Information Sciences 281 (2014) 201–210

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

# Transmission protocol for secure big data in two-hop wireless networks with cooperative jamming

Yulong Shen, Yuanyu Zhang *

*School of Computer Science and Technology, Xidian University, 710071 Xi'an, China*

ARTICLE INFO

*Article history:*
Received 17 January 2014
Received in revised form 11 May 2014
Accepted 20 May 2014
Available online 2 June 2014

*Keywords:*
Big data
Security
Wireless network
Cooperative jamming
Energy balance

ABSTRACT

Wireless communications nowadays are increasingly becoming irreplaceable networking technologies for military, governmental and financial communications where the data is exploding in volume, variety and velocity, called big data. This poses great challenges to ensuring security through cryptography. Recently, cooperative jamming has been proved as a promising physical layer technique to provide the everlasting security for wireless networks. Based on this scheme, this paper proposes a two-hop transmission protocol with parameters $l, k, r$ and $\tau$ (2HR-$(l, k, r, \tau)$) to ensure secure and reliable big data transmissions in wireless networks with multiple eavesdroppers. We first determine the relay selection region (RSR) as the square of side-length $l$ centered at the middle point between the source and the destination. Then one of the $k$ best relays located in the RSR is randomly selected as the message relay. During the forwarding in both hops, the remaining relays at least distance $r$ away from the intended receivers and with channel gain to the intended receivers less than $\tau$ are selected to generate jamming signals to confuse the eavesdroppers. The results in this paper indicate that our protocol can provide flexible control of security, reliability and the energy balance performance, which characterizes how energy consumption for forwarding message is balanced among all the relays.



## 1. Introduction

Recently, wireless networks have attracted increasing attentions in both academia and industry. Owing to the advantages of flexible and self-configuring, wireless networks are anticipated to play an important role in some mission-critical applications, like health care, battle command, and governmental and financial communication. Therefore, such networks are now becoming essential for ensuring the economic vitality, people safety and even national security. The rapid growth of the node complexity and communication technologies allow the organizations in above scenarios generate and aggregate more and more data, which is now termed as big data [14,12,1]. As we know, much of these data is very sensitive and needs to be kept away from intercepting and damaging of the eavesdroppers during the transfer and aggregation. The nature of big data – high volume, variety and velocity also makes it difficult to ensure data integrity. Thus, security is becoming one of the greatest concerns in the big data environment [21]. Since data size is growing exponentially, it is essential to use efficient data transfer protocols to move vast amounts of data. Tow-hop forwarding, where each packet travels at most two hops (source-relay-destination) to reach its destination, is increasingly becoming important and promising in wireless

* Corresponding author. Tel.: +81 080 3266 6646.
*E-mail addresses:* ylshen@mail.xidian.edu.cn (Y. Shen), yy90zhang@gmail.com (Y. Zhang).

http://dx.doi.org/10.1016/j.ins.2014.05.037
0020-0255/

communication [19] and will play an important role in big data environment. In this paper, we hence focus on the security issue of big data transmission in two-hop wireless networks.

The traditional method to provide a standard information is the cryptographic approach where a complex algorithm is developed such that any adversary with limited computing power and without the secret key cannot intercept the information. However, the everlasting secrecy cannot be achieved by such approach, since the adversary can record the transmitted messages and try any way to break them [25]. Especially, recent advances in high-performance computation (e.g. quantum computing) make it further unlikely to acquire long-lasting security via cryptographic approaches [11]. Furthermore, the need for fast data transfer in big data environment makes it very difficult and expensive to exchange and maintain secret keys among various organizations. This motivates the consideration of signaling scheme in physical layer secrecy framework to provide a strong form of security for big data, where a degraded signal at an eavesdropper is always ensured such that the original data can be hardly recovered regardless of how the signal is processed at the eavesdropper [28,27,13]. Moreover, physical layer security approaches can be used with the cryptographic method in a complementary way to augment the security achieved by cryptography.

In physical layer secrecy framework, the key to achieve the everlasting security is guaranteeing an advantage of the legitimate channel over the eavesdropper channel, which, however, cannot always be guaranteed in general. This motivates many ideas to create a better legitimate channel, like the public and error-free feedback channel [18], the space–time coding over multiple antennas for secure communication [10] and the artificial noise injection strategy in MIMO [20,8]. However, due to the cost of deploying multiple antennas and designing efficient noise, these schemes are not suitable for large scale wireless network with nodes of single antenna. That is why there is an increasing interest in exploiting cooperative jamming in large scale wireless networks to provide strong form of security [7,17,24,23,9]. The basic idea behind cooperative jamming is that the jamming signals (or artificial noises) are generated from cooperative nodes to provide secure communication for the network. In this paper, we aim to design an efficient transmission protocol to ensure secure and reliable big data transmission based on the cooperative jamming scheme.

Recently, various works have been dedicated to design the secure transmission scheme via cooperative relays in large scale wireless networks under the framework of physical layer secrecy. In the case where eavesdropper channels or locations are known, node cooperation is used to improve the performance of secure wireless communications and a few cooperative transmission protocols were proposed to jam eavesdroppers [5,6]. In the case where eavesdropper channels or locations are unknown, Goeckel et al. proposed a transmission protocol based on optimal relay selection [7]. For both one-dimensional and two-dimensional networks, a secure transmission protocol is proposed in [3]. Ding et al. considered the opportunistic use of relays and proposed two secrecy transmission protocols [4]. The two-way secrecy scheme was studied in [15,2]. Sheikholeslami et al. proposed a protocol, where the signal of a given transmitter is protected by the aggregate interference produced by the other transmitters [22]. A secure transmission protocol is presented in the case where the eavesdroppers can collude [26]. Li et al. proposed two secure transmission protocols to confound the eavesdroppers [16]. The above works mainly focus on the maximum the secrecy capacity, in which the system nodes with best link condition is always selected as information relay. Although these protocols are attractive to provides good security, they do not consider the energy balance which can measure how energy consumption to forward message from the source to the destination is balanced among all the cooperative relays. Since an imbalanced use of the nodes may cause some nodes die much earlier and thus create holes in the network, or what is worse, leave the network disconnected, providing a good energy balance performance is extremely important for energy-limited wireless networks, such as military or emergency networks. In this paper, we proposed a transmission protocol 2HR-$(l,k,r,\tau)$ in two-hop relay wireless networks with parameters to ensure secure and reliable big data communication. We first identify the RSR which is a square of side-length $l$ centered at the middle point between the source and destination. Then one of the best $k$ relays in the RSR is randomly selected to forward message. During the transmission, relays at least $r$ away from intended receivers and with channel gain to the intended receivers less than *tau* are selected to transmit jamming signals to provide physical layer security. Theoretical analysis is presented to explore the behavior of the energy balance. Extensive simulation results are also provided to evaluate the performances of the 2HR-$(l,k,r,\tau)$ protocol. The results in this paper indicate that our protocol can provide flexible control of security and reliability through proper settings of these four parameters and the energy balance can be controlled by proper setting of $l$.

The remainder of this paper is organized as follows. Section 1 introduces the system models and presents the 2HR-$(l,k,r,\tau)$ protocol. Section 3 introduces the metrics of security and reliability and presents the theoretical analysis on the energy balance. Numerical results and discussions are provided in Sections 4 and 5 concludes this paper.

## 2. System models and 2HR-$(\boldsymbol{l},\boldsymbol{k},\boldsymbol{r},\tau)$ protocol

### 2.1. Network model

A two-hop wireless network scenario is considered where a source node $S$ wishes to communicate securely with its destination node $D$ with the help of multiple half-duplex relay nodes $R_1, R_2, \ldots, R_n$. Also present in the environment are $m$ eavesdroppers $E_1, E_2, \ldots, E_m$ without knowledge of channels and locations. We assume that the eavesdroppers do not transmit in order to hide themselves and each of them attempts to decode the message based on its own observations. We consider a time-slotted system where the relay nodes and eavesdroppers choose a position independently and uniformly