommender*, or a *Recommendee*. These three types of messages share a common message structure, which is shown in Figure 1.

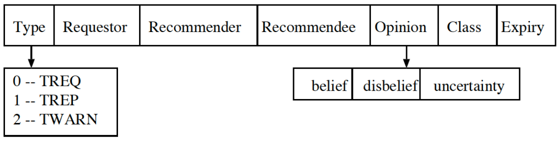

Figure 1: Message Structure of Trust Recommendation Protocol.

When a SU wants to know another SU's new trustworthiness, it will issue an TREQ message to its trusted neighbors. TREQ message uses the above structure and leaves the fields of *Recommender*, *Opinion* and *Expiry* empty. The *Type* field is set to 0. SUs which receive the TREQ message will reply with an TREP message with the *Type* field set to 1. When a SU believes that another SU has become malicious or unreliable, it will broadcast a TWARN message with the *Type* set to 2 to its neighbors.

5.6 Trusted Energy Detection in CRN

Below we illustrate how to perform trust based energy detection in CRN.

Scenario 1: Beginning of a CRN – Let us consider a simple CRN which only contains a PU and several SUs. The topology of this minimal CRN is shown in Figure 2.

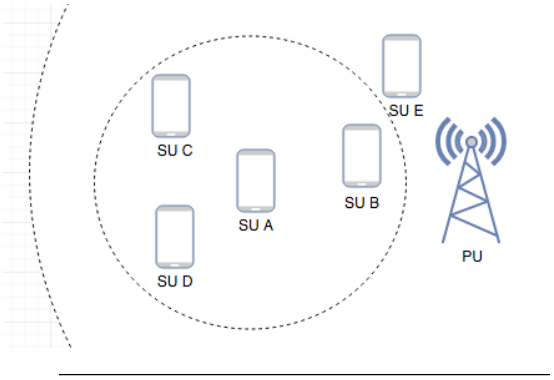

Figure 2: The beginning of a simple CRN.

In this figure, SU A has few direct neighbor but some other SUs are not A's neighbors even they are all inside PU's transmitting range. At the beginning, there is no entry in each SU's trust table, and as mentioned in section 5.3, the initial value of each SU's opinion towards one another is $(0, 0, 1)$.

Now each SU in the CRN wants to build its own trust table, they start collaborative energy detection process constantly, no matter the PU is transmitting primary signal or not. As a result, a trust table in each SU will be built up gradually. For example, the building processes are listed as below:

(1) A, B, C and D participate in the first round of energy detection, assume their local detecting results are $(1, 1, 1, 0)$ and hence the global result is 1 based on 5.1. In A's trust table, the opinions towards B, C and D will be $(0.33, 0, 0.67)$, $(0.33, 0, 0.67)$ and $(0, 0.33, 0.67)$ respectively. The opinion values in A trust table will change again after second round of energy detection due to the detecting results B, C and D make.

(2) Once there are more than a given number (which can be set differently in different SUs) neighbors of A are not *Uncertain* in A's trust table, A can start to use the channel if it believes the PU signal is absent by collaborative energy detection only with its *trusted* neighbors. At meantime, A's trust table will still be updated after each detection process. Therefore, it is possible for some SUs become to *Untrusted* from *Trusted*, or vise versa.

Scenario 2: A CRN after a period of running times – In this case, a stable CRN has run for a period time and their trust relationships have been established among almost SUs. Consequently we can give a general description of below situations:

(1) Assume SU A wants to use the channel for communication, it starts a collaborative energy detection with its trusted neighbors to see if the primary signal is at present. A will take the channel and starts transmitting in the channel if the global result is negative. Once there is another signal transmitting on the same channel and detected by A, A will employ another trust based collaborative energy detection on the same channel to check if the signal is from PU. If the global result becomes positive, which means the PU is transmitting, A will have to quit current channel and look for an alternate unoccupied channel to avoid interference. Otherwise, A stays in the channel and continues its own communication.

(2) Assume SU E used to be B's neighbor but not A's and recently moved to A's nearby hence becomes A's new neighbor. The topology of this minimal CRN is shown in Figure 3. As discussed in section 5.5 and section 3.3, A will request its trusted neighbors for their opinions towards E. A will include E as a trusted neighbor if the A's existing trusted neighbors give a positive response. Otherwise, E will be excluded from A's collaborative energy detection. If E is uncertain to all trusted neighbors of A, for example E is a new SU recently joined the CRN, becomes to A's neighbor and unknown to all other SUs in the CRN. The trust entry of E will be set as $(0, 0, 1)$ and the opinion towards E will be gradually updated after few rounds of collaborative energy detection. During the trust updating process, E's local decision will not be used to generate the global result for making the final decision, but will be used by its neighboring SUs for building their opinions towards E.

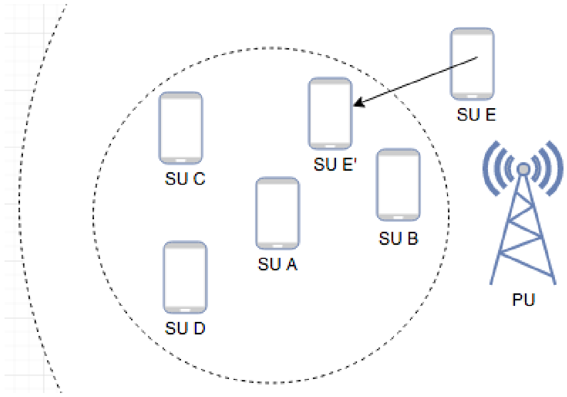

Figure 3: SU E recently moved from B's neighborhood to A's.

6. ANALYSIS

In our analysis, we set up a simply CRN that contains a PU and 8 SUs. We assume one of the 8 SUs is the SU needs to detect the existence of PU and the other 7 SUs are close to it and are all it's neighbors. Moreover, we assume 4 of it's neighbors are trusted and the other 3 are malicious.

Below table 2 shows the trust building steps. From the table 2 we can see the first 5 SUs are differentiated as trusted after only 3 step as their belief values are greater than 0.5. On the contrary, the other 2 SUs are marked as malicious because their disbelief values reach to 0.6.

Now assume the trusted SUs have a certain error when performing energy detection, which is 10%. Below table 3 shows the trust building results after 3 steps, 5 steps, 10 steps and 20 steps:

From the table 3 we can see when reliable SUs have a

Table 2: Trust updating process for 4 reliable SUs and 3 malicious SUs.

SUs	**SU 1**	**SU 2**	**SU 3**	**SU 4**	**SU 5**	**SU 6**	**SU 7**
Step 0	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$
Step 1	$(0.33, 0.67, 0)$	$(0.33, 0.67, 0)$	$(0.33, 0.67, 0)$	$(0.33, 0.67, 0)$	$(0, 0.67, 0.33)$	$(0, 0.67, 0.33)$	$(0, 0.67, 0.33)$
Step 2	$(0.5, 0.5, 0)$	$(0.5, 0.5, 0)$	$(0.5, 0.5, 0)$	$(0.5, 0.5, 0)$	$(0, 0.5, 0.5)$	$(0, 0.5, 0.5)$	$(0, 0.5, 0.5)$
Step 3	$(0.6, 0.4, 0)$	$(0.6, 0.4, 0)$	$(0.6, 0.4, 0)$	$(0.6, 0.4, 0)$	$(0, 0.4, 0.6)$	$(0, 0.4, 0.6)$	$(0, 0.4, 0.6)$

Table 3: Trust updating process for 4 reliable SUs with 10% error and 3 malicious SUs.

SUs	**SU 1**	**SU 2**	**SU 3**	**SU 4**	**SU 5**	**SU 6**	**SU 7**
Step 0	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$	$(0, 1, 0)$
Step 3	$(0.2, 0.4, 0.4)$	$(0.6, 0.4, 0)$	$(0.4, 0.6, 0.2)$	$(0.2, 0.4, 0.4)$	$(0.2, 0.4, 0.4)$	$(0.2, 0.4, 0.4)$	$(0.2, 0.4, 0.4)$
Step 5	$(0.43, 0.29, 0.28)$	$(0.28, 0.29, 0.43)$	$(0.28, 0.29, 0.43)$	$(0.71, 0.29, 0)$	$(0.14, 0.29, 0.57)$	$(0.43, 0.29, 0.28)$	$(0.43, 0.29, 0.28)$
Step 10	$(0.75, 0.17, 0.08)$	$(0.5, 0.17, 0.33)$	$(0.5, 0.17, 0.33)$	$(0.42, 0.17, 0.41)$	$(0.17, 0.17, 0.66)$	$(0.17, 0.17, 0.66)$	$(0.17, 0.17, 0.66)$
Step 20	$(0.64, 0.09, 0.27)$	$(0.59, 0.09, 0.32)$	$(0.82, 0.09, 0.09)$	$(0.59, 0.09, 0.32)$	$(0.36, 0.09, 0.55)$	$(0.27, 0.09, 0.64)$	$(0.27, 0.09, 0.64)$

certain probability(10%) to make a wrong energy detecting result, more steps are required to distinguish trusted and malicious SUs. In above example, it takes 20 steps to mark the first 4 SUs as trusted. However, after a certain number of steps, only trusted SUs will be included in energy detection for searching spectrum holes or detecting the existence of primary signal, which significantly increase the detection accuracy as the malicious SUs will be excluded in the future detecting process.

By introducing the idea of the trust model into our collaborative energy detection, we are able to establish a more flexible and less overhead spectrum sensing for CRNs.

From performance point of view, our trusted collaborative energy detection introduces less computation overheads than other spectrum sensing solutions for CRNs. This design performs collaborative energy detection compared to cyclostationary feature detection or matched filter. After the trust relationships is established, only trusted SUs will be included in decision making process instead of involving all neighbouring SUs. Therefore, the trusted collaborative energy detection improves the performance of spectrum sensing solutions. Unlike some previous security schemes [8, 5, 18], whose basis of spectrum sensing is “blind un-trust”, our proposed model does not decrease the efficiency of spectrum sensing and maintenance.

From security point of view, our design will detect SUs’ misbehavior finally and reduce the harms to the minimum extent. When a good SU is compromised and becomes a bad one, its misbehavior will be detected by its neighbors. Then with the help of trust update algorithm, the opinions from the other SUs to this SU will be updated shortly. Thus this SU will be denied access to the CRN. Similarly, a previous bad SU can become a good one if the attacker leaves. In this situation, our design allows this node’s opinion from other nodes’ points of view to be updated from $(0, 1, 0)$ to $(0, 0, 1)$ after a period of expiry time.

From flexibility point of view, our security scheme gives each SU flexibility to define its own opinion threshold. The default opinion threshold is 0.5, which can be increased by a SU to maintain a hight security level and also can be decreased to meet demands of some applications.

Furthermore, as we have already mentioned in section 1, our trust based energy detection system has few advantages compared to other trust models used in CRN. First of all, all SUs in CRN communicate to their direct neighbors only and hence the entire system does not rely on base stations. As a result, the communication overhead will be reduced and single point of failure does not exist in our proposed system. Moreover, unlike other trust models in CRN, we introduced a third field uncertainty in our trust model, which is a common phenomenon in CRN. Uncertainty in our trust model can be used to represent the SUs that recently moved to a SU’s nearby or joined to a CRN and hence has no trustworthiness and unknown to a specific SU. Traditional trust models in CRN don’t have such field and cannot express uncertainty, which don’t meet our demands gracefully.

7. CONCLUSION

This paper is the first to apply the idea of a trust model in subjective logic into the energy detection of CRNs. The trust and trust relationship among SUs can be represented, calculated and combined using an item opinion. In our trust based energy detection protocol, SUs can cooperate together to obtain an objective opinion about another SU’s trustworthiness. They can also perform trusted energy detection to determine whether the primary signal is occupying the channel according to the trust relationship among them. With an opinion threshold, SUs can flexibly choose whether a neighboring SU should be included in the decision making process. Therefore, the computational overheads are reduced without the need of requesting and verifying all neighboring SUs at every energy detection operation. In summery, our trusted collaborative energy detection is a more light-weighted but more flexible security solution than other spectrum sensing designs.

In the future we will optimize our trusted energy detection and establish some fast response mechanisms when malicious behaviors of attackers are detected. We will also work at applying the trust model into other spectrum sensing techniques (e.g., cyclostationary feature detection, matched filter detection) in CRN. A detailed simulation evaluation will be conducted in terms of message overhead, security analysis, and tolerance to mobile attackers.

8. ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions.

9. REFERENCES

[1] A. Abdul-Rahman and S. Hailes. A distributed trust model. In *Proceedings of the 1997 workshop on New*

security paradigms, pages 48–60. ACM, 1998.

[2] T. Beth, M. Borcherding, and B. Klein. *Valuation of trust in open networks*. Springer, 1994.

[3] D. Cabric, S. M. Mishra, and R. W. Brodersen. Implementation issues in spectrum sensing for cognitive radios. In *Signals, systems and computers, 2004. Conference record of the thirty-eighth Asilomar conference on*, volume 1, pages 772–776. IEEE, 2004.

[4] D. Cabric, A. Tkachenko, and R. W. Brodersen. Spectrum sensing measurements of pilot, energy, and collaborative detection. In *Military communications conference, 2006. MILCOM 2006. IEEE*, pages 1–7. IEEE, 2006.

[5] R. Chen. Enhancing attack resilience in cognitive radio networks. 2008.

[6] G. Ganesan and Y. Li. Agility improvement through cooperative diversity in cognitive radio. In *Global Telecommunications Conference, 2005. GLOBECOM'05. IEEE*, volume 5, pages 5–pp. IEEE, 2005.

[7] N. Hoven, R. Tandra, and A. Sahai. Some fundamental limits on cognitive radio. *Wireless Foundations EECS, Univ. of California, Berkeley*, 2005.

[8] F. Jin, V. Varadharajan, and U. Tupakula. Improved detection of primary user emulation attacks in cognitive radio networks. In *Telecommunication Networks and Applications Conference (ITNAC), 2015 International*, pages 274–279. IEEE, 2015.

[9] A. Jøsang. Prospectives for modelling trust in information security. In *Information Security and Privacy*, pages 2–13. Springer, 1997.

[10] A. Jøsang. A subjective metric of authentication. In *Computer Security—ESORICS 98*, pages 329–344. Springer, 1998.

[11] A. Jøsang. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(03):279–311, 2001.

[12] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web*, pages 640–651. ACM, 2003.

[13] J. Lehtomaki, M. Juntti, H. Saarnisaari, and S. Koivu. Threshold setting strategies for a quantized total power radiometer. *IEEE Signal Processing Letters*, 12(11):796, 2005.

[14] X. Li, M. R. Lyu, and J. Liu. A trust model based routing protocol for secure ad hoc networks. In *Aerospace Conference, 2004. Proceedings. 2004 IEEE*, volume 2, pages 1286–1295. IEEE, 2004.

[15] M. P. Olivieri, G. Barnett, A. Lackpour, A. Davis, and P. Ngo. A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrally agile software defined radios. In *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pages 170–179. IEEE, 2005.

[16] S. Parvin, S. Han, L. Gao, F. Hussain, and E. Chang. Towards trust establishment for spectrum selection in cognitive radio networks. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pages 579–583. IEEE, 2010.

[17] Q. Pei, R. Liang, and H. Li. A trust management model in centralized cognitive radio networks. In *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2011 International Conference on*, pages 491–496. IEEE, 2011.

[18] D. Pu, Y. Shi, A. V. Ilyashenko, and A. M. Wyglinski. Detecting primary user emulation attack in cognitive radio networks. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–5. IEEE, 2011.

[19] T. Qin, H. Yu, C. Leung, Z. Shen, and C. Miao. Towards a trust aware cognitive radio architecture. *ACM SIGMOBILE Mobile Computing and Communications Review*, 13(2):86–95, 2009.

[20] A. Sahai and D. Cabric. Spectrum sensing: fundamental limits and practical challenges. In *Proc. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, 2005.

[21] N. Sai Shankar, C. Cordeiro, and K. Challapali. Spectrum agile radios: utilization and sensing architectures. In *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pages 160–169. IEEE, 2005.

[22] H. Tang. Some physical layer issues of wide-band cognitive radio systems. In *New frontiers in dynamic spectrum access networks, 2005. DySPAN 2005. 2005 first IEEE international symposium on*, pages 151–159. IEEE, 2005.

[23] Y. Teng, V. Phoha, and B. Choi. Design of trust metrics based on dempstershafer theory, 2000.

[24] H. Urkowitz. Energy detection of unknown deterministic signals. *Proceedings of the IEEE*, 55(4):523–531, 1967.

[25] F. Weidling, D. Datla, V. Petty, P. Krishnan, and G. Minden. A framework for rf spectrum measurements and analysis. In *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, 2005.

[26] R. Yahalom, B. Klein, and T. Beth. Trust relationships in secure systems-a distributed authentication perspective. In *Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium on*, pages 150–164. IEEE, 1993.

[27] Y. Yuan, P. Bahl, R. Chandra, P. Chou, J. I. Ferrell, T. Moscibroda, S. Narlanka, Y. Wu, et al. Knows: Cognitive radio networks over white spaces. In *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pages 416–427. IEEE, 2007.

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