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

Dhanashree Yogesh Jangam
Computer Engineering Department,
JayawantraoSawant College of Engineering,
Handewadi Road, Hadapsar, Pune-28,Maharashtra,

Aruna K. Gupta
Computer Engineering Department
JayawantraoSawant College of Engineering,
Handewadi Road, Hadapsar, Pune-28, Maharashtra

*Abstract--***Recently many attentions are attracted towards the CR that is Cognitive radio, the one of the major communication technology revealed for next communication invention. But the security issues are not yet fully satisfy. A latest and prevailing routing-toward-primary-user network layer attack is projected in this paper. For increasing data transmission delay between the secondary users and hindrance the primary-user (PU), a malicious node deliberately rout large amount packets towards the primary users (PU). In the routing toward primary user attack it is very not easy to detect malicious node. Thus malicious nodes may say that, those nodes to which they forward the packet act dishonestly and cause troubles in data transmission. To protect against this attack with no of high complexity, belief propagation used to develop a defense strategy. Here a initial rout establish from source to destination, then according to it the each node keeps a feedback of other node on the route, compute belief, exchanges of feedback in a table record. On the basis of final belief values, the source node detects themalicious nodes.**

Index terms- **belief propagation,Cognitive Radio Network, Routing toward primary user attack, security.**

I. INTRODUCTION

Nowa day's wireless communication is important aspect. A spectral resources demand is continuously growing and widely used. Radio spectrum utilization is moderately low [1], [2], [3], [4], [5]. This is publicized by the spectrum measurement. The reason behind this nothing but a traditional approach towards the portion of restricted allocation spectrum of explicit wireless systems and services.In a large regions and time spans, such spectrum has a licensed. The unlicensed cannot access wireless system even if the spectrum utilized the licensed system. By considering a latest concept with a more capable way of using spectral resources one can find a solution for supplying spectral demand. Spectrum holes left by idle primary users (PUs) are used by secondary wireless users with the help of Cognitive radio (CR) which is a revolutionary technique. A CR wireless network which is looked as a multichannel multi-access network, wireless routers works like SUs for communications purpose that can opportunistically utilized by different spectral holes without causing any hindrance to the PUs. In some current work [6], [7], [8], [9], [10], [11], [12], [13], [14] network automatically establishing nodes, maintaining connectivity, dynamically self-organized and self-configured for the distributed CR networks are shown.

The CR network has many advantages, but it also has disadvantages regarding security. The collaborative sensing and multihop routing like distributed entities are inherited rely between networks. Due to this security challenges are occurred.Reporting false selection frame (FSF) attack [15], The primary user emulation (PUE) attack [16], reporting false sensing data (RFSD) [17], common false evaluation attack [18], control channel denial of service [19], and are the discovered attacks based on the CR-based network.

We are studying a latest and great routing-toward-primary-user (RPU) attack in CR networks which is proposed in this paper.Here, in the routing toward primary user attack, the malicious node purposely sends a large amount of packets on the way to the primary users (PU), purpose to cause interference to the primary users and raise the delay intransmission of data among the secondary users. This interference is not only for a single device to the PUs, but also affects the many CR devices which are transmitted at the same time around the PUs and hence the large amount of PUs performance is damaged. The malicious nodes cannot generate interference directly to the PUs. Instead of honest nodes generate this interference by receiving the packets through the malicious nodes.Due to this reason detecting the malicious nodes is very difficult.

Against the RPU attack we developed a defense strategy based on belief propagation (BP) for increasing RPU attack awareness and representing its damage. The initiate route originated from source to destination without any information of the malicious nodes. On the basis of feedback information of the other nodes on the router, the each node on the rout keeps a table record. The every node computes the belief by exchanging the feedback with its neighbor'snode. Based on the final belief values the malicious node detected by the source nodes and BP converges. By avoiding malicious nodes the data packets routs by source node to the destination node. For reducing the complexity of defense mechanism we are applying belief propagation (BP). These propose scheme is effective and efficient for detecting the RPU attackers. This is shown by the simulation result.

In this paper we learn the attacks and defense in CR network in section II, in section III we see the system overview and last conclusion and future scope of RPU in CR network.

II. THE LITERATURE SURVEY

New proportions of vulnerabilities are transports by spectrums which is access in CR systems. The different CR networks attacks are,

1. ATTACKS IN MAC LAYER

The PU's signal characteristics features and available spectrum transmission is imitated by malicious nodes. This is nothing but a PUE attack [16], [20], [21]. SUs believe that PU is present there and they avoid it with the help of spectrum holes which is actually available. Against the collaborating spectrum sensing protocol, the RFSD physical layer attack is discovered [17]. This protocol used to recognizea proficient method to deal with the problem of unpredictability in single-user spectrum sensing, and false sensing data due to the miss detection in the decision or false alarm made by the fusion center is reported by the malicious SUs.

2. ATTACKS IN PHYSICAL LAYER

On common channel the denial of service attack launch by malicious userswith the help of sending superfluous packets in such a way that genuine SUs have less chance to find common available channels and due to this they have less chance to communicate with each other. First sender send liberated channel list frame to the receiver and then by using SELection (SEL) frame receiver respond that they are going to use the data channel. This is occurs when two SUs want to set up communication channel. This attack is called as reporting FSF. With the help of channel reservation message (RES frame) the sender informs its neighbor of the channel selection after receiving the SEL frame. The claimed regarding decline to forward package for the other nodes and no available channel are claimed by selfish SU in this process [18]. SUs required evacuate the channel using evacuation protocol, if the PU turns on at the time of SUs transmission. This is a third MAC layer called as FE [19].

3. ATTACKS IN NETWORK LAYER

In Warmhole attack, which is redirection attack, the attackers plot a high speed link among them. Due to this other nodes believe wrongly that other paths are longer than the path among the plotting attackers. A large amount of data traffic, which grounds traffic analysis, congestion or manipulation of facilitates datais attracted by plotting attackers [22]. Sybil attack, is the another network layer attack. Where by claiming false identities, aspiring to achieve a disproportionately large persuadein the network, or by imitating are the behaviors of a malicious node in a larger number of nodes [23]. The attacker can abuse, drop or eavesdrop messages as it sees fit by stimulating the source node to select a rout through the attacker[24]. Without considering about the CR system model and PUs existence, there are several attackers present in a network layer. They are wireless ad hoc or mesh or sensor. RPU attack which is projected in this paper also a redirection attack. These attacks cause the failure in data transmission as well as humiliate the PUs' performance. In this attack the malicious node accidently makes an honest node to harm the network, instead of causing the problem to the network, which is difficult to detect by the attackers. Due to this reason RPU attack is different from the above attacks.

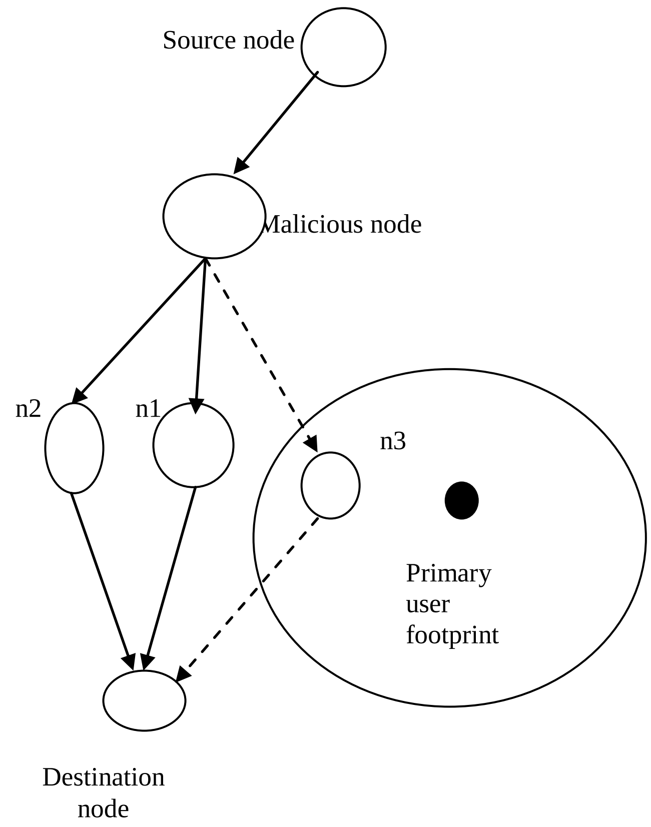
4. RPU ATTACK MODEL

Malicious nodes claim that they have best rout with low cost by sending fake routing information in the RPU attack. Due to this other honest nodes send packets through those malicious nodes.This model shows that the cost between the SU, which is near to the PU and itself is very low. And due to this reason honest node forwarded data packets this malicious node andall traffic will be routed through the attacker. In the RPU attack, malicious node can be any location; it does not require close to the PU. And it cause directly interference to the PUs or in the long delay data transmission. And it claims to those nodes to which it forwarded the packets because the source node cannot identify the bad node. It affects the data transmission failure as well as degrades the PU's performance. It also hurt the honest node instead of causing problems to the network. Due to this reason it us very difficult to convert or detect.

We consider the system performance in terms of probability, in this approach. In this case received power SU from PU falls below a certain threshold.According to application scenario and transmitter/receiver structure, the power threshold is determined.

For routing among SUs in CR wireless network is done by using shortest path routing algorithm [25], which is effective and efficient. The delay which is inversely proportional to the capacity is used to determine the cost of direct link.

III. SYSTEM OVERVIEW



Here,

● Is a primary user

○ Is a secondary user
→ Is a connection link
- -→ Is a connectionless link

This fig shows the RPU attack. In this figure SUs are n1, n2, n3, source node and destination node. The footprint of PU is the shaded region. Here secondary node n3 is inside the region it is forced to the turn off for a specific time slot. At different time slot it can change in different shapes. Due to this reason the secondary nodes should be out of the PU's footprint. If the distance to the PU's is shorter then there are higher chances of turn off. In this fig. source node wants to transmit destination node but malicious node claimed that it have a shorter path to the destination node and source node forward the entire packet to the malicious node. Which is nearer to the PU as compare to n2, even that malicious knows that n2 can also able to forward this packets. There are two chances first is malicious mode→ n1→ destination node and second is malicious node→n2→ destination node. But in second n2 near to the footprint there are chances of delay in data transmission and may be turn off frequently.

In this approach it consists of the concept of cognitive radio networks. In which here describes how routing toward primary user attack affect to data transmission delay and the defense strategy for this attack. Belief- Propagationbased defensestrategy is used for RPU attack.Only local observations are used in a single-user decision. For detecting the malicious node there is requirement of communication between all neighbor nodes and feedback exchange. For this we can use a simple flooding strategy but this give the significant like complexity of computation and overhead signaling. This problem can be overcome with the help of BP [26], [27], [28], which is calculated marginal distribution efficiently and circumvent the others node involvement which is not present in the initial rout. Can be detected which is described as follows:

Topology and network types are not considered here.
In network we are considering the source, destination and primary user node as well as attacker node

A. MATHEMATICAL MODEL

Let N be the number of nodes in the network.
Letnsbe the source node
Let nd be the destination node
Let m be the feedback information
Let $P(nv1)$be the marginal compute value
Let br be the threshold.

Transmit power signal from PU to SU
Calculate complete marginal probability by using BP

$$P(nv1)=\sum_{nv2}\sum_{nv3}\sum_{nvd} p(nv2, nv3, nd)$$

Where,

nd = destination node
n_{v2}, n_{v3}, = states of all parental nodes.
Converging BP by exact marginal value based on initial rout
And test the state of v which is unknown node.

$$v = \begin{cases} honest & bv \geq br \\ malicious & bv \leq br \end{cases}$$

If final belief $>br$ then malicious node is detected.

B. ALGORITHM

A Complete Defense Algorithm using Belief Propagation.

Step1: Obtain the initial rout from source to the destination with the help of shortest path routing algorithm.

Step2: A table recording feedbacks from the nodes 'after' is kept by each node on the initial rout.

Step3: for each iteration do

Step4: Local functions and compatibility functions are calculated by each node.

Step 5: Each node computes m value.

Step 6: The Exchanges of m values among each node and neighbor

Step 7: Belief calculated by each node

Step 8: end for

Step 9: According to final belief, the source node detect the malicious node.

Step 10: Avoid thosemalicious nodes to find new rout with the help of shortest path algorithm.

Here, system is implemented in JAVA technology and it requires minimum system specification for implementation.

IV. CONCLUSION AND FUTURE WORK

Future Scope: The detection of malicious user from this attack can be extended by considering current constraint.
In future malicious user detection from this attack can be use detection technique by considering size of network can be taken as a problem statement.

Conclusion: Here in this approach we have seena latest network layer attack that is RPU attack. The Routing toward primary user attack from cognitive radio network, in which malicious node intentionally sends the packet on the way to the primary user. Due to this it causes the delay in data transmission. And it is hard to detect this attack. To prevent such type of attack, here uses one strategy is that belief propagation based defense strategy. In this defense strategy, here without any information of the malicious nodes, found the initial rout from source to destination. The table recording of feedback is kept by an each node 'after' it on the rout. Then in each iteration, the exchanges of m values with its neighbor nodes are done by every node. After converges, on the basis of final belief value the source node can detect the malicious nodes. For avoiding a malicious node, a new rout will be found.When we eliminate the malicious node from network then there is no delay in data transmission. Hence in this way the malicious node is detected from RPU attack.

In this way, here routing toward primary user attack and its belief propagation based defense strategy from cognitive radio network is described.

REFERENCES

[1] L. Akter and B. Natarajan, "A Two-Stage Power and Rate Allocation Strategy for Secondary Users in Cognitive Radio Networks," J. Comm., Special Issue on Cognitive Radio Enabled Communication and Networking, vol. 4, no. 10, pp. 781-789, Nov.2009.

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

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

[4] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," IEEE J. Selected Areas in Comm., vol. 23, no. 2, pp. 201-220, Feb. 2005.

[5] J. Mitola III, "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio," PhD thesis, KTH Royal Inst. Of Technology, 2000.

[6] N. Nie and C. Comaniciu, "Adaptive Channel Allocation Spectrum Etiquette for Cognitive Radio Networks," Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks, pp. 269-278, Nov. 2005.

[7] R.C. Pereira, R.D. Souza, and M.E. Pellenz, "Using Cognitive Radio for Improving the Capacity of Wireless Mesh Networks," Proc. IEEE Vehicular Technology Conf., Sept. 2008.

[8] Y. Yuan, P. Bahl, R. Chandra, T. Moscibroda, and Y. Wu, "Allocating Dynamic Time-Spectrum Blocks in Cognitive Radio Networks," Proc. Eighth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing, pp. 130-139, Sept. 2007.

[9] A. Goldsmith, Wireless Communications. Cambridge Univ., 2005

[10] R.D. Taranto, H. Yomo, P. Popovski, K. Nishimori, and R.Prasad, "Cognitive Mesh Network under Interference fromPrimary User," Wireless Personal Comm., vol. 45, no. 3, pp. 385-401, May 2008.

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

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

[13] R. Etkin, A. Parekh, and D. Tse, "Spectrum Sharing for Unlicensed Bands," Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks, pp. 251-258, Nov. 2005.

[14] O. Ileri, D. Samardzija, T. Sizer, and N.B. Mandayam, "Demand Responsive Pricing and Competitive Spectrum Allocation via a Spectrum Server," Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks, pp. 194-202, Nov. 2005.

[15] K. Bian and J.M. Park, "MAC-Layer Misbehaviors in Multi-Hop Cognitive Radio Networks," Proc. US - Korea Conf. Science, Technology, and Entrepreneurship (UKC '06), Aug. 2006.

[16] R. Chen, J.M. Park, and J. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," IEEE J. SelectedAreas in Comm., 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," Proc. Conf. Information Sciences and Systems (CISS '09), Mar. 2009.

[18] G. Jakimoski and K.P. Subbalakshmi, "Denial-of-Service Attacks on Dynamic Spectrum Access Networks," Proc. IEEE Int'l Conf. Comm. Workshops (ICC Workshops '08), May 2008.

[19] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey," IEEE Comm. Surveys and Tutorials, vol. 11, no. 2, pp. 52-73, June 2009.

[20] A. Sampath, H. Dai, H. Zheng, and B.Y. Zhao, "Multi-Channel Jamming Attacks Using Cognitive Radios," Proc. 16th Int'l Conf. Computer Comm. and Networks, Aug. 2007.

[21] Z. Jin, S. Anand, and K.P. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," Proc. IEEE Int'l Conf. Comm. (ICC '09), June 2009.

[22] R. Maheshwari, J. Gao, and S.R. Das, "Detecting WormholeAttacks in Wireless Networks Using Connectivity Information,"Proc. IEEE INFOCOM, May 2007.

[23] T. Zhou, R.R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP - Sybil Attacks Detection in Vehicular Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 29, no. 3, pp. 582-594, Mar. 2011.

[24] 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," Int'l J. Network Security, vol. 5, no. 3, pp. 338-346, Nov. 2007.

[25] Z. Yuan, J.B. Song, and Z. Han, "Interference MinimizationRouting and Scheduling in Cognitive Radio Wireless MeshNetworks," Proc. IEEE Wireless Comm. and Networking Conf., Apr.2010.

[26] A.T. Ihler, J.W. Fisher, R.L. Moses, and A.S. Willsky, "Nonparametric Belief Propagation for Self-Localization of Sensor Networks," IEEE J. Selected Areas in Comm., vol. 23, no. 4, pp. 809-819, Apr. 2005.

[27] H. Li and D.K. Irick, “Collaborative Spectrum Sensing in Cognitive Radio Vehicular Ad Hoc Networks: Belief Propagation on Highway,” Proc. IEEE Vehicle Technology Conf. (VTC), May 2010.

[28] B. Frey, Graphical Models for Machine Learning and Digital Communications. MIT, 1998.

[29] J.S. Yedidia, W.T. Freeman, and Y. Weiss, “Understanding Belief Propagation and Its Generalizations,” Exploring Artificial Intelligence in the New Millennium, pp. 2282-2312, Morgan Kaufmann,2003.