Collective jamming scheme in wireless social network

T.Dhatchayani[1], S.Jayasri[2], R.Dhanapriya[3]

[1,2] Final Year CSE students, [3]Assistant Professor,CSE
Thiruvalluvar College of Engineering &Technolocy, Vandavasi. Tamil Nadu
dhatchyani2697@gmail.com[1], jayasriagila717@gmail.com[2], priyait91@gmail.com[3]

Abstract- Device-to-Device communication is seen as a major technology to overcome the most valuable wireless capacity that enables new application services. In the presence generation there arises a need to access data from different types of communication device. The heterogeneity of communication and application of changing software situation in the environment from the end users, operators as well as technologies form the basis for wireless social network. The limited bandwidth and the in an inefficiency in the bandwidth utility requires a type of novel communication to exploit existing wireless spectrum. In this wireless social network, we investigate a cooperative jamming scheme based on this space power synthesis with unknown channel state information (CSI) of eavesdroppers. In particular, we provide a multiple jamming-based anti-eavesdropping model and formulate it by a superposition principle of various jamming signals in a free space. Based on the model, we analyze the superimposed effects of jammers with different locations in a fixed area, and then present corresponding jamming schemes to minimize synthetic jamming power at a legitimate receiver but satisfying basic interference in other locations. Furthermore, we also provide power allocation schemes to maximize to worst-case secrecy rate of a legitimate receiver.

Key Terms: D2D communication, CSI, Synthetic jamming wireless social networks.

1. INTRODUCTION

Eavesdropping is the unauthorized real time interception of private communication such as a phone call , instant message, video conference or facts transmission. It is an electronic attack where digital communication are intercepted by an individual whom they are not intended .This is then in two main reason directly listening to digital or analog voice communication or the interception or sniffing of data relating to any form of communication voice over IP(VOIP) calls made using IP based communication can be picked up and recorded using protocol analyzer and then converted to audio files using other specialized software. Data sniffing is easily done on a local network that uses a HUB since all communications are send to all ports (non-recipients just drop the data and a sniffer will simply accept all of the incoming data.

With the popularity of mobile Internet applications, various kinds of users with different attribute are full of social net-works. Apart from data transmission among legitimate users, numerous illegal users hidden in the networks may wiretap privacy of users. This secure issue is traditionally solved by cryptography-based technologies over upper layers [1], [2]. These encryption methods rely on assumptions that the physical layer can provide a reliable link as well as eavesdroppers cannot crack the secret key [3], [4]. Yet, it is dif cult to ensure a perfect secure transmission due to following reasons. First, the continuous improvement of hardware technologies leads to a rapid growth of computation power, which may enhance the ability to crack. Second, a reliable wireless link is hard to achieve due to the broadcast nature of wireless medium.

As a supplemental technology, PLS aims to stop eaves-droppers from correctly receiving any private signal [3], [5]. Cooperative jamming is one of popular methods to prevent eavesdroppers. To be specific, this method is to select helpers to send artificial noise (AN) so as to degrade quality of received signals of eavesdroppers while not interfere with legitimate receivers [6].

Existing cooperative jamming schemes mainly concentrate on the optimization of secrecy rate for pre-known channel state information (CSI) of all receivers in net-works [9]. Nevertheless, it is very difficult to estimate CSI of eavesdroppers perfectly due to errors of channel estimation and quantization. Even worse, we may not obtain any information of eavesdroppers within passive receive mode. Therefore, it is not practical to design jamming-based secure transmission in the assumption of known eavesdroppers' CSI.

The synthesis of jamming signals is deliberately designed to null at legitimate receivers while satisfying interference requirements at other locations in afixed area. In that case, we can achieve secure transmission based on cooperative jamming with unknown CSI of eavesdroppers. To the best of our knowledge, our work provides a pioneering direction that has not yet been studied in cooperative jamming. The main contributions of our work are summarized as below.

- Considering eavesdroppers without known CSI, we pro-pose a novel cooperative jamming strategy based on the space power synthesis, and then formulate a signal power synthetic problem employing the superposition of various jamming signals in wireless social networks.
- Analyzing different transmit parameters of every jammer (including the number of jammers, the initial emission current and phase), we derive a series of solutions for different physical locations of jammers.
- We formulate an achievable secrecy rate optimization problem and transform it into two sub-problems. Then, a heuristic simulated annealing algorithm is presented to approximately optimize two sub-problems. To reduce computational complexity, two search methods are introduced to find a feasible solution for two sub-problems.

2. REVIEW OF LITERATURE

In the paper “A novel privacy preserving approach for smartphone[3]”, users can enjoy personalized services by various contexts aware application throughsensor equipped smartphones fake mask use to preserve users’ privacy. The fake mask privacy checking algorithm decides whether to release a fake mask context for the current context of the user .This novel privacy checking algorithm is efficient for smart phone users and hence implemented in our paper.

As mentioned the paper[4],”The general Gaussian multiple – access and two way wiretap channels: achievable rates and cooperative jamming” the multiple users communicate with an intended receiver in the presence of an eavesdropper is incorporated in our paper.

With reference to the paper”, optimal stopping theory based jammer selection for securing cooperative cognitive radionetworks [6], it is observed that problem of jammer selection for secure in cooperative cognitive radio network is possible .This gives us motivation for cooperative jamming selection scheme in wireless social networks to prevent eavesdroppers even with unknown CSI (Channel State Information)

With reference to the paper ”multiple-phase smart relaying and cooperative jamming in secure cognitive radio network [8]”,the cooperative secure communication where the secondary receiver is treated as a potential eavesdropper with respect a multiphase transmission . Here, they propose a multiphase transmission scheme to include 1) the phase of the to clean relaying with cooperative jamming and 2) the latency to successfully decode the primary message at the secondary transmitter. The cooperative jamming scheme for known CSI is understood and it can be extended for unknown CSI with a little change in the relevant algorithm.

3. SYSTEM IMPLEMENTATION

3.1 Existing System:

PLS aims to stop eavesdroppers from correctly receiving any private signal. Cooperative jamming is one of popular methods to prevent eavesdroppers. To be specific, this method is to select helpers to send artificial noise (AN) so as to degrade quality of received signals of eavesdroppers while not interfere with legitimate receivers. According to the difference of received signals quality, an indicator called as secrecy capacity is introduced to measure the maximum rate difference between legitimate users and eavesdroppers. When the secrecy capacity is positive, private information can be received by legitimate users but not eavesdroppers.

Disadvantage:

- It is very difficult to estimate CSI of eavesdroppers perfectly due to errors of channel estimation and quantization.
- Can’t obtain any information of eavesdroppers within passive receive mode.
- It is not practical to design jamming-based secure transmission in the assumption of known eavesdroppers’ CSI.

3.2 Proposed System:

This method exploits the superposition of various AN (also known as jamming signals) transmitted by different jammers in wireless social networks. Then the synthesis of jamming signals is deliberately designed to null at legitimate receivers while satisfying interference requirements at other locations in a fixed area. In that case, we can achieve secure transmission based on cooperative jamming with unknown CSI of eavesdroppers. To the best of our knowledge, our work provides a pioneering direction that has not yet been studied in cooperative jamming.

Advantage:

- It improvises the quality of identifying the eavesdropper, where there will be reduced errors in the channel estimation.
- Obtain information about the eavesdroppers in the static network.
- Can transfer the data more securely to the sink node.

We present an anti-eavesdropping model over physical layer of a wireless social network in Fig. 1. In the model, there exist a transmitter (Tx), a legitimate receiver (Rx), and several eavesdroppers (Eves). Both Tx and Rx may exchange privacy data with each other in the social network with a fixed area. During privacy data sharing, Eves may have opportunities to wiretap privacy data due to the broadcast nature of the wireless medium. In that case, Tx intends to select friendly jammers (Jms) from a set of candidate helpers (Hes) to cooperatively jam Eves. The selected jammers may broadcast interference signals during privacy data sharing. The jamming signals can degrade the received signal to interference plus noise ratio (SINR) of Eves while do not interfere with the reception of Rx.

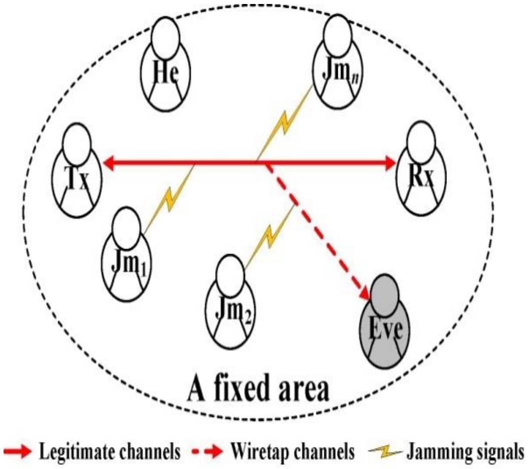

FIGURE 1. An anti-eavesdropping model over wireless physical layer.

TABLE 1. Notations.

	The length of antennas
I_i	The current on Jm_i's antenna
φ_i	The initial phase of Jm_i's transmitted signal
λ	The wavelength of transmitted signals
r_i	The distance from Jm_i to a target
η	The wave impedance of wireless medium
β	The phase constant
ω	The carrier frequency of transmitted signals

To achieve cooperative jamming for Eves based on AN, the secrecy capacity for wiretap channels is analyzed in [29]. Yet, this analysis can only implement with known CSI of both users and Eves. In a more general case, it is hard to obtain CSI of Eves in advance. Therefore, without known Eves' CSI in a social network, we intend to design a novel scheme to minimize synthetic power of jamming signals at Rx while ensuring necessary interference strength in a fixed area.

In our model, we assume that all nodes are equipped with a single antenna and they can communicate with each other over free space.[1]Based on the free space propagation model [30] [32], the corresponding synthetic electric field intensity of emitted signals from *n* jammers to a target in a far electric field.

4. CONCLUSIONS

This paper investigates a novel cooperative jamming scheme for secure communication based on the space power synthesis. Different from existing works, our scheme presents a new feasible idea to achieve cooperative jamming with unknown CSI of Eve. By discussing characteristics of jamming signals, we can null the synthetic jamming power at Rx but not other locations in a fixed area. In this case, we then maximize the worst-case achievable secrecy rate by calculating the worst location and the allocated power between Rx and jammers.

REFERENCES:

[1]X. Zheng, Z. Cai, J. Li, and H. Gao, ``Location-privacy-aware review publication mechanism for local business service systems," in *Proc.36th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2017,
pp. 1- 9.

[2]A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, ``Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550-1573, 3rd Quart., 2014.

[3]L. Zhang, Z. Cai, and X. Wang, ``Fakemask: A novel privacy preserving approach for smartphones," *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 2, pp. 335- 348, Jun. 2016.

[4]E. Tekin and A. Yener, ``The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEETrans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

[5]Q. Gao *et al.*, ``Joint design of jammer selection and beamforming for securing MIMO cooperative cognitive radio networks," *IET Commun.*, vol. 11, no. 8, pp. 1264 -1274, 2017.

[6]Q. Gao *et al.*, ``Optimal stopping theory based jammer selection for securing cooperative cognitive radio networks," in *Proc. IEEE Global Commun.Conf. (GLOBECOM)*, Dec. 2016, pp. 1-6.

[7] L. Dong, H. Youse 'zadeh, and H. Jafarkhani, ``Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2011, pp. 1-5.

[8] P.-H. Lin, F. Gabry, R. Thobaben, E. A. Jorswieck, and M. Skoglund, ``Multi-phase smart relaying and cooperative jamming in secure cogni-tive radio networks," *IEEE Trans. Cogn. Develop. Syst.*, vol. 2, no. 1,38- 52, Mar. 2016.

[9] Z. Li, T. Jing, L. Ma, Y. Huo, and J. Qian, ``Worst-case cooperative jamming for secure communications in CIOT networks," *Sensors*, vol. 16, no. 3, p. 339, 2016.

[10] H. Li, X. Wang, and W. Hou, ``Security enhancement in cooperative jamming using compromised secrecy region minimization," in *Proc. 13thCan. Workshop Inf. Theory*, Jun. 2013, pp. 214 218.