

Connectivity of Wireless Multi-hop Stochastic Networks under the Security Constraints in Rayleigh Fading Environment

Le The Dung*, Hoa T. K. Tran**, Seong-Gon Choi*

*Department of Radio and Communication Engineering, Chungbuk National University, Korea

**Faculty of Electrical and Electronic Engr., The University of Danang – University of Technology and Education, Viet Nam

dung.t.le@ieee.org, ttkhoa@ute.udn.vn, sgchoi@cbnu.ac.kr

Abstract— In this paper, we investigate the probability of existing a secure wireless multi-hop connection between two legitimate users in stochastic wireless networks under the existence of colluding eavesdroppers. Specifically, we introduce a simulation-based analysis that returns the path connectivity by averaging the connection status of a vast number of topology trails with a security-aware routing algorithm is taken into account. The behaviors of the multi-hop connectivity are examined for different network sizes and the numbers of legitimate users and eavesdroppers. The obtained results in this paper show that increasing the number of legitimate users leads to maximum path connectivity of less than one; meanwhile, path connectivity is continuously reduced as the number of eavesdroppers gets higher. Moreover, scaling down the network size does not always help to increase path connectivity.

Keywords—Stochastic wireless networks, Rayleigh fading, physical layer security, colluding eavesdroppers, multi-hop connectivity.

I. INTRODUCTION

Security is one of the major concerns in wireless communication networks because they are vulnerable to eavesdropping and impersonation attacks due to the broadcast nature of wireless medium. To protect communication confidentiality and authentication, several methods such as symmetric and asymmetrical cryptographic algorithms are often used. However, with the rapid advancement of computing technologies, cryptographic may have numerous risks. As a result, an alternative security mechanism, namely information-theoretic security or physical layer security (PHY-security) was introduced. Since PHY-security is implemented on physical layer by exploiting the random nature of the physical characteristics of wireless channels, it does not require any extra security mechanisms on other layers.

The studies of PHY-security initially focused on point-to-point communications with a single [1] or multiple antennas [2] and with non-cooperation [3] and cooperation [4]. Recently, researchers have been interested in analyzing the PHY-security in large-scale networks. It is often assumed that large-scale networks consist of many legitimate and

eavesdropper nodes distributed according to two independent Poisson Point Processes (PPT) [5]. Specifically, the authors of [6] used Poisson secure communication graph to obtain the analysis results for in-degree and out-degree of a legitimate node, the isolation probability, and the secrecy capacity between a legitimate node and its i th neighbors. In [7], based on the secrecy graph was, the out-degree in directional graph was investigated. It is noticed that the effect of eavesdropper collusion was not considered in [6], [7]. The effects of eavesdropper collusion and wireless channel fading on the secure connection between legitimate node and its i th neighbors were studied in [8], but there was a lack of the analysis of the secure connection for the case of colluding eavesdroppers in the deterministic channel.

Connectivity is a fundamental property of wireless networks. Whereas a mobile node in a cellular network is connected if it has a wireless link to at least one base station, the connection in a stochastic network is more complicated. Since mobile nodes are not only transmitters or receivers, they also act as relays and contribute to the connectivity of the entire network.

To investigate the connectivity of wireless networks, besides the percolation model [9], the PPT model has also been widely used. One of the first research works is [10], where the connectivity of a wireless ad-hoc network (AHN) was calculated with the assumption that each node has circle transmission range r_0 . Then, the analyses of the connectivity of AHNs in fading environment [11] and with directional antenna [12] were conducted. Using a similar framework, latter research papers studied the connectivity of other wireless networks in different scenarios such as the connectivity of cognitive radio networks with fading [13] and beamforming [14] and the connectivity of sensor networks [15].

We observe that all aforementioned works neglected the secure connections when considering the connectivity of wireless networks. However, for proper communications in many circumstances, security constraints should be added to the connectivity analysis of wireless networks. Motivated by this fact, we study the connectivity of multi-hop stochastic

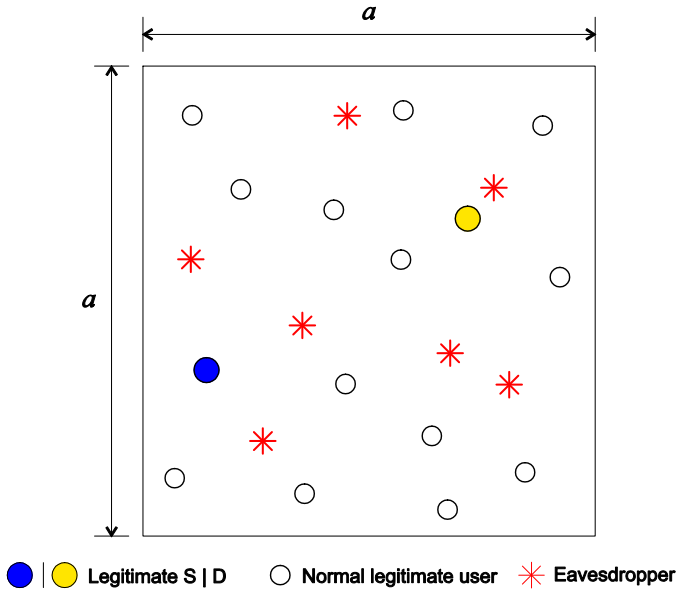


Figure 1. System model of the considered wireless stochastic network where legitimate users and eavesdroppers are randomly distributed in a square area.

networks under security constraints. The main contributions of this paper are summarized as follows:

- For the first time in the literature, we introduce a simulation-based analysis to compute the connectivity of multi-hop paths in stochastic networks from a massive number of random network topologies, taking into account the effects of wireless channel fading, routing protocol, and security constraints.
- We investigate this security-aware path connectivity as the network size, and the number of legitimate users and eavesdroppers vary. From the obtained results, we discuss some new characteristics of path connectivity, which may be useful for further studies of the security in wireless multi-hop stochastic networks.

The rest of this paper is organized as follows. Section II describes the system model used in the investigation of multi-hop connectivity under security constraints. Section III presents the criterion of a secure wireless connection between two legitimate users, the security-aware routing algorithm, and the simulation-based analysis to compute the path probability between two random legitimate users. Numerical results of path probabilities are shown in Section IV for different values of system parameters. Finally, Section V concludes the paper.

II. SYSTEM MODEL

A. Node Distribution

The wireless stochastic network considered in this paper is comprised of legitimate users and eavesdroppers as illustrated in Fig. 1. The network area is a square with the dimensions of $a \times a$. In this area, the legitimate users are distributed according to a PPP Φ_l with density $\eta_l = N_l/a^2$, where N_l refers to the number of legitimate users. Meanwhile, the eavesdroppers are distributed according to another

independent PPP Φ_e with density $\eta_e = N_e/a^2$, where N_e represents the number of eavesdroppers.

Among all legitimate users, two random ones will be selected as source S and destination D. Then, the establishment of the security-aware multi-hop path from S to D begins.

B. Wireless Channel

Considering two nodes in the network, the wireless connection between them is subject to both large-scale path loss and small-scale Rayleigh fading.

According to the Rayleigh fading, the probability density function (pdf) of the signal amplitude U at the receiver is expressed as

$$f_U(u) = \frac{u}{s^2} \exp\left(-\frac{u^2}{2s^2}\right), \quad (1)$$

where s is the scale parameter of the distribution and $E(u^2) = 2s^2$ is the average received signal power [16].

It is assumed that all nodes use omnidirectional antennas for communications. Then, the received power P_r (i.e. $P_r = P_{rl}$ at the legitimate receiver, $P_r = P_{re}$ at the eavesdropper) under the joint effects of large scale path loss and small scale Rayleigh fading is given by

$$P_r = u^2 \frac{1}{d^\alpha} P_t, \quad (2)$$

where d is the distance between two nodes, and α denotes the path-loss coefficient.

From (2), we define the signal power attenuation as

$$\gamma(d) = \frac{P_r}{P_t} = \frac{d^\alpha}{u^2}, \quad (3)$$

which can be expressed in the unit of dB as

$$\gamma(d)_{\text{dB}} = 10 \log_{10}\left(\frac{P_r}{P_t}\right) = \alpha 10 \log_{10}(d) - 20 \log_{10}(u). \quad (4)$$

The wireless connection between two legitimate users exists if the power attenuation of communicating signal is less than or equal to a specific threshold γ_{th} , i.e., $\gamma \leq \gamma_{th}$. Moreover, in this paper, we consider colluding eavesdroppers (all eavesdroppers are able to process their received message at a central processing unit jointly), which is considered as the worst case of security condition. Then, the combined received signal power at the eavesdroppers after centralized processing is

$$P_{re} = \sum_{i=1}^{N_e} P_{re_i} \quad (5)$$

where P_{re_i} is the received signal power at i th eavesdropper.

III. CONNECTIVITY OF SECURITY-AWARE MULTI-HOP STOCHASTIC NETWORK

A. Security Connection

We use physical security (PHY-security) as the criterion for evaluating whether a connection between two users is secure or not.

Based on the definition of PHY-security, the connection between a legitimate transmitter and a legitimate receiver is considered secured if the difference of the Shannon capacity between the legitimate transmitter and receiver, called *the legitimate channel*, and the Shannon capacity of the channel between the legitimate transmitter and eavesdropper, called *the eavesdropper channel*, is positive [6], i.e.,

$$\log_2 \left(1 + \frac{P_{rl}}{\sigma_l^2} \right) - \log_2 \left(1 + \frac{P_{re}}{\sigma_e^2} \right) > 0, \quad (6)$$

where σ_l^2 and σ_e^2 are the noise variance for the legitimate channel and eavesdropper channel, respectively.

After some manipulations, (6) becomes

$$\frac{P_{rl}}{P_{re}} > \beta, \quad (7)$$

where $\beta = \sigma_l^2 / \sigma_e^2$.

B. Security-aware Routing Algorithm

The establishment of a multi-hop path from S to D among legitimate users in the stochastic wireless network is based on the greedy forwarding (GF) routing algorithm, which uses two following rules:

- Every node selects secure neighbors that are nearer the destination than itself as forwarding nodes. The security criterion of a neighboring node is defined by (7).
- If a node cannot find any next-hop secure neighbors, the path from it to destination does not exist.

Thanks to the distributed and simple routing decision with a low number of control overheads, the GF algorithm is widely used in wireless multi-hop networks.

C. Connectivity Analysis

To analyze the connectivity of multi-hop stochastic networks under the PHY-security constraint, we perform a simulation-based analysis with a vast number of random topologies to obtain the probability P_{path} that two arbitrary legitimate users selected as source and destination are connected. Specifically, the simulation process can be summarized in the following steps:

- **Step 1:** Initially, a square network area $a \times a$ is created. Then, N_l legitimate users and N_e eavesdroppers are randomly deployed in this area.
- **Step 2:** Two legitimate users are randomly selected as source (S) and destination (D). The connection between them is checked by using the security-aware routing algorithm. If there is at least one path between S and D, the multi-path connectivity $p_i = 1$. Otherwise, $p_i = 0$.
- **Step 3:** The above process is repeated for Ψ times, such that the sample average

$$\frac{\# \text{ connected paths}}{\# \text{ topology trails}} = \frac{1}{\Psi} \sum_{i=1}^{\Psi} p_i \quad (8)$$

will converge toward the probability P_{path} .

Fig. 2 gives examples of unconnected and connected S-D multi-hop paths in security-aware wireless stochastic networks. These network topologies are obtained after running the

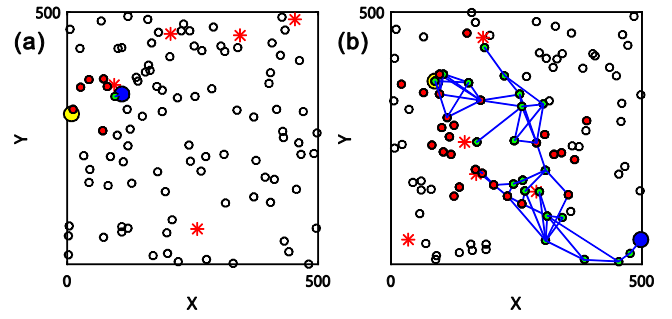


Figure 2. Illustration of (a) unconnected and (b) connected S-D multi-hop paths in security aware wireless stochastic networks with colluding eavesdroppers. $a = 500$ m, $N_l = 100$, $N_e = 5$, $\alpha = 3$, $\beta = 1$, $\gamma_{th} = 60$ dB.

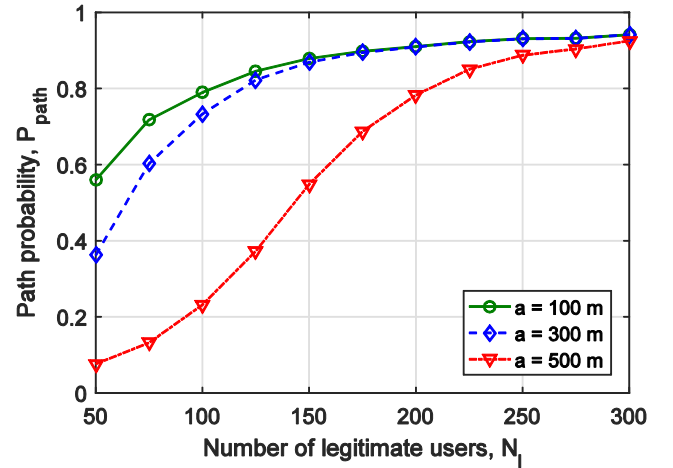


Figure 3. Path probability versus the number of legitimate users for different network sizes. $N_e = 5$, $\alpha = 3$, $\beta = 1$, $\sigma = 1$, $\gamma_{th} = 50$ dB.

simulation process on MATLAB. In Figure 2, nodes satisfying the security constraints are marked as green dots, while nodes failing to provide secure communications are marked as red dots. We can see that, in Figure 2(a), since many neighboring nodes of S are affected by the eavesdroppers, no paths can be established between S and D. However, secure communication paths are available in Figure 2(b).

IV. NUMERICAL RESULTS

In this section, we present numerical results to show the effects of network size and the number of legitimate users and eavesdropper on the security-aware connectivity of wireless multi-hop stochastic networks over Rayleigh fading channels. It should be noticed that changing in the network size has a stronger impact on the multi-hop path connectivity due to its combined effect, i.e., on the one hand, it increases the node density, and on the other hand, it reduces the average distance between two communicating nodes. Unless otherwise stated, the following parameters are used in the evaluating scenarios: colluding eavesdroppers, path loss exponent $\alpha = 4$, security threshold $\beta = 1$, power attenuation threshold $\gamma_{th} = 50$ dB.

Figure 3 plots path probability P_{path} versus the number of legitimate users N_l for different network sizes a . We vary N_l

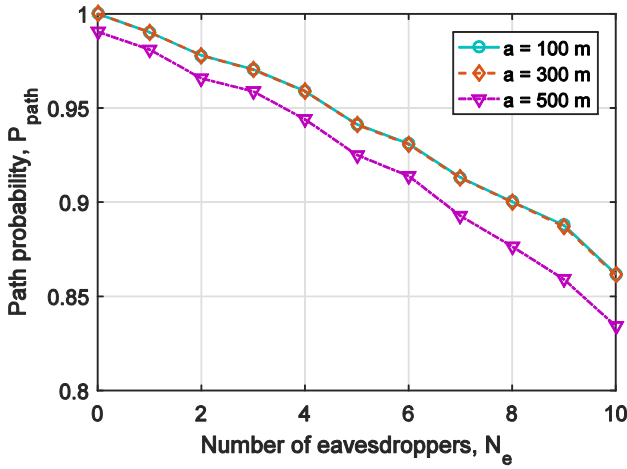


Figure 4. Path probability versus the number of eavesdroppers for different network sizes. $N_l = 300$, $\alpha = 3$, $\beta = 1$, $\sigma = 1$, $\gamma_{th} = 50$ dB.

from 50 to 300 for three network sizes $a = [100, 300, 500]$ m. As can be seen in Figure 3, P_{path} increases as N_l gets higher. For small network size, P_{path} increases rapidly, but keeps unchanged when N_l exceeds certain value. Specifically, when $a = 100$ and $a = 300$, P_{path} remains constant as $N_l > 200$. As a becomes larger, i.e. $a = 500$ m, the same behavior happens but at slower speed and with higher N_l . It is worth noticing that the maximum P_{path} is only around 0.94, indicating that perfect multi-hop connection never happens in the wireless stochastic networks with eavesdroppers.

Figure 4 depicts path probability P_{path} versus the number of eavesdroppers N_e for different network sizes a . We can see in Figure 4 that, when $N_e = 0$ (equivalent to without security constraints), $P_{path} = 1$ for the cases of $a = 100$ and $a = 300$. Then, as N_e increases, P_{path} of all cases of a greatly decrease. Moreover, for the same N_e , bigger network size leads to significantly lower P_{path} . The difference gap is larger as more eavesdroppers appear in the network. Surprisingly, further reducing a does not improve the connectivity of wireless stochastic networks with eavesdroppers. In particular, the values of P_{path} in the cases of $a = 100$ m and $a = 300$ m are very similar in the range of investigated N_e .

V. CONCLUSIONS

In this paper, we investigated the security-aware connectivity of wireless multi-hop stochastic networks with the conditions that colluding eavesdroppers exist in the system, and the wireless connection is characterized by both large-scale path loss and small-scale Rayleigh fading. To obtain this security-aware connectivity, we developed a simulation-based analysis that checks the wireless connection between two random legitimate users in a vast number of topology trails based on the security-aware routing algorithm. From the numerical results in this paper, some important conclusions are summarized as follows.

- A higher number of legitimate users leads to an increase in the path probability. However, when the number of legitimate users exceeds a specific value, the path probability remains constant, and this maximum is always less than one due to the presence of eavesdroppers. In contrast, path connectivity continuously reduces as more eavesdroppers appear in the network.
- Reducing the network size does not always result in better path connectivity. It only helps to increase the path connectivity as network size scales down to specific value.

The above observations can be used as helpful guidelines for network designers on making and evaluating multi-hop stochastic networks with security awareness.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1A2C1006167).

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [2] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," in *Proc. of IEEE ISIT 2008*. IEEE, Aug. 2008, pp. 524–528.
- [3] O. Gungor, J. Tan, C. E. Koksall, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, 2013.
- [4] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, 2013.
- [5] R. L. Streit, *Poisson Point Processes: Imaging, Tracking, and Sensing*. 1st ed., Springer US, 2010.
- [6] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer in stochastic wireless networks," in *Proc. of 2008 11th IEEE Singapore International Conference on Communication System*. IEEE, Nov. 2008, pp. 974–979.
- [7] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, 2009.
- [8] J. Bai, X. Tao, J. Xu, and Q. Cui, "The secrecy outage probability for the i th closest legitimate user in stochastic networks," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1230–1233, 2014.
- [9] R. Meester and R. Roy, "Continuum percolation," 1996.
- [10] C. Bettstetter, "On the connectivity of ad hoc networks," *The Computer Journal*, vol. 47, no. 4, pp. 432–447, 2004.
- [11] C. Bettstetter and C. Hartmann, "Connectivity of wireless multihop networks in a shadow fading environment," *Wirel. Netw.*, vol. 11, no. 5, pp. 571–579, 2005.
- [12] X. Zhou, S. Durrani, and H. M. Jones, "Connectivity analysis of wireless ad hoc networks with beamforming," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5247–5257, 2009.
- [13] L. T. Dung and B. An, "Connectivity analysis of cognitive radio adhoc networks with shadow fading," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 9, pp. 3335–3356, 2015.
- [14] L. T. Dung and S.-G. Choi, "Simulation modeling and analysis of the hop count distribution in cognitive radio ad-hoc networks with beamforming," *Simul. Model. Pract. Theory*, vol. 84, pp. 1–18, 2018.
- [15] H. T. H. Trang, L. T. Dung, and S. O. Hwang, "Connectivity analysis of underground sensors in wireless underground sensor networks," *Ad Hoc Netw.*, vol. 71, pp. 104–116, 2018.
- [16] K. Govindan, K. Zeng, and P. Mohapatra, "Probability density of the received power in mobile networks," *IEEE Trans. Wirel. Commun.*, vol. 10, no. 11, pp. 3613–3619, 2011.

- [17] B. Karp and H. T. Kung, "Gpsr: Greedy perimeter stateless routing for wireless networks," in The 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00). ACM, 2000, pp. 243–254.



Le The Dung (S'14, M'16) received the B.S. degree in Electronics and Telecommunication Engineering from Ho Chi Minh City University of Technology, Vietnam, in 2008, the M.S. degree and the Ph.D. degree in Electronics and Computer Engineering from Hongik University, Korea, in 2012 and 2016, respectively. From 2007 to 2010, he joined Signet Design Solutions Vietnam as a hardware design engineer. He has been with Chungbuk National University as a postdoctoral research fellow from May 2016. Dr. Dung has had more than 50 papers in referred international journals and conferences. He was the recipient of the IEEE IS3C2016 Best Paper Award. His major interests are routing protocols, network coding, network stability analysis and optimization in mobile ad-hoc networks, cognitive radio ad-hoc networks, and visible light communication networks. He is a member of the IEEE.



Hoa T. K. Tran received the B.S. degree in Electronics and Telecommunication Engineering from the University of Danang – University of Science and Technology, Vietnam, in 2012, and the M.S. degree in Micro and Nano Systems Technology from the University of South-Eastern Norway, Norway, in 2016. She is currently a lecturer at the Faculty of Electrical and Electronic Engineering, the University of Danang – University of Technology and Education, Viet Nam. Her major interests are digital signal processing and image processing algorithm. Her other research interests include micro/nanofabrication, ultrasonic spectroscopy, electronic sensors, modeling, and simulation.



Seong-Gon Choi received the B.S. degree in Electronics Engineering from Kyeongbuk National University in 1990, the M.S. and Ph.D. degrees from Information Communications University, Korea in 1999 and 2004, respectively. He is currently a professor in School of Information and Communication Engineering, Chungbuk National University. His research interests include smart grid, IoT, mobile communication, high-speed network architecture and protocol.