International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 11 | Nov - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

THESIS ON PROBABILITY OF DETECTION IN TRUSTED CRN

DR. SARIKA SAINI

Abstract:

This treatise is an attempt to find out the most important parameter i.e. probability of detection in trusted CRN (Cognitive Radio Network). Conventional security function cannot be implemented in practical in CRN and hence poses some questions on its quality of service overall. This paper is an attempt to introduce associative trust in CRN and define the probability of detection mathematically.

Introduction:

Cognitive radio is a revolutionary technology that promises to alleviate the spectrum shortage problem in data communication and bring about remarkable improvements in the efficiency of the spectrum utilization. However, the successful deployment of the CR networks and the realization of the benefits depend on the placement of essential security mechanism in sufficiently robust form to resist misuse of the system.

We cannot deploy the time consuming hand-shaking conventional security protocols in CRN as it would reduce the performance, making the network slow. Simultaneously we have to make sure that the security mechanism is not consuming too much power as well.

Infrastructure based architecture of CRN:

The components of infrastructure based (or centralized) CRN architecture (as shown in Fig 1) can be classified in two groups as the primary network and the CR network.

The primary network is the legacy network that has an exclusive license to a certain spectrum band. Examples of such networks are the TV broadcast and common cellular networks. On the contrary, the CR network is not allotted a license to operate in the desired band. Hence the spectrum access is allowed to only in an appropriate manner. The following are the basic components of the primary network.

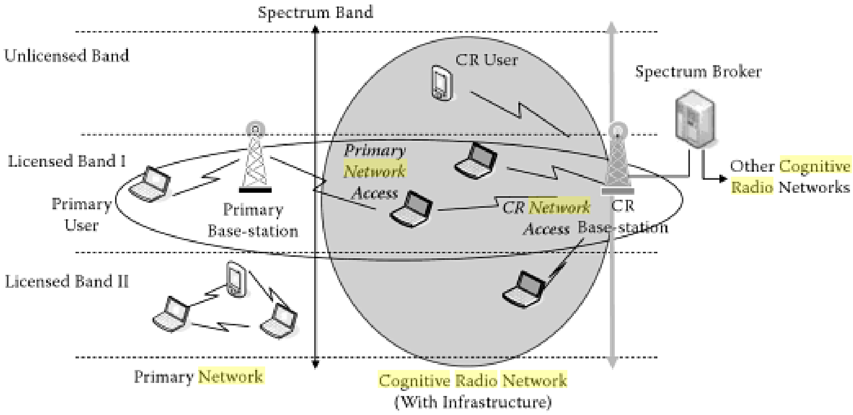

Fig 1: Infrastructure based Architecture of CRN

Primary user: Has a license to operate in a certain spectrum and the access can be only controlled by the primary base station. Primary users do not need any modification or additional functions for co-existence with CR base stations and CR users.

Primary base station: It's a fixed infrastructure network component that has a band license, such as a transceiver system at base station in a cellular network.

The basic components of the CR network are defined as follows:

CR user: Not allotted a spectrum license and hence additional functionalities are required to share the licensed spectrum band.

CR base station: It's a fixed infrastructure based component with CR capabilities. It facilitates single hop connection without spectrum licenses to CR users within transmission range and delivers control over them. Through this connection, a CR user in CRN can access other networks. It also plays key role in synchronizing the sensing activities performed at the end of different CR users. The analysis performed by the latter is generally fed to the central CR base station so that the decision on the spectrum availability can be made.

Spectrum broker: Also known as scheduling server. It's a central network entity that plays a role in sharing the spectrum the spectrum resources among different CR networks. It's not directly associated with spectrum sensing. It, rather, manages the spectrum allocation among different network according to the sensing information collected by each network.

Links in CRN:

Before kicking off this segment let's introduce the major two components in CRN viz. CR-BS (Cognitive Radio - Base Station) and CR-MS (Cognitive Radio- Mobile Station).

Cognitive Radio - Base Station: It's responsible for managing the spectrum holes which is the key mean of communication in CR. It also takes care of security and mobility of CRN. It acts like a pathway to The Cognitive Radio Mobile Stations to access internet.

Cognitive Radio- Mobile Station: It's a portable device with features of CR which is able to reconfigure itself to sense holes in spectrum and utilize them dynamically to connect to the communication systems.

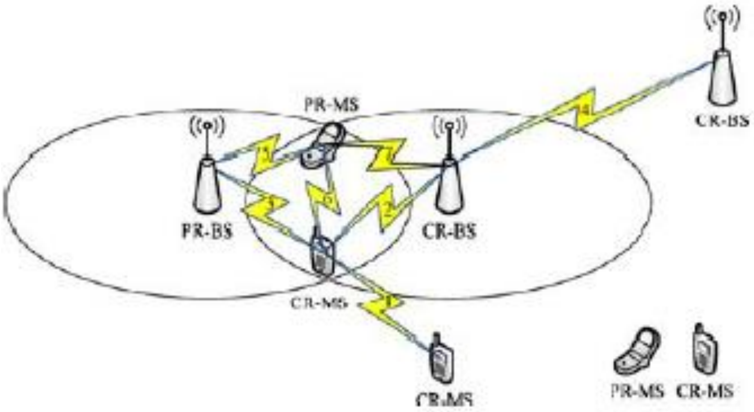

Fig 2: Possible links in CRN

Various types of Primary systems are present in the unlicensed or licensed spectrum bands and they can be classified as follows:

Primary system operating in licensed spectrum: Has the priority of highest level to use the spectrum.
Primary system operating in unlicensed spectrum: A sophisticated example of this is ISM band. There are ample of such systems in the same unlicensed spectrum and hence can cause interference unless the priority is set with a proper algorithm.

The various possible connections have been depicted in the tabular form below:

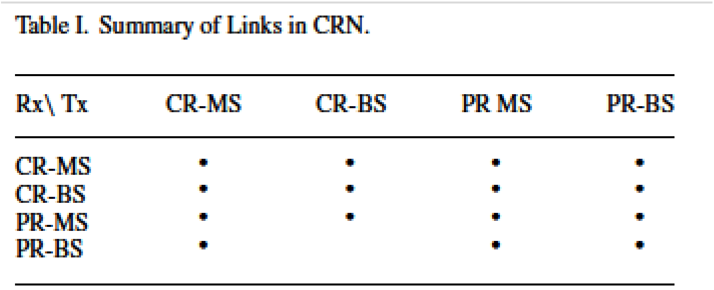

Table I. Summary of Links in CRN.

Rx\ Tx	CR-MS	CR-BS	PR MS	PR-BS
CR-MS	•	•	•	•
CR-BS	•	•	•	•
PR-MS	•	•	•	•
PR-BS	•		•	•

Mathematical preliminaries of trust in CRN:

Definition of Trust:
Let τ(I,j) be the measure of trust for j-th node for handling a packet from i-th one. We can normalize our measurement to write τ(I,j) ε [-1,1]. 1 represents the highest degree of trust in communication and 0 represents no trust. Now it's obvious that negative trust also represents the same as 0 and hence trust can be said to be a measure in [0, 1] effectively
$(\text{i.e.} \int_{-1}^{0} 1_{\tau(i,j)\in[-1,0]} \mathrm{d}\tau)$.

Lemma 1:
As a generalization we will assume that trust associated with CRN is irreversible in nature. Mathematically,

$\tau(i, j) \neq \tau(j, i)$ ------(1)

Simply put, the degree of A trusting B is not equal to the degree of B trusting A.

Lemma 2:
Trust in CRN can't be associated with a metric.
Proof:
To form a metric space the condition is
τ(I,j)≥0 which can be obtained only by introducing a bias.
However,
$\tau(i, j) + \tau(j, k) \leq \tau(i, k)$ and it flouts the condition of a metric space. This equation implies that the trust through an intermediate node is smaller or equal to than the trust straight away from the originating node.
But since trust is irreversible , it doesn't satisfy one of the important conditions of a space to be a metric.

Trust Path Theorem:

The overall trust in CRN is multiplication of each segment's trust i.e.

$$\tau(n_0, n_1, \ldots, n_L) = \prod_{l=0}^{L-1} \tau(n_l, n_{l+1}) \qquad \text{-------(2)}$$

And

$$\tau(n_0, n_1, \ldots, n_L) \neq \tau(n_0, n_L) \qquad \text{---------(3)}$$

Trust Model:

The primary point is to introduce a mathematical framework for analyzing, measuring trust in heterogeneous aura by establishing a mechanism for associating nodes with trust. Every node must be having two important attributes as follows:

(1) **Trust-association:** It represents the initial decision for a CR node to accept / reject the trusted association from a neighboring node.

(2) **Sophisticated Learning Algorithms:** To facilitate tracking of measure of trust in probabilistic way for packet routing.

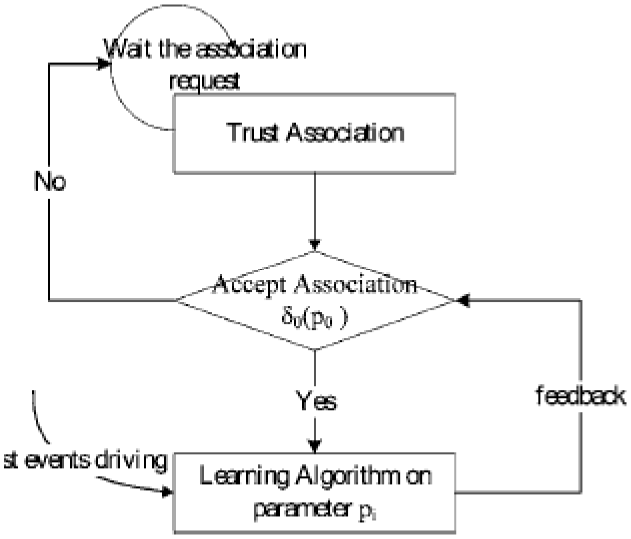

Fig 3: Flow chart of the model

In practical wireless CRN communication trust is always a dynamic entity and we must have sophisticated learning algorithms o make sure that the CRN is secure under any kind of heterogeneous environment. We must incorporate mechanisms for the nodes to retaliate from the mal-behaviors during isolations.

One of the biggest hurdles for CRN is that a CR transmitting node requests linkage with a PS node or another CR receiving node. The receiving node can either reject linkage/association or amplify-and-forward (AF) or compress-or forward. The difference in between AF and CF is that the former executes function of physical layer and doesn't pose threat of attacks whereas CF is responsible for decoding the packets to upper layers and hence can elicit security threat.

Trust Association:

The figure below delineates the association of trust in CRN in the light of Neyman-Pearson criteria. The reason it has been adapted it in the model is the absence of any priori cost function or probability in such decision.

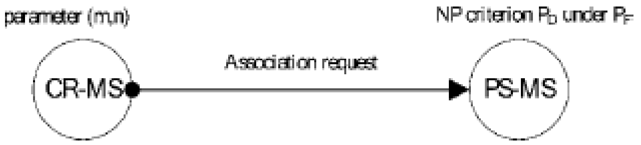

Fig 4: NP Theorem in trust decision of CRN

Let X be the random variable that measures trust and $F_\theta(x)$ be the corresponding probability distribution function for trust associated with the information for request from CR->MS to PS->MS. Let $\Theta = \Theta_0 \cup \Theta_1$ be a covering (disjoint) of the trust-space where H_I implicates $\theta \in \Theta_i$.

The PS->MS decides to trust CR->MS in case the pdf of X(trust-measure) , from CR->MS under trust space $\theta \in \Theta_1$ is larger than the space $\theta \in \Theta_0$.

Proposition 1:

When a CR node receives an association request from another CR node, it establishes a stochastic decision δ(x) based on the trust measure as

$$\delta(x) = \begin{cases} 1 & , f_{\tau|1}(x|1) > \gamma \cdot f_{\tau|0}(x|0) \\ k & , f_{\tau|1}(x|1) = \gamma \cdot f_{\tau|0}(x|0), \text{ for some } \gamma \ge 0, 0 \le k \le 1 \\ 0 & , f_{\tau|1}(x|1) < \gamma \cdot f_{\tau|0}(x|0) \end{cases}$$

--------(4)

The decision that can maximize the probability of detection (P_D) for a specific false-alarm probability (P_F) is the likelihood ratio test as given by the NP(Neyman-Pearson) theorem. To maximize P_D, for a given $P_F \le \alpha$, a PS-MS link trusts CR-MS if the likelihood ratio *l(x)* satisfies

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

------(5)

The likelihood ratio implies the likelihood of H_1 vs H_0 under each measure of trust. Hence the decision can be transformed in the following form (using (4) and (5)),

$$\delta(x) = \begin{cases} 1 & , l(x) > \gamma \\ k & , l(x) = \gamma \text{ for some } \gamma \ge 0, \quad 0 \le k \le 1 \\ 0 & , l(x) < \gamma \end{cases}$$

--------(6)

Where γ is the threshold value for making decision.

Defining P_F abd P_D :

First, let's define the probability of PS->MS trusting CR->MS given CR->MS does not trust PS->MS as false alarm probability:

$$P_F = \int_{x \in Z_1} f_\tau(x|0)\mathrm{d}x$$

-------(7)

Now, the probability of PS->MS trusting CR->MS provided CR->MS trusts PS-MS as probability of detection is given by

$$P_D = \int_{x \in Z_1} f_\tau(x|1)\mathrm{d}x$$

--------(8)

What our motive is with Neyman–Pearson criterion is to curtail the risk of PS-MS trusting CR-MS irrespective of the nature of probability density function (continuous or discrete) as a case of generalization.

Derivation:

Let the maximum value of probability of detection be a for a given value of probability of false-alarm.
Now under the following conditions of decision

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

Let the system constraint due to false alarm be defined as

$$P_F = \int_{\{x:l(x)>\gamma\}} f_{\tau|0}(x\,|0)\mathrm{d}x = \alpha \qquad \text{-------(9)}$$

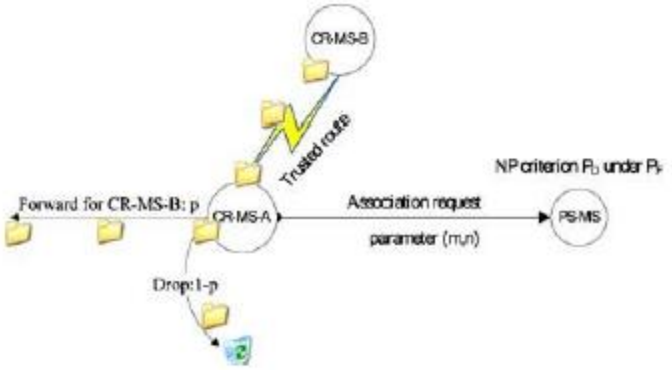

Fig 5: Association based on NP criteria

Let us consider the case in Fig 5, CR->MS A independently forwards the packet with a probability of p and ignores it when the probability id (1-p) while receiving packets from CR->MS B. Based on this information, PS->MS has to either accept or reject the association from CR->MS A by maximizing probability of detection under the constraint of P_F.

Let X be the number of packets relayed by CR->MS A and we assume that the mechanism of packet relay or drop is independent since the network will be dealing with an exorbitant amount of data. Now let's assume X to be a stochastic variable following binomial distribution with parameters (m+n,p) where p is the success-probability and m+n will be large (since the number of trials and success both will be high in a CRN), then from De-Moivre-Laplace theorem, for any numbers a b where a<b,

$$\lim_{n\to\infty} P\left(a < \frac{X-(m+n)\,p}{\sqrt{(m+n)\,p\,(1-p)}} < b\right)$$

$$= \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt \qquad \text{----------(10)}$$

Where the expectation is

$$E(X) = (m+n)p \qquad \text{-------(10)}$$

And variance can be written as

$$\sigma_X = \sqrt{(m+n)p(1-p)}$$ --------(11)

Let’s define a parameter P_r as

$$\Pr(\text{cooperation}) \approx \frac{\text{number of packets forwarding}}{\text{number of packets received}}$$ -------(12)

With these approximation being taken into the account, the probability of packets forwarded successfully by CR->MS A is $\frac{m}{m+n}$.

Now we can model the packet relay behavior with Gauss-normal distribution and now we have to consider two cases of hypothesis as follows:

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

The probability density function of x is

$$f_{\tau|0}\,|(x\,|0) = \frac{1}{\sqrt{2\pi}\sigma_0}\mathrm{e}^{\left\{-\frac{1}{2}\left(\frac{x-\mu_0}{\sigma_0}\right)^2\right\}}$$ ------(13)

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

The probability density function of x is

$$f_{\tau|1}\,(x\,|1) = \frac{|1}{\sqrt{2\pi}\sigma_1}\mathrm{e}^{\left\{-\frac{1}{2}\left(\frac{x-\mu_1}{\sigma_1}\right)^2\right\}}$$ -------(14)

In case we decide to select H_1 we can obtain the likelihood ratio as

$$l(x) = \frac{f_{\tau|1}\,(x\,|1)}{f_{\tau|0}\,(x\,|0)} = \frac{\frac{1}{\sqrt{2\pi}\sigma_1}\mathrm{e}^{\left\{-\frac{1}{2}\left(\frac{x-\mu_1}{\sigma_1}\right)^2\right\}}}{\frac{1}{\sqrt{2\pi}\sigma_0}\mathrm{e}^{\left\{-\frac{1}{2}\left(\frac{x-\mu_0}{\sigma_0}\right)^2\right\}}} > \gamma$$ -------(15)

This is stochastically equivalent to

$$x > \frac{{\sigma_1}^2}{\mu_1-\mu_0}\ln\gamma + \frac{\mu_1+\mu_0}{2} = \gamma'$$ -------(16)

We can also compute the threshold from the constraint of false alarm as

$$P_F = \Pr\left\{x > \gamma'\,|H_0\right\} \leq \alpha$$ -------(17)

Now PS->MS can make a decision by maximizing the P_D,

$$
\begin{aligned}
P_D &= \{\text{decide H}_1 \text{ given} \\
&= \Pr\{x > \gamma' \,|H_1\,\} \\
&= \int_{\gamma'}^{\infty} f_{\tau|1}\,(x\,|1)\,\mathrm{d}x \\
&= Q\left(\frac{\gamma' - \mu_1}{\sqrt{\sigma_1^2}}\right)
\end{aligned}
\quad \text{-----(18)}
$$

Where

$$
Q\,(x) = \int_{x}^{\infty} \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-t^2/2} \mathrm{d}t \quad \text{-----(19)}
$$

Under the constraint of false alarm, P_F can also be computed as

$$
\begin{aligned}
P_F &= \Pr\{\text{decide } H_1 \text{ given } H_0\} \\
&= \Pr\{x > \gamma' \,|H_0\,\} \\
&= \int_{\gamma'}^{\infty} f_{\tau|0}\,(x\,|0)\,\mathrm{d}x \\
&= Q\left(\frac{\gamma' - \mu_0}{\sqrt{\sigma_0^2}}\right)
\end{aligned}
\quad \text{-----(20)}
$$

Making use of the constraint $P_F = \alpha$, we can derive the threshold as

$$
\gamma' = \sigma_0 \cdot Q^{-1}(\alpha) + \mu_0 \quad \text{-----(21)}
$$

Combining equation (21) with equation (18),

$$
\begin{aligned}
P_D &= Q\left(\frac{\sigma_0 \cdot Q^{-1}(\alpha) - (\mu_1 - \mu_0)}{\sqrt{\sigma_1^2}}\right) \\
&= Q\left(Q^{-1}(\alpha) - \frac{(\mu_1 - \mu_0)}{\sqrt{\sigma_1^2}}\right)
\end{aligned}
\quad \text{------(21)}
$$

References

[1] Cognitive Radio Networks: Architectures, Protocols, and Standards edited by Yan Zhang, Jun Zheng, Hsiao-Hwa Chen

[2] Cognitive Radio Communication and Networking: Principles and Practice By Robert Caiming Qiu, Zhen Hu, Husheng Li, Michael C. Wicks

[3] Principles of Cognitive Radio By Ezio Biglieri, Andrea J. Goldsmith, Larry J. Greenstein, Narayan B. Mandayam, H. Vincent Poor

[4] Cognitive Radio Technology edited by Bruce A. Fette

[5] Quantitative Analysis of Cognitive Radio and Network Performance By Preston Marshall

[6] Trusted Application Centric Ad Hoc Network By Gang Xu

[7] Cognitive Radio Networking and Security: A Game-Theoretic View By K. J. Ray Liu, Beibei Wang