Trusted cognitive radio networking

Kwang-Cheng Chen1*, Peng-Yu Chen2, Neeli Prasad2, Ying-Chang Liang3 and Sumei Sun3

1 Institute of Communications Engineering and Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan, ROC
2 Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark
3 Institute for Infocom Research, A-STAR, Singapore

Summary

Networking cognitive radios and nodes from primary system (PS) results in a heterogeneous coexisting multi-radio wireless network, so that significant network throughput gain can be achieved. However, by investigating cognitive radio network (CRN) architecture, the links in CRNs are unlikely to support complete security check due to link dynamics, opportunistic availability, and uni-directional in available time window. We therefore introduce trusted cognitive radio networking (TCRN) concept to facilitate network functions such as association in dynamic spectrum access and routing. First of all, we explore the mathematical framework for trust in CRNs. We then show successful association of node to CRN based on the mathematical structure of trust from statistical decision theory. Furthermore, we modify the machine-learning algorithm to update the trust measure for each node, and develop rules of thumbs to facilitate TCRN with learning capability, based on numerical simulations. Trusted CRN can greatly alleviate heterogeneous challenge for CRN operation. Copyright © 2009 John Wiley & Sons, Ltd.

KEY WORDS: cognitive radio; cognitive radio networks; trust; trusted networking; cognitive radio network architecture; statistical decision

1. Introduction

The concept of cognitive radio (CR) was pioneered by J. Mitola, III, and has been widely discussed in literatures [1–3]. Its fundamental idea is that radio communications are possible by using the spectrum holes of primary system(s) at a given frequency band. However, after such a radio link construction to transport packets from one transmitter to another receiver, methodology to transport these packets to destination through appropriate routing protocols and networking functions to meet quality of services remains a wide-open research area, where we call such scenario as cognitive radio networking to form a cognitive radio network (CRN) by considering nodes of both primary system(s) and cognitive radios. It is obvious that CRN is a dynamically and stochastically organized network with both ad hoc networking and heterogeneous networking features, except much more dynamics in CRN topology and link availability to make static security and traditional networking functions infeasible.
1.1. The Need of Trust in Cognitive Radio Networks

It is obvious that CRN is a temporarily organized network with both *ad hoc* networking and heterogeneous networking features, except much more dynamics in CRN topology and link availability to make static security and traditional networking functions infeasible. CRN surely can be considered through 7-layer OSI model like all wireless networks and Internet applications. From the chapters regarding network layer functions, trust plays one of the key parameters in facilitation of CRN, due to its role to glue the nature of heterogeneous (wireless) networks in CRN.

There are two important steps that need trust in CRN operations: association that makes dynamic spectrum access realistic, and routing, as the major focusing issues hereafter. When a CR initially tries to connect a node to join an existing (cognitive radio) network or to form a CRN, it is practically not possible to execute conventional security functions, as

- Such an action may create security holes.
- It is not wise to consume huge computation power for security without making sure it is a valid request to form CRN.
- There is not enough available time for opportunistic CRN link to exist, for a complicated hand-shaking security protocol.

Trusted mechanism is therefore needed, while authentication is a part of trust along with other technical or non-technical factors. The next challenge happens when a node in CRN routes the traffic through another node or some part of another network. Typical *ad hoc* networks and sensor networks using *public key infrastructure* (PKI) scheme achieve secure routing and other purposes in literatures [4–9]. Such a CRN node under the request of routing packet(s) may not be able to execute security like typical PKI scheme in *ad hoc* networks or sensor networks, due to not practical to perform checking under limited communication and computation resources and due to increasing possibility of being attacked. Consequently, trusted networking and update of trust measure can be very useful to reach a compromise facing these technical challenges. Once a node passing trust evaluation that must be quick and somewhat reliable, it can function as a node in CRN to transport/relay packets, though other security and service mechanisms are still executing at later appropriate timings, which acts as the fundamental spirit behind the CRN network functions by treating trusted cognitive radio networking (TCRN) as allowing quick execution of network functions in such heterogeneous wireless networking environment without completing entire secure encryption procedure. Nodes in CRN with the same level of trust can therefore operate similar to *ad hoc* networks, except opportunistic available links and likely uni-directional links as given in Section 2 and Reference [10].

1.2. Organization of the Paper

The rest of this paper is organized as follows. Section 2 describes the CRN architecture and the links in CRN. Section 3 explores the framework of trust in CRN. We explain the operation of trusted association and trusted routing in Section 4. Update of trust based on machine learning is introduced in Section 5. Section 6 concludes this paper.

2. CRN Architecture

It has been widely recognized that the cognitive radio can efficiently improve spectrum utilization at link level. We also demonstrate that cooperative relay among CRs and nodes in PS can greatly enhance the network capacity by constructing a general sense CRN [11]. It suggests that a cognitive radio shall sense available networks and communication systems around it, to complete networking functions beyond utilizing spectrum hole at link level. Thus, the CRNs are not just another network with interconnecting cognitive radios. The CRNs are composed of various kinds of co-existing multi-radio communication systems, including cognitive radio systems. CRNs can be viewed as some sort of heterogeneous networks composed of various communication systems. The heterogeneity exists in wireless access technologies, networks, user terminals, applications, service providers and so on. The design of cognitive radio network architecture is toward the objective of improving network utilization. From the users’ perspective, the network utilization means that they can always fulfill their demands anytime and anywhere through accessing CRNs. From the operators’ perspective, they cannot only provide better services to mobile users, but also allocate radio and network resources in a more efficient way.

2.1. CRN Structure

Following the efforts in References [12–14] and above discussions, we may conclude that CRN is a sort of
cooperative (relay) networking and heterogeneous networking. Although CRN can be generally considered as a multi-hop wireless network, CRN, heterogeneous in nature, is fundamentally different from a homogeneous wireless ad hoc network. CRN can be deployed in network-centric, distributed, ad hoc and mesh architectures, and serve the needs of both licensed and unlicensed applications. The basic components of CRNs are mobile station (MS), base station/access point (BSs/APs) and backbone/core networks. These three basic components compose three kinds of network architectures in the CRNs: infrastructure, ad hoc and mesh architectures, which are introduced as follows.

2.1.1. Infrastructure architecture

In the infrastructure architecture (Figure 1), an MS can only access a BS/AP in the one-hop manner. MSs under the transmission range of the same BS/AP shall communicate with each other through the BS/AP. Communications between different cells are routed through backbone/core networks. The BS/AP may be able to run one or multiple communication standards/protocols to fulfill different demands from MSs. A cognitive radio terminal can also access various kinds of communication systems through their BS/AP.

2.1.2. Ad hoc architecture

There is no infrastructure support in ad hoc architecture (Figure 2). The network is set up on the fly. If an MS recognizes that there are some other MS nearby and are connectable through certain communication standards/protocols, they can set up a link and thus form an ad hoc network. Note that this links between nodes may be set up by different communication technology. In addition, two cognitive radio terminals can either communicate with each other by using existing communication protocols (e.g., WiFi, Bluetooth) or dynamically using spectrum holes.

2.1.3. Mesh architecture

This architecture (Figure 3) is a combination of infrastructure and ad hoc architectures plus enabling the wireless connections between BSs/APs. This network architecture is similar to the Hybrid Wireless Mesh Networks. In this architecture, BSs/APs work as wireless routers and form wireless backbones. MSs can either access the BSs/APs directly or use other MSs as multi-hop relay nodes. Some BSs/APs may connect to the wired backbone/core networks and function as gateways. Since BSs/APs can be deployed without necessarily connecting to wired backbone/core networks, it is more flexible and less cost in planning the locations of BSs/APs. If the BSs/APs have cognitive radio capabilities, they may use spectrum holes to communicate with each other. Due to the inefficiency of current spectrum utilization, there may be lots of spectrum holes detected. So the capacity of wireless communication links between cognitive radio BSs/APs may be large and it makes the wireless backbone feasible to serve more traffic.

2.2. Links in CRN

We may recall two kinds of wireless communication systems in CRNs: Primary System (PS) and Cognitive Radio (CR) System, which are classified by their priorities on frequency bands. A PS is referred as an existing system which operates in one or many fixed frequency
bands. Various kinds of primary systems work either in licensed or unlicensed bands, either in the same geographical location or in the same frequency band (or the same set of frequency bands) and are described as follows:

- **Primary system in licensed bands**: A primary system operated in the licensed band has the highest priority to use that frequency band (e.g., 2G/3G cellular, digital TV broadcast). Other unlicensed users/systems can neither interfere with the primary system in an intolerable way nor occupy the license band.

- **Primary system in unlicensed bands**: A primary system operating in the unlicensed band (e.g., ISM band) called unlicensed band primary system. Various primary systems should use the band compatibly. Specifically, primary systems operating in the same unlicensed band shall coexist with each other while considering that the interference to each other. These primary systems may have different levels of priorities which may depend on some regulations.

A cognitive radio system does not have privilege to access certain frequency band. Entities of CR system must communicate with each other by dynamically using spectrum holes and opportunistic access. There are two components in CR systems: cognitive radio base station (CR-BS) and cognitive radio mobile station (CR-MS).

- **Cognitive radio base station (CR-BS)**: A CR-BS is a fixed component in the cognitive radio system and has cognitive radio capabilities. It represents the infrastructure side of the CR system and provides supports (e.g., spectrum holes management, mobility management, security management) to CR-MSs. It provides a gateway for CR-MSs to access the backbone networks (e.g., Internet). CR-BSs can also form a mesh wireless backbone network by enabling wireless communications between them, and some of them act as gateway routers if they are connected with wired backbone networks. If a CR-BS can run PR system protocols, it can provide access network services to PR-MSs.

- **Cognitive radio mobile station (CR-MS)**: A CR-MS is a portable device with cognitive radio capabilities. It can reconfigure itself in order to connect to different communication systems. It can sense spectrum holes and dynamically use them to communicate with CR-MS or CR-BS.

### Table I. Summary of Links in CRN.

<table>
<thead>
<tr>
<th>Rx \ Tx</th>
<th>CR-MS</th>
<th>CR-BS</th>
<th>PR MS</th>
<th>PR-BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR-MS</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>CR-BS</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>PR-MS</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>PR-BS</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

*Possible link.

![Fig. 4. Links in CRNs.](image)

Since the cognitive radio system can provide interoperability among different communication systems, some inter-system connections should be enabled. We list all possibilities in Table I and illustrate them in Figure 4.

(i) **CR-MS ←→ CR-MS**: A CR-MS can communicate with other CR-MSs in direct links. They may cooperatively sense spectrum holes at different frequency bands which may be licensed or unlicensed and utilize it as their operating frequency band.

(ii) **CR-MS ←→ CR-BS**: A CR-BS can dynamically sense available frequency band around it and gather other MSs’ sensing results and provide one-hop access to CR-MSs under its coverage area. This may need cooperative sensing technique. Under the coordination of CR-BS, the CR-MS can either access the backbone networks or communicate with other communication systems.

(iii) **CR-MS ←→ PR-BS**: If there is a need for a CR-MS to connect to a PR-BS, it will reconfigure itself and become one part of the primary system (i.e., PR-MS). In this case, it can be treated as a primary user on that band.

(iv) **CR-BS ←→ CR-BS**: While enabling direct wireless links between CR-BSs, they can form a mesh wireless backbone network. Because of their cognitive radio capability, they can dynamically
choose operating frequency band and communicate with each other and may reduce deployment cost.

(v) PS-MS $\leftrightarrow$ PS-BS: It is the typical one-hop connection between mobile stations and base stations. The PR-BS is responsible for coordinating communications in its coverage and providing backbone network access to the PR-MS. This link is bi-directional all the time, which is fundamentally different from other links.

(vi) PS-MS $\leftrightarrow$ CR-MS: In order to provide interoperability between different communication systems, this kind of link may be necessary. In this case, the CR-MS shall reconfigure itself to be one part of the primary system.

(vii) PS-MS $\leftrightarrow$ CR-BS: In order to provide interoperability between different communication systems, this kind of link may be necessary. If the CR-BS can run the protocol of primary system, it can provide access service to the PR-MS.

(viii) PS-MS $\leftrightarrow$ PS-MS: This type of communication may exist in PS as a sort of ad hoc network in wireless networking systems. However, it may be prohibited in the infrastructure mode of some systems. However, if both nodes are transformed into CRs and this case folds back to CR-MS $\leftrightarrow$ CR-MS.

Note a special feature of CR links in the above list. Except the link between PS-MS and PS-BS that warrant bi-directional, each of the other seven types of links is available in only one direction, during an opportunity window of spectrum access. It is not hard to understand, as the opportunity window in time might be too short to warrant bi-directional exchange of packets and the next opportunity available time is not warranted either. This unidirectional link property plays a more critical role if we consider more network operations such as network security, and we can model link availability as a Markov chain [10,15] as an opportunistic link.

3. Framework of Trust in CRN

Trust has been studied in literatures for a long time from social science to computer science, as in References [16–20]. The immediate challenge to study trust in CRN is the mathematical definition of trust, while we want to keep in mind that distrust may be equally important as trust.

Consequently, to ensure smooth operation of CRN to support ubiquitous computing, trust forms the foundation of CRN. Trust has been widely mentioned in literatures regarding trusted computing and Internet/web computing, ad hoc network, and even social science. However, trust for CRN is quite different from these scenarios. Trusted computing deals with components inside a set or a territory. Internet/web computing treats trust as a kind of reputation/credits given by a mechanism (such as other’s scoring). We therefore need to develop a mathematical framework to model trust in CRN for quantitatively apply trust in CRN design and operation.

Trust is critical in CRN operation and beyond security design, as security usually needs communication overhead in advance. We can use the following examples to explain the need of trust other than security:

(a) A cognitive radio senses a spectrum hole or opportunity and dynamically accesses the spectrum for transmission requires ‘trust’ from originally existing system (i.e., primary system) and regulator, even without creating interference to PS.

(b) A cognitive radio may want to leverage another existing cognitive radio to route its packets, even though another CR is not the targeted recipient terminal. It requires ‘trust’ from another CR.

(c) A cognitive radio can even leverage PS to forward its packets to realize the goal of packet switching networks. It needs ‘trust’ from the PS, not only at network level but also in service provider (or network operator).

3.1. Mathematical Structure of Trust

If we temporarily ignore operator side, we just consider the trust in (CR) network. Trust must be measurable so that networks can operate based on it, such as routing and association to make dynamic spectrum access possible and practical. Intuitive measure of trust might be as follows.

Definition 1. Trust is a measure in $[-1, 1]$.

Remark. $\tau(i, j)$ denotes the trust measure for node $j$ to handle (receive and/or forward) a packet from node $i$. It is actually measured over $(-\infty, \infty)$ and can be normalized as $\tau(i, j) \in (-1, 1)$. 1 as the normalized value means trust in full (confidence); 0 means no information regarding trust or not; −1 means no trust at all. For a decision or a policy in CRN, it is obvious that negative trust and zero trust are under the same action.
Corollary 2. Trust in CRN is a measure in [0,1].

Remark. It is just like the probability measure, and enables our mathematical framework using probabilistic development and statistical decision theory. Please note that this degeneration from Definition 3.1 may result in an equivalent probabilistic atom for the trust measure at zero (i.e., $\tau(i,j) \in (-1,0]$).

Remark. The trust measure at zero means distrust. Any node in CRN being identified with zero trust shall be rejected by any action of CRN. That is, any possible link to such a node should be removed from CRN. It does not make any sense to be measured as zero or negative.

Lemma 3. Trust in CRN is generally irreversible. That is,

\[ \tau(i, j) \neq \tau(j, i) \]  

Remark. It is generally true for all consequences to adopt the concept of trust. The degree of Alice trusting Bob is not equal to the degree of Bob trusting Alice.

Definition 4. (Metric Space [16]). Every normed space can be regarded as a metric space, while distance $d(x,y)$ between x and y, with the following property:

(i) $0 \leq d(x, y) < \infty \forall x, y$
(ii) $d(x, y) = 0$ if and only if $x = y$
(iii) $d(x, y) = d(y, x) \forall x, y$
(iv) $d(x, y) \leq d(x, z) + d(y, z) \forall x, y, z$

Lemma 5. Trust in CRN is not a metric.

Proof. To form a metric space, $\tau(i, j) \geq 0$, which can be resolved by introducing a bias. However, $\tau(i, j) + \tau(j, k) \leq \tau(i, k)$ violates the requirement of metric space. This equation means that the trust through an intermediate node is not higher than the trust directly from the originating node. Furthermore, trust is irreversible, that is, $\tau(i, j) \neq \tau(j, i)$. This can be explained by the case when node i is a mobile CR and node j is the base station of a cellular network.

Remark. This lemma is usually ignored in most literatures to model trust in all research areas. However, it is critical as many trust measuring systems are constructed based on the assumption of trust measure being a metric, and such a fundamental assumption might be in jeopardy during further development.

Remark. However, if we define ‘distrust’ instead of trust (i.e., $D$ as distrust measure), the triangular inequality actually holds.

\[ D(i, j) + D(j, k) \geq D(i, k) \]  

We would like to point out, as many literatures note, modeling distrust might not be less important than modeling trust in networking research (either Internet or CRN).

Definition 6. Trust in CRN is contributed from reputation (trust measured by other nodes) and collaboration (behaviors observed by targeting node and possibly other nodes). Any zero-trust implies distrust.

Remark. Reputation is a terminology borrowed from trust in e-commerce. A CR node can increase its reputation by executing more actions under the operation rules. Both reputation and collaboration follow Definition 10.1. However, any of reputation or collaboration being zero results in zero/no trust. Definition 10.6 is different from common additive definition in literatures, and suggests ‘multiplication’ (or semi-group) to be more suitable.

Proposition 7 (Trust-Path Theorem). Trust in CRN is a function of routing path. The overall trust is the multiplication of trust in each segment. That is,

\[ \tau(n_0, n_1, \ldots, n_L) = \prod_{l=0}^{L-1} \tau(n_l, n_{l+1}) \]  

and

\[ \tau(n_0, n_1, \ldots, n_L) \neq \tau(n_0, n_L) \]  

Remark. For 3-node (2-segment) packet forwarding $\tau(i, j, k) = \tau(i, j)\tau(j, k) \neq \tau(i, k)$.

Remark. In literatures, many researchers note that trust relies on its past history, which coincides with this proposition. However, this proposition suggests that it is more than just history; the order of historical path makes sense.

Proposition 8. (Trust Processing Theorem) More processing (i.e., packet/traffic transportation) in CRN cannot increase trust.
Remark. This is a direct result from Definition 2 and Proposition 7. It is easy to understand in CRN. For any packet from the originating node, after more segments of transportation, we have no more trust.

Definition 9. (Semi-group [16]). Let X be a Banach space, and suppose that to every \( t \in [0, \infty) \) is associated an operator \( Q(t) \in B(X) \) in such a way that

(i) \( Q(0) = I \)

(ii) \( Q(s + t) = Q(s)Q(t) \forall s, t \geq 0 \)

Proposition 10. Trust in a homogeneous ad hoc network is degenerated into a semi-group as Reference [21].

Remark. Note that we require homogeneous ad hoc network condition such that ad hoc network implies the reversible (or exchange) property of trust holds as Equation (1). However, CRN, in general, is neither homogeneous nor ad hoc (CRN is likely to have infrastructure in some parts). From this mathematical property, we can also easily tell the difference of trust in CRN and trust in an ad hoc network.

It might be disputable to identify mathematical measure for trust in CRN. However, it is widely agreed that trust measure has the property like probability measure, and as Corollary 2 suggests. Let us start from Cox Axiom proposed in 1946, from a branch of artificial intelligence, mathematical reasoning.

Lemma 11 (Cox Axiom). If we want to measure any “certainty” that is consistent with the following conditions:

(a) Degree of certainty can be ordered.

(b) There exists a function to map certainty of a statement to its negation/complement.

(c) Degree of reasoning \( R(A \lor B) \) is related to the conditional reasoning \( R(A|B) \) and \( R(B) \) by some function \( g \)

\[
R(A \lor B) = g(R(A|B), R(B))
\]

Then, this reasoning system must be equivalent to the measure of probability.

Remark. Trust model in CRN indeed applies. Therefore, we subsequently treat trust to be measured just like probability and to develop as statistical decision theory [22].

3.2. Trust Model

The primary objective of trust model in CRN is to provide us a kind of mathematical framework to sense, measure, analyze, and learn the topology variation and the behavior of neighbors in such heterogeneous environment. In such heterogeneous network, trust model plays an important role among entities belonging to different systems and it will provide a mechanism for nodes to establish trust association. After trust association, cooperation between entities is possible and, therefore, they can communicate with each other to work together such as relay traffic, partner selection, and trusted routing. In this chapter, we try to build up the trust model for CRN and the trust model in CRN should provide two major components for nodes:

- **Trusted association:** It is the initial decision for a node to accept or to reject the trusted association from a neighboring CR node. To conduct networking of minimum risk is the central concept for this initial decision.

- **Learning algorithms:** Each node in CRN should keep the records of others and employ a proper learning algorithm to adapt the long-term trend of probability/trust measure of packet forwarding, so that timely judgment to hold on the trusted route or to retract it could be made.

We depict the basic components of our proposed trust model in Figure 5, which illustrates the interaction between these two functions and provides the whole scenario of the trust model. In wireless network, channel condition is always changing and trust is thus dynamic in CRN. We should develop proper

![Fig. 5. Flowchart of the trust model in CRN.](image-url)
learning algorithm to adapt the tendency of cooperation from neighbors in all kinds of environments. Each node in CRN could determine its trust policy about its neighbors according to the existing environment. The algorithm must catch the bad behaviors and punish the nodes for this attempt to deteriorate the throughput in wireless network. On the other hand, this mechanism needs to give the nodes opportunity for recovering the terrible isolation situations.

4. Trusted Association and Routing

One of the most challenging tasks for CRN is that a CR (transmitting node) initially requests association with a cooperative PS node or another CR (called receiving node) to conduct cognitive radio networking functions. Similar to cooperative networks, the receiving node in CRN can possibly conduct: (i) reject association, (ii) amplify-and-forward (AF) mode, (iii) compress-and-forward (CF) mode. The difference between AF and CF in routing lies that AF just executes physical layer function and we do not need to worry attacks and CF actually decodes the packets to upper layers under the threat of security threats. In other words, the cost for AF mode is simply communication bandwidth (and possible battery energy) waste even a wrong decision, but the cost for CF of a wrong decision might jeopardize the entire network, which suggests a security check like PKI after association before CF.

4.1. Trusted Association

We illustrate the association of CRN as Figure 6 and adopt the Neyman–Pearson criterion (since no a priori probability nor cost function is available in such a decision) as follows.

\[
\delta(x) = \begin{cases} 
1, & f_{\tau|1}(x|1) > \gamma \cdot f_{\tau|0}(x|0) \\
0, & f_{\tau|1}(x|1) < \gamma \cdot f_{\tau|0}(x|0)
\end{cases}
\]

Let \(X\) denote the trust measure with distribution \(F_0(x)\) representing the information inside the association request from CR-MS to PS-MS. Let \(\Theta = \Theta_0 \cup \Theta_1\) be a disjoint covering of the trust space, and \(H_i\) denote the hypothesis that the parameter \(\theta\) belongs to the trust space, \(\theta \in \Theta_i\). Then, the decision problem is now to distinguish between the two hypotheses by considering CRN architecture as given in Section 2:

(i) \(H_0 : \theta \in \Theta_0\): It means that CR-MS would not be worth being trusted. The probability density function for CR-MS is \(f_{\tau|0} = f_{\tau}(x|0)\), where \(x\) means the trust measure of CR-MS.

(ii) \(H_1 : \theta \in \Theta_1\): It means that the CR-MS would be worth being trusted. The probability density function for CR-MS is \(f_{\tau|1} = f_{\tau}(x|1)\), where \(x\) means the trust measure of CR-MS.

The PS-MS decides to trust CR-MS if the probability density function of trust measure, \(x\), from CR-MS under trust space \(\theta \in \Theta_1\), is larger than that under trust space \(\theta \in \Theta_0\).

**Remark.** For AF, once accept association, the packet(s) is relayed. For CF, once accept association, the transmitting node has to go through security check, and then the receiving node compresses and relays the packet(s).

**Proposition 13.** When a node in CRN (primary system or secondary systems) receives a request of association from a new node (i.e., to join this CRN), it forms a statistical decision as

Based on the trust measure \(\tau\) associated with this node, decision \(\delta(x) = a_1\) can be formed, while \(a_1\) means ‘accept’ the association and \(a_0\) means ‘reject’ the association.

The PS-MS will decide to trust CR-MS if the probability density function for trust measure, \(x\), from CR-MS under trust space \(\theta \in \Theta_1\) is larger than that under trust space \(\theta \in \Theta_0\). Therefore, with these two hypotheses, we can form the decision rule for the trust measure:

\[
\delta(x) = \begin{cases} 
1, & f_{\tau|1}(x|1) > \gamma \cdot f_{\tau|0}(x|0) \\
0, & f_{\tau|1}(x|1) < \gamma \cdot f_{\tau|0}(x|0)
\end{cases}
\]

The decision that maximizes the probability of detection for a given probability of false alarm is the likelihood ratio test as specified by the
Neyman–Pearson theorem. In order to maximize $P_D$ for a given $P_F \leq \alpha$, PS-MS decides to trust CR-MS if

$$l(x) = \frac{f_{\tau 1}(x | 1)}{f_{\tau 0}(x | 0)} > \gamma$$  \hspace{1cm} (6)$$

In the same way, PS-MS decides not to trust CR-MS if

$$l(x) = \frac{f_{\tau 1}(x | 1)}{f_{\tau 0}(x | 0)} < \gamma$$  \hspace{1cm} (7)$$

The likelihood ratio, $l(x) = \frac{f_{\tau 1}(x | 1)}{f_{\tau 0}(x | 0)}$, indicates the likelihood of $H_1$ versus the likelihood of $H_0$ under each trust measure. We can transform the decision into

$$\delta(x) = \begin{cases} 1 & , l(x) > \gamma \\ k & , l(x) = \gamma \text{ for some } \gamma \geq 0, \quad 0 \leq k \leq 1 \\ 0 & , l(x) < \gamma \end{cases}$$  \hspace{1cm} (8)$$

Remark. We successfully model the association process as a binary statistical decision problem. It can be applied to more realistic study of dynamic spectrum access to network cognitive radios. Please also note that randomized decision rule is still possible here. However, to completely define the binary decision problem, we still need to explore definitions of cost and a priori probability (i.e., trust measure) distribution. Since it is difficult to assign the cost function or a priori probabilities before establishing trust association in realistic situation, we consequently adopt the Neyman–Pearson theorem to solve the problem.

Definition 14. Following earlier Propositions, we can define the probability of false alarm and probability of detection with the meaningful interpretation for the trust association. First, we define that the probability of PS-MS trusting CR-MS given that CR-MS does not trust PS-MS as probability of false alarm:

$$P_F = \int_{x \in Z_1} f_{\tau}(x | 0)dx$$  \hspace{1cm} (9)$$

Second, we define that the probability of PS-MS trusting CR-MS given that CR-MS also trusts PS-MS as probability of detection:

$$P_D = \int_{x \in Z_1} f_{\tau}(x | 1)dx$$  \hspace{1cm} (10)$$

Remark. We can easily tell the importance of trust measure. The trust measure is composed of true trust and observation deviation (i.e., like observation noise in common communication theory). Such an observation deviation has tendency to be negatively distributed as more observation cannot increase trust as Proposition 10.8 (trust processing theorem). However, for malicious nodes, such a conclusion may not apply and observation deviation could be two-sided in distributions.

What we plan to do with Neyman–Pearson criterion in this decision problem is to minimize the risk of PS-MS trusting CR-MS given the constraint on CR-MS would not be worth being trusted. We do not make any assumptions on the probability density function of trust measure here. It could be discrete or continuous and we only want to derive a general trust decision rule for our trust model.

Proposition 15. When a priori information of trust is unknown and the cost function cannot be well defined, the decision $\delta(x) = a_i$ can be based on the Neyman–Pearson criterion. That is, given $P_F \leq a \ (0 \leq a \leq 1)$, optimize $P_D$.

Remark. The approach that maximizes the probability of detection for a given probability of false alarm is the likelihood ratio test. For a Neyman–Pearson test, the values of $P_F$ and $P_D$ completely specify the test performance. The problem in the trust decision is changed to

$$\text{maximize } P_D \text{ for a given } P_F = a$$  \hspace{1cm} (11)$$

decline $\delta(x) = \begin{cases} 1 & , l(x) > \gamma \\ k & , l(x) = \gamma \text{ for some } 0 \leq k \leq 1 \\ 0 & , l(x) < \gamma \end{cases}$$  \hspace{1cm} (12)$$

where the threshold, $\gamma$, is specified from the system constraint:

$$P_F = \int_{x \in Z_1 \mid l(x) > \gamma} f_{\tau 0}(x | 0)dx = \alpha$$  \hspace{1cm} (13)$$

If trust is based on individual perception, it is likely that different observers observe different situations; therefore, each node in CRN would adopt different significance level upon their acceptable level of malicious behaviors. Increasing $\gamma$ makes the test less sensitive for the disturbance and we accept a higher probability of detection in return for a lower probability of false alarm.
We will give an example of how nodes in CRN can make decisions using the Neyman–Pearson criterion we have described above. We start from the normal distribution for trust measure to realistically solve the trust problem here. Consider the case in Figure 7, CR-MS-A independently relays/forwards the packet with probability \( p \) and drops/ignores it with probability \( 1 - p \) as receiving packets from CR-MS-B. According to this information, PS-MS has to accept or reject the association from CR-MS-A by maximizing \( P_D \) under the system constraint, \( P_F \).

Let \( X \) be the number of packets forwarded by CR-MS-A and we assume that every packet is forwarded or dropped independently. This assumption is reasonable since the amount of the data transferred in the network is large enough. Then, in this situation, \( X \) is a binomial distribution with parameters \((m + n, p)\) which \( p \) is the probability of success. As \((m + n)\) is large and by De Moivre–Laplace theorem, we know that for any numbers \( a \) and \( b, a < b \),

\[
\lim_{n \to \infty} \Pr \left( a < \frac{X - (m + n) p}{\sqrt{(m + n) p(1 - p)}} < b \right) = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt
\]

where the expected value is

\[ E(X) = (m + n)p \]

and the variance of probability of success is

\[ \sigma_X = \sqrt{(m + n)p(1 - p)} \]

Since the probability of packets transmission successfully in next stage may be impossible to compute analytically, we could approximate this probability according to the experience rating:

\[
\Pr (\text{cooperation}) \approx \frac{\text{number of packets forwarding}}{\text{number of packets received}}
\]

With such approximation, the probability of packets forwarding successfully by CR-MS-A is \( \frac{m}{m+n} \), where we define it as probability of trusted cooperation. We can model the packet forwarding behaviors of CR-MS-A with normal distribution in this problem. Now, the problem is turned into the hypothesis problem:

\[ H_0: \text{CR-MS-A would not be worth being trusted.} \]
\[ X \sim N \left( \mu_0, \sigma_0^2 \right) \text{ where } \mu_0 = (m + n) \cdot (1 - p) \text{ and } \sigma_0^2 = (m + n) \cdot p \cdot (1 - p). \]

The probability density function of \( x \) is

\[ f_{x|0} (x | 0) = \frac{1}{\sqrt{2\pi\sigma_0}} e^{-\frac{1}{2} \left( \frac{x - \mu_0}{\sigma_0} \right)^2} \]

\[ H_1: \text{CR-MS-A would be worth being trusted.} \]
\[ X \sim N \left( \mu_1, \sigma_1^2 \right), \text{ where } \mu_1 = (m + n) p \text{ and } \sigma_1^2 = (m + n) p \cdot (1 - p). \]

The probability density function of \( x \) is

\[ f_{x|1} (x | 1) = \frac{1}{\sqrt{2\pi\sigma_1}} e^{-\frac{1}{2} \left( \frac{x - \mu_1}{\sigma_1} \right)^2} \]

We can derive the likelihood ratio by the hypothesis if we decide to choose \( H_1 \):

\[
\frac{l(x)}{l(0)} = \frac{f_{x|1} (x | 1)}{f_{x|0} (x | 0)} = \frac{1}{\sqrt{2\pi\sigma_1}} e^{-\frac{1}{2} \left( \frac{x - \mu_1}{\sigma_1} \right)^2} > \gamma
\]

Finally, it is equivalent to

\[
x > \frac{\sigma_1^2}{\mu_1 - \mu_0} \ln \gamma + \frac{\mu_1 + \mu_0}{2} = \gamma'
\]

We could determine the threshold \( \gamma \) from the false alarm constraint

\[ P_F = \Pr \{ x > \gamma' | H_0 \} \leq \alpha \]

Then, PS-MS can make the decision by maximizing the probability of detection.

Fig. 7. Execution of association based on Neyman–Pearson criterion (using normal distribution).

K.-C. CHEN ET AL.
\[ P_D = \{ \text{decide } H_1 \text{ given } H_1 \} \]
\[ = \Pr \{ x > \gamma' | H_1 \} \]
\[ = \int_{\gamma'}^{\infty} f_{\gamma|H_1} (x | 1) \, dx \]
\[ = Q \left( \frac{\gamma' - \mu_1}{\sigma_1^2} \right) \quad (23) \]

under the system constraint, probability of false alarm, which also can derive the threshold by

\[ P_F = \Pr \{ \text{decide } H_1 \text{ given } H_0 \} \]
\[ = \Pr \{ x > \gamma' | H_0 \} \]
\[ = \int_{\gamma'}^{\infty} f_{\gamma|H_0} (x | 0) \, dx \]
\[ = Q \left( \frac{\gamma' - \mu_0}{\sigma_0^2} \right) \quad (24) \]

where \(Q(x)\) is the right-tail probability of Gaussian random variable with zero mean and unit variance:

\[ Q(x) = \int_{x}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-t^2/2} \, dt \quad (25) \]

Using the constraint, \(P_F = \alpha\), we can derive the trust threshold as

\[ \gamma' = \sigma_0 \cdot Q^{-1}(\alpha) + \mu_0 \quad (26) \]

and we can obtain the probability of detection as

\[ P_D = Q \left( \frac{\sigma_0 \cdot Q^{-1}(\alpha) - (\mu_1 - \mu_0)}{\sqrt{\sigma_1^2}} \right) \]
\[ = Q \left( \frac{Q^{-1}(\alpha) - (\mu_1 - \mu_0)}{\sqrt{\sigma_1^2}} \right) \quad (27) \]

If we define the coefficient \(c^2\)

\[ c^2 = \frac{(\mu_1 - \mu_0)^2}{\sigma_1^2} = \frac{(m + n) \cdot (2p)^2}{p(1 - p)} \quad (28) \]

as the trust confidence equaling to the definition of deflection coefficient often used to approximate detection performance evaluation for most of the detection problems, we can derive the maximum probability of trusted cooperation from this system constraint:

\[ P_D = Q \left( Q^{-1}(\alpha) - \sqrt{c^2} \right) \quad (29) \]

Given the constraint on the probability of false alarm, and therefore, the trust threshold, the optimal trust decision is to

- Decide to trust if the probability of trusted cooperation from neighbors maximizes \(P_D\).
- Decide not to trust if the probability of trusted cooperation from neighbors does not maximize \(P_D\).

### 4.2. Trusted Routing

Once a node is accepted into CRN after association, as typical multi-hop networks, CRN shall update its network topology and routing table. If we treat CRN as a homogeneous amplify-and-forward network, routing is the same as any multi-hop ad hoc networks. However, it is obvious that CRN is not homogenous. As unlikely severe security is taken in CRN, it is important to develop trusted network layer function, especially topology and routing. Based on the developed mathematical framework of trust in CRN, we are ready to derive the fundamental operation of CRN at network layer, network topology establishment and routing in CRN.

Typical routing algorithms in a homogeneous network proceed on the distance measure that accounts available bandwidth/capacity and transmission cost. For routing of CRN, we have to consider trust in heterogeneous networking environments (e.g., PS is a cellular and CR is ad hoc WiFi station).

**Proposition 16 (Trusted Routing).** Routing metric between node \(i\) and node \(j\) in CRN is defined through a state-machine of state \((\tau(i, j), d(i, j))\), which represents trust measure and distance measure.

To deploy the routing algorithm, say Dijkstra algorithm, we may simply define a new trusted distance \(D(i, j) = d(i, j)/\tau(i, j)\) to iterate the algorithm to find the route, under the assumption of reversible trust relationship between any two nodes. For the case of no trust (i.e., \(\tau(i, j) = 0\)), the link is practically eliminated due to the infinite distance. Figure 8 as an example depicts both Bell-Ford and Dijkstra routing algorithms using this new trusted distance measure, with reversible trust relationship.
There exists an open problem to route under general irreversible trust relationship that invokes unequal distance measure for two directions between two nodes, which is asymmetric nature of uni-directional links in CRN [10].

**Definition 17.** CRN node (which can be an access point of PS) deciding the trust and taking an action to a packet from another CRN node can form a Markov decision process (with a decision/policy associated with a state-space) [23].

**Proposition 10.18 (Markovian Trust Process).** For packet transportation from node i to node j, the recipient node (i.e., node j in this case) can form a binary hypothesis testing (trust as $H_1$ and non-trust as $H_0$) based on certain decision policy. Trusted routing in Proposition 16 becomes a Markov process.

**Remark.** Trusted routing therefore becomes a kind of Markov decision process. As a matter of fact, randomized decision of trust is possible and meaningful in CRN. For example, $\tau(i, j) = \tau_r, 0 < \tau_r < 1$ may suggest a discount factor for trust status, due to various reasons such as roaming user/node, robustness against attacks, or simply insufficient credits in account. The number of states can be finite or infinite. This shall be subject to further study, though some touch in literatures.

5. Trust with Learning

The real challenge for trust in CRN is not only to construct the measure for trust to take proper actions but also to subsequently update the trust ‘distribution function’ for each network node to possibly conduct communication/networking functions such as requesting relay of packet(s). Each node in PSs supporting CRN or each CR shall be able to update and/or to maintain a trust table of neighboring nodes for applications described in later sections. It might be disputable to identify mathematical measure for trust in CRN. However, it is suggested that trust measure has the property like probability measure. Based on such measure, we may precede decisions based on trust measure in different application scenarios. Hereafter in this section, we focus on ways to update the distribution function of trust measure based on machine learning [16,24–26].
5.1. Modified Bayesian Learning

Suppose the probability distribution of trusted cooperation is \( f_P (p | \alpha_t, \beta_t) \), for any \( 0 \leq p \leq 1 \), where the superscript \( t \) means the discrete-time index with \( t = 0 \) as the initial distribution. \( f_P (p | \alpha_t, \beta_t) \) can be updated recursively by \( f_P (p | \alpha_{t-1}, \beta_{t-1}) \) based on current trust evidence, observation, and any further information. To resolve this challenge, we may adopt a learning algorithm for nodes in CRN to adapt the probability distribution of packets forwarding from neighbors at each (proper) time instance.

**Lemma 19 (Modified Bayesian Learning Algorithm).** Suppose the beta density \( f_P (p | \alpha_t, \beta_t) \) denote the probability distribution of trusted cooperation at time \( t \) in our trust model. The learning algorithm consists of three parts: the prediction of probability, decaying correction, and measurement modification.

\[
\hat{p}_t = \int p(x_t | P = p) \cdot f (p | \alpha_t, \beta_t) \, dp \tag{30}
\]

\[
f_{t-1} (p) = f (p | k_1 \alpha_{t-1}, k_2 \beta_{t-1}) \tag{31}
\]

and

\[
f (p | \alpha_t, \beta_t) = c \cdot f ((m_t, n_t) | p) \cdot f_{t-1} (p) \tag{32}
\]

where \( t \) is the discrete-time index, \( k_1 \) and \( k_2 \) are the decaying factors, \((m_t, n_t)\) is the new trust evidence, \( c \) is the modification factor representing the constant of the integral, and \( \hat{p}_t \) is the prediction probability of trusted cooperation.

Lemma 19 consists of the update probability distribution and the update rule. The probability density function, \( f(p | \alpha_t, \beta_t) \), for the prediction function incorporates into new trust evidence and a prior (probability) density function. It includes all the information prior to \( T = t - 1 \) where all trust evidence including the initial value is decayed as receiving new one.

\[
\begin{align*}
\alpha_t &= k_1 \alpha_{t-1} + m_t \\
&= k_1^t m_0 + k_1^{t-1} m_1 + k_1^{t-2} m_2 + \ldots + k_1 m_{t-1} + m_t \\
\beta_t &= k_2 \beta_{t-1} + n_t \\
&= k_2^t n_0 + k_2^{t-1} n_1 + k_2^{t-2} n_2 + \ldots + k_2 n_{t-1} + n_t
\end{align*}
\tag{33}
\]

Then, we carry on the decaying correction of past information prior to \( T = t \) by Equation (31) and incorporate new trust measurement after \( T = t \) in Equation (32). We use decaying correction to ‘forget’ the past trust evidence to explain the limitation of the period of validity since the trust model should gradually ignore the oldest record in order to catch the newest one. We use two constants \( k_1 \) and \( k_2 \) to represent the decaying factor as time goes on and usually \( k_1 \) is smaller than \( k_2 \) in order to catch the bad behaviors of node such like deception or throw packets away with bad intention. As we receive the new trust evidence at time \( T = t \), it would be appropriate to give the latest record more weight in order to support the dynamic and fast operation in CRN. Therefore, we can maintain the parameter update for TCRN by this learning mechanism.

**Remark.** Before deriving the prediction probability, \( \hat{p}_t \), we need to describe the details in the correction equation. At the end of time \( T = t \), we have the new trust evidence \((m_t, n_t)\) and prior probability distribution and we can calculate probability density function as

\[
f (p | \alpha_t, \beta_t) = \frac{f_t ((m_t, n_t) | p) \cdot f_{t-1} (p)}{\int f_t ((m_t, n_t) | p) \cdot f_{t-1} (p) \, dp}
\]

\[
= \frac{p ((m_t, n_t) | P = p) \cdot f (p | k_1 \alpha_{t-1}, k_2 \beta_{t-1})}{\int p ((m_t, n_t) | P = p) \cdot f (p | k_1 \alpha_{t-1}, k_2 \beta_{t-1}) \, dp}
\]

\[
= \begin{cases} 
\Gamma (\alpha_t + \beta_t) \\
\Gamma (\alpha_t) \Gamma (\beta_t) \end{cases} p^{\alpha_t - 1} (1 - p)^{\beta_t - 1}, \quad 0 \leq p \leq 1
\]

\tag{34}

**Remark.** The prediction is used to predict the (probability) measure of trusted cooperation in next stage and it is primarily designed for the decision criterion.

**Remark.** We give a flowchart for the technological processes in the learning mechanism in Figure 9. It provides two
We rewrite the equation in another form to denote that it is the weighted average of the maximum estimate of $P = p$ given $(m_t, n_t)$ and the mean of the prior information

$$
P(x_{t+1} = 1) = \int P(x_t = 1 | p = \hat{p}_t, (m_t, n_t)) f(p | \alpha_{t-1}, \beta_{t-1}) \, dp
$$

$$
= \int P(x_{t+1} = 1 | p = \hat{p}_t, (m_t, n_t)) f(p | \alpha_t, \beta_t) \, dp
$$

$$
= \int p \cdot f(p | \alpha_t, \beta_t) \, dp
$$

$$
= \frac{\Gamma((k_1\alpha_{t-1} + m_t) + (k_2\beta_{t-1} + n_t))}{\Gamma(k_1\alpha_{t-1} + m_t) \Gamma(k_2\beta_{t-1} + n_t)}

\times \int p^{k_1\alpha_{t-1}+m_t} (1-p)^{k_2\beta_{t-1}+n_t-1} \, dp
$$

$$
= \frac{k_1\alpha_{t-1} + m_t}{k_1\alpha_{t-1} + m_t + (k_2\beta_{t-1} + n_t)}
$$

(36)

When we obtain the prediction at each stage, we could make the decision by the decision criterion

$$
\delta_t(m_t, n_t) = \begin{cases} 0, & \text{means 'reject' if } \hat{p}_{t+1} \leq \gamma_t \\ 1, & \text{means 'accept' if } \hat{p}_{t+1} > \gamma_t \end{cases}
$$

(38)

If the probability measure of trusted cooperation is larger than the threshold $\gamma_t$, it means it is more probable that the packet would be delivered successfully at next stage than dropped, and vice versa.

5.2. Learning Experiments for CRN

We can describe several scenarios to demonstrate the well-suitable properties of learning algorithm applied in CRN, and we can further conclude some rule of thumbs when we build up the trust model for CRN. Since the CRN is a highly dynamic heterogeneous network, the nodes leave or join the network dynamically and promptly, and the CRN topology may change very frequently. The learning algorithm should follow up the channel variations and user behaviors instantly, to learn the update (favorable or unfavorable) changes in the behaviors of packet forwarding.
5.2.1. Nodes disconnect and the effect of initial value

The disconnection from nodes is frequently encountered in CRN and the learning algorithm should be able to catch this extreme case as soon as possible in order not to deteriorate the trust topology in the network. As we show in Figure 10, we accept the trust association from the neighbor with probability of trusted cooperation \( p = 0.8 \) at time \( t = 0 \) under \( k_1 = 0.2, k_2 = 0.5 \). At time \( t = 21 \), the neighbor disconnects from the network and the learning algorithm catches the prediction of probability immediately because the probability of trusted cooperation drops quickly. We retract the trust association at time \( t = 22 \) and determine the node has left the network at time \( t = 27 \). Since nodes in CRB are dynamic, they may leave and join the network for a while and we have to observe more time before we ascertain that it has disconnected from network. In Figure 10, we show the same scenario except that information inside the association request is different. The sum of the packets in the past in Figure 10 is 100, and that of Figure 11 is 1300. We note that the initial value affects the subsequent trust decisions at times \( t = 3 \) and \( t = 4 \). Although we learn the behaviors of node immediately, we should make the assumptions on the number of initial value to avoid such situations in the learning model. The simulations later should adopt the value of initial value, \( m_0 + n_0 = 100 \), in order to fully catch up the latest trust evidence of the nodes. Now, we propose the first rule of thumb from this example.

**Proposition 20 (Rule of thumb in different traffic model).** The learning algorithm in Lemma 19 can quickly learn the new trust evidence under heavy traffic density. Even the initial value is large or the environment is varied frequently, we can still learn quickly to catch the latest trust evidence if the traffic is heavy and the decaying factors are small enough.

5.2.2. Nodes leave and join the network suddenly

The neighbor sent association request including past 100 records with probability of trusted cooperation \( p = 0.8 \) at time \( t = 1 \) under \( k_1 = 0.2, k_2 = 0.5 \). The node leaves the network at time \( t = 21 \) and comes back at time \( t = 32 \). Because the considerable amount of packets dropped at time \( t = 22 \), we retract the trusted route right away and declare that the node has left the network. However, when the node comes back, we notice the considerable probability of trusted cooperation and we do not re-establish the trusted route immediately. We observe more time to build up the trusted route again. It is used to punish for the network performance drop and make sure that the node does not come back and leave again. We denote that the node may be back at time \( t = 35 \) and re-establish the trusted route at time \( t = 36 \). In Figure 12, we show the same scenario except that the traffic density in each time slot is different. The traffic density of Figure 12 is 100 and that of Figure 13 is 30 which represent the heavy and light traffic network, respectively. From Figure 12, we observe that the initial value significantly affects the learning algorithm because the sum of the initial value is 100 and it is larger compared to the traffic. Therefore, at times \( t = 6 \) and \( t = 7 \), the trust decisions are retracted and re-established in successive order. We are ready to propose other rules of thumb by the observations of the effect of the initial value problems.
Fig. 12. Node leaves and joins the network again under heavy traffic density.

Fig. 13. Node leaves and joins the network again under light traffic density.

Proposition 21 (Rule of thumb in the importance of decaying factor). The learning algorithm of Lemma 19 responds to the new trust evidence slowly under light traffic density. The only way we can adapt to this situation is to keep decaying factor as small as possible and making subsequent decisions between longer time intervals.

Proposition 22 (Rule of thumb in initial value problem). The initial value should be decayed as soon as possible since it reflects the past information. It contradicts the basic concept of learning algorithm which trying to respond to latest trust evidence. We can use adaptive decaying factors to ‘forget’ initial value properly and quickly under the realistic network condition.

5.2.3. Variation on the behavior of nodes

In this experiment, we consider the probability of trusted cooperation tending to perform better or worse. The nodes in CRN could incur bad channel condition and, therefore, cause to alter their behaviors on the trusted cooperation. The learning algorithm should be able to analyze the possible temporal disconnect and to make further decisions. In Figure 14, we show that the node changes its behavior at time \( t = 16 \) from probability of trusted cooperation from \( p = 0.9 \) to \( p = 0.7 \) and changes back to \( p = 0.9 \) at time \( t = 36 \) under \( k_1 = 0.2 \), \( k_2 = 0.5 \). The learning algorithm detects the variation at \( t = 20 \) although the probability of trusted cooperation is still larger than the trust threshold, \( p = 0.7 > 0.6 = \gamma_i \). The reason is the decaying factor that we punish the bad behaviors more than we reward good behaviors. Since \( k_1 = 0.2 < k_2 = 0.5 \), at time \( t = 16–20 \), the learning algorithm detects the decline in the prediction of probability and it retracts the trusted route at time \( t = 20 \). From time \( t = 16 \) to time \( t = 35 \), the learning algorithm also catches the stable packets forwarding from the node though the prediction of probability has a notable decline compared to \( t = 1–15 \). This may come from many causes and the variation between \( p = 0.9 \) and \( p = 0.7 \) can be possibly resulted from the channel condition. The learning algorithm will catch the probability from \( p = 0.9 \) to \( p = 0.7 \) immediately at time \( t = 37 \) and re-establish the trusted route when the channel condition turns better. In Figure 15, we show the same scenario except that the traffic density in each time slot is 30. We note that the prediction curve in light traffic network triggers the disturbance in the variation of behaviors and we denote the phenomenon as ‘temp disconnect’ in Figure 15. They do
not indicate real retraction of trusted route but represent the unstable oscillating across the trust threshold. However, the learning algorithm still works well in capturing the behavior changes, such as those at times $t = 16$ and $t = 36$, and detects the re-establishment of the trust association finally.

### 5.2.4. Intentionally drop the traffic

The learning algorithm should not only solve the frequent dynamic disconnections from network but also some special cases such like drop the traffic intentionally. In such situation, the nodes do not drop all the traffic. Instead, they drop some fixed portion of the traffic. This could result in a great damage to the entire CRN if the dropped portion has important parameters to network operation. In Figure 16, we show the remarkable decline in the prediction of probability of malicious users at time $t = 11$ and the usual behaviors of nodes. The malicious user is punished by the larger decaying factor to manifest the intentionally packet drops. Above examples describe the adaption of trust to allow desirable CRN operation by using the learning algorithms, so that CRN operation can progress along the operating time.

### 6. Conclusions

To realistically implement CRN, we proposed TCRN, especially for association that enables dynamic spectrum access of any CR delivering packets. From statistical decision theory and machine learning, we demonstrated successful realization of CRN functioning in association and also update of routing parameter, along with operating rules of thumb. As a matter of fact, TCRN can allow more homogeneous operation of CRN as a heterogeneous wireless network. Uncited Reference[27]

### Acknowledgements

This research is supported in part by the National Science Council, Taiwan, ROC, under the contract NSC 95-2923-I-002-001-MY2.

### References

Authors’ Biographies

Kwang-Cheng Chen received B.S. from the National Taiwan University in 1983, M.S. and Ph.D from the University of Maryland, College Park, United States, in 1987 and 1989, all in electrical engineering. From 1987 to 1998, he worked with SSE, COMSAT, IBM Thomas J. Watson Research Center, and National Tsing Hua University, in mobile communications and networks. Since 1998, he has been with the Institute of Communication Engineering and Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan, ROC, and is the Distinguished Professor and Irving T. Ho Chair. He held visiting/guest positions with Hewlett-Packard Laboratories USA, the Delft University of Technology Netherlands, and Aalborg University Denmark. He is actively involved in the technical organization of numerous leading IEEE conferences, including as the Technical Program Committee Chair of 1996 IEEE International Symposium on Personal Indoor Mobile Radio Communications, TPC co-chair for IEEE Glocom 2002, General Co-Chair for 2007 IEEE Mobile WiMAX Symposium in Orlando, for 2009 IEEE Mobile WiMAX Symposium in Napa Valley, and for IEEE 2010 Spring Vehicular Technology Conference. He has served editorship with a few IEEE journals and many international journals, and served various positions in IEEE. He is also actively participated in various wireless international standards. He has authored and co-authored over 200 technical papers and 18 granted US patents. He co-edits (with R. DeMarca) the book Mobile WiMAX published by Wiley 2008, and authors a book Principles of Communications published by River 2009, and co-author (with R. Prasad) another book Cognitive Radio Networks published by Wiley 2009. He was elected as an IEEE Fellow in 2006 and received numerous awards and honors. His research interests include wireless communications and networks, nano-computation/communication, and cognitive science.

Peng-Yu Chen received the B.S. degree in electrical engineering (EE) and M.S. degree in communication engineering from the National Taiwan University, Taipei, Taiwan, in 2006 and 2008, respectively. He has participated in Quanta project cooperated with Data Mining Lab in the department of Graduate Institute of Communication Engineering (GICE), NTU from 2006 to 2007. His research interests include trust computation, trust model in computer network and trust model for cognitive radio network.

Neeli Rashmi Prasad, Associate Professor and Coordinator of Network Architecture Thematic Group, Center for TeleInfrastruktur (CTIF), and Head of Wireless Security and Sensor Networks Group, Aalborg University, Denmark. During her industrial and academic career for over 13 years, she had lead and coordinated several projects. At present, she is leading an industry-funded project on reliable self organizing networks REASON funded by Huawei, Project Coordinator of European Commission (EC) Integrated Project (IP) ASPIRE on RFID and Middleware and EC Network of Excellence CRUISE on Wireless Sensor Networks. She is coordinating the Internet of Things working group for European Commission Future of Internet Assembly and co-caretaker of real-world Internet (RWI). She has lead EC Cluster for Mesh and Sensor Networks and Counsellor of IEEE Student Branch, Aalborg. She is Aalborg University
Ying-Chang Liang is presently a Senior Scientist in the Institute for Infocomm Research (I2R), Singapore, where he has been leading the research activities in the area of cognitive radio and cooperative communications. He also holds adjunct associate professorship positions in Nanyang Technological University (NTU) and National University of Singapore (NUS), both in Singapore, and adjunct professorship positions with Jilin University and University of Electronic Science & Technology of China (UESTC), both in China. He has been teaching graduate courses in NUS since 2004. From Dec 2002 to Dec 2003, he was a visiting scholar with the Department of Electrical Engineering, Stanford University, CA, USA. His research interest includes cognitive radio, dynamic spectrum access, reconfigurable signal processing for broadband communications, space-time wireless communications, wireless networking, information theory and statistical signal processing.

He is now an Associate Editor of IEEE Transactions on Vehicular Technology, Lead Guest-Editor of ERASIP Journal on Advances in Signal Processing, Special Issue on Advanced Signal Processing for Cognitive Radio Networks, and Lead Guest-Editor of IEEE Journal on Selected Areas in Communications, Special Issue on Advances in Cognitive Radio Networking and Communications. He was an Associate Editor of IEEE Transactions on Wireless Communications from 2002 to 2005, Lead Guest-Editor of IEEE Journal on Selected Areas in Communications, Special Issue on Cognitive Radio: Theory and Applications, and Guest-Editor of COMPUTER NETWORKS Journal (Elsevier) Special Issue on Cognitive Wireless Networks. He received the Best Paper Awards from IEEE VTC-Fall’1999 and IEEE PIMRC’2005, and 2007 Institute of Engineers Singapore (IES) Prestigious Engineering Achievement Award. He has served for various IEEE conferences as technical program committee (TPC) member. He was Publication Chair of 2001 IEEE Workshop on Statistical Signal Processing, TPC Co-Chair of 2006 IEEE International Conference on Communication Systems (ICCS’2006), Panel Co-Chair of 2008 IEEE Vehicular Technology Conference Spring (VTC’2008-Spring), TPC Co-Chair of 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom’2008), TPC Chair of 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN’2010), and Co-Chair, Thematic Program on Random matrix theory and its applications in statistics and wireless communications, Institute for Mathematical Sciences, National University of Singapore, 2006. He is a Senior Member of IEEE and holds six granted patents.