ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

Location Identification and Trainer Safety System using Cognitive Radio Network

Dr.Joseph Jeyakumar [1], M.Deepak [2], Jeswanth.V.R[3], D.K.Albert Richard[4]

Assistant Professor, Dept. of ECE, Meenakshi College of Engineering, Chennai, India[1]

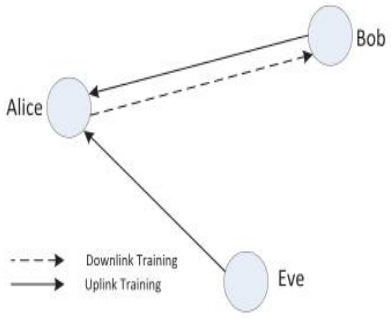
B.E, Dept. of ECE, Meenakshi College of Engineering, Chennai, India [2,3,4]

ABSTRACT: In the traditional ad hoc network, common channel is present to broadcast control channels between the nodes. This cannot be achieved in cognitive radio ad hoc network where different cognitive users acquire different channels based on the spatial and temporal usage of the primary users. Broadcasting of control signals to all the nodes of the cognitive radio ad hoc network with high success rate while minimizing the broadcast delay is difficult. Broadcast collision occurs when a node receives multiple copies of broadcast message in multi hop cognitive radio ad hoc network. This survey helps to understand different schemes used for broadcasting the control information with high success rate and low broadcast delay by eliminating the broadcast collision in multi hop cognitive radio ad hoc network. analyses spectrum sharing in cognitive radio networks, and perform the selection of relays models to reduce the interference of primary nodes and achieve the maximize the rate in secondary nodes. The trade-off between the secondary rate and the interference on the primary is also characterized. To consider a spectrum-sharing analysis they taken an Alternating Relay Protocol to investigate the performance and clustering (frame work) for to achieve an above mentioned aspects. "In the paper Rayleigh fading is used to select the relay thus rate of transfer decrease per second. To increase the Rates of frequency by proposing with an algorithm of frequency selective fading with the help of this method data loss is comparatively reduced". Finally to address the rate loss due to half- duplex relaying in the secondary and propose an alternating relay protocol and investigate its performance.

KEYWORDS: Two-Way Training-Based scheme, Pilot Spoofing attack Scheme- Location Identification-Cognitive Radio Network

I. INTRODUCTION

The main aim of this project is to achieve the goals of detecting the pilot spoofing attack and securely re-transmitting the data signal based on a two-way training detection scheme .The pilot spoofing attack is one kind of active eavesdropping activities conducted by a malicious user during the channel training phase. By transmitting the



identical pilot (training) signals as those of the legal users, such an attack is able to manipulate the channel estimation outcome, which may result in a larger channel rate for the adversary but a smaller channel rate for the legitimate receiver. With the intention of detecting the pilot spoofing attack and minimizing its damages, we design a two-way training-based scheme. The effective detector exploits the intrusive component created by the adversary, followed by a secure beamforming-assisted data transmission. In addition to the solid detection performance, this scheme is also capable of obtaining the estimations of both legitimate and illegitimate channels, which allows the users to achieve

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

secure communication in the presence of pilot spoofing attack. The detection probability is evaluated based on the derived test threshold at a given requirement on the probability of false alarming. The achievable secrecy rate is utilized to measure the security level of the data transmission. Our analysis shows that even without any pre-assumed knowledge of eavesdropper, the proposed scheme is still able to achieve the maximal secrecy rate in certain cases. Numerical results are provided to show that our scheme could achieve a high detection probability as well as secure transmission.

II. NETWORK FORMATION

As WIRELESS networks are bearing larger and larger responsibilities of our essential activities, it is crucial to protect the wireless transmission against either passive or active attack from any adversary. Classic cryptographic methods achieved secure communication by encrypting the confidential message as the unreadable cipher message, only the authentic receiver with valid secret key could decrypt and obtain the correct information. However, another method dedicated to achieve secure transmission based on the physical layer property, named as physical layer security, has been proposed even before the cryptographic method. We adopt a typical wiretap channel model, in which the transmitter Alice has multiple antennas and both the receiver Bob and the eavesdropper Eve are equipped with a single antenna. In a TDD system, Bob sends the assigned pilot signal to let Alice estimate the channel. Meantime, Eve conducts the pilot spoofing attack by sending the same pilot signals to Alice. In this work, we assume that the channels are block fading, i.e., the CSI remains constant during a given time frame length (denoted as N) and changes independently among different time frames.

III. PILOT SPOOFING ATTACK SCHEME

Pioneering works introduced the basic wire-tap channel model which consists of a transmitter, a legal receiver and an eavesdropper (adversary), and defines the secrecy rate as the information rate that could be totally kept secret from the eavesdropper. This work has been extended the general broadcast channel. In recent decades, the development of multi-input-multi- output (MIMO) techniques (e.g., beamforming) provide a great opportunity to achieve a positive secrecy rate even when the legitimate channel is worse than the illegitimate one. Other than the passive eavesdropping, the adversary could choose the active attack instead. One intelligent attack is called the spoofing attack, in which the adversary pretends to be the legitimate transmitter to spread false messages, or be the legitimate receiver to filch confidential information. This spoofing attack is originally studied in cyber network Though some related detection algorithms are designed based on utilizing the physical layer properties, comparing the channel state information (CSI) in neighbouring time slots However, recent study illustrates that spoofing attack could also happen in the physical layer of communication systems

IV. TWO-WAY TRAINING BASED SCHEME

Propose a two-way training based scheme to achieve the goals of detecting the pilot spoofing attack and securely re-transmitting the data signal, the basic process is that the reverse training is still operating as usual to allow the transmitter to estimate the CSI. Before confidential data transmission in the downlink phase, the transmitter first sends the channel estimation results to the receiver, and then conducts the traditional downlink training by having each antenna transmit the pilot signal to the receiver. The detection outcome will be fed back to the transmitter together with the downlink channel estimation if needed. our detector, named as two-way training detector (TWTD), could obtain an even higher detection rate than that of ERD. More importantly, if the detection result indicates the existence of pilot spoofing attack, the transmitter could derive the estimations of both legitimate and illegitimate channels. Thus, by applying secure beamforming, the transmitter is able to immediately recover the data transmission while keeping it secret from the adversary. we define two hypothesises: H0 denotes that there is no pilot spoofing attack; H1 indicates

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

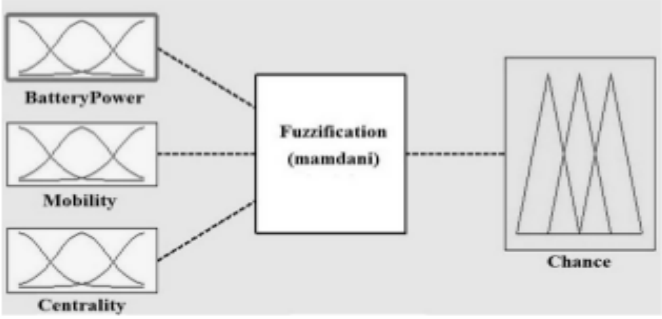
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

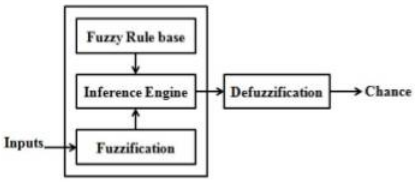
that Alice is under pilot spoofing attack. The two-way training based channel estimation phase consists of two sessions



1) Uplink Training Session; Bob transmits the assigned pilot signals to Alice. Only under H1, Eve transmits the identical pilot signals to spoof Alice 2) Downlink Training Session; We apply traditional downlink training method in this session, each antenna at Alice transmits the assigned pilot signal, and Bob then estimates every channel between that antenna of Alice and the antenna of its own. First, we have the channel between antenna at Alice to Bob, and denote the received signal and white noise at Bob, respectively the estimation result by utilizing LMMSE estimator two i.i.d. Gaussian random vectors ergodic-ally, so average even larger in this case, which indicates that Eve could more easily be detected. This matches the intuitive thought that if the adversary is more active (attacking both Alice and Bob), it shall take higher risk to be caught. Due to this reason and the fact that Eve actually could not benefit much from attacking Bob, we stay put the case that only Alice is attacked After detection, Bob will feed back the result to Alice. To protect the feedback signal from Eve's attack, Bob could assign such a signal with variable length and in different positions. Therefore, Eve could not only jam the feedback signal without jeopardizing its information stealing in the data transmission period. It is then important for Alice to know how to react to the detection result. If it shows no pilot spoofing attack, Alice could continue MRT in data transmission. When the result indicates the attack, Alice should have a backup plan to recover the secure transmission.

V.FUZZY LOGIC

In Wireless ad hoc environment it's important to choose a trustworthy node as the next hop among all encountered nodes to minimize the delay for the packet to reach destination node and maximize the packet delivery ratio. Trustiness among the nodes is detected based on the nodes behavior using fuzzy logic prediction. Based on



reputation value nodes are classified as low, medium and high priority nodes using fuzzy logic.

V. WIMAX PROTOCOL

WiMax has two main topologies ~V namely Point to Point for backhaul and Point to Multi Point Base station for Subscriber station.In each of these situations, multiple input multiple output antennas are used. The protocol structure of IEEE 802.16 ~V Broadband wireless MAN standard is shown below:

Protocol Structure of IEEE 802.16
The above picture shows four layers ~V Convergence, MAC, Transmission and Physical. These layers map to two of the lowest layers ~V physical and data link layers of the OSI model.WiMax provides many user applications and interfaces like Ethernet, TDM, ATM, IP, and VLAN.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

The IEEE 802.16 standard is versatile enough to accommodate time division multiplexing (TDM) or frequency division duplexing (FDD) deployments and also allows for both full and half-duplex terminals.
802.16 supports three physical layers. The mandatory physical mode is 256-point FFT OFDM (Orthogonal Frequency Division Multiplexing). The other modes are Single carrier (SC) and 2048 OFDMA (Orthogonal Frequency Division Multiplexing Access) modes.

The MAC uses a protocol data unit of variable length, which increases the standards efficiency. Multiple MAC protocol data unit can be sent as a single physical stream to save overload. Also, multiple Service data units (SDU) can be sent together to save on MAC header overhead. By fragmenting, you can send large volumes of data (SDUs) across frame boundaries and can guarantee a QoS (Quality of Service) of competing services. The MAC uses a self-correcting bandwidth request scheme to avoid overhead and acknowledgement delays.

This also allows better QoS handling than the traditional acknowledged schemes. The terminals have a variety of options to request for bandwidth depending on the QoS and other parameters.

VI. PHYSICAL LAYER

- Allows use of directional antennas
- Allows use of two different duplexing schemes:
  -Frequency Division Duplexing (FDD)
  -Time Division Duplexing (TDD)
- Support for both full and half duplex stations.

VII. MEDIA ACCESS CONTROL(MAC)

- Connection oriented
  -Connection ID (CID), Service Flows
  -Channel access: decided by BS
- UL-MAP
  -Defines uplink channel access
  -Defines uplink data burst profiles
- DL-MAP
  -Defines downlink data burst profiles
- UL-MAP and DL-MAP are both transmitted in the beginning of each downlink subframe

VIII.CONCLUSION

In this paper, we have studied an active eavesdropping problem, i.e., pilot spoofing attack. A two-way training based scheme has been proposed to defend such attack. The scheme first detects the attack by the unbalance of channel estimations at Alice and Bob, and then formats the secure beam forming based on the estimations of legitimate and illegitimate channels. It is shown that the proposed scheme could achieve a high detection probability. Moreover, according to the two way channel estimation, the positive secrecy rate is proven to be achievable. With the further validation of numerical results, our two-way training based scheme has been proven to be able to protect the confidential communication against the pilot spoofing attack. In order to apply the scheme to practical communication systems, some issues need to be considered, such as the design of the proper reference signal patterns and the feedback procedure.

FUZZY LOGIC avoids spoofing attack from multiple eavesdroppers. The vital role of this project is to hide the source and datapath by using COGINITIVE RADIO NETWORK (spectrum of bandwidth).These interesting topics may fall in future studies.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 3, April 2017

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2003.
[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst.Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8,pp. 1355–1387, Oct. 1975.
[4] I. Csiszár and J. Korner, "Broadcast channels with confidential messages,"*IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[5] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*,Jun. 2007, pp. 2466–2470.
[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf.Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[7] Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 357–360, Aug. 2014.
[8] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[9] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channelbased detection of Sybil attacks in wireless networks," *IEEE Trans. Inf.Forensics Security*, vol. 4, no. 3, pp. 492–503, Sep. 2009.
[10] Q. Li and W. Trappe, "Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships," *IEEE Trans. Inf.Forensics Security*, vol. 2, no. 4, pp. 793–808, Dec. 2007.