A Novel Anti-Eavesdropping Scheme in Wireless Networks: Fri-UJ

Qubeijian Wang
Macau University of Science and Technology
qubeijian.wang@gmail.com

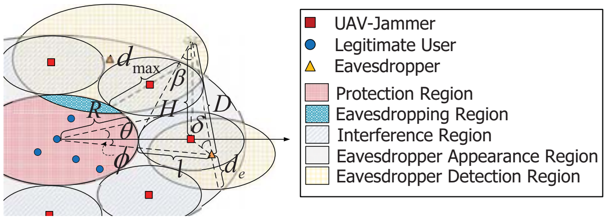
Abstract

A novel wireless network protection scheme is proposed through placing multiple unmanned aerial vehicles (UAVs) as jammers named UAV Jammers (UJs). This scheme is named as Friendly UAV Jamming (Fri-UJ). The UJs flying around the protection region emit artificial noise to disturb eavesdroppers from wiretapping confidential information. We evaluate the effectiveness of Fri-UJ via establishing analytical framework to evaluate the eavesdropping risk. Numerical results show that the proposed Fri-UJ scheme can significantly reduce the eavesdropping risk with nearly no impact on legitimate communications.

1 Introduction

The broadcasting nature of wireless networks leads to wireless networks susceptible to information leakage. In conventional wireless networks, the information protection usually makes use of encryption protocols. However, encryption protocols may not be feasible for the scenarios such as lower power Internet of Things, in which nodes with limited computational capability cannot exploit computational-extensive encryption protocols. On the other hand, encryption protocols cannot solve the privacy-exposure problem of human behavior recognition based on Wi-Fi signal [2, 3].

In this paper, we propose unmanned aerial vehicles (UAVs)-aided scheme to solve the above issues. In particular, we deploy multiple UAVs, each of which is equipped with a directional antenna to emit artificial noise to disturb eavesdroppers from wiretapping confidential information or extracting human-behavior features. We name such UAV jammers as UJs and friendly UAV Jamming scheme as Fri-UJ. The proposed Fri-UJ has many merits. First, Fri-UJ does not affect legitimate communications. Second, Fri-UJ is flexible to construct the jamming region surrounding the protection region. The flexible deployment of the Fri-UJ can also reduce the constructing cost compared with the fixed placement of jammers.



🟥	UAV-Jammer
●	Legitimate User
△	Eavesdropper
▨	Protection Region
▨	Eavesdropping Region
▨	Interference Region
□	Eavesdropper Appearance Region
▨	Eavesdropper Detection Region

Figure 1. Calculation details of Fri-UJ scheme

In this paper, we establish an analytical framework to evaluate the performance of the proposed Fri-UJ in terms of eavesdropping risk. Numerical results demonstrate the effectiveness of the proposed Fri-UJ scheme.

2 System Model

As shown in Fig. 1, the legitimate users are randomly distributed according to Homogeneous Poisson Point Process with the density of λ in a circular protection region with radius R. An eavesdropper randomly appears at the eavesdropper-appearance region (EAR) where the eavesdropper has chance to wiretap. The distance between the eavesdropper and the boundary of the protection region is l. The UJs flying on the air emit the artificial noise from air to ground to disrupt the wiretapping activity. The region affected by the artificial noise is named as the interference region (IR).

We assume that there are two channel models in this system: (1) the ground communication; (2) the air-to-ground communication [1]. The transmission between the legitimate user and the eavesdropper is modeled as the ground communication which is affected by Rayleigh fading and path loss. The transmitting power of legitimate user is P_t. The received power is $P_t h d^{-\alpha}$, where d is the distance from the legitimate user to the eavesdropper. The random variable h follows an exponential distribution with mean value $1/\mu$ and α is the path loss factor.

The interfering from a UJ to the eavesdropper is modeled as the air-to-ground communication that essentially consists of LoS (Light of Sight) link and NLoS (None Light of Sight) link. The LoS link experiences only path loss while the NLoS link experiences both path loss and Rayleigh fading. The transmitting power of the UJs is P_j. The distance from the UJ to the eavesdropper is D. The random variable

International Conference on Embedded Wireless
Systems and Networks (EWSN) 2019
25–27 February, Beijing, China

ISBN: 978-0-9949886-3-8

h_j follows an exponential distribution with mean value $1/\mu_j$ and α_j is the path loss factor. Thus, the received interfering power of eavesdropper can be expressed as $P_j g D^{-\alpha_j}$ for LoS link and $P_j g h_j D^{-\alpha_j}$ for NLoS link, where g is the directional antenna gain from $g = 2900/\beta^2$, and β is a half of the antenna beam-width. The probability of LoS link is expressed as $\mathbb{P}_{\text{LoS}} = a(\delta - 15^o)^b$, and the probability of NLoS link is $\mathbb{P}_{\text{NLoS}} = 1 - \mathbb{P}_{\text{LoS}}$

3 Eavesdropping Risk

We exploit the eavesdropping probability to evaluate the eavesdropping risk. The eavesdropping probability is the probability that at least one legitimate user is wiretapped by the eavesdropper. If the eavesdropper can successfully wiretap the legitimate communication if and only if both the following conditions are satisfied 1) the eavesdropper detection region intersects with the protection region; 2) at least one legitimate user falls in the intersection region. The intersection region is named as the eavesdropping region. We then have the eavesdropping probability $\mathbb{P}_e$ as follows,

$$\mathbb{P}_e = 1 - \mathbb{P}(x=0) = 1 - e^{-\lambda A}, \tag{1}$$

where A is the area of the eavesdropping region.

When a legitimate user is at the edge of the protection region and there is no external interference, the maximum eavesdropper detection distance is also the width of the EAR denoted by $d_{\max}$, which can be calculated as follows,

$$d_{\max} = \mathbb{E}\left[\frac{P_t h}{\sigma^2 T_e}\right]^{1/\alpha} = \frac{1}{\alpha} \cdot \left[\frac{P_t}{\mu \sigma^2 T_e}\right]^{\frac{1}{\alpha}} \cdot \Gamma(\frac{1}{\alpha}), \tag{2}$$

where $\mathbb{E}(\cdot)$ denotes the expectation and $\Gamma(\cdot)$ denotes the standard gamma function.

The UJs are deploy one by one surrounding the protection region to cover the EAR. However, there are still some small areas cannot be covered by emitted jamming signals of UJs as shown in Fig. 1. Therefore, we need to analyze the eavesdropping probability inside or outside interference region. When the eavesdropper is inside the IR, the eavesdropping probability can be derived via UJs-Covered scheme. When the eavesdropper is outside the interference region, the eavesdropping probability can be derived via UJs-Uncovered scheme. We consider the location of the eavesdropper with the polar coordinate (L, ϕ), where the center of protection region is regarded as the origin point. We then derive $\mathbb{P}_e$ of UJs-Covered scheme denoted by $\mathbb{P}_e^c(\text{J})$.

Theorem 1: The eavesdropper probability of UJs-Covered scheme is given by,

$$\begin{aligned}
\mathbb{P}_e^c(\text{J}) = 1 - \exp\Bigg\{ -\lambda \Bigg[\Bigg(& R^2 \arccos \frac{(R+l)^2 - d_e^2 + R^2}{R} \\
& - \frac{(R+l)^2 - d_e^2 + R^2}{2(R+l)} \sqrt{\frac{4(R+l)^2 R^2 - ((R+l)^2 - d_e^2 + R^2)^2}{4(R+l)^2}} \Bigg) \\
& + \Bigg(d_e^2 \arccos \frac{(R+l)^2 + d_e^2 - R^2}{2(R+l) d_e} \\
& - \frac{(R+l)^2 + d_e^2 - R^2}{2(R+l)} \sqrt{\frac{d_e^2(2R+2l+1) - (R+l)^2 - R^2}{2(R+l)}} \Bigg) \Bigg] \Bigg\},
\end{aligned} \tag{3}$$

Proof: The distance D between the nearest UJ and the eavesdropper is $D = [(R+r) - k\cos\phi]^2 + H^2$, where the flight height is $H = d_{\max}/(2\tan\beta)$. Thus, the received interference is expressed as follows,

$$I_j = \mathbb{P}_{\text{LoS}} P_j D^{-\alpha} + \mathbb{P}_{\text{NLoS}} \frac{P_j D^{-\alpha}}{\mu_j}. \tag{4}$$

The radius of eavesdropping region is given by,

$$d_e = \mathbb{E}\left[\frac{P_t h}{(I_j + \sigma^2) T_e}\right]^{\frac{1}{\alpha}} = \frac{1}{\alpha} \cdot \left[\frac{P_t}{\mu (I_j + \sigma^2) T_e}\right]^{\frac{1}{\alpha}} \cdot \Gamma(\frac{1}{\alpha}). \tag{5}$$

The area of the eavesdropping region is calculated by,

$$\begin{aligned}
A_n = & \left(R^2 \arccos \frac{x}{R} - x\sqrt{R^2 - x^2} \right) \\
& + \left(d_e^2 \arccos \frac{L-x}{d_e} - (L-x)\sqrt{d_e^2 - (L-x)^2} \right),
\end{aligned} \tag{6}$$

where $x = \frac{L^2 + d_e^2 - R^2}{2L}$, and $L = R + l$.

After combining Eq. (1) and Eq. (6), the local eavesdropping probability of UJs-Covered scheme is obtained. ■

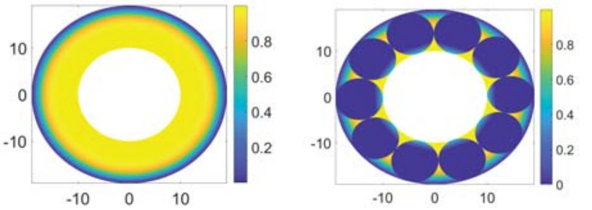


Figure 2. Local eavesdropping probability for None-Jammer scheme and Fri-UJ scheme (path loss factor $\alpha = 3$, legitimate users density $\lambda = 0.2$)

We denote the eavesdropping probability of UJs-Uncovered scheme by $\mathbb{P}_e(\text{NJ})$, which can be calculated in a similar approach. Finally, the eavesdropper probability is expressed as follows,

$$\mathbb{P}_e(\text{J}) = \begin{cases} \mathbb{P}_e^c(\text{J}) & H \le D \le \sqrt{H^2 + \frac{d_{\max}}{2}^2} \\ \mathbb{P}_e(\text{NJ}) & D > \sqrt{H^2 + \frac{d_{\max}}{2}^2} \end{cases}. \tag{7}$$

Numerical results. Fig. 2 shows the eavesdropping probability with Fri-UJ and without Fri-UJ, where the color from yellow to blue in eavesdropping region denotes the intensity of the eavesdropping probability from high to low. It is shown in Fig. 2 that Fri-UJ scheme can almost mitigate the eavesdropping probability in the EAR compared with non Fri-UJ.

4 Acknowledgments

This paper was partially supported by Macao Science and Technology Development Fund under Grant No. 0026/2018/A1. The authors would like to express their appreciation for Gordon K.-T. Hon for his thoughtful discussions.

5 References

[1] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah. Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs. *IEEE Transactions on Wireless Communications*, 15(6):3949–3963, 2016.

[2] Y. Yao, Y. Li, X. Liu, Z. Chi, W. Wang, T. Xie, and T. Zhu. Aegis: An interference-negligible rf sensing shield. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 1718–1726. IEEE, 2018.

[3] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee. A survey on behavior recognition using wifi channel state information. *IEEE Communications Magazine*, 55(10):98–104, 2017.