EURASIP Journal on
Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Security management based on trust determination in cognitive radio networks

Jianwu Li[1,2*], Zebing Feng[1], Zhiqing Wei[1], Zhiyong Feng[1] and Ping Zhang[1,2]

Abstract

Security has played a major role in cognitive radio networks. Numerous researches have mainly focused on attacking detection based on source localization and detection probability. However, few of them took the penalty of attackers into consideration and neglected how to implement effective punitive measures against attackers. To address this issue, this article proposes a novel penalty mechanism based on cognitive trust value. The main feature of this mechanism has been realized by six functions: authentication, interactive, configuration, trust value collection, storage and update, and punishment. Data fusion center (FC) and cluster heads (CHs) have been put forward as a hierarchical architecture to manage trust value of cognitive users. Misbehaving users would be punished by FC by declining their trust value; thus, guaranteeing network security via distinguishing attack users is of great necessity. Simulation results verify the rationality and effectiveness of our proposed mechanism.

Keywords: Security; CRNs; Honest users; Misbehaving users; Trust value; Punishment

1 Introduction

Wireless communication technology is in a period of rapid development, and growing business demand has driven communication technology renewal and development. In the process of development, the growing business demands are restricted by the limited spectrum resource. The report of Federal Communications Commission (FCC) suggests that currently spectrum scarcity is largely due to the inefficient and rigid regulations rather than the physical shortage of the spectrum [1]. Recently, cognitive radio network (CRN) has been brought to the forefront due to its potential to solve the conflict between limited spectrum supply and spectrum demand from ever-increasing wireless applications and services, which is defined as a wireless network employing technology to obtain knowledge of its operational and geographical environment, established policies, and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve end-to-end network objectives; and to learn from the results obtained [2].

However, CRNs are an open and random access network environment, where the unlicensed secondary users (SUs) can use the channels that are not currently used by the licensed primary users (PUs) by spectrum-sensing technology. Therefore, they not only face all the security threats in the traditional wireless networks, but also new security threats that have arisen due to their unique cognitive characteristics, such as [3] the following:

Primary user emulation attacks (PUEA) In this type of attacks, attackers may transmit at forbidden time slots and effectively emulate the primary user to make the protocol-compliant SUs erroneous conclusion that the primary user is present.

Spectrum sensing data falsification attacks (SSDF) Attackers send false observation information, intentionally or unintentionally, to the fusion center (FC), and let the FC make the wrong decision.

PUEA and SSDF attacks focus on the physical layer of a CRN. Furthermore, these could also make MAC layer threats-vulnerabilities and IEEE 802.22 specific threats, cross-layer attack that adversaries can launch attacks targeting multiple layers, software-defined radio security

*Correspondence: jianwu.lee@gmail.com
[1] Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Network information processing center, State Key Laboratory of switching technology and network, Beijing University of Posts and Telecommunications, Xitucheng Road No.10, Beijing 100876, China

that falls into two main categories: software-based protection, and hardware-based protection, and other traditional security threats.

Security issues in CRNs become unavoidable challenge, and how to solve the security problems has become a research hot-spot. In [4], Fragkiadakis et al. had given a comprehensive survey of the existing works on CRN security, which introduced some security threats and detection techniques in detail. Most of the studies in security of CRN focus on spectrum sensing techniques, where the main contributions are attack defense based on attack detection. The existing achievement discussing detailed approaches for the detection and mitigation of specific attacks, such as by Subbalakshmi et al. in [5-8] and other scholars, Chen et al. in [3,9], Zhu et al. in [10], Yu et al. in [11], Wu et al. in [12,13]. They all have made a great contribution in the CRN security areas, and their achievements will not be described here, as it is out of the scope of this paper.

Current researches are mostly focusing on signal detection based on attack defense but could not implement any punishment. A likely instance is that we cannot punish an offender, even though the person transgresses moral or civil law; the only thing we can do is offering the proof to legal operation department. We will analyze the existing security mechanisms before our proposed one.

Ding et al. in [14] provided a novel effective algorithm using kernel KMC (*k*-means clustering) method to be answerable for attacker detection, which not only improves the attacker detection performance but also offers processing and memory savings. Zhang et al. in [15] proposed a security scheme based on localized combinatorial keying (LOCK) scheme and employees ID-based secure group key management, which minimizes the number of key storage requirement and the number of the communication messages for rekeying. Sakran et al. in [16] proposed a secure relay selection scheme which selects a trusted decode and forward relay to assist the SUs and maximize the achievable secrecy rate that is subjected to the interference power constraints at the PUs for the different number of eavesdroppers and PUs under available channel knowledge in the security constrained CRNs. In [17], Chen et al. proposed a game theoretical anti-jamming scheme and modeled the jamming and anti-jamming process as a Markov decision process. With this approach, secondary users are able to avoid the jamming attack launched by external attackers. In [18], Jo et al. proposed a selfish attack detection technique, COOPON (called cooperative neighboring cognitive radio nodes). However, this approach needs to detect and decide the secondary users as legitimate SU (LSU) or selfish SU (SSU) through comparing the reported data one by one while selecting a reliable user as the comparison object. In this case, it is bound to bring a large consumption of calculation when lots of secondary users are in this scheme. In order to improve the cooperative detection performance, Ding et al. in [19] designed a joint spatio-temporal spectrum sensing algorithm, which based on three phases (i.e., a global cooperation phase, a local cooperation phase, and a joint decision phase). Gao et al. in [20] proposed a privacy preserving framework in collaborative spectrum sensing to prevent location privacy leaking from the collaborative attacks. This scheme based on encrypting authentication of fusion center can effectively thwart PUEA, SSDF attack, and misbehavior. Pietro et al. in [21] proposed an anti-jamming technology based on time-delayed broadcast scheme, which opens up a new area for cognitive radio network security. This mechanism takes the greedy malicious users into account which are mainly improving the access opportunities through misconduct.

However, the security schemes described above are still passive attack defense. How to take an active defense and impose the penalty for attack users are the main consideration of this article. In [22,23], the distributed trust models were proposed individually based on parameter modeling and time-window feedback mechanism, which have the advantages in countering strategic altering behavior and dishonest feedbacks of malicious users. The trust mechanism that based on authentication can effectively guarantee the reliability of the network. Moreover, the punishment mechanism ensures the security of networks by constraining misbehaving users effectively. So, the trust scheme and penalty scheme are two important aspects of the active defense technologies.

In this paper, a novel trust mechanism Security Management based on Trust Determination (SMTD) is proposed for solving the security issue in CRNs. A centralized management in FC [24,25] is needed to manage access of cognitive users effectively, and FC has absolute authority of cognitive user authentication management and can carry out effective punishment for the attackers, while attacks are unable to avoid only through signal detecting. Therefore, we put forward the mechanism to include the following modules: *authentication, interactive, configuration, the trust value collection, the trust store and update, and punish, etc.* In order to reduce the computational load brought by cognitive interaction between users, we put forward the two-layer network hierarchical architecture including fusion center and cluster heads (FC + CHs). FC is mainly responsible for the trust value of store/update, cognitive users access network authentication for the first time, distribution of cognitive user cluster network, resource allocation, and the most important function, to execute punishment of attack users; CHs interact with the cognitive users in sub-networks then update and report trust values to the fusion center. Details of the metric used in this paper can be seen from (Table 1).

Table 1 List of parameters

Symbol	Description
C_i	Cluster indicia
S	The cluster set
V_{ij}	Trust value
R_i	Resource
λ_i	Resource allocation threshold
V	The matrix of trust value
a, b, c, d	The weight coefficient of attribute
s	The rate of decay
α, β, γ	The weight coefficient of trust value
R_f	Covering radius of FC
ρ_r	The threshold of cluster head
L	The maximum number of cluster heads
K	Maximum number of cognitive users per cluster sub-network
N	The number of cognitive users
σ	The attenuation factor
ε	The reward factor
σ	The penalty factor
ξ	The recovery factor
ζ	The regulate factors
η	Penalty accumulation factor

The main contributions of this paper are as following:

- Proposed a centralized trust scheme
- Two-layer hierarchical architecture
- Grade of penalty mechanism

The rest of this paper is organized as follows: Section 2 presents the cognitive scenario and our proposed trust scheme. In Section 3, we introduce the function module of the dual-layer architecture. Penalty scheme is introduced in Section 4. Section 5 describes the process of the overall mechanism in detail. In Section 6, we analyze the order of complexity. Simulation and verification will be done in Section 7. At last, we conclude our work in Section 8.

2 Mechanism model

In this section, we will present the cognitive scenario of the proposed mechanism and then introduce the process of trust determination.

2.1 Application scenario

A centralized CRN scenario is illustrated as in Figure 1. There are some cognitive networks coexisting with the primary networks and each one has a central service FC. A cognitive network is divided into some cluster sub-networks that contain dozens of cognitive users. Every cluster sub-network has one centralized cluster head (CH) in charge of collecting all users' cognitive information in the sub-network and then reporting to the FC. The detailed functions of the FC and CH are as follows:

Fusion center: collecting available radio resources of primary users through cognitive users sensing reports and conduct resource management for the cognitive users; calculating trust values of all cognitive users in a cognitive network and storing them; implementing punishment for misbehaving users, and updating trust value results

Cluster heads: collecting trust values of cognitive users and reporting to FC by interaction; reporting misbehaving users' information to FC timely while an attack is detected

2.2 Trust criterion

Trust determination is a total evaluation for an user's capacity and reputation. These evaluation results are from other entities via information interplay and can be used to guide the user's further action. Reputation is an observation according to other entities or a summation of the entity's previous action. Attributes of trust determination can be shown as follows:

Attack-resistant: Trust determination should recognize and resist attacks, such as forger (PUEA), dishonest feedback (SSDF attack), slander, and united fraud.

Availability: Trust is constituted by constant learning and sufficient experience. As the time goes on, trust value gradually drops down.

Rewards and punishment: Trust determination should provide a suitable reward scheme which can serve well-performing users better with priority access or bandwidth. Punishment scheme aims to decrease the user's trust value in terms of an occurring attack.

Authentication mechanism: For a new accessing user, FC will allocate an identity authentication which consists of user identity, time, initial value, available channel (available resources list), resource utilization limits, service capacity, and so on.

Sensitivity: Sensitivity which reflects the degree of trust is affected by the changing network environment. Specifically, cognitive users could be on-line or off-line at any time, thus, a breakdown and trust model should recognize and adjust trust in accordance with various needs.

Distinction: For a cognitive user trusted enough, a sudden fraud would bring serious communication disorder. Other than that, malicious cognitive users might oscillate between establishing trust and defrauding trust. To avoid such deceit effectively, the model is expected to offer a

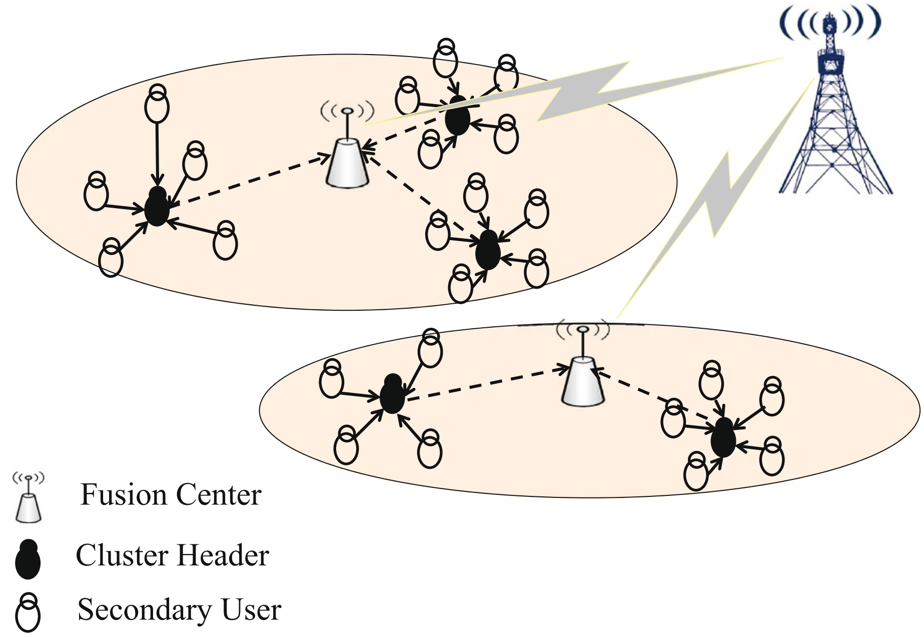

Figure 1 Scenario of proposed mechanism.

mechanism to identify the changes of users' trust value efficiently.

2.3 Trust determination model

Aside from all the attributes mentioned above, an ideal trust model should also have a trust management process which involves the generation of trust, presentation, measurement, interplay, punishment, and updating.

2.3.1 Generation of trust degree

Trust among cognitive users erects on demand by resource sharing and communication, which has been proven to be an efficient mechanism. Trust is a subject behavior which is centralized by FC and gives each accessing cognitive user an authentication header, as shown in Table 2.

Table 2 Authentication header

Symbol	Meaning
Identity	User identity
Time	Time
C_i	Cluster
v_{ij}	The initial trust value
$R_1, R_2, \cdots R_n$	Resource list
$\lambda_1, \lambda_2, \cdots \lambda_n$	Resource access threshold
SC	Service capacity

2.3.1.1 User identity

Referring to human society [22], user identities can be presented as follows:

$$\text{Identity} = h(\text{Key})||\text{Sig}_X(S_K(\text{ID})) \tag{1}$$

where $h(\cdot)$ is hash function, Key means the key word for entity service, $\text{Sig}_X(\cdot)$ is digital signature, X is the private key, ID is entity identity, S_K is scrambling algorithm, K is scrambling key, and $||$ is a binding symbol which makes the correspondence between marking identity and true identity. A signature can achieve certification while scrambling can ensure the anonymity of entity. As regard to legal authentication in distributed anonymous condition, it can be achieved in the way of zero-knowledge [26]. Details will be ignored in terms of the article length limit.

2.3.1.2 Time

This metric indicates the time when cognitive user gets access to a network. It can also be used as a start point for user interaction and time decaying.

2.3.1.3 Cluster

This metric represents the serial number of cluster. If it is not the first time for cognitive user to access cluster, C_i would remain a previous value. Otherwise, C_i would be set as 0.

2.3.1.4 Initial value of trust

When a cognitive user gets access to a network, a trust value v_{ij} would be given which is usually half less than the maximum. A high value of trust may bring baleful attack, while a low value of trust may make some users idle.

2.3.1.5 Resources list

There is more than one available resource when cognitive user gets access to network. $R_1, R_2, \ldots R_n$ are used to present the available channels.

2.3.1.6 Threshold of resource access

Thresholds of resource access are corresponding to resources lists and are presented by $\lambda_1, \lambda_2, \ldots \lambda_n$. Access permissions are set depending on these threshold. For example, if $\lambda_n = 1$, the access requests from users whose trust value is between 0 and 1 would be rejected.

2.3.1.7 Service capacity

It means the QoS guarantee for single cognitive user. Cognitive users should mark their service capacity, such as bandwidth and channels.

2.3.2 The characterization of trust

Trust is subjective, reflecting interests and demands of cognitive users. Different context and interests correspond to different value of trust. This article shall illustrate trust based on a three-layer structure, namely

$$Tr = U \cdot S \cdot A. \tag{2}$$

U present cognitive users that can be classified into honest secondary users and malicious secondary users. S is the cover region of CRN, for example, in black, gray, and white three-region scenarios [27]. To simplify the analysis, we selected a single scenario. A is the attribute made by FC in certain context and can be classed into four groups: service quality SQ, interaction quantity TQ, processing time PT, and cost and others CM. Different users calculate the interactive trust value by adjusting attribute weight vector, as follows:

$$V = a \cdot \mathrm{SQ} + b \cdot \mathrm{TQ} + c \cdot \mathrm{PT} + d \cdot \mathrm{CM} \tag{3}$$

where a, b, c, d is the attribute weight satisfying $a + b + c + d = 1$. As FC's assessment of attribute is fuzzy, trust should be quantified according to users' behavior in the network, e.g., $V_{\text{level}} \in \{-2, 1, 0, 1, 2\}$, respectively, corresponding to five levels, namely, extremely distrusted, little trusted, general trust, considerably trust, and extremely trusted.

2.3.3 Trust metrics

The basic metrics related to trust of SUs are considered as follows:

1. *The direct trust value*

$$\mathrm{DirTr}_{ih} = \frac{1}{n} \sum_{l=1}^{n} A(s, t_l) \cdot \mathrm{Attr}_{ih} \cdot \mathrm{DS}_{ih}^{l} \tag{4}$$

where l is the frequency of interactions, and DS_{ih} is the satisfaction evaluation of SU_h to SU_i, which contains four attribute evaluations $\mathrm{DS}_{ih} = \{\mathrm{SQ,TQ,PT,CM}\}$.
The bigger the value of DS_{ih}, the higher is the reliability of SU_i; $\mathrm{Attr}_{ih} = [\ a\ b\ c\ d\ ]$ is the weight coefficient matrix of DS_{ih}; $A(s, t_l)$ is attenuation function defined as

$$A(s, t_l) = \nu \cdot e^{-s \cdot L(t_l)} \tag{5}$$

where S is the decay rate and meets the condition $0 < s \leq 1$; $L(t_l)$ is interactive function on time, $L(t_l) = \mathrm{Round}((t_l - t_0)/T)$, and T is scanning period that can be set according to different needs (e.g., days, hours, minutes, etc.).
The degree of satisfaction DS_{ih}^{l} is the value that derived from interaction between SU_i and SU_h in l times.

2. *The indirect trust value* The indirect trust value is similar to the direct ones, but the objects of interaction are not cluster heads, but the other $m - 2$ SUs in the same cluster sub-network.

$$\mathrm{IndTr}_{ij} = \frac{1}{n \cdot (m-2)} \sum_{k=1}^{m-2} \sum_{l=1}^{n} A(s, t_l) \cdot \mathrm{Attr}_{ik} \cdot \mathrm{DS}_{ik}^{l} \tag{6}$$

3. *The historical trust value* HistTr_i is determined by the final trust value of target user that accessed the cognitive network last time.

4. *The reward value* The reward value is used to encourage the honest users, and it is relevant to $\mathrm{Dev}(t)$, $\mathrm{Act}_i(t)$ and $A(s, t)$.

$$\mathrm{Rew}(t) = \varepsilon \cdot G\left(\frac{\mathrm{Act}_i(t) \cdot A(s, t)}{\mathrm{Dev}(t)}\right) \tag{7}$$

where $G(\cdot)$ is normalized function, ε presents the rewarded factor that restricts the value rang of the reward.

Based on the analysis above, we can define the user-related trust metric as follows:

User evaluation difference of trust It is defined to measure SUs trust value transformation in a period of time.

$$\mathrm{Dev}(t) = \mathrm{Var}(\mathrm{Tr}_i(t)) \tag{8}$$

where $\mathrm{Tr}_i(t)$ is the trust value of target user SU_i in t time slot.

Reliability evaluation of trust The reciprocal of trust evaluation deviation from other users to the target user is expressed as

$$\mathrm{Rel}(t) = \frac{1}{\mathrm{Var}(\mathrm{Tr}_{ij})} \tag{9}$$

where Tr_{ij} is the interaction trust value between the target user SU_i and cognitive user SU_j. The smaller the variance is, the higher the reliability of user trust is.

Activity metric of cognitive user

$$\mathrm{Act}_i(t) = \frac{\sum\limits_{j\in C} \mathrm{IndTr}_{ij}}{\sum\limits_{k,j\in C} \mathrm{IndTr}_{kj}} \tag{10}$$

which reflects the interaction degree of target user compared with other users in the same sub-network.

Trust value attenuation The degree of trust value attenuation with time is defined as

$$A(s,t) = \sigma \cdot \mathrm{round}(10 \cdot \nu \cdot e^{-st}) \tag{11}$$

where σ is the attenuation factor, ν is the initial trust value, t is scanning period, s is the rate of attenuation and $\mathrm{round}(\cdot)$ denotes the minimum integer large than $\cdot$.

2.3.4 Information interaction

Interaction relates to the trust value evaluation among cognitive users in the communication process to update the trust value. Interaction occurs between CHs and SUs and CHs and FC.

The evaluation trust value from user SU_i to user SU_j is

$$\begin{aligned}\mathrm{Tr}_{ij} =& \alpha \cdot \mathrm{DirTr}_{ij} + \beta \cdot \mathrm{IndTr}_{ij}\\ &+ \gamma \cdot \mathrm{HistTr}_i + \mathrm{Rew}\end{aligned} \tag{12}$$

where α, β, and γ are the normalized weight factor, corresponding to direct trust DirTr_{ij}, indirect trust IndTr_{ij} and historical trust HistTr_i value satisfying $\alpha+\beta+\gamma = 1$. Rew is the value of reward feedback.

The trust value will be reported to FC by CHs after information interaction. FC owns the rights to control SUs' access and resource allocation depending on the status of trust.

There will be a trust value lists matrix V, stored in the fusion center after FC gets the whole trust value of SUs in CWNs. Afterwards, FC provides service to SUs whose trust value exceeds than the access threshold ($\nu_{ij} \geq \lambda_i$).

2.3.5 Rewards and penalties

Rewards and penalties are for trustable and malicious users, and the scheme is performed by FC. We define reward's form as (7).

The coefficient is predefined as $\varepsilon = 0.1$ through the test. Considering the scope of value span, the reward value is limited below 0.5.

Penalty for misbehaving users refers to adjust the trust value. When an attack user or misbehaving user is detected by FC via the trust value analysis, the cognitive user's trust value is reduced so that the user is constrained to access the cognitive networks. The detailed illustration will be presented in Section 4.

2.3.6 Update

There are two update forms of trust value stored in FC:

- CHs report the updated trust value of cognitive users in its related sub-network to FC in period T_{report}.
- FC polls all cognitive users including the cluster heads periodically in T_{polling}.

In addition to the above trust value to update through the interactive mode, the trust value of SUs has the characteristics of self-damping and self-restoring. For example, the trust value is approaching to 0 with the time increasing regardless of the value greater than 0 or not in the case of no reward feedback.

3 Analysis of two-layer hierarchical architecture

Considering the scalability of the uploading process of all cognitive users, for the sake of decreasing the complexity and enhancing the management reliability, we take a two-level uploading scheme via introducing the cluster head. A cluster head is an advanced cognitive user who manages a certain number of cognitive users, which possesses the functions as manager of its sub-network cognitive users' trust value and reporting to FC. With the cluster head's assistance, cognitive users can be split into groups and interact with FC in a centralized manner, which brings high management efficiency. In this section, we use the particle swarm algorithm to select the cluster head from general cognitive users. Then the detailed interaction processes between the cluster head and cognitive users as well as the cluster head and the FC are designed, which guarantees the trust value update of the cognitive users.

3.1 Cluster head selection

In our scheme, the head has high-priority rights to utilize the spectrum. We choose the K cluster heads based on the following three principles [28]:

- The heads must have the highest trust value to fuse the transmitted information. We select the prior SUs according to the reliability.
- The heads are not so far away from the FC as the propagation loss will be larger with the distance expanding.
- The distance between two cluster heads should exceed a specific value.

Based on the three principles above, we apply the particle swarm algorithm to conduct the cluster head selection process. A detailed algorithm implementation flow is presented as follows:

Step 1 Initialize all the cognitive trust value memorizer and setting FC coverage radius R_f, the selected cluster head threshold ρ_f, and the allowed maximum number of cluster heads L.

Step 2 Cognitive users report their location (r, θ) and trust value v to FC.

Step 3 FC picks up the users whose trust value are larger than the threshold and records the total number as N.

Step 4 If $N > L$, FC should conduct extra selection criteria as follows:

- Cluster heads should be near the FC.
- Any two selected cluster heads should be far with each other enough.

Step 5 According to 4, L cognitive users are selected as the cluster heads and the trust value are stored as matrix V in the FC.

A proper CH selection algorithm makes a great difference to the network operation. A trustable and stable CH can distinguish the malicious users in its sub-network and perform relative punishment strategies. While an irresponsible CH could leave the malicious users to perform intrusion attack behavior and even malicious itself.

3.2 Trust value storage and interaction between FC and CH

3.2.1 *Trust value storage*

In a CH sub-network, cognitive users interact with the CH, thus producing a trust value for each user, judged by CH. The trust value can be described as a vector as $V_i = [v_{i1}\ v_{i2}\ \cdots\ v_{in}]$, where i represents the ith CH and n represents the total number of cognitive users inside the sub-network. CH reports this trust sector to the FC which forms a trust value matrix as

$$V = \begin{bmatrix} v_{11} & v_{22} & \cdots & v_{1k_1} \\ v_{21} & v_{22} & \cdots & v_{2k_2} \\ \vdots & \vdots & & \vdots \\ v_{\iota 1} & v_{\iota 2} & \cdots & v_{\iota k_t} \end{bmatrix} \tag{13}$$

where l is the number of CHs in the network, and $k_i\ (i = 1, 2, \ldots, l)$ is the number of cognitive users inside each CH sub-network. The trust value of call users can be stored in the FC in two forms:

Form 1 The number of users in each CH is different. The matrix V is a cell matrix: the number of elements in each row is distinct. FC should reserve a dynamic space to store the trust value matrix. This storage style could save the storage space, on condition that extra users' number configuration overhead is needed. Because the storage is simple, we set the trust value matrix row size as the same $\kappa = \max\{k_1, k_2, \ldots, k_t\}$. This forms a normal matrix by supplementing zero in the element scarce position.

Form 2 The maximum number of users in each CH is constrained by κ. A CH sub-network that contains users more than κ should split into two sub-network. Storage mode i.e., the matrix style, is the same as form 1.

3.2.2 *The trust value interaction between FC and CHs*

FC is in charge of the resource allocation to the sub-network. A malicious user would be prone to the trust evaluation of other normal cognitive users then causing severe resource utilization problems. This kind of users should be published by the FC by means of declining its trust value or avoiding frequent interaction with other users, for example. To implement the storage process, FC should interact with the CHs for the cognitive users trust value. We propose two approaches for the interaction behavior:

Approach 1 Cluster heads report the trust value vector to FC and the value is updated in the FC side.

Approach 2 FC conducts polling to all the cognitive users inside the network periodically and update the trust value matrix. Discovering an abnormal user would trigger a punishment implementing.

3.3 Interaction between CH and its associated cognitive users

CH should interact with cognitive users to obtain the trust value. For k users in a cluster sub-network, CH performs trust value estimation for each user which forms a vector as

$$\mathrm{Tr}C_i = \{\mathrm{Tr}_{i1}, \mathrm{Tr}_{i2}, \ldots, \mathrm{Tr}t_{ik}\}. \tag{14}$$

Frequent interaction requires more power loss and calculation source consumption of the CH users. Considering the trade-off between overhead and reward, CH users are allowed to access the primary network preferentially and obtain more spectrum bands. CH is not responsible for the punishment implementing, which is performed in FC, and CHs report the trust value status to FC periodically.

4 Punishment

The FC can not only store the trust value of each user, but also punish the illegal users in CRNs. In the criminal law, the arbiter will implement different punishments according to different criminal charges and give the criminals to start with a clean slate opportunity. Modeled on the social law, we proposed the punishment mechanism; the main form of penalty concludes the reduced rate and recovery degree of trust value, which represent the punishment and release degree, respectively. In order to analyze the punishment mechanism more effectively, the attackers are classified into three categories as follows:

Malicious users (MUs): This type of attackers sends false observations in order to confuse other users or the FC, causing extensive DoS (denial of service) attacks making a CRN hop from band to band, severely disrupting its operation. Furthermore, adversaries could also cause DoS attacks in PU networks by creating harmful interference, such as PUEA and SSDF. Malicious users are harmful to the cognitive radio networks. Thus, the punishment should be harsh and the form is that MUs should be punished quickly and released slowly.

Greedy users (GUs): These attackers continuously report that a specific spectrum hole is occupied by incumbent signals, which forces all other users to vacate the specific band (spectrum hole) in order to acquire its exclusive use. The goals of these attackers are to monopolize the specific band privately. Selfish attack is a typical example. Because the greedy users are not devastating, the greedy users should be both punished and released slowly.

Unintentionally misbehaving users (UMUs): This type of users reports faulty observations for spectrum availability, which is not from their subjective consciousness, but from the malfunction of their software or hardware. Because of unknown destructiveness, the unintentionally misbehaving users should be punished quickly and be also released quickly.

For different kinds of attackers, we punish them according to diverse punishment model as illustrated in the following:

Case 1: MUs This kind of attackers are highly destructive, e.g., PUEA and SSDF; thus, the punishment is the severest for these attackers. Firstly, once the malicious users are detected, the trust values of these users are reduced to below 0 and then they are forbidden to access the network in the next time slot. These users must increase their trust values to access the network again. The punishment function is defined as

$$\mathrm{Pena}_1(t) = -\sigma \cdot e^{-\xi t} + \zeta \tag{15}$$

where $\sigma \in (0, 2)$ is the penalty factor whose value is determined according to the trust value, (which follows the same rules in the following punishment model). $\xi > 0$ is the recovery factor, whose value is bigger when the trust value is bigger (which follows the same rules in the following punishment model). ζ is the regulate factor, which restricts the trust value in a reasonable range.

Case 2: GUs When greedy users are detected, the punishment should be lighter, because they are less destructive than the malicious users. The trust value should be decreased slowly and increased slowly too. This kind of punishment function should be

$$\mathrm{Pena}_2(t) = -\sigma \cdot e^{-\xi t^2} + \zeta \tag{16}$$

Case 3: UMUs This kind of attack is not intentional, and the trust value should be decreased quickly and be recovered quickly. Once the user's hardware is repaired, the user can access the network simultaneously. Thus, the punishment function should be

$$\mathrm{Pena}_3(t) = -\sigma \cdot [\, u(t) - u(t - T_{\mathrm{rep}})] + \zeta \tag{17}$$

where $u(\cdot)$ is the step function, and T_{rep} is the repair time.

Except for the punishment functions, there is a penalty period T_{penalty} that means the duration of punishment. For the unmeant attacking users, the punishment is fixed. But for the frequent attacking users, the punishment is cumulative, and the period for cumulative punishment can be described as

$$T_{\mathrm{accumupenalty}} = \sum_{i=1} \eta_i T_{\mathrm{penalty}}, i = \{1, 2, \dots\} \tag{18}$$

where η_i means the penalty factor.

On one hand, the extent of punishment is relevant to the type of attack; the greater the threat is, the more serious the punishment is. On the premise of security, the trust value can be directly reduced below the critical value 0. Because the trust mechanism we proposed is that the users' request is rejected while the trust value is below 0, the other users can be protected from an attack.

On the other hand, the penalty scheme should follow a habit of human society. The initial criminal punishment is light, and the cumulative crime will be punished heavily. It will not be forbidden to access the cognitive networks forever, unless the attack users are destructive.

Moreover, the punishment level for the cluster heads is much higher than the general cognitive user. It is a great threat to the networks, when the cluster head launches an attack, because the cluster head is highly reliable for FC. The punishment of CHs will not be introduced for lack of space, which involves the knowledge of the game theory.

5 The mechanism flow

When a new SU_i starts a network accessing session, as shown in Figure 2, it will query the networks in a round-robin way and interact with the FC. The network will get the access authentication and the authentication time and query the historical trust value HistTr_i. If the trust value is smaller than 0, then this user is forbidden to access the network and wait for a time T before starting another network accessing session. If it is the first time for this user to access the network or the historical trust value $\mathrm{HistTr}_i \geq 0$, then the FC would allow this user to access the network. Then FC analyzes the value of cluster C_i and allocate the user in the corresponding sub-cluster network according to the value of C_i. The classifications include the following three situations:

- When C_i has a history value, then the user can be allocated to the corresponding sub-cluster network instantly.

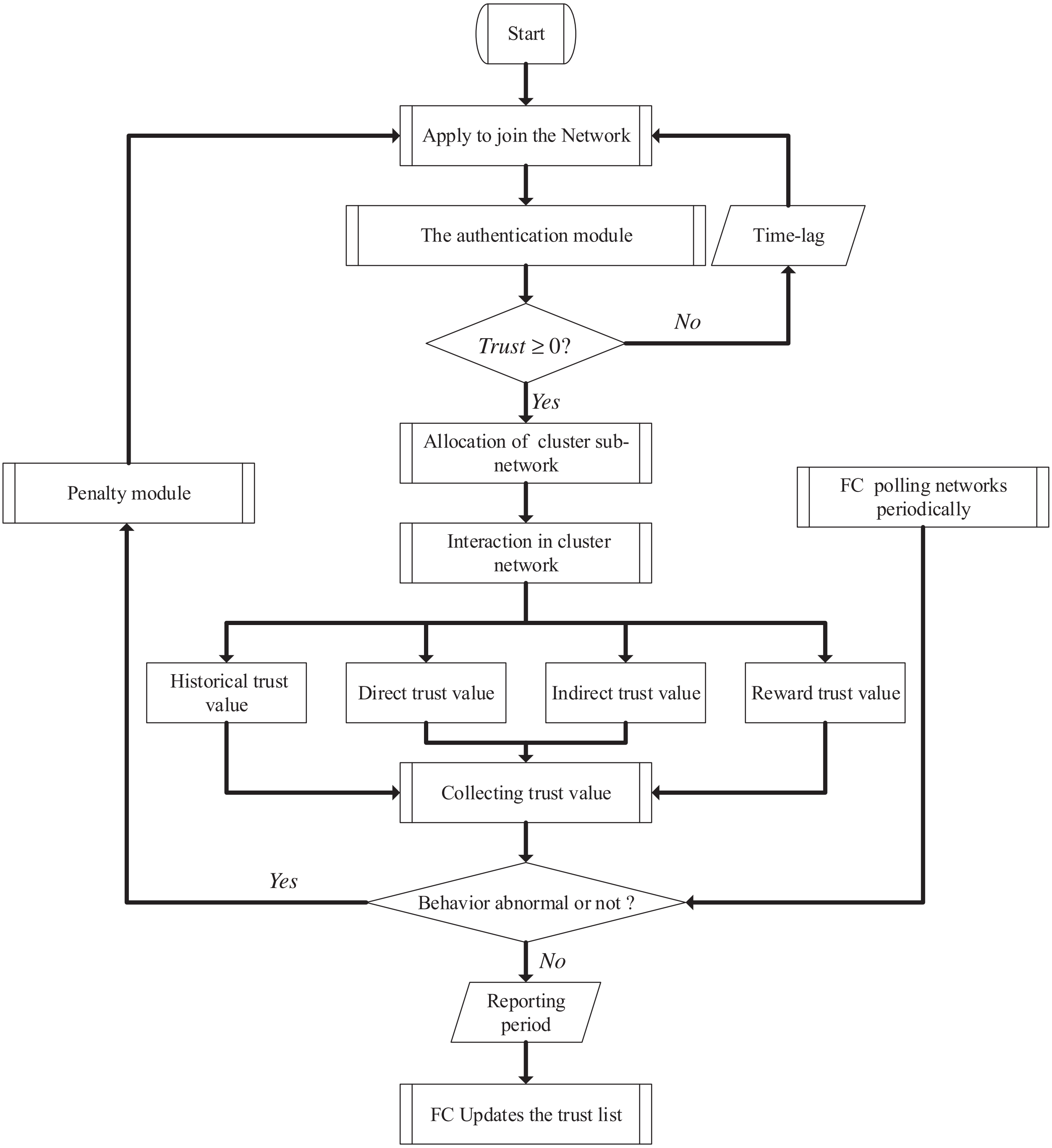
Start
Apply to join the Network
The authentication module
Time-lag
Trust ≥ 0?
No
Yes
Allocation of cluster sub-network
Penalty module
FC polling networks periodically
Interaction in cluster network
Historical trust value
Direct trust value
Indirect trust value
Reward trust value
Collecting trust value
Yes
Behavior abnormal or not ?
No
Reporting period
FC Updates the trust list

Figure 2 The flow graph of scheme.

- When C_i has a history value, but the corresponding sub-cluster network is overloading, the user should access the other nearer sub-cluster according to the geographic information.
- When C_i is empty, the user should access the nearest sub-cluster according to the geographic information.

Within the permission of authorization, the cognitive users in the cluster networks will share the trust values with the cluster header.

Denote the set of clusters as $S = \{S^1, S^2, \ldots, S^\iota\}$. The set of cognitive user cluster that has resource R_i is $S^i_{R_i}$, where $S^i_{R_i} \subset S, R_i \in \{R_1, R_2, \ldots, R_n\}$. The trust value information is in set S_{R_i}, containing direct trust value, indirect trust value, historical trust value, and rewarding trust value.

5.1 Direct trust value

Assume the number of cognitive users in $S^i_{R_i}$ is m. When a new cognitive user SU_i wants to access the network, the network firstly checks the direct interaction experience between user SU_i and the cluster header SU_h as follows:

$$\mathrm{DirTr}_{ih} = \{\mathrm{DirTr}^1_{ih}, \mathrm{DirTr}^2_{ih} \ldots \mathrm{DirTr}^n_{ih}\} \tag{19}$$

where n is the number of direct interactions.

5.2 Indirect trust value

Indirect trust value is got from the interactions between the cognitive user SU_i and other user SU_j. There are at most $m-2$ (except of SU_i and the cluster header U_h) users that can interact with SU_i. Then SU_j produces the indirect trust value sequence on SU_i as follows:

$$\mathrm{IndTr}_{ij} = \{\mathrm{IndTr}_{i1}, \mathrm{IndTr}_{i2}, \ldots, \mathrm{IndTr}_{i(m-1)}\} \tag{20}$$

and

$$\mathrm{IndTr}_{ik} = \{\mathrm{IndTr}^1_{ik}, \mathrm{IndTr}^2_{ik}, \ldots, \mathrm{IndTr}^l_{ik}\} \tag{21}$$

where $k \in \{1, 2, \ldots, m-2\}$, $k \neq h$, $k \neq i$, and l is the number of interaction. If there is no interaction occurring between user k and i, then $\mathrm{IndTr}_{ik} = 0$.

5.3 History trust value

The cognitive users that once have accessed the network but have left the network or their trust value license has expired will record the trust value $\mathrm{Hist}T_i$ during the observation period among the user, cluster header, and FC, which is a deterministic value but not a vector.

5.4 Rewarding trust value

The rewarding trust value of cognitive user at time t can be obtained as $\mathrm{Rew}d_i(t)$ according to formula (7).

The overall trust value can be obtained by substituting the four kinds of trust values into formula (12). While cluster heads collect all cognitive users' trust values, they will report the generated values to FC. Then, the FC will make a response according to the trust value, which determines the network access permission of secondary networks, and allocates the network resource and services level by the value of λ_i. If there are criminal users, the punishment threshold will be activated. Simultaneously, FC queries the network in the period of T_{polling} and punishes or rewards the users according to their trust values. Finally, the FC updates the trust value matrix. In Figure 3, it illustrates the demonstration process of trust value interaction.

6 Complexity analysis

We proposed a dual-layer hierarchical architecture that adds cluster heads as the trust agents and is different from the general centralized management. Its main significance is to reduce the amount of calculation and to protect the security and reliability of the network environment.

6.1 The analysis of complexity from computational aspect

A centralized control scheme is presented in [16,17], which needs setting a cognitive user as the target user to compare with others, then FC adjudges whether the user is abnormal by iteration. This scheme will bring FC huge amount of computation as $\binom{N}{2}$ because direct and indirect information interactions have occurred in any of the two or more users. In order to reduce these costs of communication, a dual-layer hierarchical architecture was proposed. Adding cluster heads between FC and SUs, the trust value of comparison of SUs will be accomplished in the cluster heads, and then the results will be reported to FC by CHs. A plurality of cluster parallel computing brings the complexity decrease to $\binom{\frac{N}{K}}{2}$ and greatly improves the efficiency of information interaction among the cognitive users.

6.2 The analysis of complexity from security

To control access complexity, the trust mechanism adds the function of querying historical trust values. A white list and trustable resource lists are defined, which can assist FC to make a decision quickly. The historical trust values, stored in the list, are the last value of trust evaluation by the last accessed network, and this value can be used as reference values of trust in the next access to the networks. When the cognitive users apply for accessing to the cognitive network, FC can query the history of user trust and make rapid certification decision. Therefore, it reduces the decision cycle.

7 Numerical and simulation results

In this section, we present the numerical results for the proposed mechanism. The main parameters used for the simulations are $L = 10$, $K = 50$, $\lambda = \{1.2, 1.5, 1.8\}$, R_f =1,500 ms and the simulations are conducted in MATLAB R2012b environment. The main simulation objects are variation rule of trust value, attenuation characteristics of trust value, cluster head selection scheme, penalty scheme, complexity analysis, and so on.

7.1 The general rule of trust value

The trust values consist of four kinds of trust values as shown in formula (12). We present the variation rule of honest users without attacking and misbehavior, in Figure 4, in which Y-axis is the trust level that range

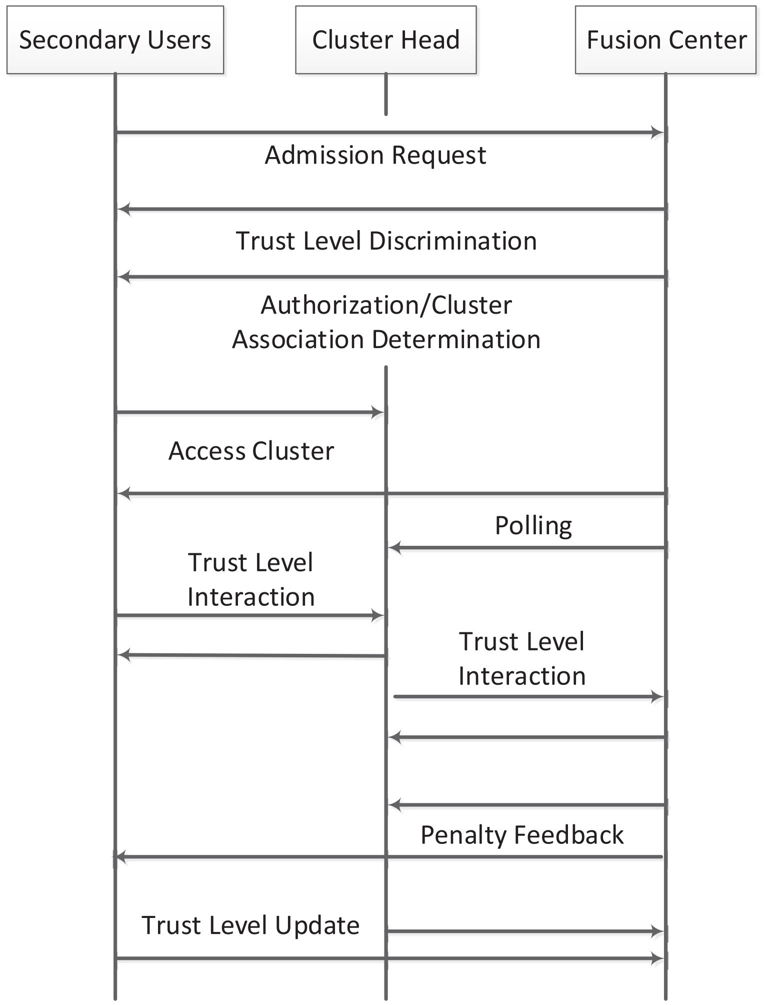

Figure 3 The graph of trust interaction.

from −2 to 2 described in Subsection 2.3.2, and X-axis is the interaction time. The normalized weight factors are set as $\alpha = 0.85$, $\beta = 0.1$, and $\gamma = 0.05$ produced a sequence of direct trust value that increases gradually and tends to be stable. Then, we substitute them into the formula (12). For the initial historical trust value which is equal to the existing value in the last time, the historical trust value is set as 0 for simplicity. In case of complexity, we do not consider the attenuation of trust value. From Figure 4, we can see that the trust value of an honest user is increasing with time that complies with the rule of the network arising constantly and gradually closing to the highest value of 2.

7.2 Attenuation

In Subsection 2.3.3, the definition and calculation formula of attenuation function are described in the formulas (5) and (11), respectively, which express that the trust value tends to approach the minimum access threshold along with the time development. We set the attenuation factor $\sigma = 0.1$ and calculate the theoretical attenuation results to get the expected real value through discretization processing, as shown in Figure 5. The curves that describe the general rule of attenuation that the trust values, even if above or below 0, are regressing to the minimum access threshold when time increases gradually.

7.3 The selection of cluster heads

We assume that 100 cognitive users are uniformly random-distributed in the coverage area of FC and their trust value is $\nu \in (-2, 2)$. The selective threshold of the cluster heads is $\rho_r = 1.5$, through calculation of algorithm that we proposed in Subsection 3.1. As shown in Figure 6, five cluster heads are selected from all the candidate cognitive users, which are marked by black pentacle. The cluster heads' sub-network coverage may be overlapped, and the trust value of the overlapped users will be reported by the respective regnant CHs. In other words,

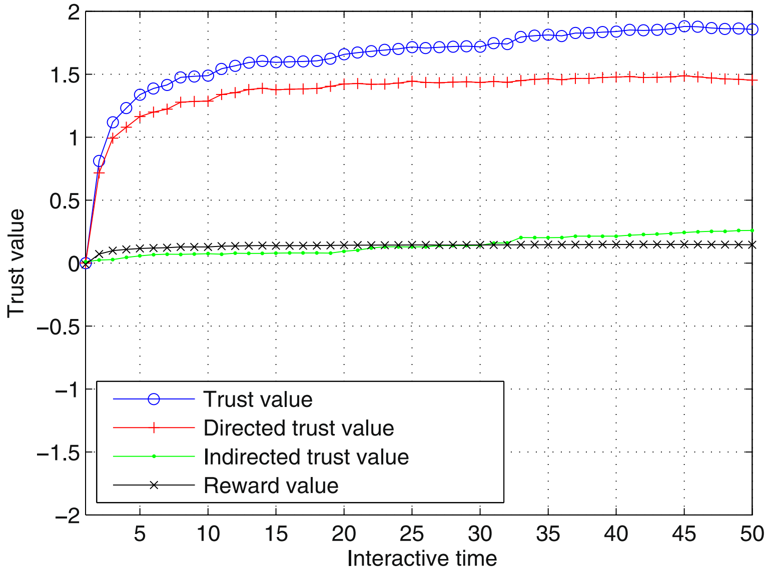

Figure 4 The variation of an honest user's trust values.

the trust value of a cognitive user will be reported to FC by two or more than two CHs.

7.4 The penalty scheme

In Section 4, we have introduced three different types of attacks and corresponding punishments. Figure 7 describes the changed curves of trust value under three kinds of attack users. The trust values of users are equal to each other at the beginning. Once the user launches an attack, its trust value will change. The malicious users are severely punished due to their destruction to the network. Therefore, they are applicable to case 1, and their trust values decrease immediately to below −1. However, the trust value gradually restored is aimed to re-access network after a penalty period, which is in consonance with the attenuation, and the recovery of trust value is a slow process. For greedy users, which are applicable to case 2, punishment is to reduce the user-assigned resources through regulating the trust value continually until the trust value is reduced to less than 0 and is no longer allowed to access the network. The recovery of greedy users is similar to the malicious user. The unintentionally misbehaving users are

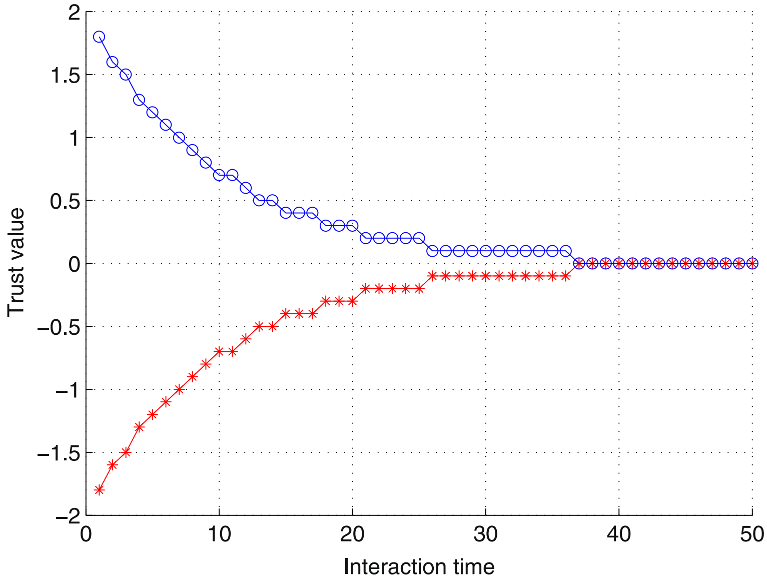

Figure 5 The attenuation trend graph.

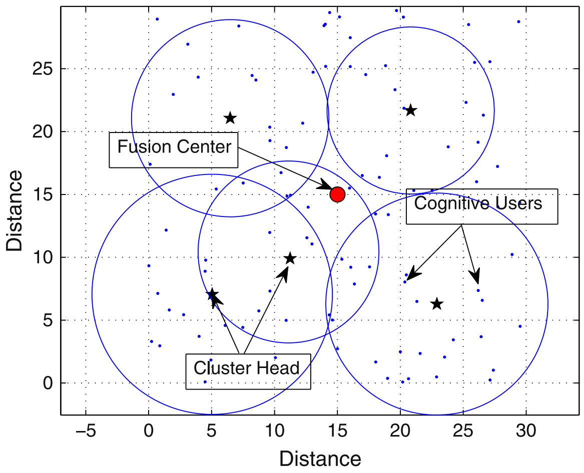

Figure 6 Cluster heads selection.

applicable to case 3, and their trust values will be reduced less than 0 immediately once they have launched attack. However, once the users are repaired, their trust value will be restored to the former value.

Figure 8 describes that the recovery period of trust values under the three kinds of frequent attack. From the graph, it shows that the reinstated trust value is slightly lower than the value before punishment. Through this penalty scheme to achieve constraint for attackers, the users will be prohibited from accessing network if they attacked consistently.

We also analyze the cumulative punishment scheme for frequent attack in formula (18). From Figure 9, it can be seen that the penalty time is increasing along with the increasing number of attacks, accompanied by the trust value decreases gradually at the same time. The cumulative punishment scheme mainly imposes the tough penalties for users who are repeating offenders, which is more serious than the simple punishment.

7.5 The successful transmission rate

Figure 10 simulates the changing rules of user's successful transmission rate in various attacks. We fully consider penalty scheme, reward scheme from FC, and the trust values attenuation of cognitive users, etc. We assume that all the users' initial successful transmission rates are 0.9. While there are no attackers, the successful transmission rate of honest cognitive users rises steadily with the interactional time increasing, and gradually approach to 1 that conformed to the reward scheme.

Reversely, the successful transmission rate is dropping gradually when attacks occur, because FC dominates all users and has the punitive power of misbehavior to reduce the trust value in order to achieve the purpose of prohibiting access to the cognitive networks. Among all the attackers, the first class is UMUs. This type of attack is easy to be detected and has no malicious subjective attacks to the network. Therefore, FC has high tolerance for this attack and the corresponding penalty level is lower, so the curve of successful transmission rate appears to be jumping with decreasing tendency. The second class of attacker is GUs that easily destruct the network which results in uneven distributions of resource. Therefore, FC

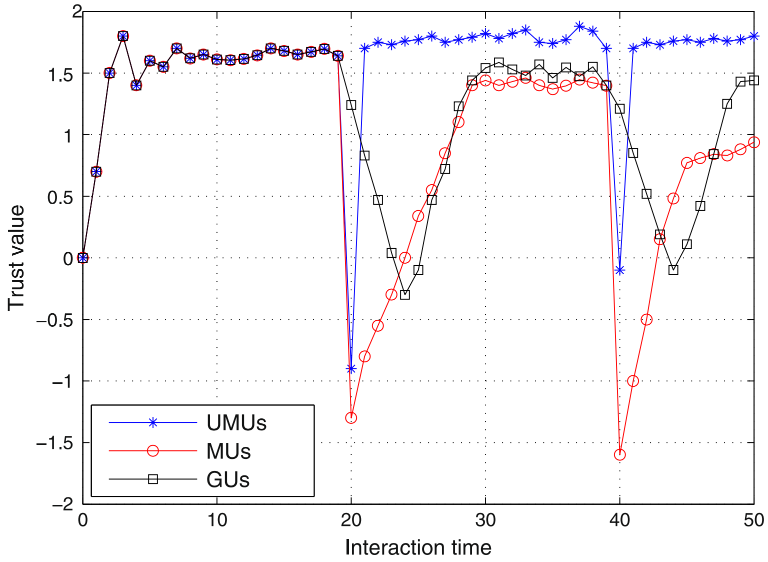

Figure 7 The change of trust value under the three kinds of attack.

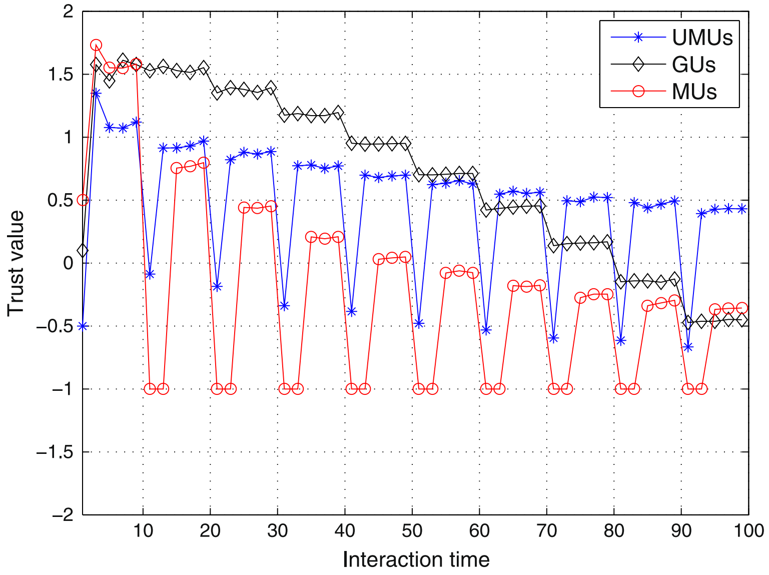

Figure 8 The period gram of punishment, the penalty accumulation factor $\eta = 0$ the recovery cycle diagram of trust value.

has heavier penalty involved in this type of attack. Due to existing punishment period and reduced trust values, the punishment effect is obvious and successful transmission rate declines more greatly. The third class is MUs includes SSDF and PUEA. The penalty is the most severe under this type of attack, and the attackers will be punished quickly once detected. Consequently, the curve graphs of successful transmission rate are declining sharply. The detection probability of PUEA is larger than SSDF under centralized control [4]; thus, the PUEA can be detected by FC easily and their transmission rate falls faster than SSDF. Simulation results show that successful transmission rate of honest users are safeguarded effectively, under the security management based on trust value mechanism, whereas misbehaving users are shielded in part or entirely, and also validate a better anti-attack ability than the mechanism has.

7.6 Complexity analysis

Network burden is an essential performance evaluation index to measure the proposed mechanism, and we define it as the complexity of user management. The parameters

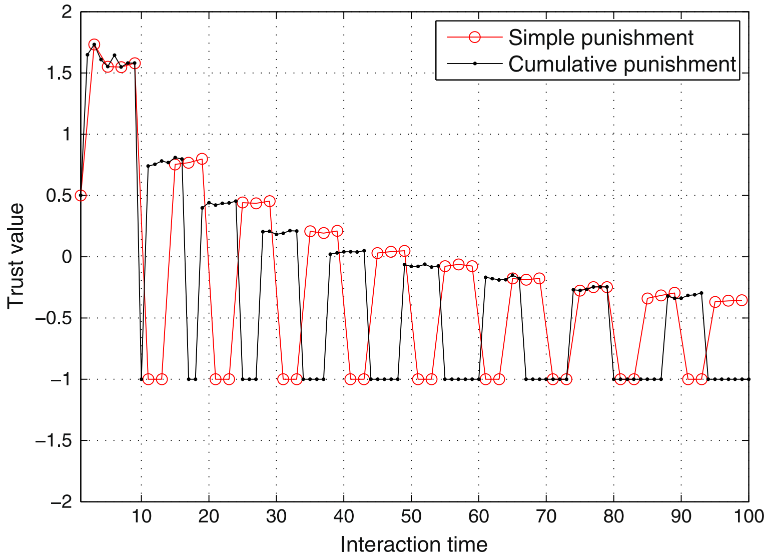

Figure 9 Contrast gram of punishment taking malicious users, for instance, the penalty accumulation factor $\eta = 0$ and $\eta = 1$.

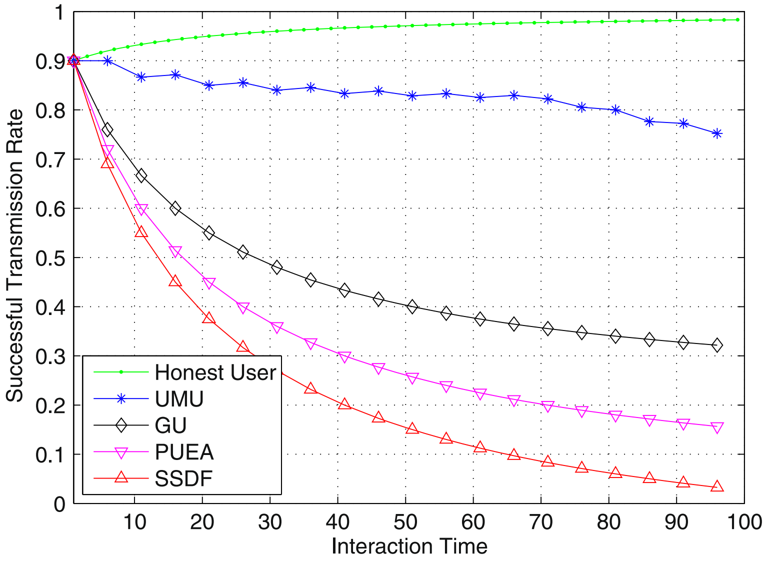

Figure 10 The successful transmission rate of different cognitive users.

of the network scale are the number of cognitive users $N = 100$ and the number of cluster heads $L = \{2 \quad 5 \quad 10\}$. Comparing with the single-stage centralized control mechanism (SSCCM for short) in [17] and from the analysis in Section 6, we get the relation of the network burden versus the number of users as shown in Figure 11. It can be seen that the network burden of our proposed mechanism is relatively larger than SSCCM when the network scale is small, because the proposed mechanism has extra burden for added trust authentication function, cluster heads selection function, penalty function, and so on. However, with the increasing network scale, our proposed mechanism shows a better performance than SSCCM.

7.7 Simulation summary

The rationality and effectiveness of the mechanism proposed in this paper through the above simulation have been verified. The advantages of the mechanism compared with others are mainly embodied as follows:

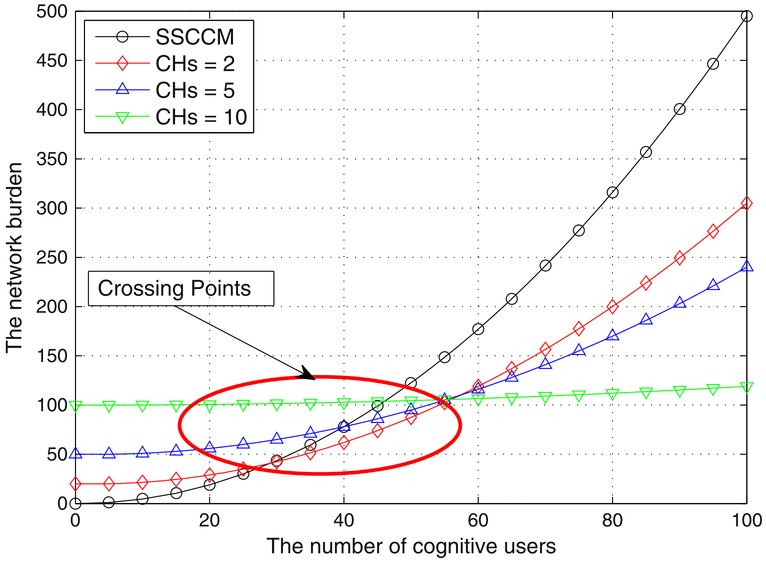

Figure 11 The relationship between the network load and user scale.

- Trust model which accords with the basic characteristic of human society
- According to the different types of attacks to implement different punishment
- The FC + CH hierarchical architecture effectively reduces the network management complexity.

8 Conclusion

In this paper, we have discussed the challenges in defending attacks in cognitive wireless networks. In addition, we have found that a mass of studies focus on the attacker detection, but precious few relevant literatures are studied how to address those attackers while they were detected. Therefore, we proposed a novel management mechanism SMTD, which is based on trust and penalty, to deal with security problems in CRNs. The proposed mechanism has been verified that is has obvious superiority compared with other mechanisms and it accords with requirements for deployment in the actual environment. The next researches are to optimize the punishment mechanism model and how to realize the more effective punishment, optimize the cognitive radio network, and find the Nash Equilibrium between cluster heads and network scale.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61227801, 61121001, 61201152), the Program for New Century Excellent Talents in University (NCET-01-0259) and the Fundamental Research Funds for the Central Universities (2013RC0106).

Received: 30 November 2013 Accepted: 25 March 2014
Published: 7 April 2014

References

1. Spectrum Efficiency Working Group, Spectrum policy task force report, Federal Communications Commission. http://www.fcc.gov/sptf/files/SEWGFinalReport_1.pdf (2002)
2. P Zhang, In the development of wireless cognitive science. Chin. Sci. Bull. **57**, 3661–3661 (2012)
3. R Chen, JM Park, J Reed, Defense against primary user emulation attacks in cognitive radio networks. IEEE J. Selected Areas Commun. **26**, 25–37 (2008)
4. AG Fragkiadakis, EZ Tragos, IG Askoxylakis, A survey on security threats and detection techniques in cognitive radio networks. IEEE Commun. Surv. Tutorials. **15**, 428–445 (2013)
5. Z Jin, KP Subbalakshmi, Detecting primary user emulation attacks in dynamic spectrum access networks. Proc. ICC, 1–5 (2009)
6. Y Tan, S Sengupta, KP Subbalakshmi, Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach. IET Commun. **6**, 964–973 (2012)
7. Y Tan, S Sengupta, KP Subbalakshmi, Analysis of coordinated denial-of-service attacks in IEEE 802.22 networks. IEEE J. Selected Areas Commun. **29**, 890–902 (2011)
8. S Sengupta, KP Subbalakshmi, Open research issues in multi-hop cognitive radio networks. IEEE Commun. Mag. **51**, 168–176 (2013)
9. R Chen, JM Park, T Hou, J Reed, Toward secure distributed spectrum sensing in cognitive radio networks. IEEE Commun. Mag. **46**, 50–55 (2008)
10. F Zhu, S Seo, Enhanced robust cooperative spectrum sensing in cognitive radio. J. Commun. Netw. **11**, 122–133 (2009)
11. F Yu, M Huang, Z Li, P Mason, Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios. Proc. Milcom, 1–7 (2009)
12. Q Wu, G Ding, J Wang, Y Yao, Spatial-temporal opportunity detection for spectrum-heterogeneous cognitive radio networks: two-dimensional sensing. IEEE Trans. Wireless Commun. **12**, 516–526 (2013)
13. J Wang, J Yao, Q Wu, Stealthy-attacker detection with a multidimensional feature vector for collaborative spectrum sensing. IEEE Trans. Vehicular Technol. **62**, 3996–4009 (2013)
14. G Ding, Q Wu, Y Yao, J Wang, Y Chen, Kernel-based learning for statistical signal processing in cognitive radio networks. IEEE Signal Process. Mag. **30**, 126–136 (2013)
15. J Zhang, V Varadharajan, A new security scheme for wireless sensor networks. IEEE Globecom 2008, 1–5 (2008)
16. H Sakran, M Shokair, O Nasr, S El-Rabaie, AA El-Azm, Proposed relay selection scheme for physical layer security in cognitive radio networks. IET Commun. **6**, 2676–2687 (2012)
17. C Chen, M Song, C Xin, J Backens, A game-theoretical anti-jamming scheme for cognitive radio networks. IEEE Netw. **27**, 22–27 (2013)
18. M Jo, L Han, D Kim, HP In, Selfish attack and detection in cognitive radio ad-hoc networks. IEEE Netw. **27**, 46–50 (2013)
19. G Ding, J Wang, Q Wu, F Song, Y Chen, Spectrum sensing in opportunity-heterogeneous cognitive sensor networks: how to cooperate? IEEE Sensors J. **13**, 4247–4255 (2013)
20. Z Gao, H Zhu, S Li, S Du, Security and privacy of collaborative spectrum sensing in cognitive radio networks. IEEE Wireless Commun. **19**, 106–112 (2012)
21. RD Pietro, G Oligeri, Jamming mitigation in cognitive radio networks. IEEE Netw. **27**, 10–15 (2013)
22. J Wang, B Sun, X Niu, Y Yang, Distributed trust model based on parameter modeling. J. Commun. **34**, 1–13 (2013)
23. Z Shi, J Liu, Z Wang, Dynamic P2P trust model based on time-window feedback mechanism. J. Commun. **31**, 120–129 (2010)
24. L Duan, AW Min, J Huang, KG Shin, Attack prevention for collaborative spectrum sensing in cognitive radio networks. IEEE J. Selected Areas Commun. **30**, 1658–1665 (2012)
25. X He, H Dai, P Ning, A Byzantine attack defender in cognitive radio networks: the conditional frequency check. IEEE Trans. Wireless Commun. **12**, 1658–1665 (2013)
26. L Gu, S Zheng, Y Yang, *Modern Cryptography*, (Beijing University of Posts and Telecommunications press, 2009). http://www.buptpress.com/product/book_content.jsp?pid=4136&cid=1&pstate=5.
27. Z Wei, Z Feng, Q Zhang, W Li, Three regions for space-time spectrum sensing and access in cognitive radio networks. IEEE Globecom 2012, 1283–1288 (2012)
28. S Liu, I Ahmad, Y Bai, Z Feng, Q Zhang, Y Zhang, A novel cooperative sensing based on spatial distance and reliability clustering scheme in cognitive radio system. VTC Fall 2013, 1–5 (2013)

doi:10.1186/1687-6180-2014-48
Cite this article as: Li *et al.*: **Security management based on trust determination in cognitive radio networks.** *EURASIP Journal on Advances in Signal Processing* 2014 **2014**:48.