Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Secure connectivity analysis in unmanned aerial vehicle networks*

Xin YUAN[1], Zhi-yong FENG‡[1], Wen-jun XU[1], Zhi-qing WEI[1], Ren-ping LIU[2]

[1]*MOE Key Laboratory of Universal Wireless Communications, Beijing 100876, China*

[2]*Global Big Data Technologies Centre, University of Technology Sydney, Sydney NSW2007, Australia*

E-mail: yuanxin@bupt.edu.cn; fengzy@bupt.edu.cn; wjxu@bupt.edu.cn; weizhiqing@bupt.edu.cn; RenPing.Liu@uts.edu.au

Received Jan. 10, 2017; Revision accepted Mar. 20, 2017; Crosschecked Mar. 15, 2018

Abstract: The distinctive characteristics of unmanned aerial vehicle networks (UAVNs), including highly dynamic network topology, high mobility, and open-air wireless environments, may make UAVNs vulnerable to attacks and threats. In this study, we propose a novel trust model for UAVNs that is based on the behavior and mobility pattern of UAV nodes and the characteristics of inter-UAV channels. The proposed trust model consists of four parts: direct trust section, indirect trust section, integrated trust section, and trust update section. Based on the trust model, the concept of a secure link in UAVNs is formulated that exists only when there is both a physical link and a trust link between two UAVs. Moreover, the metrics of both the physical connectivity probability and the secure connectivity probability between two UAVs are adopted to analyze the connectivity of UAVNs. We derive accurate and analytical expressions of both the physical connectivity probability and the secure connectivity probability using stochastic geometry with or without Doppler shift. Extensive simulations show that compared with the physical connection probability with or without malicious attacks, the proposed trust model can guarantee secure communication and reliable connectivity between UAVs and enhance network performance when UAVNs face malicious attacks and other security risks.

Key words: Unmanned aerial vehicle networks (UAVNs); Trust model; Secure connectivity; Doppler shift
https://doi.org/10.1631/FITEE.1700032 **CLC number:** TN92

1 Introduction

Unmanned aerial vehicles (UAVs) can be roughly categorized as quadrotors, unmanned miniature helicopters, unmanned airships, and fixed-wing unmanned aerial vehicles, etc., and are widely used in environmental and natural monitoring, disaster recovery, search and rescue, goods delivery, and construction (Bekmezci et al., 2013; Andre et al., 2014; Gupta et al., 2015). UAVs can also be used as relays or aerial base stations for network provisioning in an emergency due to their easy deployment and wide coverage (Hayat et al., 2016). When the task is complex, e.g., providing temporary communication for an earthquake area, a single UAV is usually insufficient. In addition, due to their typically low transmission power and limited processing ability, UAVs usually have a limited transmission range. As such, UAVs are generally organized in an ad hoc manner, forming unmanned aerial vehicle networks (UAVNs), and multi-hop relay is adopted for long-distance transmission. Thus, it is essential to consider how the connectivity varies among nodes in UAVNs, and evaluate the successful delivery of gathered information from a probabilistic angle.

Consider a search-and-rescue scenario after an earthquake. Several key issues need to be addressed,

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (No. 61631003)

ORCID: Xin YUAN, http://orcid.org/0000-0002-9167-1613

e.g., victims rescue and environment exploration. UAVNs may be established for temporary communication between rescuers and disaster victims, or for exploring the terrain and environment information to facilitate the subsequent search and rescue. Disaster areas are more likely to experience power interruption, so some types of UAVs (e.g., quadrotors) frequently need to operate on battery power and UAVNs must meet energy efficiency challenges (Kandeepan et al., 2014). Meanwhile, security is essential for UAVNs. Nodes in UAVNs 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.

Many researchers have developed trust models to evaluate the trust relationships among nodes in mobile ad hoc networks (MANETs) (Govindan and Mohapatra, 2012; Wei et al., 2014). A detailed survey on various trust models that are geared toward wireless sensor networks (WSNs) was presented by Han et al. (2014), who also analyzed various applications of trust models. Movahedi et al. (2016) proposed a unified trust management scheme using uncertain reasoning, which consists of two components: trust from direct observation and indirect observation. The trust from direct observation is derived using Bayesian inference, whereas the trust from indirect observation is derived using the Dempster-Shafer theory. An efficient distributed trust model (EDTM) for WSNs was proposed by Jiang et al. (2015), and direct trust and recommendation trust were selectively calculated according to the number of packets received by sensor nodes. However, these trust models are based mainly on communication behaviors, and important factors such as a node's residual energy, the channel between nodes, and the mobility pattern of the nodes are not considered. An information theoretic framework was presented by Xia et al. (2014), and the trust model considers the dynamic behaviors of nodes and the wireless environment. Moreover, a fuzzy-logic based prediction mechanism was adopted to update a node's trust for future decision-making. Han et al. (2015) proposed an attack-resistant trust model based on multidimensional trust metrics (ARTMM) for underwater acoustic sensor networks (UASNs), which consists of three types of trust metrics, i.e., link trust, data trust, and node trust. It also considers the slow movement of underwater sensor nodes. However, these trust models may not function well in UAVNs, because of their highly dynamic network topology, the high mobility of UAV nodes, and the open-air wireless environment. Due to this dynamic topology, the trust relationships between UAVs change frequently in UAVNs. Trust is a dynamic process and changes with time and the surrounding environment, but most existing trust models do not address the dynamic issues. To solve the above problems, we propose a novel trust model that can evaluate the trust levels between UAV nodes by considering multiple practical factors and their highly dynamic nature.

In this study, trust is defined as the degree of belief (probability) that a UAV will execute a task correctly according to the previous observation of its behavior. That is, the trust value reflects whether a given UAV node behaves in a trustworthy manner and maintains reliable communications with other nodes in UAVNs. A trust value is a number in the range of 0 to 1. Value 1 means 'completely trustworthy' and 0 means 'completely untrustworthy'.

The contributions of this study are outlined as follows:

1. We propose an efficient hierarchical trust model (EHTM) that considers the UAVs' behaviors, the characteristics of channels between UAV nodes, and the mobility of UAV nodes. The detailed calculation procedure of EHTM is also presented.

2. We propose the concept of 'secure links' in UAVNs. A secure link exists between two UAVs only when there is both a physical link and a trust link between them. The physical link indicates physical connectivity between two UAVs, which means each UAV node on a routing path is within the communication range of its previous UAV node. Based on the proposed trust model, the trust link between two UAVs can be viewed as a logical connectivity between these two nodes. Trust value or belief degree P_{T} is introduced to quantify the trustworthiness of the trust link between two nodes.

3. We derive both the physical connectivity probability and the secure connectivity probability between two UAVs in the presence of Doppler shift. The proposed trust model, physical connectivity probability, and secure connectivity probability in UAVNs are evaluated by simulation.

Extensive simulation results show that the proposed trust model can guarantee secure and reliable communication between UAVs and enhance the connectivity probability when UAVNs suffer from network attacks and other security risks.

2 System model

In this section, we first present the network model, considering mainly the search and rescue scenario. Then, we describe the basic mobility model for UAVs. Finally, we give a brief definition of the secure link in UAVNs.

2.1 Network model

We consider a UAVN, in which UAVs are deployed in an infinite three-dimensional (3D) Euclidean space according to a homogeneous Poisson point process (PPP) with a density λ (Fig. 1). The UAVs have a maximum one-hop communication range r. A UAV can transmit information to the intended destination directly, or via a relay by one or more UAVs. The multi-hop scheme is decode-and-forward, in which the relaying UAV decodes an arriving packet and then transmits to the next hop.

2.2 Mobility model

We adopt the smooth turn (ST) mobility model (Wan et al., 2013; Xie et al., 2014) for the motion of UAVs. ST captures the tendency of UAVs to make smooth trajectories (e.g., straight trajectories or typical turns with a large radius) and is widely used in UAVN analysis. The ST mobility model captures the correlation of acceleration of UAVs across the temporal and spatial domains and is tractable for analysis and design. Wan et al. (2013) proved that the stationary node distribution of the ST model is uniform, which leads to a series of closed-form results for connectivity.

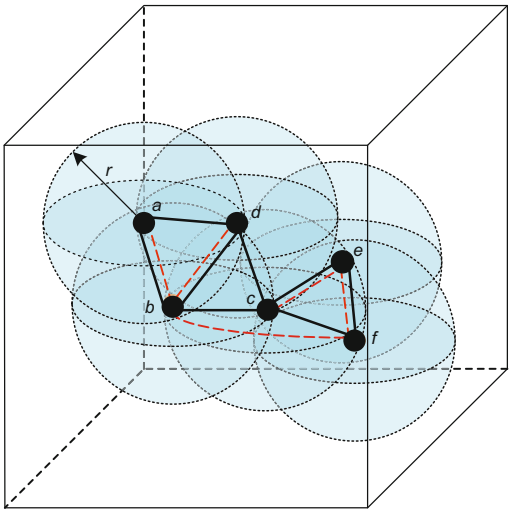

Fig. 1 An illustration of an unmanned aerial vehicle network with a trust link

Solid lines and dotted lines denote physical links and trust links, respectively

2.3 Definition of the secure link

2.3.1 Physical link

Two UAVs a and b have a physical wireless link if their Euclidean distance is no greater than the communication range r, and a and b are called 'physical neighbors' (Fig. 2a). Two UAVs are physically connected if there is a physical path from the source node to the destination node and each node on the path lies in the communication range of its previous node.

2.3.2 Trust link

A trust link can be viewed as a logical connection between two UAVs in UAVNs (Fig. 2b). One simple parameter, the trust value or belief degree, P_{T}, is introduced to quantify the existence of the trust link between two UAVs in UAVNs. If P_{T} is greater than or equal to 0.5, the trust link is considered to exist. Otherwise, it does not exist. We call

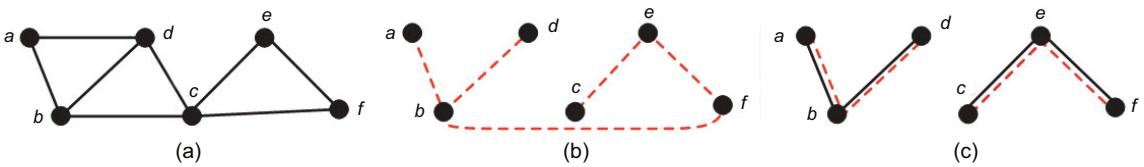

Fig. 2 Secure link abstracted from unmanned aerial vehicle networks in Fig. 1: (a) physical link; (b) trust link; (c) secure link

Solid lines and dotted lines denote physical links and trust links, respectively

two UAVs with a trust link 'friends'.

2.3.3 Secure link

A secure link exists between two UAVs in UAVNs only when there is both a physical link and a trust link between these two nodes (Fig. 2c). This means that each UAV not only has neighbor nodes within its communication range, but also can establish trust links with these neighbor nodes. We call a the 'neighboring friend' of b if a secure link exists between a and b.

3 Overview of the trust model

In this section, we propose an efficient hierarchical trust model (EHTM). To compute the trust value of UAVs, it is important to understand the trust definition and properties that are used in the trust calculation. Then, we describe the overall structure of the EHTM.

3.1 Definition and properties of trust

3.1.1 Definition

There are several definitions of trust in the literature (Govindan and Mohapatra, 2012), spannig aspects including reliability, utility, availability, risk, and quality of service. In this study, trust is defined as the degree of belief that a UAV will execute a task correctly according to the previous observation of its behavior. Thus, trust reflects whether a UAV behaves in a trustworthy manner and maintains reliable communications with other nodes in UAVNs. A trust value from 0 to 1 is assigned to each node, with 1 meaning 'completely trustworthy' and 0 'completely untrustworthy'.

Direct trust is evaluated based on direct communication with the target node. It reflects the trust relationship between two neighboring UAVs which are within each other's maximum communication range. When the target node is not accessible in one hop, its trust value is calculated using assessments from other nodes.

3.1.2 Trust properties

Trust properties are of significance for trust calculation. Based on Govindan and Mohapatra (2012), we consider three main properties of trust: asymmetry, transitivity, and composability. Asymmetry indicates that if UAV a trusts b to some degree, it does not necessarily mean that node b trusts a at the same degree. Transitivity implies that the trust value can be transferred along a path of trustworthy UAVs. If UAV a trusts UAV b and UAV b trusts UAV c, then we can deduce that a trusts c at a certain level. Composability means that trust values acquired from multiple available paths can be combined to obtain an integrated value.

3.2 Structure of the efficient hierarchical trust model

In Fig. 3, the trust model is composed of four sections: direct trust section, indirect trust section, integrated trust section, and trust update section.

In a direct trust model, the trust value is computed based on the communication behaviors of UAVs, the channels between UAVs, and the mobility of UAVs. However, due to malicious attacks, adopting only direct trust is not sufficient. In addition,

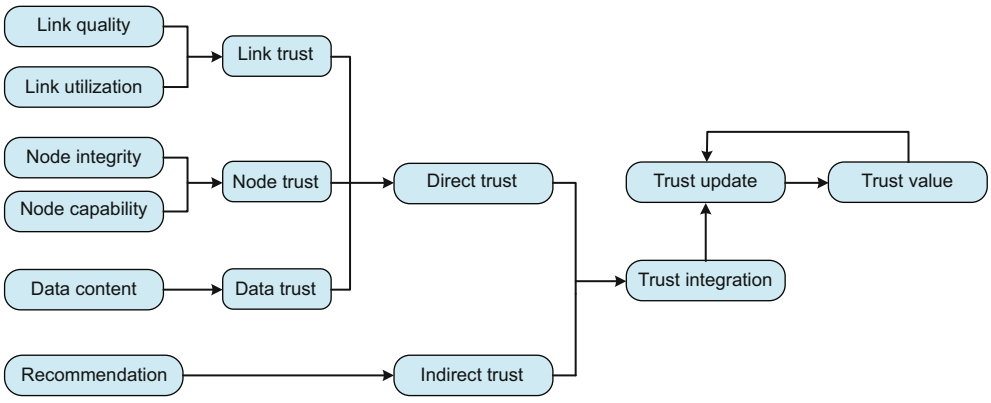

Fig. 3 Structure of the trust model

it is difficult to decide whether a UAV is benign or malicious based on only a few interactions when the number of packet exchanges between two UAVs is small. Therefore, the threshold for the number of packet exchanges is defined and denoted as ζ_{th}. If the number of packet exchanges between a pair of nodes exceeds the threshold ζ_{th}, the trust value is calculated only by the direct trust. Otherwise, assessments from other nodes are required for trust estimation. In this case, we need to calculate both the direct trust and the indirect trust, and then combine them using a weighted average to obtain the integrated trust.

In UAVNs, UAVs collaborate with each other to transmit information through communication channels. In a natural disaster, UAVs can be easily attacked or launch many kinds of malicious attacks, e.g., packet modification attacks and packet dropping attacks, which can result in low link quality. In addition, the communication channel between UAVs is unreliable, which may introduce a high packet error rate (PER) and packet loss rate (PLR). The communication performance and data transmission are affected by the quality of the channel. Therefore, the trust value is not only related to the participating UAVs but also impaired by the link quality.

In Fig. 3, the direct trust module consists of three components: link trust, node trust, and data trust. Link trust is evaluated by link quality and link utilization. Link quality illustrates the performance of the communication channel between UAVs, which is calculated based on the PER and PLR estimations of the link. Link utilization is defined as the ratio of the number of times that a link is used to the maximum possible number of times that it can be used. Data trust reflects the trustworthiness of data content transmitted between UAVs, which can be assessed by the fault tolerance and consistency of data. Node trust is determined by node integrity and node capability. Node integrity indicates the degree to which one UAV believes that its neighboring node is honest based on their communication behaviors (successful and failure communications). Node capability refers to whether the residual energy in one UAV is adequate to perform the desired task; i.e., it is computed according to the energy consumption of UAVs. According to the link trust, node trust, and data trust, we can obtain the direct trust using the weighted average method. In addition, the indirect trust can be calculated from the third-party recommendation. Finally, the trust value can be obtained through the trust integration and trust update sections.

4 Trust calculation in the efficient hierarchical trust model

In this section, we present the detailed EHTM trust calculation procedure.

4.1 Calculation of direct trust

In this study, direct trust considers link trust, data trust, and node trust.

4.1.1 Link trust

Link trust is determined by link quality and link utilization in this study.

1. Calculation of the packet error rate

We choose the Rician fading model for the UAV channel, due to the existence of a line-of-sight (LOS) path between UAVs in an open-air scenario. The average bit error rate (BER) for two-phase differential phase shift keying (2DPSK) modulation under the Rician fading channel was given in Simon and Alouini (2000) as

$$P_{\text{ber}} = \frac{1}{2}\left(\frac{1+K}{1+K+\bar{\gamma}}\right)\exp\left(-\frac{K\bar{\gamma}}{1+K+\bar{\gamma}}\right), \quad (1)$$

where K is the Rician factor, $\bar{\gamma}$ is the average signal-to-noise ratio (SNR), and $\bar{\gamma} = P_0/(\sigma_{\text{N}}^2 d^2)$ (P_0 is the transmitting power, σ_{N}^2 is the noise power, and d is the distance between the source UAV and the destination UAV). In the next step, we compute the PER based on the BER. The probability of not having a bit error is equal to the probability that all the bits are received correctly. Thus, the PER is calculated as

$$P_{\text{per}} = 1 - (1 - P_{\text{ber}})^n, \quad (2)$$

where n denotes the number of bits in a packet.

2. Calculation of the packet loss rate

There are several metrics for link quality in UAVNs, such as the received signal strength indicator (RSSI), packet receiving ratio (PRR), and link quality indicator (LQI). In this study, we choose the PRR for link quality evaluation. The PRR is usually calculated by the destination node and expressed as $P_{\text{prr}} = p_{\text{rec}}/p_{\text{sen}}$, where p_{rec} and p_{sen} denote the

number of successfully received packets in the object UAV node and the total number of packets sent from the subject node, respectively.

Then, the packet loss rate can be calculated by by $P_{\text{loss}} = 1 - P_{\text{prr}}$. According to Eqs. (1) and (2), the link quality L_{lq} can be computed by

$$L_{\text{lq}} = (1 - P_{\text{per}})(1 - P_{\text{loss}}) = (1 - P_{\text{per}})\, P_{\text{prr}}. \quad (3)$$

3. Calculation of link utilization

According to the routing table entry of UAVs, the maximum possible number of utilization times can be obtained:

$$L_{\text{lu}} = \frac{N_{\text{use}}}{N_{\text{max}}}, \quad (4)$$

where N_{use} is the number of times that a link is used in the current time window and N_{max} is the maximum possible number of times that the link can be used.

We define 0.5 as the chosen trust threshold. The link trust depends on the link quality and link utilization. If the link is of poor quality, $L_{\text{lq}} < 0.5$, the link is considered untrustworthy even if the link utilization is high. Therefore, when $L_{\text{lq}} < 0.5$, the link trust is defined as $L_{\text{lq}}L_{\text{lu}}$. However, the definition is not suitable when $L_{\text{lq}} > 0.5$. For example, if $L_{\text{lq}} = 0.8$ and $L_{\text{lu}} = 0.6$, the link trust is 0.48. In this case, the link should be trustworthy even though its calculated trust value is less than 0.5. Therefore, the link trust is redefined as $0.5 + (L_{\text{lq}} - 0.5)\, L_{\text{lu}}$. Then the link trust can be obtained as

$$T_{\text{link}} = \begin{cases} 0.5 + (L_{\text{lq}} - 0.5)\, L_{\text{lu}}, & L_{\text{lq}} \geq 0.5, \\ L_{\text{lq}}L_{\text{lu}}. & \text{otherwise.} \end{cases} \quad (5)$$

4.1.2 Node trust

Node trust is computed by considering both node integrity and node capability. Node integrity is evaluated based on the direct communication behaviors of one UAV to check whether the node is reliable or not.

1. Node integrity

In UAVNs, UAVs move rapidly, the network topology changes dynamically, and the communication links between UAVs are unstable; thus, UAV communication behaviors in UAVNs involve considerable uncertainty. To deal with this uncertainty, we adopt a subjective logic framework (Jøsang, 1999). The trust value in the subjective logic framework is denoted by a triplet $\tau = \{\tau_{\text{b}}, \tau_{\text{d}}, \tau_{\text{u}}\}$, where τ_{b}, τ_{d}, and τ_{u} correspond to belief, disbelief, and uncertainty, respectively ($\tau_{\text{b}}, \tau_{\text{d}}, \tau_{\text{u}} \in [0, 1]$, $\tau_{\text{b}} + \tau_{\text{d}} + \tau_{\text{u}} = 1$). On the basis of a subjective logic framework, the trust model for node integrity is established, and node integrity N_{ni} can be calculated by

$$N_{\text{ni}} = \frac{2\tau_{\text{b}} + \tau_{\text{u}}}{2}, \quad (6)$$

where $\tau_{\text{b}} = s/(s + f + 1)$, $\tau_{\text{u}} = 1/(s + f + 1)$, and s and f are the numbers of successful and unsuccessful communications between UAVs in UAVNs, respectively. Successful or failed communication between two nodes depends on the link quality (packet loss ratio), and thus the numbers of successful and failed communications between UAVs can be adjusted as

$$s' = s + P_{\text{loss}}(s + f), \quad (7)$$

$$f' = f - P_{\text{loss}}(s + f). \quad (8)$$

2. Node capability

Node capability is the assessment of the residual energy level of UAVs. It is assumed that the initial energy sets and energy consumption rates of all UAVs are the same in UAVNs. However, when malicious UAVs launch malicious attacks in UAVNs, the energy consumed by them is abnormal. Normal nodes consume less energy than malicious nodes. Therefore, we determine whether a node is malicious or not according to its energy consumption. First, we define an energy consumption threshold E_{th}. When the residual energy of the UAV is below the threshold, the node cannot accomplish the expected task. In this case, node capability is assumed to be zero. Otherwise, node capability can be computed by the energy consumption rate r_{ene} ($r_{\text{ene}} \in [0, 1]$). The higher the energy consumption rate is, the less residual energy remains, and the weaker the node capability will be. Thus, node capability N_{nc} is expressed as

$$N_{\text{nc}} = (1 - r_{\text{ene}})\, S(E_{\text{res}}, E_{\text{th}}), \quad (9)$$

where r_{ene} is calculated using the method introduced by Vazifehdan et al. (2014), and

$$S(E_{\text{res}}, E_{\text{th}}) = \begin{cases} 1, & E_{\text{res}} \geq E_{\text{th}}, \\ 0, & E_{\text{res}} < E_{\text{th}}. \end{cases}$$

Based on node integrity and node capability, node trust can be evaluated as

$$T_{\text{node}} = \begin{cases} 0.5 + (N_{\text{ni}} - 0.5)\, N_{\text{nc}}, & N_{\text{nc}} \geq 0.5, \\ N_{\text{ni}}N_{\text{nc}}, & \text{otherwise.} \end{cases} \quad (10)$$

4.1.3 Data trust

Data transmission is subject to several sources of errors such as noise from external sources, hardware noise, inaccuracy, and imprecision, and various environmental effects (Elnahrawy and Nath, 2003). Such errors may seriously impact the trustworthiness of the data. Therefore, data trust evaluation is introduced in this study. It assesses the trust value of the fault tolerance and data consistency. Generally, data information has temporal and spatial correlations; that is, in a certain time period the data sent among neighboring UAVs are always similar in the same area. The numerical value of the data information always follows some certain distribution, such as normal distribution and exponential distribution. For simplicity, we assume that the distribution of data items complies with a normal distribution and that the probability density function is

$$f(x)=\frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right),$$

where x is the attribute value of a data item, and μ and σ^2 are the mean and variance of the data, respectively. Based on Lim et al. (2010), the trust value of the data item is defined as

$$T_{\mathrm{data}}=2\left(0.5-\int_{\mu}^{v_{\mathrm{d}}}f(x)\,\mathrm{d}x\right)=2\int_{v_{\mathrm{d}}}^{\infty}f(x)\,\mathrm{d}x, \tag{11}$$

where v_{d} is the value of a data item.

Based on link trust T_{link}, node trust T_{node}, and data trust T_{data}, we can obtain the direct trust between two neighboring UAV nodes as

$$T_{\mathrm{direct}}=\omega_{\mathrm{link}}T_{\mathrm{link}}+\omega_{\mathrm{node}}T_{\mathrm{node}}+\omega_{\mathrm{data}}T_{\mathrm{data}}, \tag{12}$$

where ω_{link}, ω_{node}, and ω_{data} are the weights of link trust, node trust, and data trust, respectively, $\omega_{\mathrm{link}}\in[0,1]$, $\omega_{\mathrm{node}}\in[0,1]$, $\omega_{\mathrm{data}}\in[0,1]$, and $\omega_{\mathrm{link}}+\omega_{\mathrm{node}}+\omega_{\mathrm{data}}=1$.

4.2 Calculation of indirect trust

4.2.1 Recommendation

Third-party recommendation needs to be considered in indirect trust calculation. However, some recommendations are dishonest, and using these false recommendations may lead to an unreliable trust evaluation. Therefore, it is necessary to identify these false recommendations before trust calculation. In this study, we use recommendation trust to evaluate to what extent the recommendation from other nodes can be trusted. Recommendation trust is evaluated based on both node integrity and the recommendation value of each recommendation node. First, it is assumed that one UAV receives the node integrity from l neighboring UAVs. Then, weighting factor χ_i of recommendations from each recommendation node is computed based on these node integrities:

$$\chi_i=\frac{N_{\mathrm{ni}}(i)}{\sum\limits_{k\in R}N_{\mathrm{ni}}(k)},$$

where $N_{\mathrm{ni}}(i)$ denotes the node integrity of node i and R is the set of recommendation nodes. Finally, the recommendation trust is obtained as

$$T_{\mathrm{rec}}=\frac{1}{l}\sum_{i=1}^{l}\chi_i\cdot T_i, \tag{13}$$

where T_i is the recommendation value from recommendation node i.

4.3 Integrated trust calculation

When the communication packets between the subject UAV nodes and object UAV nodes are higher than the threshold ζ_{th}, the trust value is calculated only by direct trust. Otherwise, the recommendations from third parties are needed for trust estimation. Therefore, the trust value can be calculated as

$$P_{\mathrm{T}}=\begin{cases}T_{\mathrm{direct}}, & s'\geq\zeta_{\mathrm{th}},\\ \omega T_{\mathrm{direct}}+(1-\omega)T_{\mathrm{rec}}, & \text{otherwise},\end{cases} \tag{14}$$

where ω is the weight for direct trust.

4.4 Trust update

Due to the highly dynamic nature of the UAVN, UAVs enter and leave the network rapidly, so the trust value needs to be updated periodically. The length of the update interval will affect network performance. If the update interval is too long, it cannot effectively reflect the current behavior of the object UAV node. If the update time is too short, it may consume too much energy. Therefore, the concept of 'sliding time window' is adopted to update the trust value.

A time window consists of several time slots. During each time window, the current trust value

of the object UAV can be calculated. Then, in the next time window, the historical trust values can be used to update the new trust value. As we all know, time decay is an important property of trust, which means that historical behavior is not as important as current behavior. Thus, when using historical trust values to update current values, it is necessary to consider a time decay factor for historical trust values. In Salmanian et al. (2010), the trust value decayed exponentially with time, while it decreased linearly with time in Wang and Wu (2007). In this study, we choose the exponential decay in the trust model, which is defined as

$$\omega_{\mathrm{d}} = \exp\left(-\delta\left(t_i - t_{i-1}\right)\right), \tag{15}$$

where $\delta \in (0,1)$ is the a regulatory factor, and t_i and t_{i-1} are the trust calculation times of the current and historical trust values, respectively.

Based on the current trust values $P_{\mathrm{T}}(i)$ and the historical trust values $P_{\mathrm{T}}(i-1)$, the trust value can be updated as

$$P_{\mathrm{T}}(i)_{\mathrm{new}} = \omega_{\mathrm{d}} P_{\mathrm{T}}(i-1) + (1-\omega_{\mathrm{d}}) P_{\mathrm{T}}(i). \tag{16}$$

5 Secure connection between UAVs in UAVNs

In this section, we first analyze the physical connectivity probability between UAVs using stochastic geometry. Then, based on the EHTM, the secure connectivity probability between UAVs is derived.

5.1 Physical connection in unmanned aerial vehicle networks

Physical connection in UAVNs is closely related to the existence of a physical link. Besides, the physical connectivity probability in this study refers to the probability that each node on the path falls within the communication range of its previous node.

5.1.1 Unmanned aerial vehicle isolation probability

Let M be a random variable denoting the number of UAVs that is present in the communication range of UAV A. Because the UAVs in the UAVN are uniformly distributed with density λ, it can be shown that M is Poisson distributed with the following probability mass function (PMF):

$$P_M(m) = \frac{1}{m!}\left(\frac{4}{3}\pi r^3\lambda\right)^m \exp\left(-\frac{4}{3}\pi r^3\lambda\right). \tag{17}$$

A UAV will be isolated in UAVNs if there is no UAV in its communication range. Let P_{i} represent the probability that no UAV appears within its communication range. Thus the probability of one UAV being isolated is

$$P_{\mathrm{i}} = P_M(0) = \exp\left(-\frac{4}{3}\pi r^3\lambda\right). \tag{18}$$

5.1.2 Unmanned aerial vehicle isolation probability with Doppler shift

The Doppler effect is the change in the frequency of a wave perceived by the receiver, due to the relative motion between the transmitter and the receiver. Doppler shift is the value of the frequency change. In most cases, Doppler shift can be eliminated by techniques such as frequency offset estimation in the physical layer. However, if the Doppler frequency offset exceeds a certain threshold f_{th}, it is difficult to compensate for and the signal quality will be severely affected. The threshold of Doppler shift is determined mainly by the receiver's hardware. The high mobility of UAVs will cause serious Doppler shift, which will affect the communication quality between UAVs. In a 3D mobile radio environment, the Doppler shift of a signal reaching a UAV receiver is

$$f_{\mathrm{d}} = \frac{v}{c} f_{\mathrm{c}} \cos\theta\cos\beta = f_{\mathrm{m}}\cos\theta\cos\beta, \tag{19}$$

where f_{c} is the carrier frequency of the signal without Doppler shift, v is the relative moving velocity of the UAV node pair, c is the velocity of light, θ and β are the azimuth angle (AA) and elevation angle (EA) of the arriving signal, respectively, and $f_{\mathrm{m}} = \frac{v}{c} f_{\mathrm{c}}$ is the maximum Doppler shift. For the environment of interest and without loss of generality, we focus on the cases where (1) the AA and EA are random variables that are independent of each other and (2) the AA is uniformly distributed in $(-\pi, \pi)$, that is,

$$p_\theta(\theta) = \frac{1}{2\pi}, \quad |\theta| \le \pi. \tag{20}$$

The EA is distributed within $(0, \pi/2)$, with its probability density function (PDF) denoted by $p_\beta(\beta)$. To facilitate the calculation, we define the normalized Doppler shift as $\rho \equiv f_{\mathrm{d}}/f_{\mathrm{m}} = \cos\theta\cos\beta, \quad |\rho| \le 1$, which implies that $|\gamma| \le \cos\theta$ and $|\gamma| \le \cos\beta$. The

cumulative distribution function of ρ is

$$F_\rho(\rho) = \Pr\{\cos\theta\cos\beta \le \rho\} = \frac{1}{\pi}\int_0^{\pi/2} p_\beta(\beta)\left[\int_{\arccos(\rho/\cos\beta)}^{\pi} \mathrm{d}\theta\right]\mathrm{d}\beta. \quad (21)$$

It is difficult to analyze the Doppler shift distribution between two moving UAVs. For convenience, we transform the original problem between two moving UAVs into an equivalent problem between a stationary UAV and a moving UAV with respect to the stationary one. In Fig. 4, the position of the receiving UAV (UAV A) is chosen as the coordinate origin, and the sending UAV (UAV B) locates at the surface of the oblate spheroid space that surrounds the receiving UAV. If it is assumed that all scatters are uniformly distributed in the space, then the PDF of EA can be obtained according to Janaswamy (2002):

$$p_\beta(\beta) = \frac{ab^2\cos\beta}{\left(a^2\sin^2\beta + b^2\cos^2\beta\right)^{3/2}}, \quad (22)$$

where a and b are the semi-principle axes along the x and z axes, respectively. Defining $\varepsilon \equiv a/b$, we have

$$p_\beta(\beta) = \frac{\varepsilon\cos\beta}{\left(\varepsilon^2\sin^2\beta + \cos^2\beta\right)^{3/2}}, \quad (23)$$

which is dependent only on parameter ε. Then we obtain

$$p_\rho(\rho) = \frac{\varepsilon}{\pi(\varepsilon^2-1)^{3/2}} H(\rho), \quad (24)$$

where

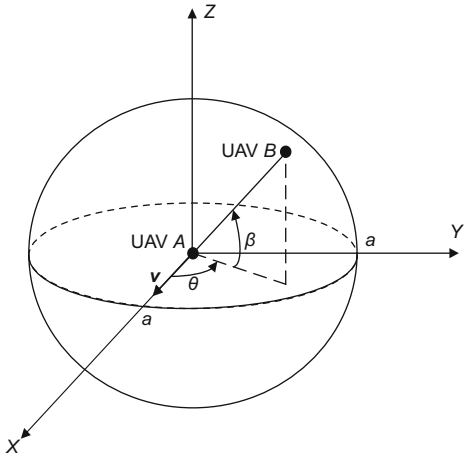

Fig. 4 An illustration of the oblate spheroid model

$$H(\rho) = \int_0^{\sqrt{1-\rho^2}} \left[\left(x^2 + \frac{1}{\varepsilon^2-1}\right)^3 \left(1-\rho^2-x^2\right)\right]^{-\frac{1}{2}} \mathrm{d}x. \quad (25)$$

The integral in Eq. (25) can be computed according to Formula 3.158 provided in Gradshteyn and Ryzhik (2000). Then we can obtain the PDF of the Doppler shift:

$$p_\rho(\rho) = \frac{\varepsilon}{\pi\sqrt{(\varepsilon^2-1)(1-\rho^2)}} E\left(\frac{\sqrt{(\varepsilon^2-1)(1-\rho^2)}}{\sqrt{1+(\varepsilon^2-1)(1-\rho^2)}}\right), \quad (26)$$

where $E(k) = \int_0^{\pi/2}\sqrt{1-k^2\sin^2\alpha}\,\mathrm{d}\alpha$ is the complete elliptic integral of the second kind with $k \in [0,1]$ being the elliptic eccentricity.

It is assumed that all UAVs in UAVNs have the same Doppler shift threshold f_{th}. If the Doppler shift is greater than the threshold, then two UAVs within the communication range of each other will not be able to communicate successfully (Li et al., 2010). Therefore, the communication link between two adjacent UAVs is available when two conditions are satisfied at the same time: (1) Two UAVs are within the communication range of each other; (2) The Doppler shift meets the threshold requirement, i.e., $f_{\mathrm{d}} \le f_{\mathrm{th}}$ (Li et al., 2010).

According to the PDF of the Doppler shift, we can obtain the probability that the frequency deviation between two UAVs is less than the threshold:

$$P_{\mathrm{th}} = F_\rho(\rho_{\mathrm{th}}) = \int_0^{\rho_{\mathrm{th}}} p_\rho(\rho)\,\mathrm{d}\rho, \quad (27)$$

where $\rho_{\mathrm{th}} = f_{\mathrm{th}}/f_m$. The probability that one UAV is not isolated can also be obtained based on the UAV isolation probability. Finally, the physical probability of the available link between two UAV nodes is calculated as

$$P_{\mathrm{phy}} = (1-P_{\mathrm{i}})P_{\mathrm{th}} = \left[1-\exp\left(-\frac{4}{3}\pi r^3\lambda\right)\right] F_\rho(\rho_{\mathrm{th}}). \quad (28)$$

5.2 Secure connection analysis in unmanned aerial vehicle networks

In this study, we assume that the UAVs are distributed in a 3D Euclidean space according to a homogeneous PPP with density λ, so the number of UAVs within the communication range r of the object UAV is $4\pi r^3\lambda/3$. In addition, if the trust value

P_{T} of the object UAV node is considered, we define the UAV that has trust links to the object node as friends. Then we can acquire the number of neighboring friends that are within the communication range of the object UAV node as $P'_{\mathrm{T}} \cdot 4\pi r^3\lambda/3$, where $P'_{\mathrm{T}} = (\sum_{i=1}^{M} P_{\mathrm{T}i})/M$, $P_{\mathrm{T}i}$ is the trust value of UAV i, and M is the number of UAVs that are present in the communication range of the object node. Similar to the derivation of the physical probability of the available link between two UAVs, the probability of secure connectivity between two UAVs in UAVNs can be obtained as

$$\begin{aligned} P_{\mathrm{sec}} &= (1 - P'_{\mathrm{i}})\, P_{\mathrm{th}} \\ &= \left[1 - \exp\left(-P'_{\mathrm{T}} \cdot \frac{4}{3}\pi r^3\lambda\right)\right] F_{\rho}\left(\rho_{\mathrm{th}}\right), \end{aligned} \quad (29)$$

where $P'_{\mathrm{i}} = \exp\left(-P'_{\mathrm{T}} \cdot 4\pi r^3\lambda/3\right)$ is the probability that there are no friends within the communication range of the object UAV node.

6 Simulation results and analysis

In this section, the trust model, physical connectivity probability, and secure connectivity probability in UAVNs are evaluated by simulations. We implement two different sets of simulations. First, we evaluate the performance of the trust model under various parameters, e.g., different weights and different trust update time. Then, we compare the physical connectivity probability and secure connectivity probability with or without the trust model based on the proposed trust model. The deployment area is set to be 10 km×10 km×10 km. There are 30 UAV nodes uniformly deployed in the network area initially. Then they move according to the ST mobility model within the region. Some important parameters are listed in Table 1.

Table 1 Simulation parameters (Jiang et al., 2015)

Parameter	Value
Transmit power P_0	5 W
Noise power σ_{N}^2	−20 dBm
Rician factor K	10 dB
Energy consumption rate r_{ene}	0.4
Residual energy threshold	0.3
Communication packets threshold ζ_{th}	300

6.1 Performance of the trust model

We first evaluate the trust model between two UAVs. To compare the trust value calculated by the proposed trust model, we first derive the objective trust. The objective trust is computed on the basis of each UAV's actual information without considering any malicious attacks. Then, the malicious UAV nodes are simulated by a denial-of-service (DoS) attack, and the proportion of malicious UAV nodes is set at 30%.

Fig. 5a shows the results of direct trust, integrated trust, and objective trust values with the update of UAVs when the number of communication packets is higher than the threshold ζ_{th}. In this case, direct trust is closer to objective trust compared with integrated trust, because integrated trust is influenced by the malicious recommenders. Thus, in this case, we need only to calculate the direct trust values for trust evaluation.

Fig. 5b shows that when there are fewer communication packets between the subject and object UAVs than the threshold ζ_{th}, the integrated trust values are closer to the objective trust values compared with the direct trust values, because there are not enough communication packets between these two UAVs to reflect accurately the actual node behaviors. Therefore, it is essential to take recommendation into consideration for trust evaluation when the number of communication packets is small or the communication time is short. Also, in Figs. 5a and 5b, we can find that the trust values increase gradually with the simulation time.

According to Figs. 5a and 5b, we can conclude that it is important to integrate direct trust and indirect trust when there are not enough packet exchanges for nodes' trust evaluation. In addition, the proper weights for direct and indirect trusts change with the environmental conditions. In our trust model, the subject UAV adopts the recommendations from neighboring UAVs concerning the object UAV. We assume that the proportion of malicious neighbor UAVs that launch the attack ranges from 0 to 70% with a 10% increment. It is also assumed that there are enough communication packets between UAVs and that the number of average packets is 300 during each period. The weights for the direct trust are denoted as ω.

Fig. 6 shows the relationship between the trust

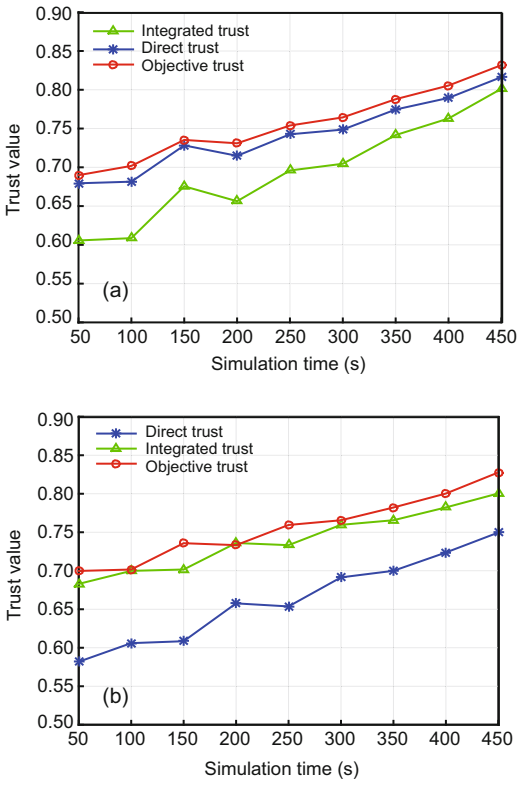

Fig. 5 Direct trust, integrated trust, and trust values with the update of UAVs when the number of communication packets is higher (a) or lower (b) than the threshold

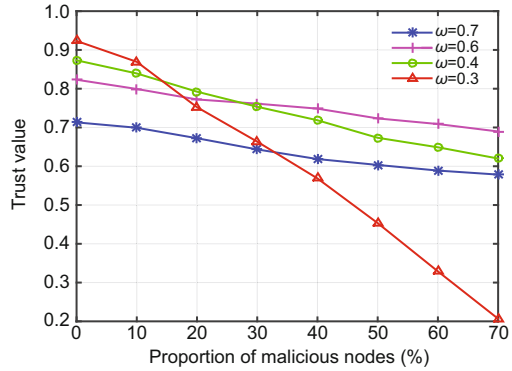

Fig. 6 Influence of the weights on the relationship between the trust value and the proportion of malicious nodes in the UAVNs

value and malicious node proportion with different weights ω. The trust value is highest when $\omega = 0.3$ and the proportion of malicious UAVs is less than 10%. In this case, we evaluate the trust by calculating only the direct trust value because of the small impact from malicious UAVs. In addition, the trust value is higher than 0.5 when the proportion of malicious UAV nodes is below 45%. However, as the proportion of malicious UAVs increases continually, the trust value decreases significantly. As the proportion of malicious UAVs in the UAVNs grows, the weight of direct trust becomes lower and the obtained trust value becomes lower. Thus, we can conclude that more malicious nodes in the UAVNs will result in lower trust values between UAVs. Moreover, the weights for direct and indirect trusts need to be adjusted dynamically according to the number of malicious nodes in the network.

In the trust model, the trust values are updated dynamically. Generally, updating the trust value frequently may consume a large amount of energy. Conversely, if the update time interval is too long, the actual behavior of the object UAV node cannot be effectively determined. The influence of the trust update time interval on the trust value is evaluated, and the results are shown in Fig. 7. The trust value decreases slowly at first and then rapidly with the increased update time interval. In addition, as the simulation time increases, the trust value increases constantly. Thus, we can choose a larger time interval for trust evaluation to reduce energy consumption. However, when a more accurate trust value is required, a smaller time interval may be selected.

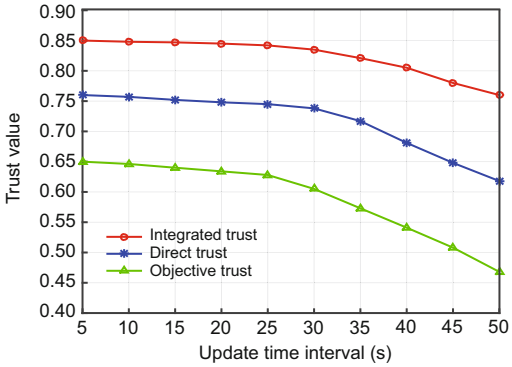

Fig. 7 Influence of the trust update time interval on trust values

In Fig. 8, the robustness of the proposed trust model is evaluated. We adopt the ST mobility model for UAVs, where the velocity of the UAV nodes ranges from 50 to 500 m/s. We can see that the proposed trust model can work well in the open-air scenario and be robust against the mobility of UAVs.

6.2 Physical connectivity probability

In this section, we simulate the physical connectivity probability between two UAVs in UAVNs according to the above calculation. We will illustrate

how the probability changes with different parameters: communication range $r_{\rm th}$ and flight speed V. To make the simulation more realistic, we set the carrier frequency at 5 GHz based on IEEE 802.11n, and assume that the Doppler shift threshold of the receiver is 1000 Hz.

Fig. 9 shows the relationship between physical connectivity probability $P_{\rm phy}$ and communication range $r_{\rm th}$ of the UAV. With $r_{\rm th}$ increasing from 1000 m to 4000 m, the physical connectivity probability between neighboring UAVs increases a lot. It also shows that the physical connectivity probability with Doppler shift is significantly lower than that without Doppler shift, which means that the Doppler effect caused by the high-speed movement of UAVs may degrade the network performance. Therefore, it is necessary to eliminate the Doppler shift at the receiving end and improve the performance of the UAVNs.

Fig. 10 shows the relationship between $P_{\rm phy}$ and the flight speed of the UAV. The flight speed of the UAV has a negative impact on the connectivity between neighboring UAVs, especially when the Doppler shift is considered. As the speed of the UAV increases, the Doppler frequency offset grows gradually, leading to a continuous decrease in physical connectivity probability.

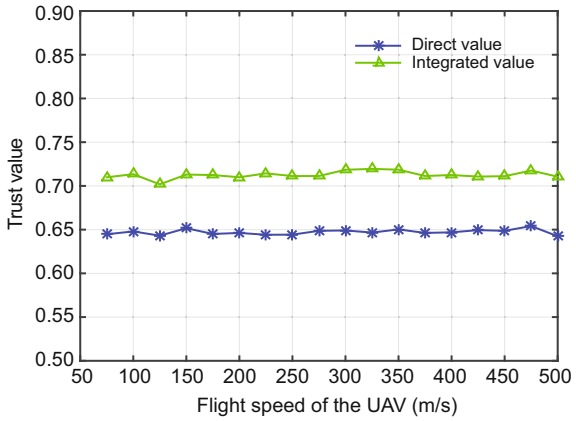

Fig. 8 Robustness of the proposed trust model against mobility

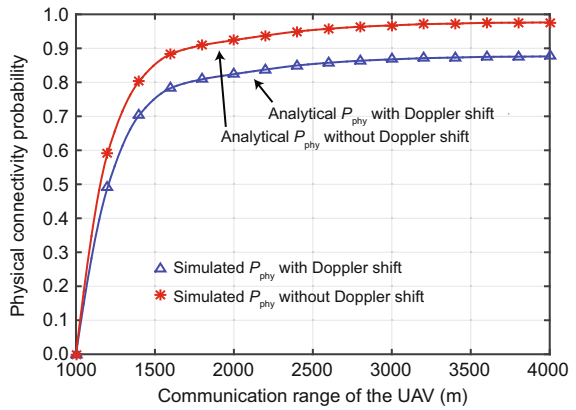

Fig. 9 The relationship between physical connectivity probability $P_{\rm phy}$ and communication range $r_{\rm th}$

6.3 Secure connectivity probability

In this section, the secure connectivity probability between two UAVs in UAVNs is simulated. We compare the secure connectivity probability with the physical connectivity probability in the presence of malicious UAV nodes. It is assumed that the proportion of malicious UAVs in the network is 30%.

Fig. 11 shows the relationship between the connectivity probability and the communication range of the UAV. With an increase in the communication range $r_{\rm th}$, both physical and secure connectivity

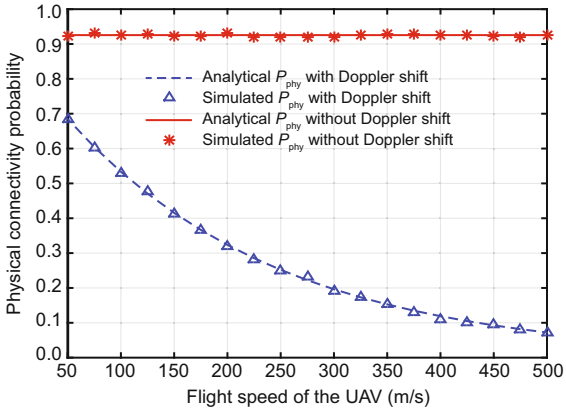

Fig. 10 The relationship between physical connectivity probability $P_{\rm phy}$ and flight speed of the UAV V

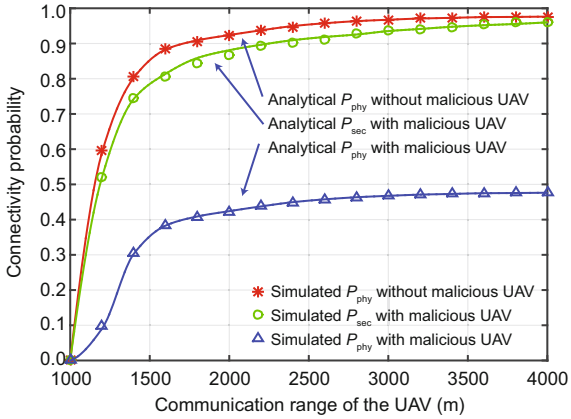

Fig. 11 The relationship between the connectivity probability and communication range $r_{\rm th}$

probabilities increase. In addition, the secure connectivity probability P_{sec} between two neighboring UAVs with malicious UAVs is much higher than P_{phy} with malicious UAVs, and is closer to the P_{phy} without malicious UAVs. The trust evaluation occurring between the subject and object UAV may consume time, energy, and other resources, resulting in a slightly lower secure connectivity probability with malicious nodes than without malicious nodes. However, when there are malicious UAVs in the networks, the connectivity probability can be improved greatly with the trust model of UAVs. This proves the effectiveness of the trust model.

Fig. 12 depicts the relationship between the connectivity probability in UAVNs and the flight speed of UAVs. We can observe that both P_{sec} and P_{phy} are almost unchanged as the flight speed increases. In the presence of malicious UAV nodes, P_{sec} is clearly higher than P_{phy}. Therefore, we can conclude that the proposed trust model has good robustness and reliability, and can effectively improve network performance. According to theoretical analysis and simulation, we find that the trust model established in this study can guarantee secure and reliable communication between UAVs and boost the connectivity probability when the UAVNs suffer from network attacks and other security risks.

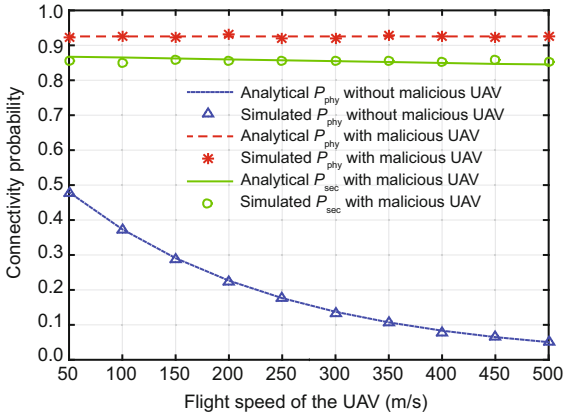

Fig. 12 The relationship between the connectivity probability and flight speed of the UAV V

7 Conclusions

In this study, we have proposed a novel trust model that can be used to evaluate the reliability and security of UAVNs. The trust model is established based on UAV communication behaviors, the characteristics of channels between UAV nodes, and the mobility of UAV nodes. In addition, it consists of four sections: direct trust section, indirect trust section, integrated trust section, and trust update section. The concept of 'secure link' in UAVNs is also presented based on the proposed trust model, and it exists only when there is both a physical link and a trust link between two UAVs. In addition, both the physical connectivity probability and the secure connectivity probability between two UAVs in the presence of Doppler shift have been derived. Simulations show that compared to the physical connection probability with or without malicious attacks, the proposed trust model can ensure secure communication and reliable connectivity between UAVs and enhance network performance when the UAVNs suffer from malicious attacks and other security risks.

References

Andre T, Hummel K, Schoellig A, et al., 2014. Application-driven design of aerial communication networks. *IEEE Commun Mag*, 52(5):129-137. https://doi.org/10.1109/MCOM.2014.6815903

Bekmezci I, Sahingoz OK, Temel S, 2013. Flying ad-hoc networks (FANETs): a survey. *Ad Hoc Netw*, 11(3):1254-1270. https://doi.org/10.1016/j.adhoc.2012.12.004

Elnahrawy E, Nath B, 2003. Cleaning and querying noisy sensors. Proc 2nd ACM Int Conf on Wireless Sensor Networks and Applications, p.78-87. https://doi.org/10.1145/941350.941362

Govindan K, Mohapatra P, 2012. Trust computations and trust dynamics in mobile ad hoc networks: a survey. *IEEE Commun Surv Tutor*, 14(2):279-298. https://doi.org/10.1109/SURV.2011.042711.00083

Gradshteyn IS, Ryzhik IM, 2000. Tables of Integrals, Series, and Products. Academic Press, USA.

Gupta L, Jain R, Vaszkun G, 2015. Survey of important issues in UAV communication networks. *IEEE Commun Surv Tutor*, 18(2):1123-1152. https://doi.org/10.1109/COMST.2015.2495297

Han GJ, Jiang JF, Shu L, et al., 2014. Managements and applications of trust in wireless sensor networks: a survey. *J Comput Syst Sci*, 80(3):602-617. https://doi.org/10.1016/j.jcss.2013.06.014

Han GJ, Jiang JF, Shu L, et al., 2015. An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network. *IEEE Trans Mob Comput*, 14(12):2447-2459. https://doi.org/10.1109/TMC.2015.2402120

Hayat S, Yanmaz E, Muzaffar R, 2016. Survey on unmanned aerial vehicle networks for civil applications: a communications viewpoint. *IEEE Commun Surv Tutor*, 18(4):2624-2661. https://doi.org/10.1109/COMST.2016.2560343

Janaswamy R, 2002. Angle of arrival statistics for a 3-D spheroid model. *IEEE Trans Veh Technol*, 51(5):1242-1247. https://doi.org/10.1109/TVT.2002.801756

Jiang JF, Han GJ, Wang F, et al., 2015. An efficient distributed trust model for wireless sensor networks. *IEEE Trans Parall Distr Syst*, 26(5):1228-1237. https://doi.org/10.1109/TPDS.2014.2320505

Jøsang A, 1999. An algebra for assessing trust in certification chains. Proc Network and Distributed Systems Security Symposium, p.1-10.

Kandeepan S, Gomez K, Reynaud L, et al., 2014. Aerial-terrestrial communications: terrestrial cooperation and energy-efficient transmissions to aerial base stations. *IEEE Trans Aerosp Electron Syst*, 50(4):2715-2735. https://doi.org/10.1109/TAES.2014.130012

Li H, Yang B, Chen CL, et al., 2010. Connectivity of aeronautical ad hoc networks. IEEE GLOBECOM Workshops, p.1788-1792. https://doi.org/10.1109/GLOCOMW.2010.5700249

Lim HS, Moon YS, Bertino E, 2010. Provenance based trustworthiness assessment in sensor networks. Proc 7th Int Workshop on Data Management for Sensor Networks, p.2-7. https://doi.org/10.1145/1858158.1858162

Movahedi Z, Hosseini Z, Bayan F, et al., 2016. Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey. *IEEE Commun Surv Tutor*, 18(2):1287-1309. https://doi.org/10.1109/COMST.2015.2496147

Salmanian M, Mason PC, Treurniet J, et al., 2010. A modular security architecture for managing security associations in MANETs. IEEE 7th Int Conf on Mobile Ad-hoc and Sensor Systems, p.525-530. https://doi.org/10.1109/MASS.2010.5663906

Simon MK, Alouini MS, 2000. Digital Communication over Fading Channels. John Wiley & Sons, New York, USA.

Vazifehdan J, Prasad RV, Niemegeers I, 2014. Energy-efficient reliable routing considering residual energy in wireless ad hoc networks. *IEEE Trans Mob Comput*, 13(2):434-447. https://doi.org/10.1109/TMC.2013.7

Wan Y, Namuduri K, Zhou Y, et al., 2013. A smooth-turn mobility model for airborne networks. *IEEE Trans Veh Technol*, 62(7):3359-3370. https://doi.org/10.1109/TVT.2013.2251686

Wang K, Wu M, 2007. A trust approach for node cooperation in MANET. Proc 3rd Int Conf on Mobile Ad-hoc and Sensor Networks, p.481-491.

Wei ZX, Tang H, Yu FR, et al., 2014. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. *IEEE Trans Veh Technol*, 63(9):4647-4658. https://doi.org/10.1109/TVT.2014.2313865

Xia H, Jia ZP, Sha EHM, 2014. Research of trust model based on fuzzy theory in mobile ad hoc networks. *IET Inform Secur*, 8(2):88-103. https://doi.org/10.1049/iet-ifs.2012.0145

Xie JF, Wan Y, Kim JH, et al., 2014. A survey and analysis of mobility models for airborne networks. *IEEE Commun Surv Tutor*, 16(3):1221-1238. https://doi.org/10.1109/SURV.2013.111313.00138