Routing-Toward-Primary-User Attack and Belief Propagation Based Defense in Cognitive Radio Networks

Zhou Yuan[†], Zhu Han[†§], Yan Lindsay Sun[‡], Husheng Li[♯], and Ju Bin Song[§]

[†]Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA

[‡]Department of Electrical and Computer Engineering, University of Rhode Island, Kingston, RI, USA

[♯]Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN, USA

[§]Department of Electronics and Radio Engineering, Kyung Hee University, Yongin, South Korea

Abstract

Cognitive radio (CR) networks have attracted many attentions recently, while the security issues are not fully studied yet. In this paper, we propose a new and powerful network layer attack, routing-toward-primary-user (RPU) attack in CR networks. In this attack, malicious nodes intentionally route a large amount of packets toward the primary users, aiming to cause interference to the primary users and to increase delay in the data transmission among the secondary users. In the RPU attack, it is difficult to detect the malicious nodes since the malicious nodes may claim that those nodes, to which they forward the packets, behave dishonestly and cause problems in the data transmission. To defend against this attack without introducing high complexity, we develop a defense strategy using belief propagation (BP). Firstly, an initial route is found from the source to the destination. Each node keeps a table recording the feedbacks from the other nodes on the route, exchanges feedback information and computes beliefs. Finally, the source node can detect the malicious nodes based on the final belief values. Simulation results show that the proposed defense strategy against the RPU attack is effective and efficient in terms of significant reduction in the delay and interference caused by the RPU attack.

Index Terms

Cognitive radio, security, routing toward primary user attack, belief propagation.

Corresponding author is Dr. Ju Bin Song. This work is partially supported by US NSF CNS-0905556, CNS-0910461, CNS-0953377, CNS-0643532, CNS-0831315, ECCS-1028782 and Korean KRF-20090075107.

I. Introduction

As wireless applications become increasingly sophisticated and widely used, the demand for more spectral resources is growing substantially. Recent spectrum measurement studies have shown that utilization of radio spectrum is quite low [1]–[5]. This is largely due to the traditional approach of exclusive allocation of portions of spectrum to specific wireless systems and services. Given that such spectrum is licensed over large regions and time spans, it is inaccessible to unlicensed wireless systems even if the licensed systems are under-utilizing the spectrum. In the process of finding a solution for supplying the limited spectral resources to the almost unlimited spectrum demand, one has to conceive new concepts for a more efficient way of using spectral resources. Cognitive radio (CR) is a revolutionary technique that allows secondary user (SU) wireless devices to use spectrum holes left by idle primary users (PUs). A cognitive radio wireless network can be seen as a multichannel multiaccess network. In CR wireless networks, wireless routers work as secondary users that can opportunistically utilize various spectral holes for communications without causing interference to the primary users. For distributed cognitive radio networks, the network is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining connectivity, as shown in some recent work [6]–[14].

Although CR wireless networks have so many advantages, most CR networks do not offer sufficient security. Many of the security challenges are due to the fact that the networks inherently rely on cooperation among distributed entities, such as collaborative sensing and multi-hop routing. Cooperation can be fragile under malicious attacks. Many attacks have been discovered for cognitive radio based networks, such as common control channel denial of service (CCC-DoS) [15], primary user emulation (PUE) attack [16], reporting false sensing data (RFSD) attack [17], reporting false selection frame (FSF) attack [18], and false evacuation (FE) attack [19].

In this paper, we introduce a new and powerful network layer attack in cognitive radio networks: routing-toward-primary-user (RPU) attack. In the RPU attack, the malicious nodes intentionally route a large amount of packets toward or around the primary users, aiming to cause interference to the primary

users and to increase delay in data transmission along the CR routes. In this attack, even if the interference from a single CR device to the primary users is not severe, the aggregate effects from many cognitive radio devices transmitting at the same time around the primary users can be significant, which can largely impair the primary users' performance. Furthermore, the interference to the primary users is not directly generated by the malicious nodes. Instead, the interference is from the honest nodes that received the packets from the malicious nodes. In other words, malicious nodes "neutralize the route by the hands of the others." Therefore, it is difficult to detect the malicious nodes.

Besides raising the awareness of the RPU attack and demonstrating its damage, we develop a defense strategy based on belief propagation (BP) against the RPU attack. Firstly, an initial route will be found from the source to the destination without knowledge of the malicious nodes. Each node on the route will keep a table recording the feedback information from the other nodes on the route. Then, every node exchanges the feedbacks with its neighboring nodes and computes beliefs. After this belief propagation converges, the source node can detect the malicious nodes based on the final belief values. Finally, the source node will re-route data packets to the destination, avoiding the detected malicious nodes. The underlying reason for applying BP is to reduce the inherit complexity for such defense mechanism. Simulation results show that the proposed scheme is efficient and effective to detect the RPU attackers.

The paper is organized as follows. Section II introduces related works for attack and defense in CR networks. Section III states the RPU attack model and the problem formulation. In Section IV the defense strategy is developed. Finally, simulation results and conclusions are given in Section V and Section VI, respectively.

II. Related Work

New mechanism of spectrum access in cognitive radio systems brings many new dimensions of vulnerabilities. There have been several types of attacks discovered in cognitive radio networks, as follows:

(1) Physical layer attacks: *Primary user emulation* (PUE) is an attack that malicious nodes emulate the feature of primary user's signal characteristics and transmit in available spectrum [16], [20], [21].

Then normal secondary users may believe primary user is present and avoid using the actually available spectrum holes. Another physical layer attack, which is called *reporting false sensing data* (RFSD), has also been discovered against collaborative spectrum sensing protocols [17]. Collaborative spectrum sensing is recognized as an efficient method to cope with the problem of unreliability in single-user spectrum sensing, and the malicious secondary users can report false sensing data to cause false alarm or miss detection in the decision made by the fusion center.

(2) MAC layer attacks: Malicious users can launch *denial of service* (DoS) attack on common control channel by sending superfluous packets, such that legitimate secondary users have less chance to find common available channels and therefore, less chance to communicate with each other. In another attack, which is called *reporting false selection frame*, when two secondary users want to establish communication channel, the sender first sends a free channel list (FCL) frame to the receiver, then the receiver will respond with a SELection (SEL) frame to indicate the data channel they are going to use. Upon receiving the SEL frame, the sender will notify its neighbors of the channel selection via a channel reservation message (RES frame). In this process, a selfish secondary user may always claim that there is no available channel and refuse to forward package for the other nodes [18]. A third MAC layer attack is called *false evacuation* [19]. If the primary user turns on while secondary users are transmitting, secondary users need to evacuate the channel through an evacuation protocol. A malicious node can attack the evacuation protocol by sending false warning information to other secondary users, to force evacuation even if the primary user is off.

(3) Network layer attacks: In *blackhole* attack, which is a redirection attack, attacker induces the source node to choose a route through the attacker and the attacker can then misuse, eavesdrop or drop messages as it sees fit [22]. *Wormhole attack* is another kind of redirection attack, in which two colluding attackers have a high speed link between them. This will make other nodes wrongly believe that the path between the colluding attackers is much shorter than other paths. The colluding attackers can then attract a large amount of data traffic, which causes congestion or facilitates data manipulation and traffic analysis [23].

Another network layer attack is called *sybil attack*, in which a malicious node behaves as if it were a larger number of nodes, for example by impersonating other nodes or simply by claiming false identities, aiming to gain a disproportionately large influence in the network [24]. There are also some other attacks in the network layer, most of which are the same as the attack models in wireless mesh/sensor/ad hoc networks, without considering much about the CR system model and existence of the primary users. The RPU attack proposed in the next section is also a redirection attack, but it is different from the above attacks. In the framework of the cognitive radio network, the RPU attack can not only cause data transmission failure, but also degrade the primary users' performance. Instead of causing problems to the networks by the malicious node itself, it makes the honest node unintentionally hurt the network, which makes the attacker difficult to be detected.

III. RPU Attack Model and Problem Formulation

A. RPU Attack Model in CR Networks

In the RPU attack, malicious nodes send fake routing information, claiming that they have optimum route with low costs, which will cause other honest nodes to route data packets through those malicious nodes. For example, using a simple shortest path routing algorithm[1] and assuming that there is only one malicious node, this malicious node may claim that the cost between itself and a secondary user, which is very close to the primary user, is very low. In this way, the honest nodes will forward data packets to this malicious node and all traffic will be routed through the attacker.

As shown in Fig. 1, n_S, n_D, n_1, n_2 and n_3 are secondary users, and n_S and n_D represent source and destination nodes, respectively. The shaded region is the footprint of a primary user. Since secondary node[2] n_3 is inside this region, it is forced to be turned off at a specific time slot. Note that because

[1]The RPU attack is not limited for the shortest path routing algorithm, but also for other routing algorithms, like QoS routing, etc. In any routing algorithm, the malicious node can suggest to forward the packets to a node that is closer to the primary users to reduce QoS.

[2]In this paper, "secondary user", "secondary router", and "secondary node" are interchangeably used.

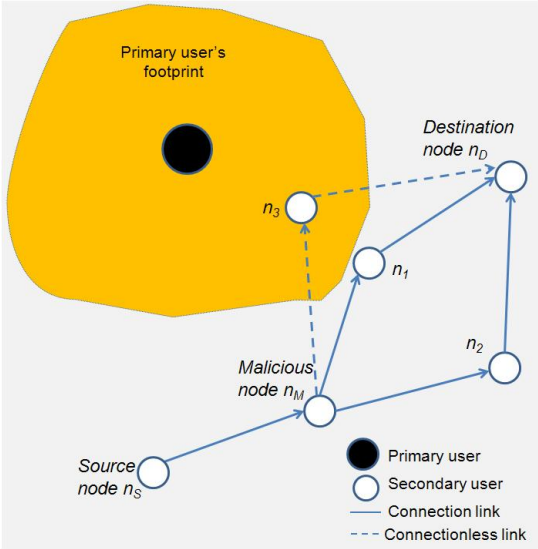

Fig. 1. Illustration of the RPU attack.

of channel fading, primary users' footprint can change and have different shapes at different time slots. Therefore, each secondary node has a probability to be out of the primary user's footprint. If its distance to the primary user is shorter, it will have a higher probability to be inside the primary user's footprint and be turned off. In Fig. 1, when source node n_S wants to transmit some packets to destination node n_D, since malicious node n_M claims that it has the shortest path to destination node n_D, source node n_S will forward all the packets to node n_M. Then node n_M tries to forward the data to node n_1, which is closer to the primary user compared to node n_2, even though node n_M knows clearly that node n_2 can also help to forward the packets. This has two consequences. First, the interference to the primary user along the route $n_M \rightarrow n_1 \rightarrow n_D$ is higher than the route $n_M \rightarrow n_2 \rightarrow n_D$. Second, since node n_1 is closer to the primary user and has a higher probability to be inside the primary user's footprint, it may be turned off more frequently and a larger transmission delay may occur. In the RPU attack, the malicious node itself can be at any location and it does not need to be close to the primary users. In other words, the malicious nodes are not the nodes that directly cause interference to the primary users or introduce long delay in data transmission. As a consequence, the source node cannot easily identify

which node is a bad guy since the malicious node can argue that those nodes, to which it forwards the packets (i.e. node n_1 in this example), behave dishonestly and cause problems in data transmission.

We need to emphasize that the RPU attack is different from many known attacks in the literature. The RPU attack can not only cause data transmission failure, but also degrade the primary users' performance. Moreover, in the proposed RPU attack, instead of causing problems to the networks by the malicious node itself, the malicious node makes the honest nodes unintentionally hurt the network. As a consequence, the malicious nodes can be pretty covert and difficult to detect.

B. Channel Model

In cognitive radio wireless networks, secondary users need to sense the spectrum to see whether the spectrum is occupied by the primary users or not to avoid the interference with the primary users' transmissions. When a primary user $k_j \in \mathcal{K}$ is transmitting, the received signal at secondary user $n_i \in \mathcal{N}$ can be modeled as:

$$y_{n_i} = \sqrt{P_{t,k_j} K d_{n_i,k_j}^{-\alpha_{pl}}} h_{n_i,k_j} x_{n_i,k_j} + w, \tag{1}$$

where P_{t,k_j} is the transmitted signal power from primary user k_j, K is a constant that depends on the antennas design, d_{n_i,k_j} is the distance between secondary user n_i and primary user k_j, α_{pl} is the path loss constant, x_{n_i,k_j} is the transmitted data with unit power, h_{n_i,k_j} is the channel fading gain, and w represents the noise. The channel fading of any link is modeled as an independent zero mean circularly symmetric complex Gaussian random variable with unit variance. Therefore, the received primary user k_j's signal power at secondary user n_i can be defined as

$$P(d_{n_i,k_j})_{n_i} = |h_{n_i,k_j}|^2 K d_{n_i,k_j}^{-\alpha_{pl}} P_{t,k_j}. \tag{2}$$

In this paper, we consider the system performance in terms of the probability that the received power at secondary user n_i from primary user k_j falls below a certain threshold P_τ, which means the spectrum is available for secondary user n_i. Therefore, n_i can be turned on and communicate with other secondary users in the CR networks causing negligible errors in primary user k_j's transmission. The power threshold

P_τ is determined by secondary user n_i according to application scenarios and the transmitter/receiver structure. Only when the received primary user's power is lower than this threshold, could the second users transmit. The probability that secondary user n_i can be turned on is defined as

$$\mathcal{P}_{on,n_i} = \mathcal{P}\left[P(d_{n_i,k_j})_{n_i} \leq P_\tau, \forall_{k_j}\right], \tag{3}$$

in which we need to consider the received power from any primary user $k_j \in \mathcal{K}$. Therefore, the probability that secondary user n_i can be turned on is calculated as [25]

$$\mathcal{P}_{on,n_i} = \prod_{k_j \in \mathcal{K}} \left[1 - \exp\left(-\frac{P_\tau d_{n_i,k_j}^{\alpha_{pl}}}{K P_{t,k_j}}\right)\right]. \tag{4}$$

From (4), we can see that when the distance between a secondary user and a primary user increases, the probability that this secondary user can be turned on also increases, since it has a lower probability to interfere with primary users' transmissions.

C. Routing Cost for Secondary User

Shortest path routing algorithm can be used for routing among secondary users in CR wireless networks [26], which has been proved to be effective and efficient. The cost of each direct link can be defined considering the delay, which is inverse proportional to the capacity. In addition, we need to consider the availability of each link. When the capacity of the link is higher and the probability of the secondary nodes along the link being available is higher, the cost of the link is lower. Considering a geometric distribution, the probability that secondary user n_i is not available until the m^{th} trial is $(1-\mathcal{P}_{n_i})^m \mathcal{P}_{n_i}$, and the expectation is calculated as $\frac{1-\mathcal{P}_{n_i}}{\mathcal{P}_{n_i}}$, where $\mathcal{P}_{n_i}$ represents the probability of availability of secondary user n_i on each trial. Therefore, the cost $\mathcal{C}_{n_{i_1},n_{i_2}}$ for edge (direct link) $e_{n_{i_1},n_{i_2}}$ can be defined as

$$\mathcal{C}_{n_{i_1},n_{i_2}} = \frac{1}{c_{n_{i_1},n_{i_2}}} \frac{1-\mathcal{P}_{n_{i_1}}}{\mathcal{P}_{n_{i_1}}}, \tag{5}$$

where $c_{n_{i_1},n_{i_2}}$ is edge $e_{n_{i_1},n_{i_2}}$'s capacity. Consequently, from (4), the final cost for edge $e_{n_{i_1},n_{i_2}}$ is

$$\mathcal{C}_{n_{i_1},n_{i_2}} = \frac{1}{c_{n_{i_1},n_{i_2}}} \frac{1 - \prod_{k_j \in \mathcal{K}} \left[1 - \exp\left(-\frac{P_\tau d_{n_{i_1},k_j}^{\alpha_{pl}}}{K P_{t,k_j}}\right)\right]}{\prod_{k_j \in \mathcal{K}} \left[1 - \exp\left(-\frac{P_\tau d_{n_{i_1},k_j}^{\alpha_{pl}}}{K P_{t,k_j}}\right)\right]}. \tag{6}$$

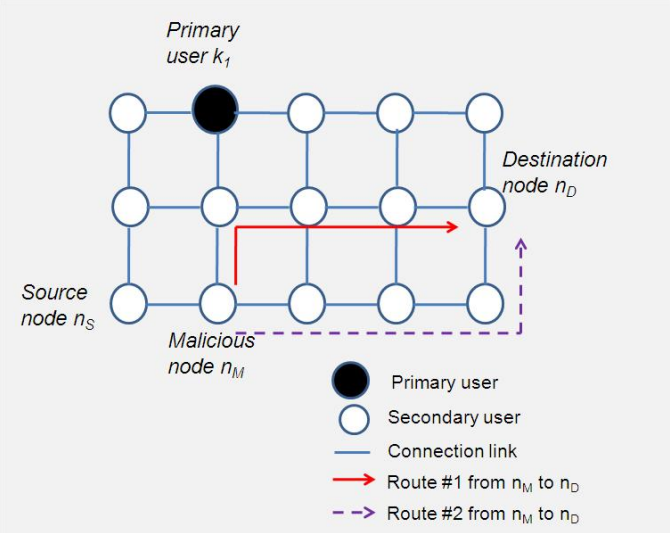

Fig. 2. Toy example.

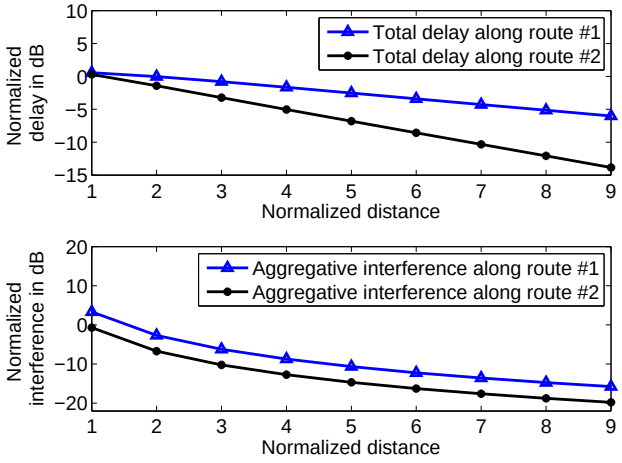

Fig. 3. Effect of the RPU attack for the toy example.

D. Strength of the RPU Attack: A Toy Example

To demonstrate the strength of the proposed attack, a toy example is studied, which is illustrated in Fig. 2. All of the nodes are located in a grid topology, and we assume that each link has a unit capacity no matter what the length of each link is. The black node is the primary user and white nodes are secondary

cognitive radio devices. Source node n_S wants to transmit data to destination node n_D. The malicious node n_M can attract all the traffic from n_S and route the data towards the primary user (i.e. forwarding data to the nodes that are close to the primary users). There are two different routes from n_M to n_D, with the same number of hops, labeled as route 1 and route 2, shown in Fig. 2. Considering the position of the primary user, those two routes have different delays and different amount of interference to the primary user.

We simulated the data transmission using route 1 and route 2, respectively, and the simulation results are shown in Fig. 3. We used the similar simulation setup as in Section V. X-axis is the length of each link, and the y-axis represents the total delay and the aggregative interference respectively. Even though both routes have the same number of hops, they have different delays and different aggregative interference. Because route 1 is closer to the primary user, the total delay and interference is much higher than that of route 2. This example effectively demonstrates the damage of the RPU attack, in which attackers make the worse route (i.e. route 1) being chosen.

E. Routing Problem Formulation

Each source and destination pair will decide which route to choose. Because of some intermediate malicious nodes, which will try to forward the packets toward primary users and cause large delay in data transmission, the problem can be formulated as minimizing the delay through the route. For source-destination pair l, the utility function U_l can be calculated as

$$U_l = \sum_{e_{n_{i_1},n_{i_2}} \in R_l} \mathcal{C}_{n_{i_1},n_{i_2}}, \tag{7}$$

where R_l is one possible route for the source and destination pair l. The physical meaning of the utility function is the summation of delays along the route from the source to the destination. Therefore, the problem can be mathematically formulated as:

$$\min_{l} \; U_l. \tag{8}$$

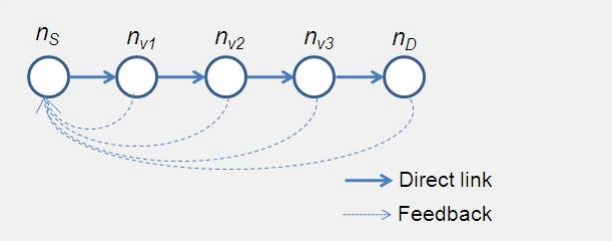

Fig. 4. Illustration of the defense strategy against RPU attack.

Notice that the same philosophy proposed in this paper can be used for other type of routing mechanisms in a similar way.

IV. Defense Strategy Using BP

In this section, we present the defense strategy for the RPU attack. Firstly, for indirect links in cognitive radio networks, the shortest path algorithm will be used to find the initial route from the source to the destination, without considering whether there are malicious nodes on the route or not. Clearly, the initial route is a directed acyclic graph G with a set of nodes on the route indexed by $v \in V$. Using the concept of chain, for any node on the route, all its descendant nodes are called the nodes "after" it in the graph G. For example, in Fig. 4, n_{v_2}, n_{v_3} and n_D are the nodes "after" node n_{v_1}, while the source node n_S is not "after" n_{v_1}. In order to find possible malicious nodes, each node on the route will send a certain amount of initialization packets to the nodes "after" it, and collect the feedback information from the nodes "after" it. The feedback information is also called m value, which is authenticated and encrypted, and cannot be modified by malicious nodes. Then each node will keep a table recording the feedbacks from all the nodes that are "after" it on the route. Clearly, the source node will keep the records of the feedbacks from all other nodes on the route.

In a single-user decision making, only the local observation is used. To detect the malicious nodes, all neighboring nodes need to communicate with each other and exchange the feedbacks. A simple flooding strategy can be used, but the computation complexity and signaling overhead can be significant. To

overcome this problem, we will use BP [28]–[30], which is an efficient way to calculate the marginal distribution and can avoid the involvement of other secondary nodes that are not on the initial route.

In the general framework of BP, the joint probability for the unknown variable X_v is defined as

$$\mathcal{P}(\{X_v\}) = \prod_{v=1}^{V} \phi_v(X_v) \prod_{v \neq w} \psi_{vw}(X_v), \tag{9}$$

where ψ_{vw} is called compatibility function and ϕ_v is called local function. In our case, we denote by X_v the state of node v. When $X_v = 1$, it is an honest node; otherwise, $X_v = 0$.

Our goal is to compute the marginal probabilities of each node, which can be mathematically defined as sums over all possible states of all its parents. For example, for node n_{v_1} in Fig. 4, we can have

$$\mathcal{P}(n_{v_1}) = \sum_{n_{v_2}} \sum_{n_{v_3}} \sum_{n_D} \mathcal{P}(n_{v_2}, n_{v_3}, n_D). \tag{10}$$

We call this marginal probability "beliefs", and denote the belief at node v by b_v. A Bayesian network is a probabilistic graphical model that represents a set of random variables and their conditional dependencies. For small Bayesian networks, we can easily do marginalization sums directly. Nevertheless, when the number of nodes in the network increases, the number of terms in the sums will grow exponentially. This means that it is unreliable to do marginalization sums directly in large Bayesian networks. Therefore, we will use BP to compute marginal probabilities, which grows only linearly with the number of nodes.

BP can be used to compute marginal probability of node v iteratively. In the *l*-th iteration, node w sends a feedback $m_{wv}^{l}(X_v)$ to node v, which can be given by

$$m_{wv}^{l}(X_v) = \sum_{X_w} \psi_{wv}(X_w, X_v) \phi_w(X_w) \prod_{u \neq w,v} m_{uw}^{l-1}(X_w). \tag{11}$$

Intuitively, m_{wv}^{l} means the belief about the state of node w tested by node v.

In each iteration, each node computes its belief, based on the equation proposed in [31]:

$$b_v(X_v) = k_v \phi_v(X_v) \prod_{w \neq v} m_{wv}^{M}(X_v), \tag{12}$$

where k_v is a normalization constant and $m_{wv}^{M}(X_v)$ denotes the feedback from node w to node v about what state node w should be in.

Theorem 1: In the graph of chain, BP converges and gives the exact marginal probabilities.

Proof of Theorem 1 is provided in Appendix.

Based on Theorem 1, for the initial route in our case, which is a chain, we can have

$$b_v(X_v) = p(X_v). \tag{13}$$

If the final belief for a node is higher than a threshold, denoted by b_τ, this node is an honest node. In contrast, if the final belief for a node is lower than a threshold b_τ, this node can be seen as a malicious node. Therefore,

$$v = \begin{cases} \text{honest}, & b_v \geq b_\tau; \\ \text{malicious}, & b_v < b_\tau. \end{cases} \tag{14}$$

Note that each node only needs to send one packet to each of the other nodes "after" it. This packet is just used to initialize a feedback request from all the other nodes "after" it. The feedback packet is calculated using Eq. (11). In our specific problem, the feedback only contains an "m" value between 0 and 1. So the packet size is very small. Therefore, we can see that the overhead of communication is very low. Moreover, we want to emphasize that these transmissions only happen in order to catch the malicious node, and do not happen normally. In addition, one of the advantages of BP is that when there are many observations in each round of the detection, BP can automatically aggregate the observations into a much lower dimensional space of parameters to reduce the curse of dimension. In our proposed algorithm, only one parameter needs to be exchanged between the users in each message, while the direct observation exchange may incur substantial communication overhead. So the communication complexity of BP is only a linear function of the number of nodes on the route, i.e., $O(N)$.

A. Local Function

The feedback information can be defined as the probability that whether this node is an honest node or not. First, let us define the link quality between two nodes, which can be described by a *trust value* that represents how much a wireless link can be trusted to deliver packets correctly in the routing problem

[27]. Trust value (link quality) of each link can be represented in the form of Beta function, which is often used in the scenarios where one node has collected binary observation about the other node. Assume that node n_{v_a} and node n_{v_b} are in each other's direct transmission range and node n_{v_a} sends a certain amount of packets to node n_{v_b}. Assume that $\alpha - 1$ packets from node n_{v_a} are received by node n_{v_b} successfully and $\beta - 1$ packets fail to arrive at node n_{v_b}, then the qualify of link $e_{n_{v_a},n_{v_b}}$ can be represented as

$$B(\alpha, \beta)_{e_{n_{v_a},n_{v_b}}} = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}, \tag{15}$$

where Γ is the gamma distribution, and a Bernoulli distribution with parameter p governs whether transmissions success or fail. In other words, the probability that n_{v_b} successfully forward packets is denoted by p. The mean and variance of the $B(\alpha, \beta)$ can be calculated as

$$\mu = \frac{\alpha}{\alpha+\beta}; \sigma = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}. \tag{16}$$

A probability density function of this type expresses the uncertainty that future interactions will success or fail. The cumulative distribution function (CDF) of Beta distribution is defined as

$$F(p; \alpha, \beta) \quad = \quad I_p(\alpha, \beta) = \sum_{j=\alpha}^{\alpha+\beta-1} \frac{(\alpha+\beta-1)!}{j!(\alpha+\beta-1-j)!} p^j (1-p)^{\alpha+\beta-1-j}, \tag{17}$$

where $I_p(\alpha, \beta)$ is called regularized incomplete Beta function. If we set a threshold p_τ for the Bernoulli parameter p in the CDF function, then the local function can be defined as

$$\phi_v = 1 - F(p \geq p_\tau; \alpha, \beta). \tag{18}$$

The physical meaning of the local function is the probability that the node who sends back the feedback is an honest node or not. Obviously, we have $0 \leq \phi_v \leq 1$, and the lower value of ϕ_v, the higher probability this node is a malicious node. Fig. 5 shows the cumulative distribution functions (CDF) of Beta distribution for the two cases $\alpha = 2, \beta = 2$ and $\alpha = 10, \beta = 10$. Although in these two cases, they have the same mean value of $\frac{\alpha}{\alpha+\beta} = 0.5$, the variance in the second case is much smaller than that in the first case (since the number of observations is more). Therefore, the CDF curves are different. If we set an appropriate threshold for the Bernoulli parameter p, e.g. 0.4 in Fig. 5, the probability of success

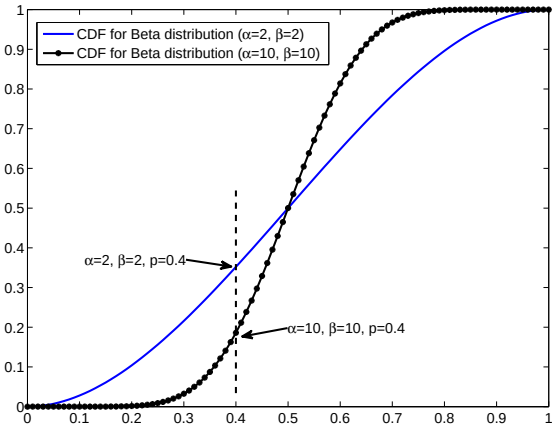

Fig. 5. Comparison of the CDF curves for different α and β parameters.

transmission in the second case is higher than in the first cases, considering there are more trials in the second case. In addition, with the increasing of the values of α and β, as well as the ratio between α and β, the success rate increases, which means that the probability that this node is a malicious node will decrease, and the local function ϕ_v will increase.

B. Compatibility Function

It is prohibitively difficult to find an explicit expression for the compatibility function $\psi_{wv}(X_w, X_v)$, and we can only propose a heuristic one. We notice that $\psi_{wv}(X_w, X_v)$ is dependent on the correlation between states X_w and X_v. If X_w and X_v are highly positively correlated, i.e., they tend to be the same, $\psi_{wv}(X_w, X_v)$ should yield a large probability for $X_w = X_v$ and a small probability for $X_w \neq X_v$. Therefore, we propose to use the following simple compatibility function, which is given by

$$\psi_{wv}(X_w, X_v) = \begin{cases} \eta, & X_w = X_v, \\ 1-\eta, & X_w \neq X_v, \end{cases} \tag{19}$$

where $0.5 < \eta < 1$ is a predetermined value. The larger η is, the more correlation between neighboring nodes we assume. [3]

C. Complete Algorithm

Algorithm 1 Complete defense algorithm using belief propagation

1: Using shortest path routing algorithm to obtain an initial route from the source to the destination.
2: Each node on the initial route keeps a table recording feedbacks from the nodes "after" it.
3: **for** Each iteration **do**
4: Each node computes the local function using (18) and the compatibility function using (19).
5: Each node computes m values using (11).
6: Each node exchanges m values with neighbors.
7: Each node computes its belief using (12).
8: **end for**
9: The source node detects the malicious nodes according to final beliefs.
10: Using shortest path algorithm to find a new route avoiding those malicious nodes.

The complete routing algorithm is summarized in Algorithm 1. In the first step, for a given source and destination pair, using shortest path routing algorithm[4] with cost function defined in (6), a path can be found, which may include some malicious nodes. In the second step, each node on the initial route keeps a table used for recording feedbacks from other nodes on the route. Each feedback is just one calculated *m* value (see Equation 11). The memory for each node to keep the table is proportional to the size of the number of the nodes on the route, which makes the overhead very low. In addition, considering the

[3]A reasonable value of η can be adjusted considering the possibility of bad-mouthing attacks, which is beyond the coverage of this paper [33].

[4]In this paper, we are just using the shortest path routing algorithm as an example, and other routing algorithms can be employed in a similar way.

fact that BP only grows linearly with the number of nodes, therefore, the computation complexity of our algorithm is also very low. From step 3 to step 7, in an iterative way, each node on the route will carry out the measurements and calculates the local functions, as well as the compatibility functions. Each node will then send some packets to the nodes "after" it, and collect the feedback information (i.e. m values) from all those nodes. They will also exchange feedbacks with the neighboring nodes and compute belief values until convergence. As a result, in step 9, the source node will detect the malicious according to final beliefs. If the final belief values of some nodes are below a threshold, those nodes will be seen as malicious nodes. Finally, in step 10 the shortest path algorithm will be used to find a new route from the source to the destination, avoiding those malicious nodes.

V. Simulation Results and Analysis

In this section, we present the simulation results. We use Matlab to simulate the CR network, in which 1 primary user and 500 secondary cognitive devices are randomly deployed in a 100 meter-by-100 meter area. The maximum transmission range for each secondary user is 20 meters, and the path loss factor is set to be 2.5. The noise variance is set to be 0.01, the transmit power is set to be 1W, the parameter K is set to be 1, SNR threshold γ_{k_j} is set to be 10dB, Beta CDF threshold p_τ is set to be 0.8, η in the compatibility function and the belief threshold b_τ are set to be 0.7 and 0.3, respectively.

Figure 6 shows the simulation results for one snap shot. The primary user is located at $(40m, 60m)$, and the source and the destination nodes are located at $(70m, 5m)$ and $(90m, 90m)$ respectively. We can see that in Fig. 6, there is a blank region around the primary user, which represents the footprint of the primary user. The footprint depends on the fading channel model, and any secondary user that is inside this region is blocked to avoid interference to the primary user. Only the secondary users that are outside the footprint of the primary user are allowed to be turned on, shown as the black dots in Fig. 6. There is only one malicious node in this case, which is located at $(75.52m, 17.30m)$. If all the nodes behave honestly, the source will find the route as shown in the red dashed path on the right. However, if the malicious node behaves dishonestly, it will route the packets to the node located at $(65.49m, 25.71m)$,

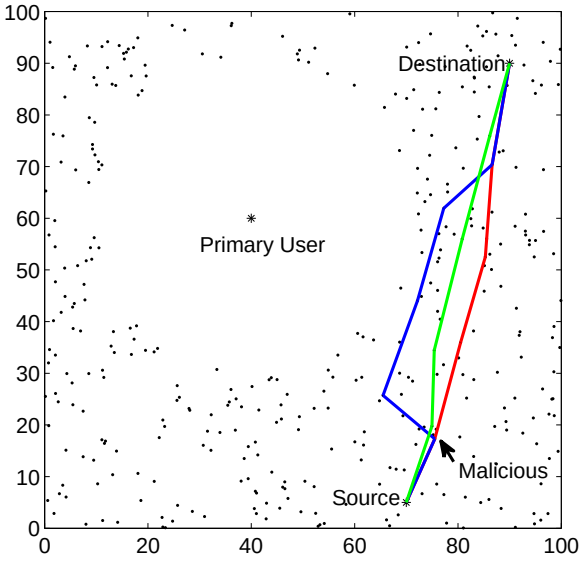

Fig. 6. One snap shot of simulated topology from source to destination. 1 primary user and 500 secondary users are randomly deployed in a 100 meter-by-100 meter area. From the left to the right, the three routes from the source to the destination represent the three cases that the malicious node attacks the network, after the malicious node is detected, all the nodes behave honestly, respectively.

which is close to the primary user, shown as the blue dashed route on the left. After the source node detects the malicious node using the proposed defense strategy, it will adjust the path, shown as the solid route, which avoids the malicious node.

Figure 7 shows the simulation results for the case that there is only one malicious node on the route from the source to the destination. The x-axis represents iterations and the y-axis represents belief values. From the top down, the curves represent the belief of source node, belief of honest intermediate node #1, belief of honest intermediate node #2, and belief of the malicious node, respectively. We can see that the convergence for belief propagation is within a couple of loops. We can also find that for the source node, the belief value will converge to 1, and for the other two honest intermediate nodes, their belief values converge to a value above 0.5. However, for the malicious node, the final belief value will be at

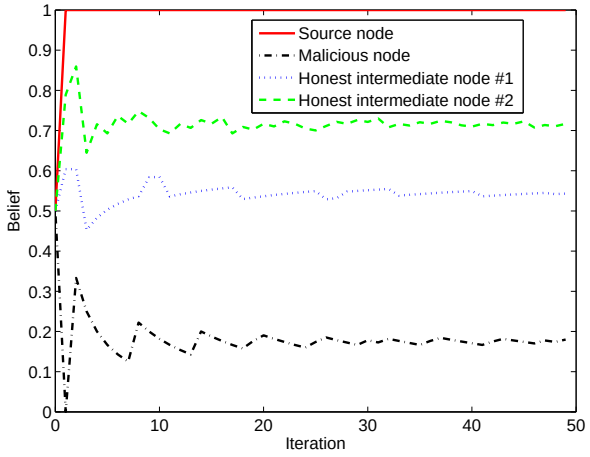

Fig. 7. Simulation results about the beliefs over iterations for four different secondary nodes. X-axis represents the iteration and Y-axis represents the belief value. We can see that the final belief of the malicious node is only about 0.2, while the beliefs of the other honest nodes are all above 0.5.

around 0.2. In this way, we can set a belief threshold of 0.3, and the malicious node can be detected easily. In addition, for the case if there are more than one malicious node on the initial route, based on simulation results, only the first malicious node "after" the source on the route can be detected, while the final belief values of other malicious node "after" the first malicious node may be above the threshold. To avoid the first malicious node, the source will re-route and get a new path to the destination. There is a high probability that those malicious nodes "after" the first malicious node on the initial route will not be on the new route. If some malicious nodes are still on the new route, the source node needs to perform detection again. Therefore, to make sure that we can avoid all malicious nodes, we need to run a certain number of iterations. As far as the final beliefs of all the nodes on the route are above the threshold, we can stop the iteration and know that all the nodes on the route are honest nodes. This does not mean that the system performance or the routing speed is degraded. After finding the malicious nodes, all nodes can keep a table recording the information of malicious nodes and exchange the information with honest neighboring nodes. Therefore, in the future when some nodes want to find a path to other nodes, they

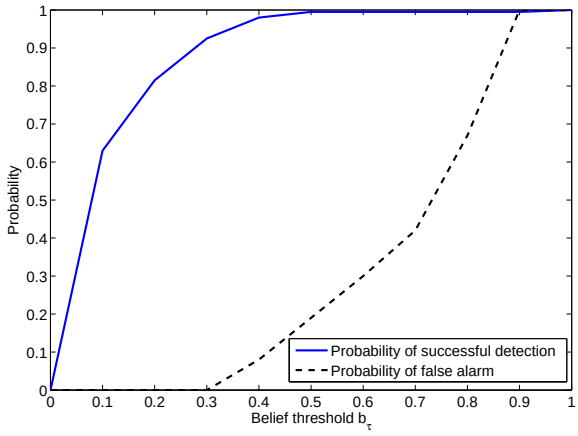

Fig. 8. Simulation results for the probability of successful detection and the probability of false alarm given different belief thresholds.

will automatically avoid those malicious nodes that have already been detected based on their records.

Figure 8 shows the probability of successful detection of malicious nodes and the probability of false alarm when the belief threshold changes. We can find that as the belief threshold b_τ increases, the probability of successful detection increases. When b_τ is 0.3, successful detection rate is 0.91 and the probability of false alarm is 0. When b_τ is above 0.5, we can have 100% detection rate. However, when b_τ is bigger than 0.3, the probability of false alarm will not be 0 anymore. Therefore, when we decide the value of b_τ, we need to consider the tradeoff between the successful detection rate and the probability of false alarm.

Figure 9 shows the simulation results for delay when the number of malicious nodes increases. X-axis is the number of malicious nodes and y-axis represents the delay which is normalized based on the delay of 15 meters. From the top down, the curves respectively represent the delay with the malicious nodes having attack probability 1, with the malicious nodes having attack probability 0.8, with the malicious nodes having attack probability 0.6 and after the source node detects the malicious nodes and re-routes avoiding those malicious nodes. Here, attack probability is the probability that the malicious node will conduct the RPU attack. It is clear that delay will increase with the increasing of the number of malicious

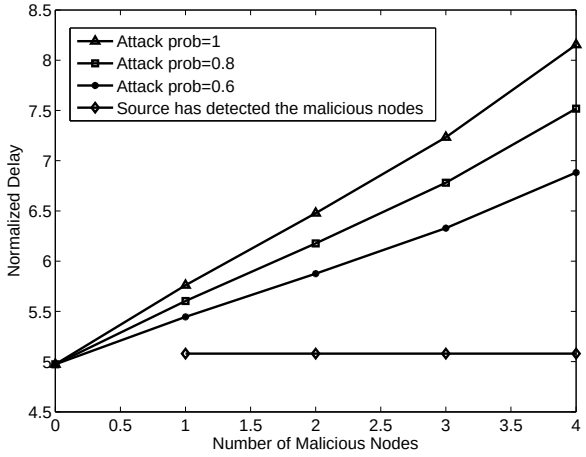

Fig. 9. Simulation results for the delay along the route when the number of the malicious nodes changes.

nodes, as well as when the attack probability increases. In addition, from the curve representing the delay after source node detects the malicious nodes and re-routes, we can find that the delay is greatly decreased, which can be 3.1dB lower than if we have 4 malicious nodes. However, the delay of the new route is slightly higher than that in the case there are no malicious nodes, about 0.1dB. This is because when the source node tries to avoid the malicious nodes, it may re-route to some nodes that are slighter closer to the primary user, or the number of intermediate nodes along the route may increase. In addition, when there is no malicious node in the network, the source node does not need to re-route.

In Fig. 10, the system performance in terms of delay is shown when the probability of attack increases. From the top down, the curves represent the cases of four malicious nodes, three malicious nodes, two malicious nodes, one malicious node and no malicious node, respectively. We can find that delay increases when the probability of attack increases, which makes perfect sense. Compared to the situation that there is no malicious node, the delay can be 4.7dB higher in the case if we have four malicious nodes. Note that this is the simulation result for only one source-destination pair, and if there are multiple source-destination pairs, the difference will be even bigger. In addition, when the number of malicious nodes increases, the delay also increases.

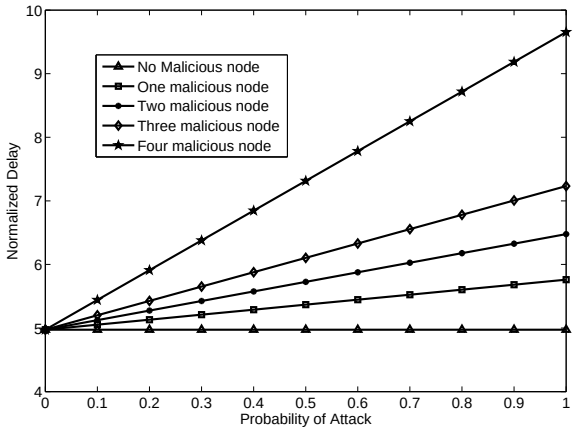

Fig. 10. Simulation results for the delay along the route when the probability of attack changes.

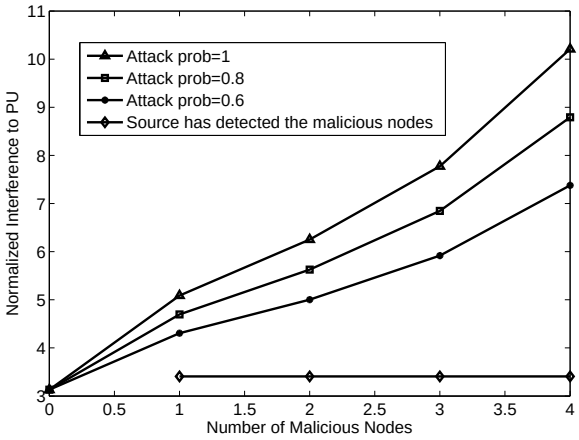

Fig. 11. Simulation results for the aggregate interference to the primary user when the number of the malicious nodes changes.

Figure 11 and Fig. 12 show the simulation results about the aggregate interference to the primary user when the number of malicious nodes and attack probability changes, respectively. Aggregate interference is calculated by adding the interference from all the secondary users along the route. Also in the results, the interference is normalized based on the interference from 1 secondary user localized at a distance of 50 meters away from the primary user. Clearly, we can find that when the number of malicious nodes increases or the attack probability increases, the aggregate interference to the primary user increases. The

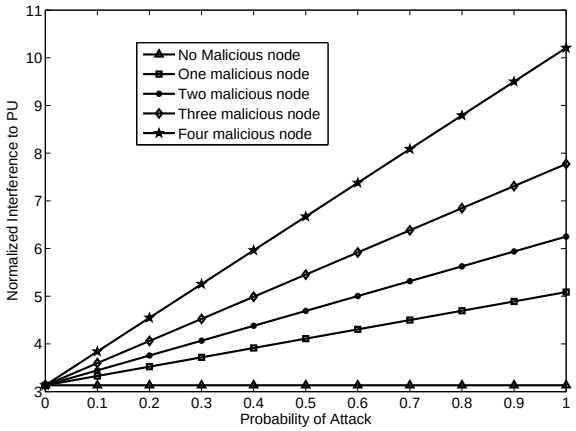

Fig. 12. Simulation results for the aggregate interference to the primary user when the probability of attack changes.

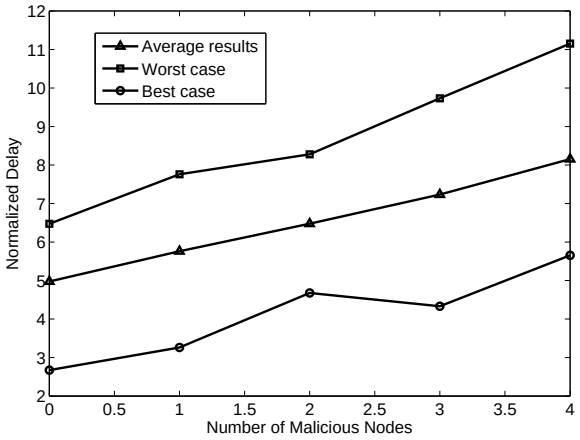

Fig. 13. Different from Fig. 9, the average results and the results of the worst case and the best case about delay along the route are shown when the number of the malicious nodes changes given attack probability of 1.

aggregate interference can be reduced by 7dB for only one source-destination pair, which justifies our claim about the harm of the RPU attack and the effectiveness of the proposed defense scheme. These results are consistent with the results shown in Fig. 9 and Fig. 10.

In Fig. 13 and Fig. 14, the average results and the results of the worst case and the best case of 1000 simulations about delay along the route as well as aggregate interference are shown, when the number

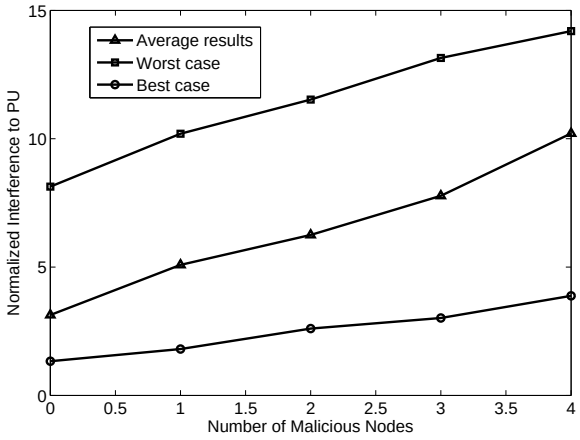

Fig. 14. Different from Fig. 11, the average results and the results of the worst case and the best case about aggregate interference are shown when the number of the malicious nodes changes given attack probability of 1.

of malicious nodes changes. Best case means that the malicious nodes are close to the boundary of the primary user's footprint, and worst case represents that the malicious nodes are far away from the primary user. From the simulation results, we can see that different locations of the malicious nodes may have great impact on the performance of attack. Given a certain source and destination pair, when the malicious nodes are close to the boundary of the primary user's footprint, the performance degradation is not so big compared to the case that the malicious nodes are far away from the primary user.

Figure 15 shows the simulation results of the aggregate interference along the route, when the number of the malicious nodes changes for two different secondary transmission ranges. We can find that when the secondary transmission range decreases, the aggregate interference increases. This is because that the number of nodes along the route increases when the secondary transmission range decreases.

VI. Conclusion

In this paper, we proposed a new network layer attack, routing-toward-primary-user attack, in cognitive radio wireless networks. In the RPU attack, malicious nodes intentionally route a large amount of packets toward the primary users, aiming to cause large interference to the primary users and to increase delay

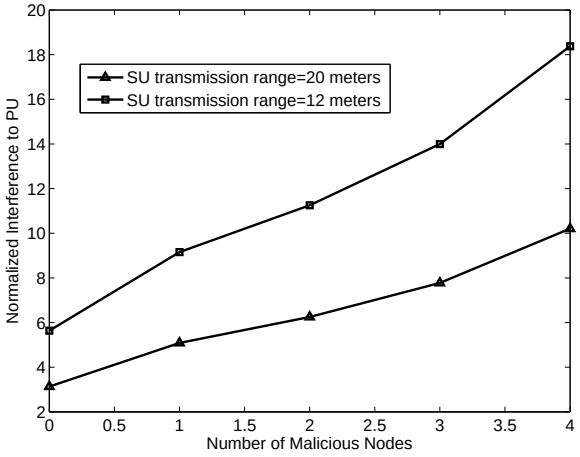

Fig. 15. Simulation results about the aggregate interference along the route when the number of the malicious nodes changes given different secondary transmission ranges.

along the routes. In the RPU attack, the malicious nodes "neutralize the route by the hands of the others", and it is hard to detect the malicious nodes. To overcome this attack, we developed a defense strategy using belief propagation. Firstly, an initial route will be found from the source to the destination without the knowledge of the malicious nodes. Each node on the route keeps a table recording the feedbacks from all the other nodes "after" it on the route. Then in each iteration, every node exchanges the m values with its neighboring nodes and computes beliefs. After convergence, the source node can detect the malicious nodes based on the final belief values. Finally, a new route will be found, avoiding malicious nodes. Simulation results show that the convergence of BP is very fast, and the proposed defense strategy against the RPU attack is effective and efficient. Delay can be significantly reduced by 4.7dB for only one source-destination pair and the aggregate interference to the PUs can be reduced by 7dB caused by the RPU attack.

REFERENCES

[1] J. Mitola III, *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*, Ph.D. thesis, KTH Royal Institute of Technology, 2000.

[2] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications", *IEEE J. Selected Areas in Communications*, vol. 23, pp. 201-220, Feb. 2005.

[3] E. Hossain, D. Niyato, and Z. Han, *Dynamic Spectrum Access in Cognitive Radio Networks*, Cambridge University Press, 2009.

[4] L. Akter and B. Natarajan, "Distributed Approach for Power and Rate Allocation to Secondary Users in Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 4, pp. 1526-1538, May 2011.

[5] L. Akter and B. Natarajan, "A Two-Stage Power and Rate Allocation Strategy for Secondary Users in Cognitive Radio Networks," *Journal of Communication, Special Issue on Cognitive Radio enabled Communications and Networking*, vol. 4, no. 10, pp. 781-789, Nov. 2009.

[6] R. D. Taranto, H. Yomo, P. Popovski, K. Nishimori, and R. Prasad, "Cognitive Mesh Network Under Interference from Primary User," *Wireless Personal Communications*, vol. 45, no. 3, pp. 385-401, May 2008.

[7] A. Goldsmith, *Wireless Communications*, Cambridge University Press, Cambridge, NY, 2005.

[8] Y. Yuan, P. Bahl, R. Chandra, T. Moscibroda, and Y. Wu, "Allocating Dynamic Time-Spectrum Blocks in Cognitive Radio Networks," in Proc. of *the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 130-139, Montreal, Canada, Sept. 9-14, 2007.

[9] R. C. Pereira, R. D. Souza, and M. E. Pellenz, "Using Cognitive Radio for Improving the Capacity of Wireless Mesh Networks," in Proc. of *IEEE Vehicular Technology Conference*, Calgary, Canada, Sep. 2008.

[10] N. Nie and C. Comaniciu, "Adaptive Channel Allocation Spectrum Etiquette for Cognitive Radio Networks," in Proc. of *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 269-278, Baltimore, MD, Nov. 8-11, 2005.

[11] O. Ileri, D. Samardzija, T. Sizer, and N. B. Mandayam, "Demand Responsive Pricing and Competitive Spectrum Allocation via a Spectrum Server," in Proc. of *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 194-202, Baltimore, MD, Nov. 8-11, 2005.

[12] R. Etkin, A. Parekh, and D. Tse, "Spectrum Sharing for Unlicensed Bands," in Proc. of *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 251-258, Baltimore, MD, Nov. 8-11, 2005.

[13] D. I. Kim, L. B. Le, and E. Hossain, "Joint Rate and Power Allocation for Cognitive Radios in Dynamic Spectrum Access Environment", *IEEE Trans. on Wireless Commun.*, vol.7, no. 12, pp. 5517-5527, Dec. 2008.

[14] K. R. Chowdhury and I. F. Akyildiz, "Cognitive Wireless Mesh Networks with Dynamic Spectrum Access," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 168-181, Jan. 2008.

[15] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey", *IEEE Communications Surveys and Tutorials*, vol. 11, pp. 52-73, Jun. 2009.

[16] R. Chen, J. M. Park, and J. Reed, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks", *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25-37, Jan. 2008.

[17] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof Collaborative Spectrum Sensing in Cognitive Radio Systems", in Proc. of *Conference on Information Sciences and Systems (CISS'09)*, Baltimore, MD, USA, Mar. 2009.

[18] K. Bian and J. M. Park, "Mac-layer Misbehaviors in Multi-hop Cognitive Radio Networks", in Proc. of *2006 US - Korea Conference on Science, Technology, and Entrepreneurship (UKC2006)*, New Jersey, USA, Aug. 2006.

[19] G. Jakimoski and K. P. Subbalakshmi, "Denial-of-service Attacks on Dynamic Spectrum Access Networks", in Proc. of *IEEE International Conference on Communications Workshops (ICC Workshops'08)*, Beijing, China, May 2008.

[20] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks", in Proc. of *IEEE International Conference on Communication (ICC'09)*, Dresden, Germany, Jun. 2009.

[21] A. Sampath, H. Dai, H. Zheng, and B.Y. Zhao, "Multi-channel Jamming Attacks Using Cognitive Radios", in Proc. of *16th International Conference on Computer Communications and Networks*, Honolulu, Hawaii, USA, Aug. 2007.

[22] S. Kurosawa1, H. Nakayama1, N. Kato1, A. Jamalipour2, and Y. Nemoto1, "Detecting Blackhole Attack on Aodv-based Mobile Ad hoc Networks by Dynamic Learning Method", *International Journal of Network Security*, vol. 5, no. 3, pp. 338-346, Nov. 2007.

[23] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", in Proc. of *26th IEEE International Conference on Computer Communications (Infocom'07)*, Alaska , USA, May 2007.

[24] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP - Sybil Attacks Detection in Vehicular Ad Hoc Networks", *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582 - 594, March 2011.

[25] A. K. Sadek, Z. Han, and K. J. R. Liu, "Distributed Relay-Assignment Protocols for Coverage Expansion in Cooperative Wireless Networks", accepted, *IEEE Transactions on Mobile Computing*, vol. 9, no. 4, pp. 505-515, April 2010.

[26] Z. Yuan, J. B. Song, and Z. Han, "Interference Minimization Routing and Scheduling in Cognitive Radio Wireless Mesh Networks", in Proc. of *IEEE Wireless Communications and Networking Conference*, April 2010.

[27] Z. Han and Y. Sun, "Securing Cooperative Transmission in Wireless Communications", in Procs. of *First Workshop on the Security and Privacy of Emerging Ubiquitous Communication Systems*, Pennsylvania, USA, Aug. 2007.

[28] A. T. Ihler, J. W. Fisher, R. L. Moses and A. S. Willsky, "Nonparametric Belief Propagation for Self-Localization of Sensor Networks," *IEEE J. Select. Areas Commun.*, Vol. 23, pp. 809-819, April 2005.

[29] H. Li and D. K. Irick, "Collaborative Spectrum Sensing in Cognitive Radio Vehicular Ad hoc Networks: Belief Propagation on Highway", in Proc. of *IEEE Vehicle Technology Conference (VTC)*, Taipei, Taiwan, May 2010.

[30] B. Frey, *Graphical Models for Machine Learning and Digital Communications*, MIT Press, Boston, MA, 1998.

[31] J. S. Yedidia, W. T. Freeman, and Y. Weiss, "Understanding Belief Propagation and its Generalizations", in *Exploring Artificial Intelligence in the New Millennium*, Chap. 8, pp. 2282-2312, Science and Technology Books, 2003.

[32] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan KauFmann Publishers, Inc., 1998.

[33] C. Dellarocas, "Mechanisms for Coping with Unfair Ratings and Discriminatory Behavior in Online Reputation Reporting Systems," in Proc. of *21st International Conference on Information Systems*, Brisbane, Queensland, Australia, Dec. 2000.