Trust based channel preference in cognitive radio networks under collaborative selfish attacks

Shameek Bhattacharjee and Mainak Chatterjee
Electrical Engineering & Computer Science, University of Central Florida, Orlando,
Email: {shameek, mainak}@eecs.ucf.edu.

***Abstract*—Secondary spectrum data falsification (SSDF) is a common attack in cognitive radio networks, where dishonest nodes share spurious local sensing data. This behavior misleads the collective inference on spectrum occupancy. The situation is more aggravated when a *collaborative* SSDF attack is launched by a *coalition* of selfish nodes. Defense against such collaborative attacks is difficult with popularly used voting based inference models.**

This paper proposes a method based on Bayesian inference that indicates how much the collective decision on a channel's occupancy can be trusted. Using an anomaly monitoring technique, we check if the reports sent by a node match with the expected occupancy and classify the outcomes into three categories: i) if there is a match, ii) if there is a mismatch, and iii) if it cannot be decided. Based on the measured observations over time, we estimate the parameters of the hypothesis of match and mismatch events using a multinomial Bayesian based inference. We quantitatively define the trust as the difference between the posterior beliefs associated with matches and that of mismatches. The posterior beliefs are updated based on a weighted average of the prior information on the belief itself and the recently observed data. We conduct simulation experiments that show that the proposed trust model is able to distinguish the attacked channels from the non-attacked ones. Also, a node is able to rank the channels based on how trustworthy the inference on a channel is. We are also able to show that attacked channels have significantly lower trust values than channels that are not.

I. Introduction

In cognitive radio networks, secondary users (i.e., unlicensed users) cooperate with each other by sharing their locally sensed information on spectrum occupancy facilitating more accurate inference on spatio-temporal spectrum usage statistics. The fused information is then used by the secondary users to dynamically access channel based on some mutually agreed upon channel access etiquettes. [1].

Oftentimes, to reduce the adverse effect of wireless channel characteristics like signal fading and noise, data gathered at multiple locations are fused together [7]. Thus, the cognitive radios employ cooperative sensing where the spectrum decision is made after fusing the individual spectrum reports sent by a number of radios at various locations. Such fusion has been proven to effectively mitigate shadowing and multipath effects and significantly improve spectrum usage through coordination among competing cognitive radios [7]. Popular fusion techniques are usually based on k out of K fusion or majority voting [12]. However, reliance on cooperation has also opened up potential vulnerabilities [4]. An example could be the case where dishonest radios provide misleading information resulting in wrong decisions by the other radios. An easy manipulation can be achieved through secondary spectrum data falsification (SSDF) attacks where spurious occupancy information is sent by the rogue radios. From now, we use the terms 'radio' and 'nodes' interchangeably.

978-1-4799-4912-0/14/$31.00 ©2014 IEEE

To counter SSDF attacks, the common approach has been on the *identification* or *isolation* of dishonest nodes [5], [10]. But, there has not been much effort on distinguishing between selfish and malicious rationale of rogue nodes, or the effect of a coalition formation. While a malicious attacker's only objective is maximum damage to other nodes in a network, selfish attacks are launched by rational nodes on a few strategic channels so as to gain some tangible benefit. A classic example of a collaborative selfish SSDF attack is a group of nodes belonging to a certain network provider which wants access to some selected channel(s); hence all nodes belonging to that provider send false information for those channels while truthfully reporting on all other channels in order to remain undetected. Compared to the number of malicious nodes, the number of selfish nodes can be high, considering every node has a natural proclivity to maximize its benefits. Hence selfish attacks are more plausible form of a vulnerability. But total isolation of all such selfish nodes is perhaps not the right approach. This is because in such a case the fusion process *loses the correct information* that the selfish nodes might share [3]. This loss is even more pronounced when the selfish nodes collaboratively falsify (on same channel sets) with a low probability and tell the truth more often [4]. In fact, it is often difficult to detect such selfish behavior of nodes through malicious node detection techniques. Thus, instead of isolating and not considering the selfish nodes at all, we ought to consider shared information on specific channels and discount or completely ignore information on other channels. Thus, we argue for the need of a *channel-centric defense* instead of a node-centric defense.

In this paper, we propose a trust based channel centric approach towards evading selfish collaborative SSDF attacks. We discuss two variants of selfish collaboration: static and dynamic. In the static case, the set of channels that is attacked does not change over time, while in the dynamic case, it does. First, we present a 3 step monitoring technique that gathers *channel centric evidence* by capturing the anomalies in the advertised occupancy of a channel. First we estimate the lower and upper bounds on the received power level from a neighbor. The bounds are then compared with some predefined threshold that results in a predicted ternary decision: occupied, not occupied, or cannot be decided. This predicted decision is compared with what a neighboring node actually advertised. The comparison yields three possible outcomes– match, mismatch or undecided. The observation data formed by the outcomes from all neighbors on a particular channel gives the frequency of occurrence of matches, mismatches or undecided. More matches is indicative of agreement on channel occupancy while more mismatches means presence of mis-leading advertisements.

The outcomes can be conceptualized as multinomial hypothesis of a Bayesian inference model with three parameters. We seek to build a Bayesian inference based trust model, where a value is assigned to each channel that indicates the level of trustworthiness of the occupancy inference of that channel. We do this by calculating the posterior Bayesian belief of the hypothesis based on incrementally incoming observation data and prior belief of the hypothesis itself. The difference between the posterior beliefs associated with a match and a mismatch is reported as the net trust. We use the net trust for ranking the channels allowing the nodes to choose the channels based on how trustworthy the cooperative inference on a channel is. Such a choice enables less policy violations and better spectrum utilization.

Our results show that for both variants (i.e., static and dynamic) the channels that were attacked have a significantly lower trust value than channels that were not. Moreover, for static attacks it is also possible to identify the channels that were selected by the adversarial group. We also show that the proposed trust model is effective even for a high density of selfish nodes. We demonstrate that the proposed channel centric defense mechanism is not effected by node mobility and does not require knowledge of the locations of secondary nodes, thus obviating the need for addressing location falsification.

II. System Model and Assumptions

We consider a distributed secondary cognitive radio network with honest nodes denoted by H and a set of selfish nodes denoted by D. Each node i fuses the spectrum sensing data it receives from its neighboring nodes, denoted by N^i. For any channel k, there are N_k^i advertised opinions on the occupancy of channel k at node i. We assume all secondary nodes continuously undergo spectrum sensing to determine whether a channel is occupied or not by comparing the sensed energy with some common threshold, γ_{th}. Let us assume secondary node i constructs its observed binary occupancy vector as $B_{act}^i = [d_1, d_2, \cdots, d_K]$, where d_k is 1 or 0 depending on whether the channel is occupied or unoccupied, and K is the number of channels being monitored. B_{act}^i denotes the actual binary occupancy vector that was formed at i. Once this binary vector is created, a secondary node would advertise this information to its neighboring nodes as B_{adv}^i. For a selfish node, $B_{adv}^i \neq B_{act}^i$ and for honest nodes both of them are equal. Similarly, a secondary node would also hear broadcast messages (binary occupancy vectors) from its neighbors. Based on the vectors a node receives, the node will employ a majority voting based fusion technique to obtain a better estimate about the spectrum usage.

We consider that the selfish nodes do not report their occupancy vectors truthfully; rather they inject errors in their occupancy vectors by flipping the bits in the vector collaboratively. Flipping 0 to 1 implies that the channel is occupied when in reality it is unoccupied. Flipping 1 to 0 implies that an occupied channel is reported as unoccupied. The selfish nodes collaborate to attack (i.e., flip) the same set of channels to mislead the voting based fusion technique. We denote I_{attack}, as the fraction of channels that a selfish node flips/changes from its observed vector. Unlike the attacks from malicious nodes, selfish nodes attack on fewer but a specific channels (based on certain statistical criteria).

We assume the transmit power level of all secondary nodes during sharing of binary vectors is equal and takes place through a common control channel. Given this, along with channel losses, and antenna gains with the appropriate path loss model we can compute the distance between the two nodes using received signal strength (RSS) of reporting signal through localization or lateration [2], [9]. Hence, location falsification is no more a limiting factor and location privacy preserved.

As for the primary users, each primary transmitter, transmits on one channel; so the channel associated with a primary transmitter is known. The primary transmitter that transmits on channel k, is referred as T_k, and has fixed coordinates (x_{T_k}, y_{T_k}) which are known to the nodes.

III. Gathering Trust Evidence

Consider Fig. 1. Let O be the position of any node i. Let j be its neighbor whose exact location is not known, but the mutual distance can be estimated through RSS localization. Through RSS localization, whenever node j sends an advertisement, we can estimate the mutual distance s_{ij} and the locus of neighbor j is anywhere on the circle centered around node i with a radius s_{ij} when transmit powers are same for all nodes. (See Fig. 1) Using commonly used propagation model for RSS [8], we know RSS at node i on channel k due to primary tower T_k is:

$$\gamma_k^i = P_k \times \frac{A^2}{s_{i,k}^{\omega}}; \tag{1}$$

where A is a constant, ω is path loss factor, $s_{i,k}$ is the distance between T_k and node i, and P_k is the transmit power of T_k. On any channel k, the highest and lowest bounds on the received power for neighbor j due to the primary transmitter T_k transmitting on channel k is given by:

$$[\gamma_k^j]_{high} = P_k \times \frac{A^2}{s_{j_{min},k}^{\omega}} \tag{2}$$

$$[\gamma_k^j]_{low} = P_k \times \frac{A^2}{s_{j_{max},k}^{\omega}} \tag{3}$$

where the minimum and maximum distances are $s_{j_{min},k}$ and $s_{j_{min},k}$ from T_k respectively (also shown in Fig. 1). The details of this procedure are given in [3].

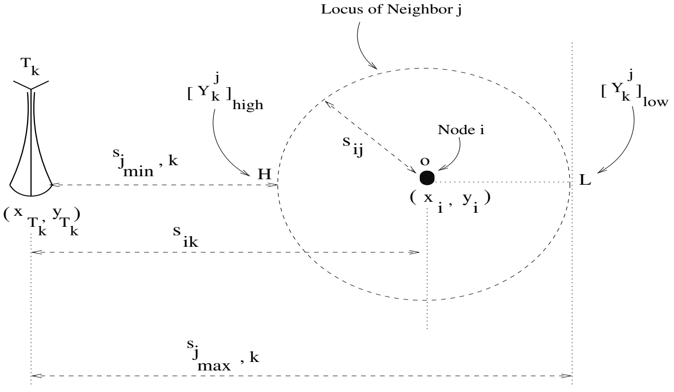


Fig. 1. Bounds of RSS on channel k of neighbor node j

Thus the predicted power vector for node j on channel k as calculated by i is given as
$P^j_{predict}$= $\big[\ ([\gamma^j_1]_{low}, [\gamma^j_1]_{high}), ([\gamma^j_2]_{low}, [\gamma^j_2]_{high}), \cdots,$
$([\gamma^j_K]_{low}, [\gamma^j_K]_{high})\big]$.

The inference drawn by node i for node j on channel k is given as

$$d^j_k|_{infer} = \begin{cases} 0 & \text{if both } [\gamma^j_k]_{low} \text{ and } [\gamma^j_k]_{high} \leq \gamma_{th} \\ 1 & \text{if both } [\gamma^j_k]_{low} \text{ and } [\gamma^j_k]_{high} \geq \gamma_{th} \\ X & \text{otherwise} \end{cases} \quad (4)$$

where X denotes that no inference could be drawn, and γ_{th} is the common threshold used by all nodes to decide if a channel is occupied or not.

A. Formation of Trust Evidence

The predicted occupancy vector, given the mutual distance between node i and j, is given as

$$D^j_i = [d^j_1|_{infer}, ..., d^j_K|_{infer}]; \quad d^j_k|_{infer} \in \{0, 1, X\} \quad (5)$$

We compare D^j_i from Eqn. (5) with received $B^j_{adv} = [d^j_1, .., d^j_k..d^j_K]$. We record the results of comparison in a vector *Trust Evidence* Q^k_j, where a match (denoted as α), a mismatch (denoted by β), and channels with value X in D^j_i are recorded as μ based on Eqn. (6): If Q^j_k is the result of the comparison, then

$$Q^j_k = \begin{cases} \alpha & \text{if } d^j_k|_{infer} = d^j_k \\ \beta & \text{if } d^j_k|_{infer} \neq d^j_k \\ \mu & \text{otherwise} \end{cases} \quad (6)$$

From Eqn. (6), for each channel k and for each neighbor j, we have one of three categories of outcomes: match, mismatch, undecided. We arrange the Q^j_k for all neighbors and look for total number of occurrences for each category with respect to channel k. The number of matches, mismatches and undecided observed for channel k are given by n_{α_k}, n_{β_k}, and n_{μ_k} respectively. Also, $n_{\alpha_k} + n_{\beta_k} + n_{\mu_k} = N_k$ equals the total number of opinions from N neighbors on channel k. Note this is equally valid for all nodes and therefore we drop the index i for the node concerned.

IV. Trust based Channel Preference

From the previous section, we get N_k independantly monitored observations on channel k, comprising one of the three possible outcomes per observation. We seek to obtain the Bayesian belief (also called subjective probability) of occurrence of each possible outcome known as *bayesian belief parameters* based on prior observations gathered from the observed trust evidence. With more observations, we update the Bayesian belief parameter for the hypothesis increasing the accuracy of the parameters. Since a match indicates a non-anomalous behavior, a channel with higher posterior belief for match is considered more trustworthy.

To model how node i can compute the belief on channel k, we use the observation counts to calculate the Bayesian estimate of each of the parameters. Since the following analysis is valid for any channel k, we drop the suffix k for simplicity. Let $X(\bar{\theta})$ denote the hypothesis described by the underlying unknown bayesian probability parameter of a random trial yielding match, mismatch or undecided as $\bar{\theta} = \{\theta_\alpha, \theta_\beta, \theta_\mu\}$. Here, θ_α, θ_β, and θ_μ are the unknown probability of $X(\bar{\theta})$ exhibiting a match, mismatch or undecided respectively. Since these observation outcomes are exhaustive and mutually exclusive, $\theta_\alpha + \theta_\beta + \theta_\mu = 1$. Let D_α, D_β, D_μ denote the random variables that represent the number of times, the outcomes α, β and μ occur. The observation data can be represented as random observation vector $D(N) = \{D_\alpha, D_\beta, D_\mu\}$ having a multinomial distribution with 3 tuple parameter described by θ_α, θ_β, and θ_μ.

Our objective is to estimate and update the probability parameters in $X(\bar{\theta})$ based on observation evidence $D(N)$ and prior information on the hypothesis parameter $\bar{\theta}$, itself. Since there is no information about $\bar{\theta}$ initially, we consider it to be uniformly distributed a-priori. Subsequent observations dictates how these parameters are updated. Our first step is to calculate the Bayesian estimate of $\bar{\theta}$.

First, we show the case of estimating belief that a match occurs (θ_α). Since in Bayesian inference, the assumption is that prior and posterior probability have the same distribution, we can formally define the probability parameters as:

$$\begin{aligned} P(X(\bar{\theta}) = \alpha|\bar{\theta}) &= \theta_\alpha \\ P(X(\bar{\theta}) = \beta|\bar{\theta}) &= \theta_\beta \\ P(X(\bar{\theta})) = \mu|\bar{\theta}) &= \theta_\mu \end{aligned} \quad (7)$$

This assumption is due to the well known fact that a Dirichlet distribution acts as a conjugate prior to multinomial distributions. Hence prior and posterior preserve the same form [11].

The observations data $D(N)$ can be treated as a multinomial distribution with probability parameter θ_α,θ_β, and $\theta\mu$, where the probability mass function is given by:

$$\begin{aligned} P(D_\alpha = n_\alpha, D_\beta = n_\beta, D_\mu = n_\mu|\bar{\theta}) &= P(D(N)|\bar{\theta}) \\ &= \frac{N!}{n_\alpha! n_\beta! n_\mu!} \theta_\alpha^{n_\alpha} \theta_\beta^{n_\beta} \theta_\mu^{n_\mu} \end{aligned} \quad (8)$$

Given this we can use Bayes theorem to calculate the posterior belief estimate on the event of a match $\hat{X}(\bar{\theta}) = \alpha$, given observation data $D(N)$ as:

$$P(\hat{X}(\bar{\theta}) = \alpha | D(N)) = \frac{P(\hat{X}(\bar{\theta}) = \alpha, D(N))}{P(D(N))} \tag{9}$$

Denominator of the above equation is the marginal probability that can be conditioned or marginalized on all possible outcomes for $\bar{\theta}$ and since probabilities are continuous

$$P(D(N)) = \int\limits_{D(N)(\bar{\theta})} P(D(N)|\bar{\theta}) f(\bar{\theta}) d(\bar{\theta}) \tag{10}$$

Since there is no prior information on $\bar{\theta}$ (before any observations) in Eqn. (10), we can assume it to be uniformly distributed such that $f(\bar{\theta}) = 1$ and we can put Eqn. (8) in Eqn. (10), and get

$$P(D(N)) = \frac{N!}{n_\alpha! n_\beta! n_\mu!} \int\limits_{D(N)(\theta_\alpha, \theta_\beta, \theta_\mu)} \theta_\alpha^{n_\alpha} \theta_\beta^{n_\beta} \theta_\mu^{n_\mu} d\theta_\alpha d\theta_\beta d\theta_\mu \tag{11}$$

For simplicity, let $\int\limits_{D(N)(\theta_\alpha, \theta_\beta, \theta_\mu)} \theta_\alpha^{n_\alpha} \theta_\beta^{n_\beta} \theta_\mu^{n_\mu} d\theta_\alpha d\theta_\beta d\theta_\mu = I_1$
To solve for I_1 we use the multivariate generalization of the Eulerian integral of first kind. Note that $D(N)(\theta_\alpha, \theta_\beta, \theta_\mu)$ denotes a space and we know that a space of $m(= 3)$ parameters has only $m - 1(= 2)$ degrees of freedom due to the additivity constraint $\theta_\alpha + \theta_\beta + \theta_\mu = 1$. Therefore when we integrate over this space, the integration has $m - 1 = 2$ dimensions. Hence

$$I_1 = \int_0^1 \int_0^{1-\theta_\alpha-\theta_\beta} \theta_\alpha^{(n_\alpha+1)-1} \theta_\beta^{(n_\beta+1)-1} (1 - \theta_\alpha - \theta_\beta)^{(n_\mu+1)-1} d\theta_\alpha d\theta_\beta \tag{12}$$

Eqn. (12) is a known form for the multivariate extension of the Beta function which in this case is defined as $B(n_\alpha + 1, n_\beta + 1, n_\mu + 1)$. The proof can be found in Lemma 2.4.1 of [6]. In general $B(\alpha_1, \cdots, \alpha_m)$

$$\begin{aligned} &= \int\limits_{D(x_1, \cdots, x_{m-1})} x_1^{\alpha_1 - 1} ... (1 - \sum_{i=1}^{m-1} x_i)^{\alpha_m - 1} dx_1 ... dx_{m-1} \\ &= \frac{\prod_{i=1}^{m} \Gamma(\alpha_i)}{\Gamma(\sum_{i=1}^{m} \alpha_i)} = \frac{\Gamma(\alpha_1) \cdots \Gamma(\alpha_m)}{\Gamma(\alpha_1 + \cdots + \alpha_m)} \end{aligned} \tag{13}$$

Using the above result, we can write Eqn. (12) as

$$\begin{aligned} I_1 &= B(n_\alpha + 1, n_\beta + 1, n_\mu + 1) \\ &= \frac{\Gamma(n_\alpha + 1)\Gamma(n_\beta + 1)\Gamma(n_\beta + 1)}{\Gamma(n_\alpha + 1 + n_\beta + 1 + n_\mu + 1)} \end{aligned} \tag{14}$$

Putting Eqn. (14) in Eqn. (11) we get:

$$P(D(N)) = \frac{N!}{n_\alpha! n_\beta! n_\mu!} \frac{\Gamma(n_\alpha + 1)\Gamma(n_\beta + 1)\Gamma(n_\beta + 1)}{\Gamma(n_\alpha + 1 + n_\beta + 1 + n_\mu + 1)} \tag{15}$$

Since the parameters in gamma functions $n_\alpha + 1$ etc. are all non zero positive values, we can use the result $\Gamma(z) = (z - 1)!$ to calculate Eqn. (15) as

$$P(D(N)) = \frac{N!}{(N+2)!} \tag{16}$$

Assuming conditional independence between the $\hat{X}(\bar{\theta})$, $D(N)$ and $\bar{\theta}$, we calculate the numerator of Eqn. (9), $P(\hat{X}(\bar{\theta}) = \alpha, D(N))$, as:

$$\begin{aligned} &= \int\limits_{D(N)(\bar{\theta})} P(X(\bar{\theta}) = \alpha, D(N)|\bar{\theta}) f(\bar{\theta}).d(\bar{\theta}) \\ &= \int\limits_{D(N)(\bar{\theta})} P(X(\bar{\theta}) = \alpha|\bar{\theta}) P(D(N)|\bar{\theta}) d(\bar{\theta}) \\ &= \frac{N!}{n_\alpha! n_\beta! n_\mu!} \int\limits_{D(N)(\theta_\alpha, \theta_\beta, \theta_\mu)} \theta_\alpha \theta_\alpha^{n_\alpha} \theta_\beta^{n_\beta} \theta_\mu^{n_\mu} d\theta_\alpha d\theta_\beta d\theta_\mu \\ &= \frac{N!}{n_\alpha! n_\beta! n_\mu!} \int\limits_{D(N)(\theta_\alpha, \theta_\beta, \theta_\mu)} \theta_\alpha^{n_\alpha+1} \theta_\beta^{n_\beta} \theta_\mu^{n_\mu} d\theta_\alpha d\theta_\beta d\theta_\mu \end{aligned} \tag{17}$$

The above integral has the same form as Eqns. (11), (12), and (13). Hence the integral portion of Eqn. (17) can be rewritten as

$$= \int_0^1 \int_0^{1-\theta_\alpha-\theta_\beta} \theta_\alpha^{(n_\alpha+2)-1} \theta_\beta^{(n_\beta+1)-1} (1 - \theta_\alpha - \theta_\beta)^{(n_\mu+1)-1} d\theta_\alpha d\theta_\beta$$

which can be solved using Eqn. (13).

Using the above result, Eqn. (17) can be simplified as

$$P(\hat{X}(\bar{\theta}) = \alpha, D(N)) = \frac{N!(n_\alpha + 1)}{(N+3)!} \tag{18}$$

Thus, Eqn. (9), can be solved by dividing Eqn. (18) by Eqn. (16), which gives

$$P(\hat{X}(\bar{\theta}) = \alpha | D(N)) = \frac{n_\alpha + 1}{N + 3} \tag{19}$$

Similarly, $P(\hat{X}(\bar{\theta}) = \beta | D(N)) = \frac{n_\beta + 1}{N+3}$ and $P(\hat{X}(\bar{\theta}) = \mu | D(N)) = \frac{n_\mu + 1}{N+3}$. These equations are the expressions for posterior belief of matches, mismatches, and undecided. For any channel k, we again use the suffix k, for example n_{α_k}. For simplicity of notations, we rewrite the left hand side of Eqn. (20) for channel k as $R_{\alpha_k} = \frac{n_{\alpha_k} + 1}{N_k + 3}$; $R_{\beta_k} = \frac{n_{\beta_k} + 1}{N_k + 3}$; and $R_{\mu_k} = \frac{n_{\mu_k} + 1}{N_k + 3}$ respectively. Of course, it can be verified that $R_{\alpha_k} + R_{\beta_k} + R_{\mu_k} = 1$ and it satisfies the Cromwell's rule.

A. Trust Updates

A node observes channels over several time slots. Let at any time t the number of matches, mismatches, and undecided for channel k are $n_{\alpha_k}(t)$, $n_{\beta_k}(t)$ and $n_{\mu_k}(t)$ respectively. The total number of neighbors advertising on channel k at time t is $N_k(t)$. The time window after which a trust update is made may vary depending on the user requirement and computational resource availability. The system under question may have selfish nodes that employ static attacks, where channels attacked remain the same over time, or a dynamic variation, where channel sets that are attacked may change with time. If we assume a dynamic variation of collaborative attack, then channel attacked in previous slot may not be attacked in subsequent slots, and since channel usage is based on the current spectrum scenario, the weightage to old observations should be minimal. Hence we propose an update model with high sensitivity to latest observations and low sensitivity to old observations. This not only addresses dynamic attacks but automatically consider static attacks.

We also recommend that the length of the window for a trust update should be small, so as to capture frequent changes in the attacked channel sets. However, it may also be noted that frequent changes in collaborative channel sets increase the cost of attack for the adversary. Hence it is unlikely that the channel sets attacked will be changed on every slot.

Let the current time slot be denoted as t_n. The updated belief corresponding to match on a channel k at time t_n is

$$R^{t_n}_{\alpha_k} = \frac{1 + \sum_{t=1}^{n} \lambda^{t_n - t}\; n_{\alpha_k}(t)}{3 + \sum_{t=1}^{n} \lambda^{t_n - t} N_k(t)} \tag{20}$$

where $0 < \lambda < 1$ is a sensitivity factor that determines the extent to which old observations are weighted. $t = 1$ denotes the oldest observation and $t = n$ denotes the latest. Smaller values of λ implies that old observations have less weight and vice-versa. $R^{t_n}_{\beta_k}$ and $R^{t_n}_{\mu_k}$ can be calculated in similar ways from Eq. (20).

B. Net Trust

To capture the effect of both the updated beliefs for matches as well as mismatches into a single parameter, we define *net trust* as the difference between $R^{t_n}_{\alpha_k}$ and $R^{t_n}_{\beta_k}$. More formally,

$$R^{t_n}_{net_k} = R^{t_n}_{\alpha_k} - R^{t_n}_{\beta_k} \tag{21}$$

Note, the range of $R^{t_n}_{net_k}$ lies between -1 and 1. We use net trust to rank channels from the best to worst. The greater the posterior belief for mismatch, the lesser is its net trust. This is consistent with the idea that mismatches indicate dishonest opinions. Hence we expect channels that were attacked to have significantly lower trust.

V. Simulation Model and Results

To validate the trust model and to compute the net trust for each channel, we simulate a distributed network over a 3000 × 3000 m grid. 20 primaries are considered; thus 20 channels. We consider a total of 30 (honest and malicious) mobile secondary nodes. The received power at each receiver depends on the path loss factor ω which was varied between 3 and 5. We show the results for different nodes that belong to different parts of the network. As for the update periodicity, we update the beliefs every 3 time slots which we refer to as a *window*. The sensitivity factor λ was kept at 0.2.

A. Trust Based Channel Preference

We consider 40% of the nodes as selfish which collaboratively attacked the channels $S = \{1, 3, 5, 7, 9, 11, 15, 16, 19\}$. The channels attacked remained static over time. In Fig. 2, we show the net trust of the channels sorted in an descending manner as calculated by an honest node 12. As expected, the 9 channels that were attacked have significantly lower trust values than others. For node 12, the best channel is 8 and the second best is 2. The worst channel is 19. Therefore, the fused decision on channel 8 can be trusted the most followed by 2 and so on. The strategy for node 12 will be to check whether channel 8 can be used to communicate with its intended receiver. If not, it will check channel 2 and so on.

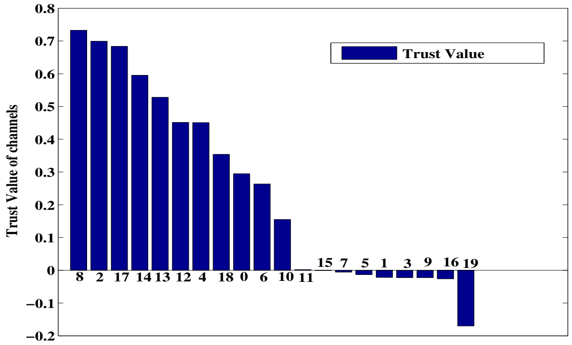
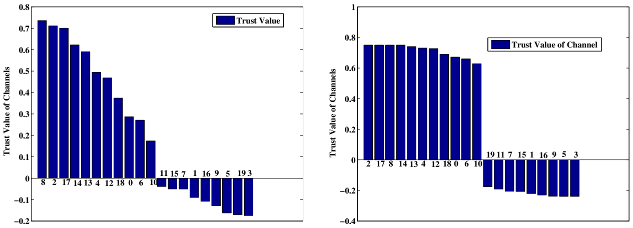


Fig. 2. Channel preference order by node 12 and $\omega = 3.5$

B. Channel Preference with more selfish nodes

Now, we set the number of selfish nodes to 60% of the total number of nodes i.e., 18. In Fig. 3(a), we show the net trust of the channels sorted in an descending manner as calculated by the honest node 14. As per most previous works, it is difficult to distinguish dishonest behavior when the adversary density is higher than 50% [10]. It is to be noted that node 14 is able to identify the 9 channels that were attacked inspite of the increased number of selfish nodes. The trust values for those channels are even lower– enabling a better differentiation of the channels. However, the order is different from what was observed by node 12 because of being at a different location. Fig. 3(b), shows that results hold true for a higher value of $\omega = 5.0$, which is applicable to dense urban scenarios.



(a)

(b)

Fig. 3. Channel preference of node no. 14 with 18 selfish nodes: (a) For $\omega = 3.5$ (b) For $\omega = 5.0$

C. Trust propagation under static attacks

In Fig. 4, we observe how trust values evolve over time with the proposed trust update model for static attacks. It clearly exhibits the difference between a channel that was attacked and a channel that was not. We consider two channels: one from the attacked channel set (i.e., 1) and another from the non-attacked channel set (i.e., 4). We plot the *weighted moving average* of the net trust after every 3 time slots. As time progresses, we see a clear difference in the trust values for channels 1 and 4.

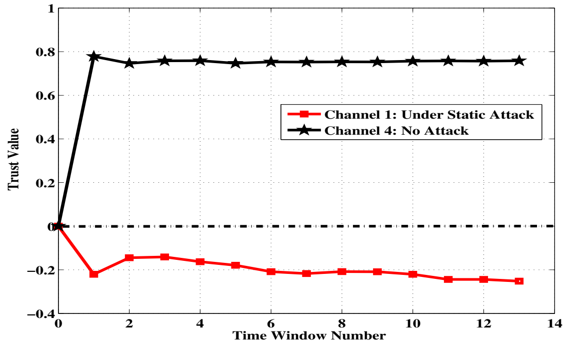


Fig. 4. Net trust for attacked and not-attacked channels

D. Effect of fraction of selfish nodes

We investigate how the trust values for channels vary with different fractions of selfish nodes. In Fig. 5, we show the average trust values for attacked channel set and the non-attacked channel set, for increasing number of attackers. As expected, there is hardly any change on channels that are not attacked, whereas, the average trust value for the channels that were attacked decreases. This result is in contrast with the commonly used voting schemes or Kullback-Leibler divergence based defense models that fail to detect anomaly when the number of attackers is more than 50%.

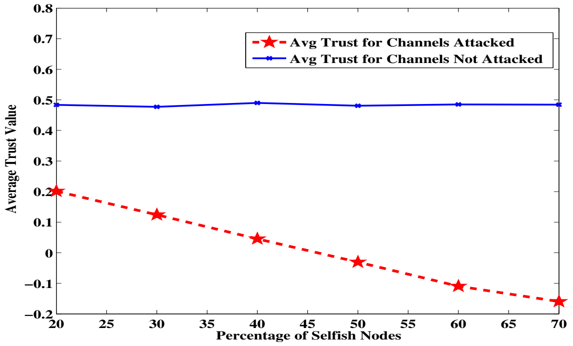
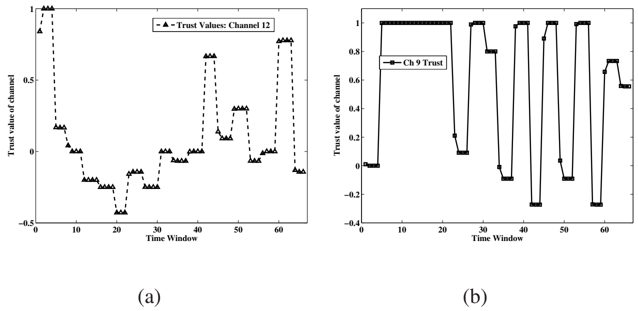


Fig. 5. Avg. trust with increasing number of selfish nodes

E. Trust variation under dynamic attacks

To prove that our model is able to capture the frequent changes in the attacked channel set, we vary the attacked channel set every 10 time slots on an average. We show how the net trust is updated for two specific channels (12 and 9) in Fig. 6(a) and Fig. 6(b) respectively. Note, the plots are shown in time windows (3 time slots = 1 window). These two representative channels were intermittently and randomly chosen by the coalition of selfish nodes. Trust of channel 12 starts with a high value for 10 time windows, but then attacked consistently for next 15 windows (i.e., 45 time slots); hence its trust exhibits a steady decrease. After that channel 12, is intermittently chosen for attack, which causes the rapid fluctuations of the trusts values. Channel 9 is not attacked for 22 windows then attacked for a few windows. Hence, its trust value is initially high followed by a sudden decrease which stays unchanged for 4 windows and then increases for the remaining windows.



(a)

(b)

Fig. 6. Net trust updates for dynamic attacks (a) Channel 12 (b) Channel 9

VI. Conclusions

In this paper, we address the importance of anomalies in advertised spectrum usage reports that could occur due to attacks by a coalition of selfish nodes Based on observations from the proposed monitoring techique, we presented a Bayesian inference model that can be used for deciding how much trustworthy the the collective decision on a channel is. We test our proposed method under static and dynamic variants of collaborative SSDF attack; results show that the channels that were attacked could be quantified based on the net trust metric. The net trust also allows a node to select the best channels based on the trustworthiness of the channel occupancy decision. We show how our model is able to distinguish among channels even when the population of selfish nodes is more than 50%– a shortcoming of most voting or entropy divergence based models.

References

[1] DARPA XG WG, The XG Architectural Framework V1.0, 2003.

[2] http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility /wifich2.html#wp1049544.

[3] S. Bhattacharjee, S. Debroy, M. Chatterjee, “Trust Computation through Anomaly monitoring in Distributed Cognitive Radio Networks”, *IEEE PIMRC*, 2011.

[4] S. Bhattacharjee, S. Sengupta and M. Chatterjee,“Vulnerabilities in Cognitive Radio Networks: A survey”, *Elsevier Journal of Computer Communications*, 36(2013), pp: 1387-1398.

[5] R. Chen, J.M. Park, K. Bian, “Robust Distributed Spectrum Sensing in Cognitive Radio Networks”, *IEEE INFOCOM*, pp. 1876-1884, 2008.

[6] K. Fang and Y.T. Zhang, “Generalized Multivariate Analysis”, *Springer-Verlag*, Pg. 47-49, 1990.

[7] A. Ghasemi, E. Sousa, Collaborative spectrum sensing for opportunistic access in fading environments, Proc. of IEEE DySPAN 2005, pp.131136.

[8] S.-W. Jeon, N. Devroye, M. Vu, S.-Y. Chung and V. Tarokh, “Cognitive networks achieve throughput scaling of a homogeneous network”, *IEEE Trans. Inform. Theory*, March 2008, Volume: 57, Issue: 8, 5103-5115.

[9] K. Pahlavan and P. Krishnamurthy,“Principles of Wireless Networks: A Unified Approach”, *Prentice Hall*, 2002.

[10] A.S. Rawat, P. Anand, H.Chen, P.K. Varshney, “Countering Byzantine Attacks in Cognitive Radio Networks”, *IEEE ICASSP*, 2010.

[11] Y.L. Sun, W. Yu, Z. Han and K.J.R. Liu,“Information Theoretic Framework of Trust Modeling and. Evaluation for Ad-Hoc Networks”, *IEEE J. Sel. Areas in Communications*, Feb. 2006, Vol: 24, pp. 305-317.

[12] E.C. Yeow, Y.C Liang. Y.L. Guan, Y. Zeng,“Optimization of Cooperative Sensing in Cognitive Radio Networks: A Sensing-Throughput Tradeoff View”, *Transactions on Vehicular Technology*, Vol. 58(9), 2009.