Xin YUAN, Zhi-yong FENG, Wen-jun XU, Zhi-qing WEI, Ren-ping LIU, 2018. Secure connectivity analysis in unmanned aerial vehicle networks. *Frontiers of Information Technology and Electronic Engineering,* 19(3):409-422. https://doi.org/10.1631/FITEE.1700032

Secure connectivity analysis in unmanned aerial vehicle networks

Key words: Unmanned aerial vehicle networks (UAVNs); Trust model; Secure connectivity; Doppler shift

Corresponding author: Zhi-yong FENG
E-mail: fengzy@bupt.edu.cn

Motivations

1. UAVs can be used as relays or aerial base stations for network provisioning in an emergency due to their easy deployment. However, a single UAV is usually insufficient due to their typically low transmission power and is limited processing ability. UAVs usually have a limited transmission range.

2. Security is essential for UAVs. UAV nodes are prone to power failure and equipment damage, which may cause errors in information delivery. Worse still, hostile nodes may try to intercept the information transfer between legitimate nodes or act in malicious ways to prevent UAVs from proper functioning.

Main ideas

1. An efficient hierarchical trust model (EHTM) that takes into consideration the UAVs' behaviors, the characteristics of channels between UAV nodes and the mobility of UAV nodes are proposed. The detailed calculation procedure of EHTM is also presented.

2. Based on EHTM, the secure links is established when there are both a physical link and a trust link between two UAVs.

3. The physical connectivity probability and the secure connectivity probability between two UAVs in the presence of Doppler shift are both derived and evaluated.

Methods

1. A UAVN in which UAVs are deployed in an infinite three-dimensional Euclidean space according to a homogeneous Poisson point process with a density λ.

2. Smooth Turn (ST) mobility model is adopted for the motion of UAVs, which captures the correlation of acceleration of UAVs across the temporal and spatial domain.

3. The EHTM model is composed of four sections: direct trust, indirect trust, integrated trust, and trust update. A secure link exists between two UAVs only when there is both a physical link and a trust link between these two nodes.

3. According to the above system model, the physical connectivity probability and the secure connectivity probability between two UAVs in the presence of Doppler shift were both derived and evaluated.

4. Simulation is carried to verify analysis results.

Major results (1)

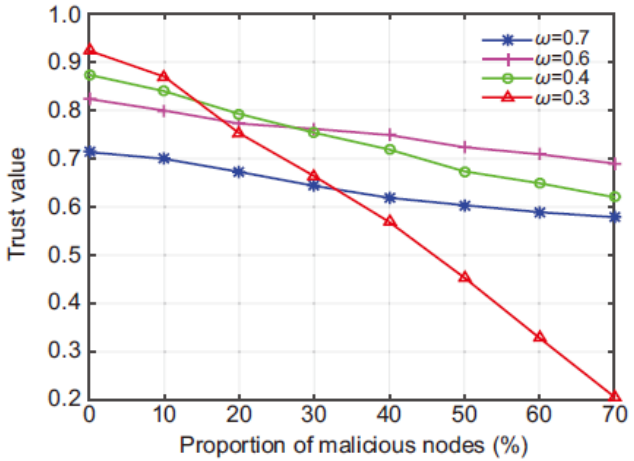

Fig. 6 Influence of the weights on the relationship between the trust value and the proportion of malicious nodes in the UAVNs

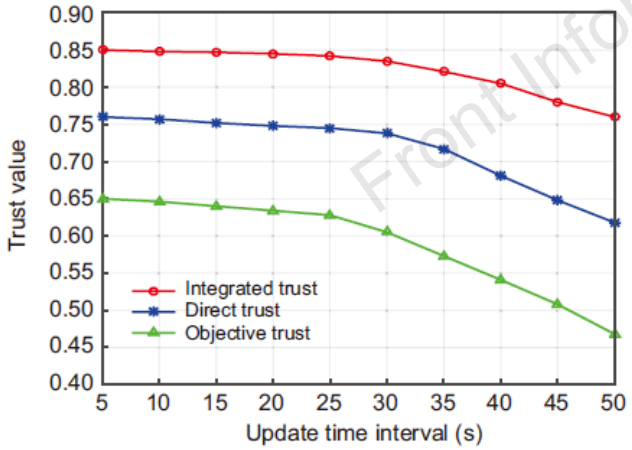

Fig. 7 Influence of the trust update time interval on trust values

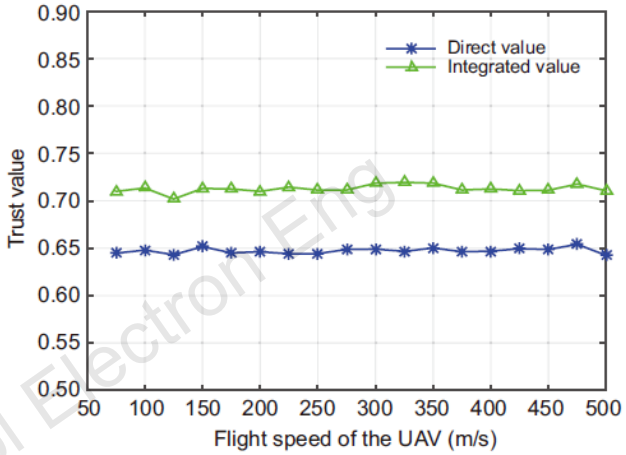

Fig. 8 Robustness of the proposed trust model against mobility

Fig. 6 shows that more malicious nodes in UAVNs will result in lower trust values. Moreover, the weight value need to be adjusted dynamically according to the number of malicious nodes.

Fig. 7 shows that the trust value decreases slowly at first and then rapidly with the increased update time interval.

Fig. 8 shows that the proposed trust model can work well and will be robust against the mobility of UAVs.

Major results (2)

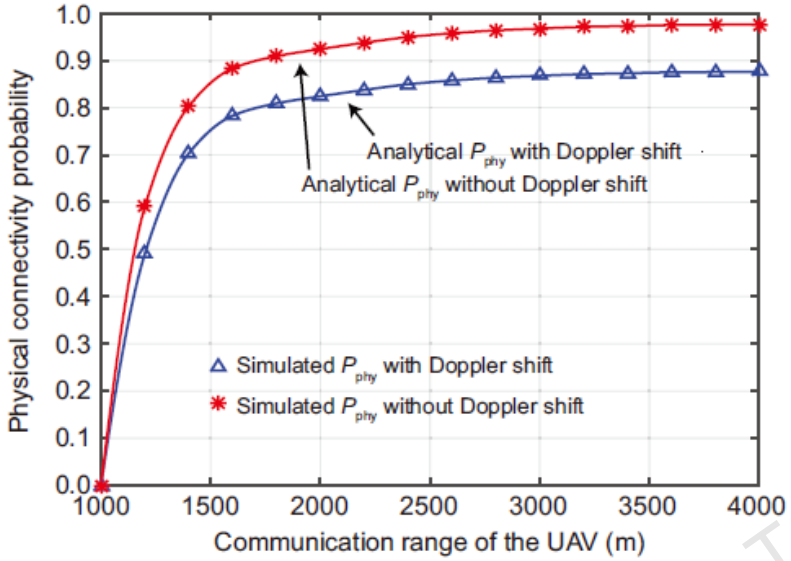

Fig. 9 The relationship between physical connectivity probability P_{phy} and communication range r_{th}

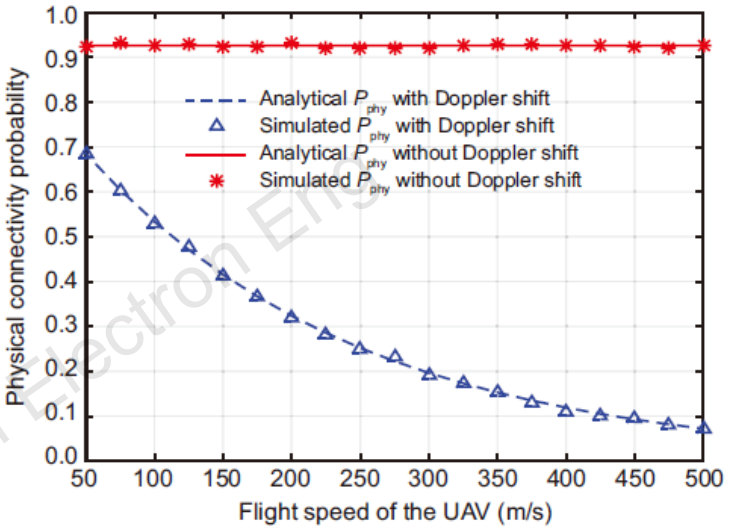

Fig. 10 The relationship between physical connectivity probability P_{phy} and flight speed of the UAV V

Fig. 9 shows that the physical connectivity probability with Doppler shift is significantly lower than that without Doppler shift, which means that Doppler effect caused by the high-speed movement of UAVs degrades the network performance.

Fig. 10 shows the flight speed has a negative impact on the connectivity probability, when Doppler shift is taken into consideration. As the speed increases, the Doppler shift grows gradually, leading to a continuous decrease in physical connectivity probability.

Major results (3)

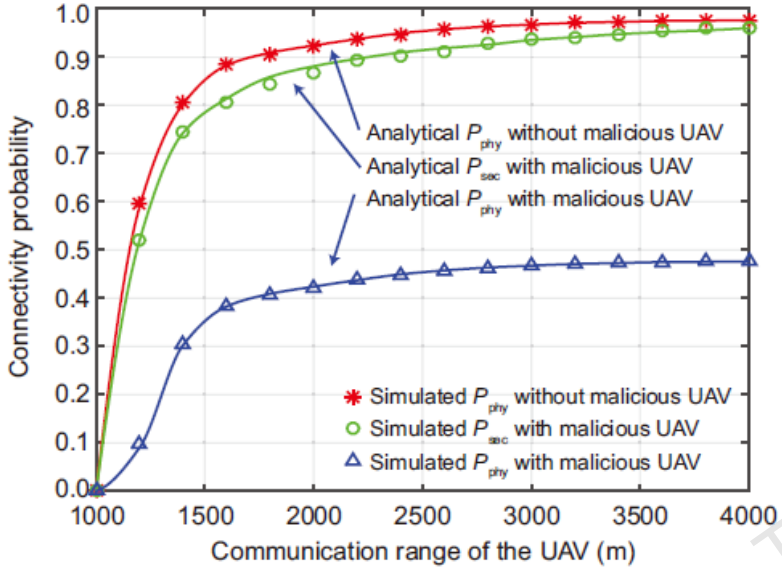

Fig. 11 The relationship between the connectivity probability and communication range r_{th}

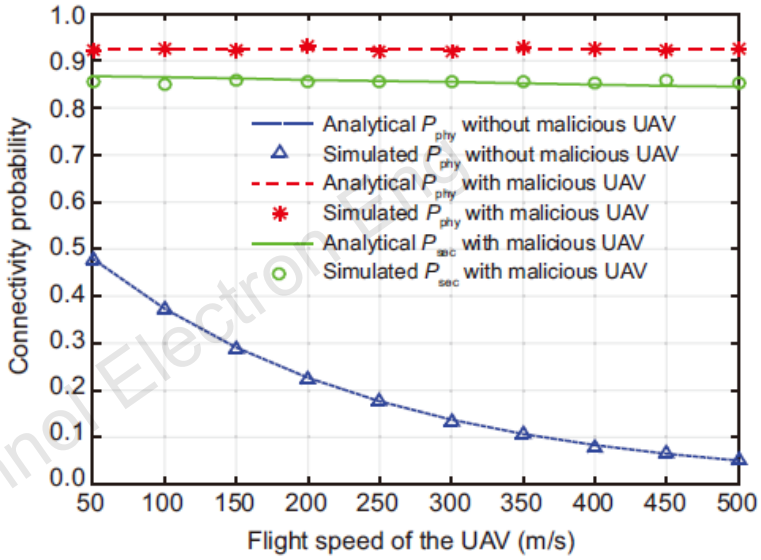

Fig. 12 The relationship between the connectivity probability and flight speed of the UAV V

Fig. 11 shows that P_{sec} between two UAVs with malicious UAVs is much higher than P_{phy} with malicious UAVs, and is closer to the P_{phy} without malicious UAVs. This proves the effectiveness of the trust model.

According to Fig. 12, the proposed trust model has good robustness and reliability, and can effectively improve network performance.

Conclusions

1. A novel trust model that can evaluate the reliability and security of UAVNs is proposed and established based on UAV communication behaviors, the characteristics of channels between UAV nodes, and the mobility of UAV nodes.

2. The proposed trust model can effectively ensure secure communication and reliable connectivity between UAVs and enhance network performance when the UAVNs suffer malicious attacks and other security risks.