This article has been accepted for publication in a future issue of this jourral, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

A Tri-Phases Message Oriented Trust Model in FANET

Xueru Du, Yue Cao, Senior Member, IEEE, Di Wang, Chenchen Lv, Celimuge Wu, Senior Member, IEEE and Kezhi Wang, Senior Member, IEEE

Abstract—With advantages of convenience and flexibility, Unmanned Aerial Vehicles (UAVs) are widely applied in various fields, such as inspection, agriculture, transportation, and so on. However, due to characteristics of Flying Ad Hoc Network (FANET) consisting of UAVs, such as dynamic topology and limited bandwidth, the security of messages is threatened by cyber attacks. A Tri-Phases Message Oriented Trust Model for FANET is proposed, called TPMOTM, to secure messages. In the proposed work, the message collection process is divided into three phases, including message generation, message transmission, and message integration. In each phase, by analyzing potential attacks and the circumstance of network, the TPMOTM quantifies the specific detection factors to obtain the trust value of messages, including timeliness, detection accuracy, message error rate, relay performance, authentication result, and message loss rate. After messages have been received by the Ground Station (GS), the GS integrates all messages in relation to the detected event, employing the message trust value as the weight, to obtain the state of detected event. Extensive simulations are conducted based on the Opportunistic Network Environment (ONE) simulator, with attack message detection rates reaching up to 95% (±0.89%) and event detection accuracy rates typically above 85% (±1.21%).

Index Terms—Trust model, Unmanned Aerial Vehicle (UAV), Flying Ad Hoc Network (FANET)

1 Introduction

Thanks to technological advancement and policy support, Unmanned Aerial Vehicles (UAVs) have garnered considerable interest from both industry and academics. The benefits of UAVs are their portability, affordability, convenience, and flexibility. Therefore, UAVs are widely applied in a variety of applications, such as health monitoring, power inspection, load transportation, fire detection [1], etc.

In order to execute large-scale tasks (e.g., inspection, transportation, rescue), multiple UAVs usually collaborate and form a self-organized network, which is known as the Flying Ad Hoc Network (FANET). In FANET, UAVs move quickly and the topology of network changes dramatically. Moreover, in the complex environment, FANET is exposed to the strong interference. Compared with the infrastructure-based network, UAVs are difficult to supervise. Both authenticated and unauthenticated UAVs can join or leave the network at any moment.

Due to the mobility of UAVs [2], the communication between UAVs is often interrupted. In complex electromagnetic environments, signal interference may cause message distortion. If UAVs carry sensitive information, these information may be threatened by unauthenticated UAVs. In addition, attacks may be launched to compromise messages [3], such as false message injection, message tampering, and black hole attack. These attacks not only threaten the message privacy, but also damage the network performance. Consequently, it is crucial to guarantee the privacy and security of messages in FANET.

One solution to assure the privacy and security is employing cryptography technology, such as symmetric encryption, asymmetric encryption, hybrid encryption, Diffie-Hellman key exchange, message authentication codes, digital signature, and digital certificate [4], [5]. However, cryptography technology is only a precaution. Numerous occasions show that even with thoughtfully designed precautions, systems are still vulnerable to external attacks. In addition, cryptography can only passively defend,but it cannot actively detect anomalies in the network. Kerrache et al. [6] pointed out that trust management can be an alternative solution of cryptography, such as direct trust evaluation, indirect trust evaluation, and reputation management [7].

Trust management schemes can actively detect malicious behaviors, resist external attacks, and take measures to avoid persistent adverse effects on the network. Cho et al. [8] proposed a Provenance-based Trust Model to achieve accurate peer-to-peer trust evaluation. Asuquo et al. [9] designed a distributed trust management scheme to filter malicious UAVs in Delay Tolerant Networks (DTNs). Although these trust model are well applied in DTNs, limited energy and frequent topological changes make these schemes unavailable for FANET. Singh et al. [10] proposed a trust model based on fuzzy classification to identify misbehaviors of malicious UAVs for FANET. Singh et al [11] presented a genetic algorithm-based trust assessment model, to categorize UAVs and remove

- Xueru Du, Yue Cao (corresponding author), Di Wang, and Chenchen Lv are with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430073, China (email: xuerudu.cs@whu.edu.cn; yue.cao@whu.edu.cn; diwang@whu.edu.cn; lvbuer@whu.edu.cn).
- Celimuge Wu is with Meta-Networking Research Center, The University of Electro-Communications, 1-5-1, Chofugaoka, Chofushi, Tokyo,182-8585 Japan (email: celimuge@uec.ac.jp)
- Kezhi Wang is with the Department of Computer Science, Brunel University London, UB8 3PH Uxbridge, U.K. (email: kezhi.wang@brunel.ac.uk)

- The research is supported in part by Wuhan Knowledge Innovation Program (2022010801010117) and Hubei Province International Science and Technology Collaboration Program (2023EHA044) and MIC/SCOPE #JP235006102.

This article has been accepted for publication in a future issue of this jourral, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

harmful UAVs from FANET based on the risk assessment. However, these models ignore the security of messages in the FANET.

Cryptography can actively defend against internal attackers (nodes already hidden in the FANET), while trust management can passively defend against external attackers (attackers without authorization to access FANETs). Combining cryptography and trust management can simultaneously resist internal and external attackers in the FANET, ensuring the security of messages and UAVs. Liu et al. [12] proposed a lightweight trusted message exchange scheme, that integrates cryptography and trust management to protect message privacy. However, their work relies entirely on the results of decryption, without considering factors related to the message, such as timeliness, accuracy, and so on.

In order to secure messages in FANET and overcome the aforementioned shortcomings of previous works, a Tri-Phases Message Oriented Trust Model (TPMOTM) that fully considers message features with low overhead is proposed. This work is mainly applied in event detection scenarios and focuses on the security of messages in FANET. The following is primary contributions of this work:

- Message oriented trust model: Several recent schemes combine the cryptography and the trust management to secure messages, but most of these works lay more emphasis on encryption and decryption, rather than features of messages. In this work, cryptography-based authentication is only a subpart of trust model. The TPMOTM analyzes the potential threats of messages, and then determines the related detection factors based on features of messages in different phases. Specifically, the TPMOTM is established based on the three phases: (1) The message generation phase evaluates the timeliness of message and detection accuracy of message generator; (2) The message transmission phase evaluates the message error rate, relay performance, message authentication, and message loss rate; (3) The message transmission integrates trust values of these factors to obtain the total trust value of message.
- Dynamic trust value: In FANET, if only one UAV evaluates messages, there is a considerable chance of misjudgment. In order to reduce the probability of misjudgment, this work applies evaluations on the given message by multiple UAVs. The trust value of given message is initialized by the generating UAV, who observes the event and reports it, and then dynamically changes with those UAVs in replaying. The evaluation of messages is based on the circumstance of network, message features, and UAV performances.

The rest of this paper is organized as follows. Section 2 reviews a few related works. Section 3 introduces the system model and attack model. Afterwards, Section 4 details the proposed model. Section 5 and Section 6 present the simulation and conclusion, respectively.

2 Related Work

There have been a number of schemes proposed to secure UAVs and messages in FANETs. In this section, we discuss the existing cryptography-based schemes, trust management-based schemes and hybrid schemes, which combines cryptography and trust management.

2.1 Cryptography-Based Schemes

Elliptic Curve Cryptography (ECC) is a popular technique, since it has a shorter key and lower overhead than traditional authentication. Li et al. [13] proposed a lightweight authentication scheme based on ECC to verify the identity of UAVs. Safavat et al. [14] also proposed an improved authentication scheme based on ECC. However, ECC-based schemes need the support of specific hardware or certificate authority.

Khan et al. [15] proposed an authentication scheme to enhance the security and reliability of transportation system. Their work combines digital signature, hash function, and hyper elliptic curve cryptography technologies to ensure the privacy. In addition, Alladi et al. [16] proposed a physical unclonable function-based authentication scheme to ensure the security of communication between the UAV and GS. Moreover, Yoon et al. [17] proposed an additional encrypted communication channel and authentication scheme on commercial UAVs. De Melo et al. [18] proposed a public-key-based authentication mechanism with a movement plausibility check for UAVs in the military domain. Although these schemes are effective, they are only suitable for limited scenarios, such as transportation systems, commercial applications, and military domains.

Ghribi et al. [19] proposed a new consensus-building mechanism by combining the blockchain with the public key encryption. Liu et al. [20] proposed a trusted storage scheme based on blockchain and trusted certificate. Their work employs asymmetric passwords in identity authentication, to ensure the data integrity and the security of blockchain system. Although blockchain guarantees the traceability of data, it also incurs the high overhead of computation that UAVs cannot afford. Thus, the support of other facilities is necessary in blockchain-based schemes.

2.2 Trust Management-Based Schemes

Bhoi et al. [21] proposed a direct trust model to determine the trustworthiness of UAVs. In their work, relay UAVs discards messages sent by untrusted UAVs. Barka et al. [22] proposed a context-aware trust model. The model implements semantic analysis on the UAV that contains malicious behavior. Both models can distinguish intentional and unintentional misbehaviors, and significantly reduces the probability of false positive rate of malicious UAV identification.

Chen et al. [23] proposed a role-based trust model for heterogeneous network. Their work categorizes UAVs into commanders, subtask leaders, and common UAVs according to the mission. UAVs are evaluated according to the quality of service characters (competence and cooperativeness) and social behaviors (connectivity, intimacy and honesty). Li et al. [24] proposed a tri-layer trust model for the location security in deception and interference. The model consists of transaction layer, rating layer and communication layer. Each layer calculates the trust value through the communication of demander, tenderer and the third party. In role-based and layer-based model, roles and layers are generally evaluated by various standards.

This article has been accepted for publication in a future issue of this jourral, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

Singh et al. [11] proposed a trust evaluation model based on genetic algorithm. Their work utilizes genetic algorithm to optimize the trust value, and carries out additional risk assessment for suspicious UAVs. In the literature [10], a trust model based on fuzzy classification is introduced. Their work manages the trust relationship between UAVs, and discriminates behaviors of UAVs based on fuzzy classification and optimization principles [25]. Trust models based on artificial intelligence can defend against unidentified threats. However, these models have the high computational overhead.

2.3 Hybrid Schemes

The hybrid scheme combines cryptography and trust management. Liu et al. [26] proposed a privacy protection trust management strategy for the emergency message dissemination in space–air–ground-integrated VANETs. Li et al. [27] proposed a reputation system that allows for the evaluation of message dependability in VANETs. Liu et al. [28] proposed an emergency message propagation model built on the trust cascade. Their work integrates the entity-oriented trust evaluation with the data-oriented trust evaluation. These schemes not only achieve the accurate trust management, but also robust the privacy protection. However, they are all applicable to the VANET rather than FANET.

Liu et al. [12] proposed a lightweight message exchange trust scheme by incorporating the trust management and encryption technologies. In their work, only UAVs that are verified as trustworthy can decrypt the content of message. Andreas et al. [29] presented a secure two-way communications to realize the confidential data sharing. The ciphertext comprising sensitive information can be encrypted and decrypted in real-time. On the one hand, these schemes can offer the robustness against internal and external attackers. On the other hand, applicable scenarios of these schemes are limited.

This work develops a FANET-tailored trust model based on cryptography and trust management. Table 1 summarizes the comparison of this proposal and the analyzed related work, in terms of technology, multiple attacks resistance, multiple detection factors, high accuracy, and low overhead.

3 System Architecture

In this section, the scenario setting and common attacks (including false message injection, message tampering and black hole attack) are introduced.

3.1 Scenario Setting

This work is applied to civilian applications, where UAVs are deployed around the event to collect information, such as fire detection, power inspection, environment exploration, etc. As illustrated in Fig. 1, the detection area is divided into equal sub-areas. At the beginning, the UAVs are evenly deployed in these sub-areas, and then the UAVs randomly move to stay or through the sub-areas.The GS is deployed on the center of detection area. Upon detecting the event, UAVs generate messages to report the event location and state. The message is denoted by a six-tuple, $m = \{E_{id}, E_{loc}, E_{rpt}, t_{gen}, u_{gen}, u_{rly}\}$. E_{id} is the identification of event, E_{loc} is the location of event, E_{rpt} is the reported state of event, t_{gen} is the generation time of message, u_{gen} is the UAV generating the message, and u_{rly} is a group of UAVs relaying the message. The reported state is dichotomous to indicate whether the event actually happens. For instance, the reported state can point out whether the forest fire breaks out or the machine malfunctions. Generally, there are numerous messages related to one event for following reasons:

- Multiple detection UAVs: A number of UAVs may pass through the event location, and then generate messages to report the event.
- Multiple copies: Given that the communication link is unstable, to increase the chance of a reported message to be finally delivered by the GC, this work employs the Epidemic routing protocol [30], which is deemed as a classic flooding routing protocol in the mobile network.

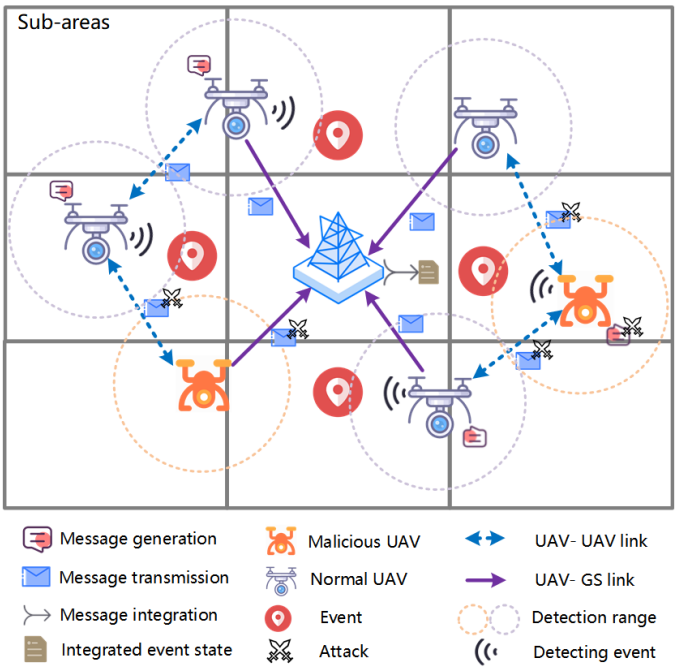

Fig. 1. Network scenario for event detection.

It is noted that to save the computational resources, UAVs only generate and transmit messages, while GS is responsible for integrating messages from multiple UAVs in reporting a given event, and determining the state of event.

3.2 Common Attacks

There is the inevitable interference in open-air environment. In addition, messages are exposed to following attacks:

- False message injection: Malicious UAVs generate false messages and spread throughout the network in message generation phase. If the GS receives a large number of false messages in reporting an event, the GS will incorrectly evaluate the event state. As shown in Fig. 2 (a), a great deal of false messages are generated, by replicating the infected source message. Thus, the false message injection substantially makes a negative impact on the event state.

This article has been accepted for publication in a future issue of this jounal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

TABLE 1
Summarization of related work.

Related work	Technology	Multiple attacks resistance	Multiple detection factors	High accuracy	Low overhead
Li et al. [13]	Cryptography	✓			
Safavat et al. [14]	Cryptography	✓		✓	✓
Khan et al. [15]	Cryptography				✓
Alladi et al. [16]	Cryptography	✓			✓
Yoon et al. [17]	Cryptography				
De Melo et al. [18]	Cryptography	✓		✓	✓
Ghribi et al. [19]	Cryptography				
Liu et al. [20]	Cryptography				
Bhoi et al. [21]	Trust management		✓	✓	✓
Barka et al. [22]	Trust management	✓	✓	✓	
Chen et al. [23]	Trust management	✓	✓	✓	
Li et al. [24]	Trust management	✓	✓		
Singh et al. [11]	Trust management		✓	✓	
Singh et al. [10]	Trust management		✓	✓	✓
Liu et al. [26]	Cryptography and trust management	✓		✓	✓
Li et al. [27]	Cryptography and trust management	✓			✓
Liu et al. [28]	Cryptography and trust management	✓	✓	✓	
Liu et al. [12]	Cryptography and trust management	✓			✓
Andreas et al. [29]	Cryptography and trust management				
The proposed model	Cryptography and trust management	✓	✓	✓	✓

- Message tampering: Malicious UAVs tamper with the messages in message transmission phase, instead of generating false messages directly. As seen in Fig. 2 (b), this approach only tampers with relayed messages rather than source messages. Compared to the false message injection, message tampering generates less number of false messages, and makes slighter adverse effect on event state.
- Black hole attack: As depicted in Fig. 2 (c), malicious UAVs discard messages in message transmission phase. As a result, the GS without receiving sufficient number of normal messages, may be unable to determine the event state. If the black hole attack and message tampering are combined, the proportion of infected messages will increase. Consequently, hybrid attacks significantly raise the risk of state misjudgment.

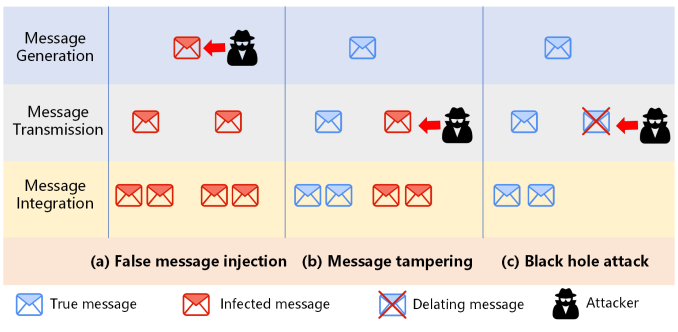

Fig. 2. Illustration of false message injection, message tampering, and black hole attack.

4 The Tri-Phases Message Oriented Trust Model

The procedure of detecting an event can be separated into three phases. Correspondingly, vulnerabilities can be addressed in these phases as follows.

- Phase one (Message generation phase): UAVs generate messages in the phase one. Correspondingly, malicious UAVs can also generate false messages in this phase.
- Phase two (Message transmission phase): UAVs transmit messages in the second phase. However, malicious UAVs can tamper with or drop these messages.
- Phase three (Message integration phase): The GS aggregates all messages to obtain the event state. In this phase, malicious UAVs can impede the determination ability of GS.

The GS is regarded as completely secure in this work, since it has sufficient resources to support an effective security system. Therefore, this work only considers assaults in the first and second phases, and how to integrate numerous messages in the third phase. Fig. 3 shows the architecture of TPMOTM and details factors of message trustworthiness in three phases.

As the message generator and relay nodes, UAVs play a crucial role in message generation and transmission. Although evaluating UAVs is not the primary goal, this work also takes the UAV related factors into account. In message generation phase, the message trust value is initialized based on the property of message generator and the feature of message. In message transmission phase, the trust value is adjusted based on the performance of relay UAVs and the circumstance of network. In message integration phase, reported messages are integrated to obtain the integrated event state. The difference between the integrated event and the reported state can evaluate the performance of message generator. Main notations and meanings are summarized in Table 2.

This article has been accepted for publication in a future issue of this joural, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

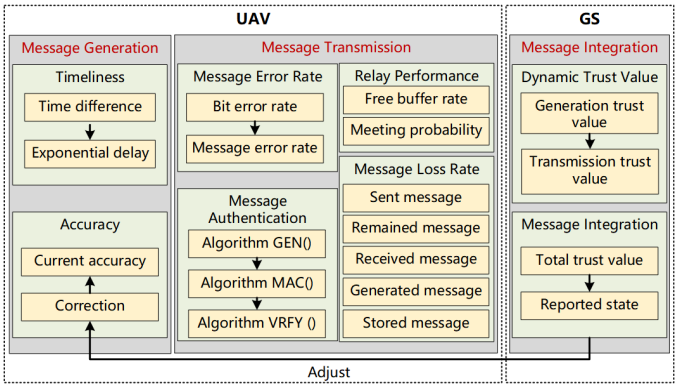

Fig. 3. Model architecture.

TABLE 2
Notations and meanings

m=(m_{id}, E_{loc}, E_{rpt}, t_{gen}, u_{gen}, u_{rly})	Six-tuple of message (message identification, event location, event state, generation time,) generator UAV, relay UAVs
$\mathcal{T}=\{1,2,...T\}$	Set of time slots
$\mathcal{M}=\{1,2...M\}$	Set of messages
$\mathcal{U}=\{1,2...U\}$	Set of UAVs
$\mathcal{R}=\{1,2,...R\}$	Set of accuracy evaluation rounds
TV_{time}	Trust value of timeliness
TV_{acc}	Trust value of detection accuracy
TV_{mer}	Trust value of message error rate
TV_{rp}	Trust value of relay performance
TV_{mlr}	Trust value of message loss rate
T_m	Total trust value of message m
Th	Message trust value threshold
RA_{ber}	Bit error rate
RA_{mer}	Message error rate
RA_{free}	Free buffer rate
RA_{meet}	UAV meeting rate
RA_{mlr}	Message loss rate
E_{itg}	Integrated event state
$E_{rpt}(m)$	Reported state of message m
$Gen()$	Generation trust value calculation function
$Tra()$	Transmission trust value calculation function
$T()$	Dynamic trust value calculation function

4.1 Message Generation Phase

In message generation phase, the following issues may exits:

- Poor timeliness: The instability of the FANET causes an increase in message transmission time. The messages generated by UAVs far from the GS may take a long time to reach the GS, and these messages have poor timeliness. How to evaluate timeliness is described in Section 4.1.1.
- False message injection: Malicious UAVs may intentionally generate false messages to confuse the GS. The continuous injection of false messages can lead to a decrease in the accuracy of UAVs. Therefore, in Section 4.1.2, we detect false message injection through the detection accuracy of message generators.

4.1.1 Timeliness

There could be numerous UAVs passing through the event location, and each of them would generate a message to the GS based on the discovered circumstance. The event state may alter dramatically if this event lasts a long time. For instance, there is no fire in the forest at beginning, yet fire breaks out a half-hour later. Even if there are no attacks and inference, messages reported at the beginning of event and messages reported after half an hour would be different. Thus, timeliness is a crucial metric to evaluate the trustworthiness of messages. The later a message is reported, the better it can reflect the timeliness of event. According to Wang et al. [31], the timeliness delays exponentially with time, and the trust value of timeliness TV_{time} is defined as:

$$TV_{time} = \frac{t_{gen} - t_{str}}{t_{end} - t_{str}} \exp\left(-\delta\left(t - t_{gen}\right)\right) \tag{1}$$

where δ is the delay factor to make sure that TV_{time} falls within the range of $[0,1]$, and δ is preset by simulating the same scenario in advance. $t \in \mathcal{T}$ is the current time, and $\mathcal{T}=\{1,2,...T\}$ is the set of time slots. t_{gen} is the generation time of message recorded in message m. t_{str} is the event start time, t_{end} is the event end time, and both of them are determined by selecting the earliest and latest messages of event in message integration phase.

4.1.2 Detection Accuracy

UAVs generate messages based on the detected information, while the detection accuracy of various message generators is different. The only detection device, according to Jena et al. [32], is the installed sensors. Even if kinds of sensors are known in advance, the detection accuracy of message generators cannot be assessed. This is due to the fact that UAVs are subject to various angles, distances, and interference. In addition, sensors of malicious UAVs cannot be known in advance. Therefore, comparing the reported state with the integrated state is the only way to determine the detection accuracy of message generators. UAVs with low detection accuracy may launch false message injection attacks.

The GS maintains an Accuracy-table to record the detection accuracy of UAVs in FANET. An example of Accuracy-table is shown in Fig. 4. When messages arrive at the GS, the GS checks the Accuracy-table to determine the detection accuracy of message generators. If a message generator is not recorded in Accuracy-table, its detection accuracy rate would be set as the trust threshold of message Th. Upon obtaining the integrated state, the GS compares the integrated state with the reported state, and updates the Accuracy-table. More details on how to update the Accuracy-table are shown in Section 4.3.4.

With the continuous detection of event, the message generator is evaluated multiple rounds. The set of detection accuracy evaluation round is denoted as $\mathcal{R}=\{1,2,...R\}$. Adjusted detection accuracy can be adopted to evaluate message in the next round. Eq. (2) illustrates how to calculate the detection accuracy of UAV. $r \in \mathcal{R}$ is the current round. $TV_{acc}(r) \in [0,1]$ is the trust value of detection accuracy in round r. N_{cm} is the number of consistent messages, whose reported state is consistent with the integrated state. N_{im} is the number of inconsistent messages, whose reported state is inconsistent with the integrated state. V_{rwd} and V_{pns} are the reward value and the punish value respectively, and they are designed to ensure that the detection accuracy is within [0,1].

4.2 Message Transmission Phase

Following issues may appear in message transmission phase:

This article has been accepted for publication in a future issue of this joural, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

$$TV_{acc}(r) = \begin{cases} TV_{acc}(r-1) + N_{cm}V_{rwd} + N_{im}V_{pns} & \text{if } r > 1 \\ Th & \text{if } r = 1 \end{cases} \quad (2)$$

Accuracy-table

UAV ID	Detection Accuracy	Update Time
1	0.75	100s
3	0.40	200s
5	0.62	300s
.....	.....	.....

Fig. 4. An example of Accuracy-table.

- Propagation loss: As an air-to-air link, links in FANET may be obstructed by buildings, vegetation, and aircraft fuselage. The signal shadow fading that results from these occlusions might lead to signal error and propagation loss. How to analyze the propagation loss is mentioned in Section 4.2.1.
- Low relay probability: The TPMOTM relays messages via the store-carry-forward mechanism. The UAV stores messages when neighbor UAVs are unavailable, carries messages to continue flying, and forwards messages when meeting available UAVs. However, the limited buffer restricts the storage capacity of UAV. If the size of messages exceeds the upper limit of buffer, the UAV cannot receive messages. In addition, if the UAV cannot connect to available UAVs for a long time, the probability of forwarding messages is low. All these conditions may reduce the relay probability. More information can be seen in Section 4.2.2.
- Message tampering: Message tampering is conducted by malicious UAVs. When malicious UAVs receive messages, they tamper messages to confuse the GS rather than relay messages in time. If there are lots of tampered messages, it will consume a lot of computing resources of GS to analyze the consistency of messages. Therefore, message tampering should be prevented rather than detected. The authentication is an appropriate way to prevent message tampering. A message authentication suited for FANET is introduced in Section 4.2.3.
- Message dropping: The message dropping happens due to the message expiration (because of time to live), duplication (because of multi UAVs detection), etc. Thus, slight message dropping is reasonable in FANET. In contrast, substantial message dropping implies the black hole attack. Hence, the message loss rate can be applied as the indicator of black hole attack, as explained in Section 4.2.4.

The following describes how to deal with these issues in message trust evaluation.

4.2.1 Message Error Rate

Considering that there are line-of-sight in outdoor, the Rician fading model [33] is selected as the channel model in FANET. For two-phase differential phase shift keying modulation under the Rician fading model, the bit error rate RA_{be} is:

$$RA_{be} = \frac{1}{2}\left(\frac{1+\gamma}{1+\gamma+\overline{\eta}}\right) exp\left(\frac{-\gamma\overline{\eta}}{1+\gamma+\overline{\eta}}\right) \quad (3)$$

where γ presents the Rician factor decided by environment, and it is set by referring to the literature [33]. $RA_{be} \in [0,1]$, and $\overline{\eta}$ represents the average signal-to-noise ratio. $\overline{\eta} = P_{tra}/(P_{nos}Dis^2)$, where P_{tra} is the transmitting power, P_{nos} presents the noise power, and Dis is the distance between the sender and receiver.

Afterwards, the message error rate is obtained according to the bit error rate. The probability that a message is delivered without error is same as the probability that all bits are accurately received. Therefore, the message error rate RA_{me} is:

$$RA_{me} = 1 - (1 - RA_{be})^{N_{bit}} \quad (4)$$

where $RA_{me} \in [0,1]$, N_{bit} is the number of bits in a message. The higher the message error rate, the lower the trust value. Thus, the trust value of message error rate TV_{mer} is expressed as:

$$TV_{mer} = 1 - RA_{me} = (1 - RA_{be})^{N_{bit}} \quad (5)$$

4.2.2 Relay Performance

As mentioned above, the UAV employs the store-carry-forward mechanism to relay messages. Hence, relay performance is not only reflected by its ability to forward messages, but also by its ability to store messages. The storage capacity depends on the size of buffer. If the free buffer is zero and stored messages do not expire, the UAV cannot receive other messages. Therefore, the storage capacity can be represented by the free buffer rate RA_{free}:

$$RA_{free} = 1 - \frac{\sum_{m=1}^{N_{sm}} S_m + \sum_{m'=1}^{N_{wm}} S_{m'} - \int s(t)\,dt}{S_{buf}} \quad (6)$$

where $RA_{free} \in [0,1]$, and S_{buf} is the maximum size of available buffer. $m \in \mathcal{M}$ is the current message, and $\mathcal{M} = \{1, 2...M\}$ is the set of messages. N_{sm} is the number of stored messages in buffer, and S_m is the size of stored message m. N_{wm} is the number of messages waiting to be cached before the current message, and $S_{m'}$ is the size of waiting message m'. $s(t)$ is the transmission speed of UAV at time slot t, that is, the speed of messages leaving the buffer.

In the Epidemic routing protocol, the relaying ability of UAV depends on the probability that the UAV meets other UAVs. The meeting probability RA_{meet} can be calculated based on previous time slots as follows:

$$RA_{meet} = \frac{\frac{1}{N_{pts}}\sum_{t'=t-N_{pts}}^{t} N_{meet}^{t'}}{N_{all}} f(u) \quad (7)$$

This article has been accepted for publication in a future issue of this jourral, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

$$f(u) = 1 + \frac{N_{au} - N_{avg}}{N_{avg}} \tag{8}$$

where $RA_{meet} \in [0, 1]$. $N_{meet}^{t'}$ is the number of meeting UAVs at time slot t', and N_{all} is all UAVs in FANET. N_{pts} is the number of previous time slots. As depicted in Fig. 5, previous time slots start from $t - N_{pts}$. $u \in \mathcal{U}$ is the current UAV, and $\mathcal{U} = \{1, 2...U\}$ is the set of UAVs. $f(u)$ is the prediction function, decided by the sub-area where the UAV is located. N_{au} is the number of times that UAVs have appeared in the sub-area in previous time slots, and N_{avg} is the average number of times that UAVs have appeared in all sub-areas in previous time slots.

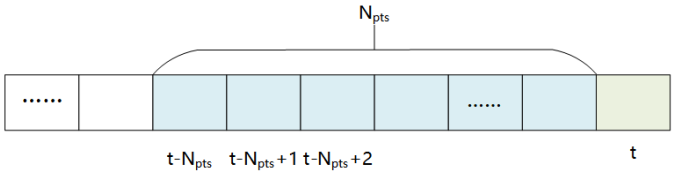

Fig. 5. Time slot.

The trust value of relay performance TV_{rp} can be obtained by combining the store ability and relaying ability:

$$TV_{rp} = \rho_1 RA_{free} + \rho_2 RA_{meet} \tag{9}$$

where ρ_1 and ρ_2 are weighted value, and $\rho_1 + \rho_2 = 1$.

4.2.3 Message Authentication

The proposed trust management model only facilitates the outcome of message authentication, rather than designing a perfect message authentication scheme. Hence, the fast Message Authentication Code (MAC) proposed by Vosoughi and Katti [34] is adopted. Their work is useful when many messages have to be authenticated at once. In MAC, the UAV generates and shares a key before the communication. Then the sender creates a label based on this key utilizing label generating algorithm, and transmits it along with the message. Upon receiving the message, the receiver verifies whether the message label is valid. If the message is not tampered with, the output result of verification algorithm is 1. Otherwise, it is considered that the message is tampered with, so the message would be deleted.

Formally, the MAC is a tuple of probability polynomial time algorithm $(GEN(), MAC(), VRFY())$, where $GEN()$ is the key generation algorithm, $MAC()$ is the label generation algorithm, and $VRFY()$ is the verification algorithm. Authentication steps are as follows:

- Run $GEN()$ to obtain a random key.
- Run $MAC()$ to generate label based on the key.
- Run $VRFY()$ to verify the label.

4.2.4 Message Loss Rate

The message loss rate RA_{mlr} can not only indicate network congestion, but also imply the black hole attack. Normal UAVs only discard duplicate or expired messages, and the message loss rate is controlled within a certain range. However, malicious UAVs would deliberately drop messages to reduce the number of messages that are expected to be received by the GS. Thus, message loss rate of malicious UAVs would be much higher than that of normal UAVs. Normally, the message loss rate of malicious UAVs depends on the probability of black hole attack, and it is expressed as:

$$RA_{mlr} = 1 - \frac{M_{rly} + M_{rem}}{M_{rec} + M_{gen} + M_{sto}} \tag{10}$$

where $R_{mlr} \in [0, 1]$. M_{rly} is the number of relayed messages, and M_{rem} is the number of remained messages after relaying. M_{rec}, M_{gen} and M_{sto} are the number of received messages, generated messages and stored messages before relaying, respectively.

The trust value of message loss rate TV_{mlr} is defined as:

$$TV_{mlr} = 1 - RA_{mlr} = \frac{M_{send} + M_{rem}}{M_{rec} + M_{gen} + M_{sto}} \tag{11}$$

4.3 Message Integration Phase

In this section, the GS calculates the trust value of messages, and then integrates messages to obtain the event state based on the trust value and reported state.

4.3.1 Dynamic Trust Value

The trust value of message is dynamically adjusted according to message generator and relay UAVs recorded in the message. The generation trust value and the transmission trust value are calculated based on mentioned factors (timeliness, detection accuracy, message error rate, relay performance, and message loss rate). The transmission trust value is calculated by relay UAVs in message transmission. Then the transmission trust value is transmitted to the GS along with the message. However, the generation trust value is calculated in message integration phase, since it needs to wait for the arrival of all messages to determine the event start time. Upon messages arriving at the GS, the GS analyzes all messages related to the given event to determine the t_{base} mentioned in Section 4.1.1, and calculate TV_{time}. Then as described in 4.1.2, the GS checks the $TV_{acc}(r)$ on the Accuracy-table. The initial trust value of message is obtained in the following way:

$$Gen(1) = \alpha_1 TV_{time} + \alpha_2 TV_{acc} \tag{12}$$

where $Gen(1)$ is the function to calculate the generation trust value depended on the message generator. α_1 and α_2 are weighted values, where $\alpha_1 + \alpha_2 = 1$.

The relay UAV calculates the transmission trust value as follows:

$$Tra(u) = \beta_1 TV_{mer} + \beta_2 TV_{rp} + \beta_3 TV_{mlr} \tag{13}$$

where $Tra(u)$ is the function to calculate the transmission trust value based on the relay UAV u. β_1, β_2, β_3 are weighted values, where $\beta_1 + \beta_2 + \beta_3 = 1$.

By combining the generation trust value and the transmission trust value, the total trust value is consolidated as Eq. 14. $T(u)$ is the function to calculate the trust value when the message is relayed by the UAV u. ω_1 and ω_2 are weighted values, where $\omega_1 + \omega_2 = 1$. Upon the message arriving at the GS, the trust value stops fluctuating, and the total trust value of message m is obtained, denoted as TV_m.

This article has been accepted for publication in a future issue of this jounal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

$$T(u) = \begin{cases} \omega_1 T(u-1) + \omega_2 Tra(u) & \text{if } u \text{ is relay } UAV \\ \frac{1}{2}(Gen(1) + Tra(1)) & \text{if } u \text{ is generator} \end{cases} \tag{14}$$

$$\beta_1' = \begin{cases} \frac{N_{mer}}{N_{mer}+N_{rp}+N_{mlr}} & \text{if } N_{mer} > 0 \parallel N_{rp} > 0 \parallel N_{mlr} > 0 \\ \beta_1 & else \end{cases} \tag{17}$$

$$\beta_2' = \begin{cases} \frac{N_{rp}}{N_{mer}+N_{rp}+N_{mlr}} & \text{if } N_{mer} > 0 \parallel N_{rp} > 0 \parallel N_{mlr} > 0 \\ \beta_2 & else \end{cases} \tag{18}$$

$$\beta_3' = \begin{cases} \frac{N_{mlr}}{N_{mer}+N_{rp}+N_{mlr}} & \text{if } N_{mer} > 0 \parallel N_{rp} > 0 \parallel N_{mlr} > 0 \\ \beta_3 & else \end{cases} \tag{19}$$

4.3.2 Dynamic Weighted Values

If the trust value of one factor falls below the threshold, it implies that there are attacks or environmental interference in FANET. In this case, the GS would update weight values before message integration in an offline manner. For low trust values (below the Th), the TPMOTM increases the corresponding weighted values to improve detection accuracy. For instance, if TV_{acc} is consistently lower than the threshold, the false message injection may happen. In this case, increasing α_2 would amplify the impact of this attack onto the overall trust value. Adjusting weighted value increases the ability of TPMOTM to detect potential attacks. It is worth noting that at each phase of evaluation, as one weight value increases, the other weights would decrease to ensure that the total weight value is 1. Adjusted weighted values can derived from Eq. 15 to Eq. 19.

$$\alpha_1' = \begin{cases} \frac{N_{time}}{N_{time}+N_{acc}} & \text{if } N_{time} > 0 \parallel N_{acc} > 0 \\ \alpha_1 & else \end{cases} \tag{15}$$

$$\alpha_2' = \begin{cases} \frac{N_{acc}}{N_{time}+N_{acc}} & \text{if } N_{time} > 0 \parallel N_{acc} > 0 \\ \alpha_2 & else \end{cases} \tag{16}$$

where α_1', α_2', β_1', β_2', and β_3' are adjusted α_1, α_2, β_1, β_2, and β_3, respectively. N_{time}, N_{acc}, N_{mer}, N_{rp}, and N_{mlr} are times of low TV_{time}, low TV_{acc}, low TV_{mer}, low TV_{rp}, and low TV_{mlr} in previous N_{pts} (explained in Section 4.2.2) time slots. It indicates that for each detection factor, as the relative frequency of low trust values increases, the weight value increases. On the contrary, the weight value decreases, and the total weight value is always 1.

4.3.3 Message Integration

As explained in Section 3.1, the GS may receive multiple messages related to the given event. Since the event state is dichotomous, the integration mechanism takes the trust value of message as the weighted value to obtain the event state. The following is the integration equation:

$$E_{itg} = \sum_{m=1}^{N_{re}} TV_m E_{rpt}(m) \tag{20}$$

where E_{itg} is the integrated event state. If E_{itg} is a positive number, it means the event has happened; otherwise, it has not. N_{re} is the number of messages related to a given event, and $E_{rpt}(m)$ is the reported state of message m given by Eq.(21). Here, $E_{rpt}(m) = 1$ denotes the occurrence of event, while $E_{rpt}(m) = -1$ denotes the non-occurrence.

$$E_{rpt}(m) = \begin{cases} 1 & \text{if } event \text{ happens} \\ -1 & \text{if } event \text{ does not happen} \end{cases} \tag{21}$$

4.3.4 Accuracy-Table Update

As mentioned in Section 4.1.2, the GS compares the reported state of all messages with the integrated state, to adjust the detection accuracy of message generators. The adjusted accuracy is updated in Accuracy-table for the next message evaluation. Algorithm 1 illustrates this process. Due to the detection accuracy of generator for each message needs to be adjusted, the time complexity of Algorithm 1 is O(n) (n represents the size of messages $\mathcal{M}$).

Algorithm 1 Message Integration Progress.

Input: Messages $\mathcal{M} = \{1, 2...M\}$
Output: Event state E_{itg}

```
Integrating messages to obtain the event state
for m = 1 to M do
    E_itg = Σ_{m=1}^{N_re} TV_m E_rpt(m)
end for
Adjusting detection accuracy
for m = 1 to M do
    if ((E_rpt(m) = 1 && E_itg > 1) || (E_rpt(m) = −1 && E_itg < 1)) then
        TV_acc(r) = TV_acc(r − 1) + V_rwd
    else
        TV_acc(r) = TV_acc(r − 1) + V_pns
    end if
end for
return E_itg
```

This article has been accepted for publication in a future issue of this jourral, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

5 Simulation and Evaluation

To verify the performance of the proposed model, the simulations are conducted and results are evaluated.

5.1 Experimental Setup

The Opportunistic Network Environment (ONE) [35] is applied to simulate the realistic FANET. There are 40-120 UAVs in the 900m*400m simulation scenario. Since the occurrence of event is unpredictable, UAVs move based on the random movement model. In the random movement model, both the flying distance and the direction are random. Messages are transmitted with the Epidemic router protocol. In addition, FANET is exposed to a variety of attacks, including false message injection, message tampering and black hole attack. The Attacker Ratio (AR) is set as 10%, 20%, and 30% in different case. Specifically, each experiment is repeated twenty times to account for any potential variability or errors, and results are plotted with 95 % confidence interval. The related parameters of simulation are shown in Table 3.

TABLE 3
Simulation parameters

Area size	$900 \times 400m^2$	Simulation time	10800s
UAV number	$40 - 120$	Time slot	1s
UAV speed	$3 - 5m/s$	Buffer size time	10M
Routing Protocol	Epidemic router	Message size	128kB
Movement model	Random movement model	Rician factor	10dB
Attack	False message injection, message tampering, and black hole attack	V_{rwd}	0.01
Communication range	100m	V_{pns}	-0.02
Detection range	50m	Th	0.5
Transmit power	5W	Noise power	-20dBm
Delay factor	0.5	Warm-up time	200s
Initial α_1, α_2	0.5	ρ_1, ρ_2	0.5
Initial β_1, β_2, β_3	0.33	ω_1, ω_2	0.5

The TPMOTM is compared with the UAVN-pro [36] and COI-HiTrust [23] under the same scenario.

- UAVN-pro: UAVN-pro evaluates the behavior of message creators and operators based on message provenance. By generating and collecting observational evidence, UAVN-pro can identify malicious UAVs in FANET.
- COI-HiTrust: COI-HiTrust focuses on evaluating entities in the Community of Interest (COI), for instance, UAVs in FANET. In their work, COI commanders or subtask leaders would measure social behaviors (e.g., connectivity, intimacy, and honesty) and quality of service (e.g., competence and cooperativeness) cognition to evaluate the UAV.

5.2 Performance Evaluation

The performance of the proposed model is evaluated from four perspectives: the effectiveness of detection factors, the accuracy of message evaluation, the accuracy of event evaluation, and communication overhead.

5.2.1 Detection Factors Analysis

In the Section 4, lots of detection factors are taken into account to evaluate the message. Thus, it is necessary to figure out if these factors are effective to reflect network conditions or attacks. How trust values of these factors vary with environmental conditions or attacks is analyzed as follow:

As mentioned in Section 4.1.1, message timeliness is crucial for changing events. Thus, the relationship between the TV_{time} (derived from Eq. 1) and Message Generation Timeliness (MGT) is analyzed, which is denoted as $\frac{t_{gen}-t_{str}}{t_{end}-t_{str}}$ in Eq.1. Specifically, the interval between the current time and message generation is set as 10 seconds. As shown in Fig. 6 (a), with the increase of MGT, the TV_{time} smoothly increases. When MGT approaches 1, the TV_{time} also closes to 1. However, when MGT approaches 0, TV_{time} is above the 0.5, because non attacking factors have a slighter impact on trust values. Thus, mathematical measures are taken, to ensure that trust values determined by non attacking factors do not fall below the trust threshold 0.5.

In addition, it is considered how the trust value of detection accuracy of normal and malicious UAVs changes with the evaluation rounds. With the 20% AR, 80 UAVs, and the 20% probability of false message injection attack (denoted as P_{fmi}), the TV_{acc} (derived from Eq. 2) of normal UAV and malicious UAV is tracked for 50 rounds. As shown in Fig. 6 (b), with the increase of evaluation rounds, the TV_{acc} of normal UAV gradually increases, while the TV_{acc} of malicious UAV decreases with fluctuations. Accordingly, the difference of TV_{acc} between the normal UAV and malicious UAV gradually widens. This indicates that after a while of running, the TPMOTM can effectively distinguish malicious UAVs from normal UAVs.

According to Section 4.2.1, the message error rate is influenced by the communication distance between the sender and receiver. Therefore, the relationship between the Dis and TV_{mer} (derived from Eq. 5) is analyzed. As shown in Fig. 6 (c), when the Dis is less than 30 metres, the TV_{mer} is 1. Then the TV_{mer} decreases, with the Dis increases from 30 metres to 100 metres. When the communication distance between two UAVs reaches the maximum communication distance 100, the TV_{mer} closes to 0.6 (± 0.02).

Moreover, the impact of Average Meeting UAVs (AMU) is analyzed, denoted as $\frac{1}{N_{pts}} \sum_{t'=t-N_{pts}}^{t} N_{meet}^{t'}$ in Eq. 7, on the meeting probability. In concrete terms, the variation trend of AMU and that of RA_{me} (derived from Eq. 7) are compared with time t. As shown in Fig. 6 (d), the number of AMU rapidly increases from 0 to 100 seconds, and then stabilizes after 200 seconds. This is because UAVs hava not yet had enough time to traverse sub areas at the begging. To eliminate its impact, the warm-up time is set as 200 seconds before the formal simulation. The variation trend of RA_{me} is consistent with that of AMU, and as the non attacking factor, the RA_{me} is always greater than 0.5.

Section 4.2.3 introduces that the TPMOTM applies the MAC algorithm to verify whether messages are tampered

This article has been accepted for publication in a future issue of this jounal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

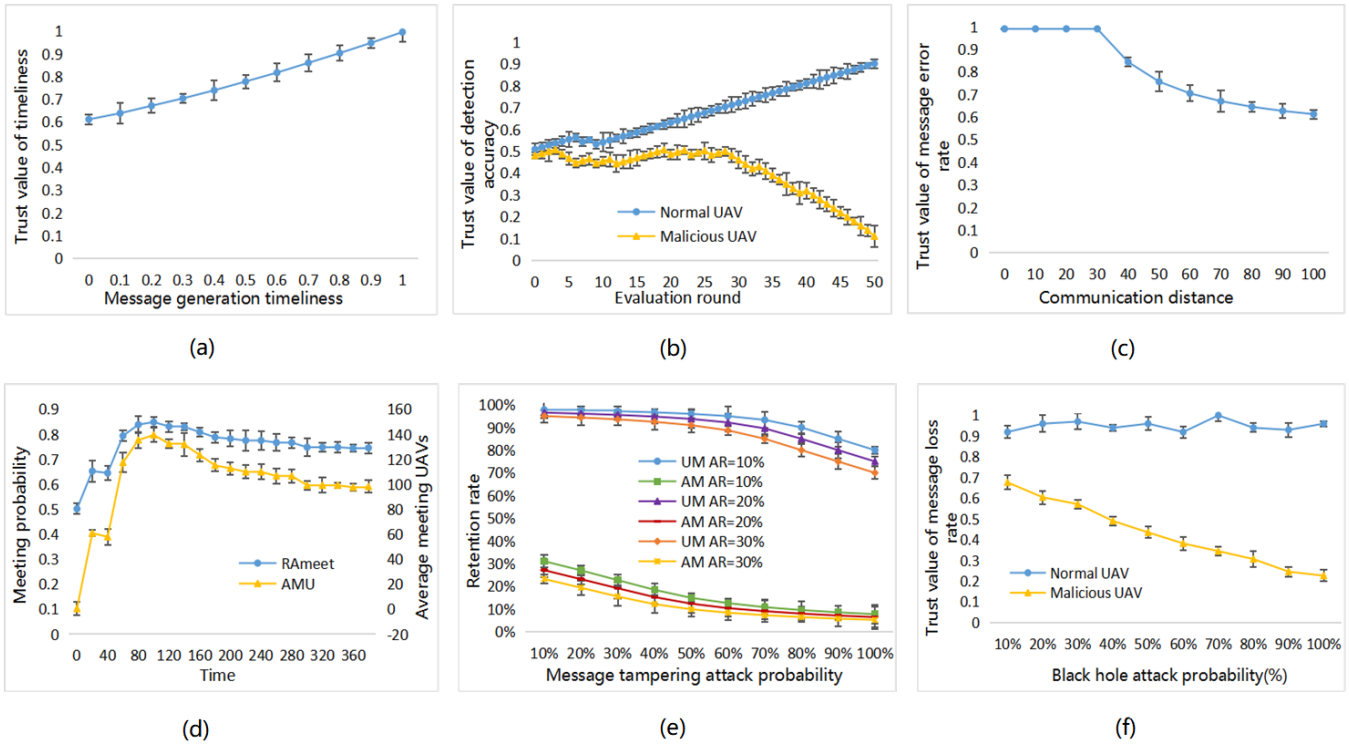

Fig. 6. Variation of (a) Trust value of timeliness with message generation timeliness, (b) Trust value of detection accuracy with evaluation rounds, (c) Trust value of message error rate with communication distance, (d) UAV meeting rate and average meeting UAVs with time, (e) Retention rate with message tampering attack probability, and (f) Trust value of message loss rate with black hole attack probability.

with. The MAC algorithm deletes Attacked Messages (AMs) and saves Unattacked Messages (UMs). Therefore, the retention rate of AMs and UMs are evaluated, in different message tampering attack probabilities (denoted as P_{mt}) and different ARs. The retention rate is defined as the ratio of saved messages to verified messages. As shown in Fig. 6 (e), the retention rate of all cases decreases as the P_{mt} increases. In the same P_{mt}, the higher the AR, the lower the retention rate of messages. However, compared to UMs, the retention rate of AMs is significantly reduced. The retention rate of UMs is mostly higher than 80% ($\pm$2.54%), while the retention rate of AMs is lower than 32% ($\pm$1.63%).

In addition, the impact of black hole attack probability (denoted as P_{bh}) on TV_{mlr} (derived from Eq. 11) is analyzed. Specifically, there are 80 UAVs, and the AR is set as 20%. The average TV_{mlr} of normal UAVs and malicious UAVs are compared with different P_{bh}. As shown in Fig. 6 (f), the TV_{mlr} of normal UAV is not affected by the P_{bh}, and it is always greater than 0.9 ($\pm$0.02). In comparison, the TV_{mlr} of malicious UAVs is significantly lower than that of normal UAV, and it decreases dramatically with the increasing P_{bh}. When the P_{bh} is up to 40%, the TV_{mlr} of malicious UAV is below the 0.5.

The above experiments prove that trust values of detection factors can accurately reflect the impact of network circumstance or attack on messages. It is worth noting that attacks can cause the greater fluctuation on the trust value than circumstance of network.

5.2.2 Message Evaluation

Considering that the TPMOTM focuses on evaluating messages, the following three aspects are concentrated on to evaluate the effectiveness of the TPMOTM:

- Detection rate: In Section 4.3.4, the message reported state and event integrated state are compared. Meaagses with consistent states are considered as true messages, while others are fake messages. The detection rate is the ratio of correctly distinguished messages among all messages.
- False positive rate: The false positive rate is the number of messages that are incorrectly classified as fake messages, over the number of unattacked messages.
- False negative rate: The false negative rate is the number of messages that are incorrectly classified as true messages, over the number of attacked messages.

The AR is set as 20%, the number of UAVs is 80, and hybrid attacks (false message injection attack, message tampering attack, and black hole attack) launch with the same probability. The probability of hybrid attacks (denoted as P_{hyb}) ranges from 5% to 50%. As shown in the Fig. 7 (a), the detection rate of all three models decreases with the increase of P_{hyb}. However, the detection rate of TPMOTM is always up to 95% ($\pm$0.89%), which is higher than that of UAVN-pro and COI-HiTrust. This indicates that the TPMOTM is more suitable for message-sensitive scenarios, than trust models focusing on the evaluation of UAVs, i.e., UAVN-pro and COI-HiTrust.

The false positive rate and false negative rate are evaluated with the same configuration. As shown in Fig. 7 (b), with the

This article has been accepted for publication in a future issue of this joural, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

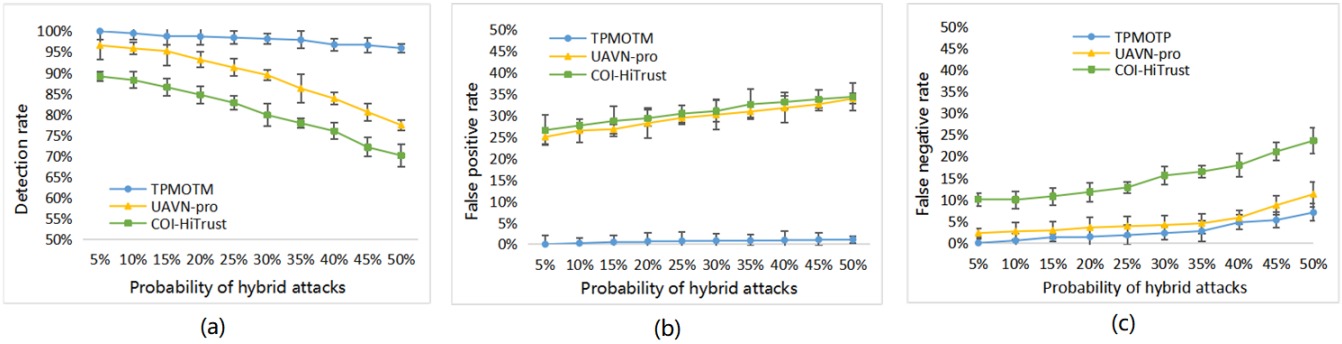

Fig. 7. Variation of (a) Detection rate with probability of hybrid attacks, (b) False positive rate with probability of hybrid attacks, (c) False negative rate with probability of hybrid attacks.

increase of P_{hyb}, the false positive rate of TPMOTM slightly increases. Even P_{hyb} is as high as 50%, the R_{fp} of TPMOTM is below 1.2% ($\pm$0.12%). As illustrated in Fig. 7 (c), the false negative rate generated by the TPMOTM increases slowly, as compared to the UAVN-pro and COI-HiTrust when the P_{hyb} increases. Low false positive rate and false negative rate are attributed to the dynamic trust value mechanism mentioned in Section 4.3.1. This mechanism weakens the misjudgment impact of individual UAV on the total trust value of message.

According to the result of detection rate, false positive rate, and false negative rate, it demonstrates that the TPMOTM can accurately identify AMs and UMs, and assign low trust values to the AMs.

5.2.3 Event Evaluation

The TPMOTM includes the message integration phase that is ignored by most trust models. Therefore, in this section, the event detection accuracy rate is evaluated, that is, the ratio of correctly detected events to detected events. To check the attack-resistance of TPMOTM, the event detection accuracy rate is evaluated in three types of attacks: single false message injection attack, single message tampering attack, and hybrid attacks. Considering the single black hole attack cannot directly change the reported state of messages to affect the event detection accuracy rate, the impact of single black hole attack does not be evaluated. The event detection accuracy rate of TPMOTM is compared with that of UAVN-pro and COI-HiTrust with 80 UAVs and 20% AR.

As shown in Fig. 8 (a) - (c), in each attack, the event detection accuracy rate of all three models decreases with the increase of attack probability. Fig. 8 (a) and Fig. 8 (b) show that comparing to the false message injection attack, the event detection accuracy rate of message tampering attack is higher. As explained in Section 3.2, this is because injection affects the AM and all copies it generates, while tampering only affects part of copies. As mentioned in Section 3.2, Fig. 8 (c) illustrates that hybrid attacks can raise more risks than the single attack. Nevertheless, the event detection accuracy rate of TPMOTM is mostly greater than 85% ($\pm$1.21%), and the TPMOTM performs better than other two models in the same case. As P_{hyb} increases from 50% to 100%, the difference of event detection accuracy rate between the TPMOTM and other two schemes gradually widens.

To figure out how the number of UAVs affects the event detection accuracy rate, the AR is set as 20%, and the number of UAVs ranges from 40 to 120. As shown in the Fig. 8 (d), as the number of UAVs grows, the event detection accuracy rate increases. This is because more UAVs can generate a large amount of messages, helping to improve the accuracy of event judgment in message integration phase. However, too many UAVs bring more overhead, which would be analyzed in Section 5.2.4. Therefore, an appropriate number of UAVs should be selected based on the scenario, to achieve a balance between accuracy and overhead.

Through the above experiments, it proves that the TPMOTM can effectively resist potential attacks, and it has more accurate event detection capabilities than other two models.

5.2.4 Communication Overhead

Communication overhead is the number of bytes generated in the FANETs to accurately detect events. According to Xu et al. [37], communication overhead is determined by the number and size of messages.

The probability of hybrid attacks (false message injection attack, message tampering attack, and black hole attack) is set as 20%, and the AR is set as 20%. The number of UAVs ranges from 40 to 120, to analyze how the number of UAVs affects communication overhead. As shown in Fig. 9, the communication overhead of the TPMOTM is lower than that of UAVN-pro and COI-HiTrust in the same case. This is because the trust value in the TPMOTM is attached to messages, without generating additional monitoring messages. In addition, communication overhead in the TPMOTM increases slowly with the growth of the number of UAVs, avoiding the excessive burden on the network.

6 Conclusion

In this work, it is pointed out that UAVs may be exposed to potential attacks, resulting in the error of event detection. Therefore, a message oriented trust model called TPMOTM is proposed to evaluate the trustworthiness of messages. In the proposed TPMOTM, the evaluation includes three phases: message generation, message transmission, and message integration. Message are evaluated by specific detection factors in message generation and message transmission, and integrated in message integration phase. Then event state is determined based on messages and their trust values. Finally, the ONE simulator is utilized to simulate FANET and attacks, and a

This article has been accepted for publication in a future issue of this jounal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI10.1109/TNSE.2024.3374733, IEEE Transactions on Network Science and Engineering

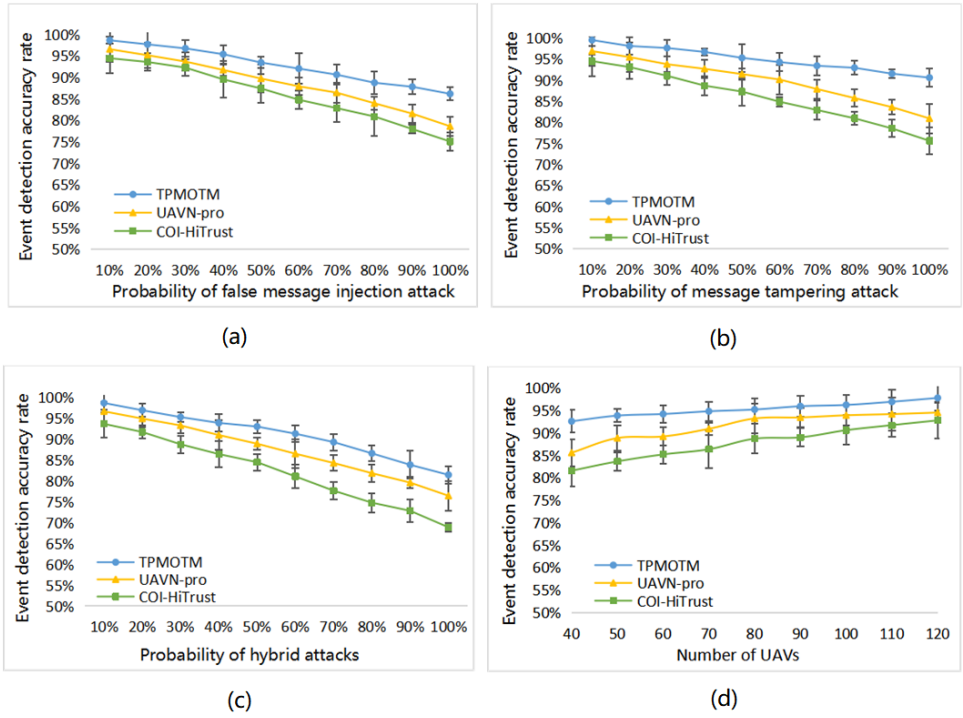

Fig. 8. Event detection accuracy rate with (a) Probability of single false message injection attack, (b) Probability of single message tampering attack, (c) Probability of hybrid attacks, and (d) Number of UAVs.

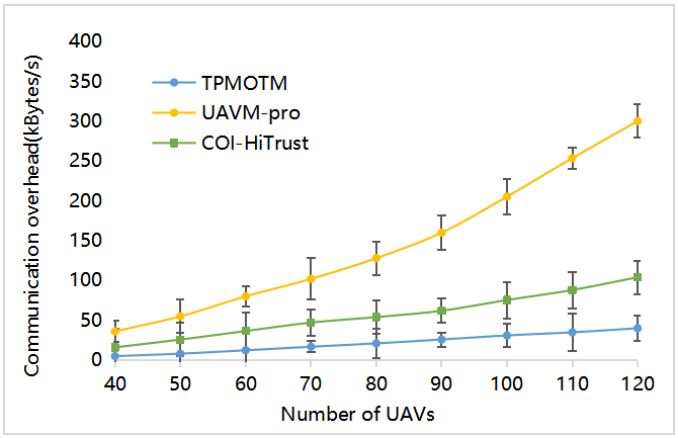

Fig. 9. Communication overhead.

comprehensive simulation evaluation is conducted on the TPMOTM. The availability of detection factors, the effectiveness of message evaluation, the accuracy of event detection, and low overhead are proved. In addition, the TPMOTM is compared with UAVN-pro and COI-HiTrust, and the experiments show that the proposed model outperforms existing models in message evaluation, event detection, and communication overhead.

Future directions focus on improving the TPMOTM to resist more attacks. In order to detect more attacks, it is necessary to study and quantify features of these attacks. While in the common case the solution is designed for dedicated attack detection, in the extreme case where attackers can intelligently switch their attack modes, it is necessary to shorten the detection time of each attack to address this issue in the feature.

References

[1] L. Merino, F. Caballero, J. Martínez-de Dios, J. Ferruz, and A. Ollero, "A cooperative perception system for multiple uavs: Application to automatic detection of forest fires," Journal of Field Robotics, vol. 23, pp. 165–184, 2006, doi:10.1002/rob.20108.

[2] T. Duong and E. Garcia-Palacios, "Adaptive d-hop connected dominating set in highly dynamic flying ad-hoc networks," IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, Sep. 2021, doi: 10.1109/TNSE.2021.3103873.

[3] Y.-J. Chen, X.-C. Chen, and M. Pan, "Defense against machine learning based attacks in multi-uav networks: A network coding based approach," IEEE Transactions on Network Science and Engineering, vol. 9, pp. 2562–2578, 2022, doi:10.1109/TNSE.2022.3165971.

[4] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent iov," IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13 784–13 795, 2020, doi:10.1109/.2020.3027568.

[5] T. D. Khanh, I. I. Komarov, L. D. Don, R. A. Iureva, and S. Chuprov, "Tra: Effective authentication mechanism for swarms of unmanned aerial vehicles," 2020 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1852–1858, 2020, doi:10.1109/SSCI47803.2020.9308140.

[6] C. A. Kerrache, A. Lakas, N. Lagraa, and E. Barka, "Uav-assisted technique for the detection of malicious and selfish nodes in vanets," Vehicular Communications, vol. 11, pp. 1–11, 01 2018, doi: 10.1016/j.vehcom.2017.12.001.

[7] J. Guo, A. Liu, K. Ota, M. Dong, X. Deng, and N. N. Xiong, "Itcn: An intelligent trust collaboration network system in iot," IEEE Trans. Netw. Sci. Eng., vol. 9, pp. 203–218, 2021, doi:10.1109/TNSE.2021.3057881.

[8] J.-H. Cho and I.-R. Chen, "Provest: Provenance-based trust model for delay tolerant networks," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, pp. 151–165, 2018, doi:10.1109/TDSC.2016.2530705.

[9] P. Asuquo, H. Cruickshank, C. P. A. Ogah, A. Lei, and Z. Sun, "A distributed trust management scheme for data forwarding in satellite dtn emergency communications," IEEE Journal on Selected Areas in Communications, vol. 36, no. 2, pp. 246–256, 2018, doi:10.1109/JSAC.2018.2804098.

[10] K. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (fanets)," International Journal of Communication Systems, vol. 31, p. e3517, 01 2018, doi: 10.1002/dac.3517.

[11] K. Singh and A. K. Verma, "A trust model for effective cooperation in flying ad hoc networks using genetic algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), pp. 0491–0495, 2018, doi:10.1109/ICCSP.2018.8524558.

[12] Z. Liu, J. Guo, F. Huang, D. Cai, Y. Wu, X. Chen, and K. K. Igorevich, "Lightweight trustworthy message exchange in unmanned aerial vehicle networks," IEEE Transactions on Intelligent Transportation Systems, vol. 24, pp. 2144–2157, 2023, doi:10.1109/TITS.2021.3136304.

[13] T. Li, J. Ma, P. Feng, Y. Meng, X. Ma, J. Zhang, C. Gao, and D. Lu, "Lightweight security authentication mechanism towards uav networks," 2019 International Conference on Networking and Network Applications (NaNA), pp. 379–384, 2019, doi:10.1109/NaNA.2019.00072.

[14] S. Safavat and D. B. Rawat, "Securing unmanned aerial vehicular networks using modified elliptic curve cryptography," in MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM). IEEE Press, 2021, p. 999–1004, doi: 10.1109/MILCOM52596.2021.9652982.

[15] M. A. Khan, I. Ullah, A. Alkhalifah, S. U. Rehman, J. A. Shah, M. I. Uddin, M. H. Alsharif, and F. Algarni, "A provable and privacy-preserving authentication scheme for uav-enabled intelligent transportation systems," IEEE Transactions on Industrial Informatics, vol. 18, p. 3416–3425, 05 2022, doi: 10.1109/TII.2021.3101651.

[16] T. Alladi, Naren, G. Bansal, V. Chamola, and M. Guizani, "Secauthuav:a novel authentication scheme for uav-ground station and uav-uav communication," IEEE Transactions on Vehicular Technology, vol. 69, pp. 15 068–15 077, 12 2020, doi: 10.1109/TVT.2020.3033060.

[17] K. Yoon, D.-I. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, "Security authentication system using encrypted channel on uav network," 2017 First IEEE International Conference on Robotic Computing (IRC), pp. 393–398, 2017, doi:10.1109/IRC.2017.56.

[18] C. F. E. de Melo, T. Dapper e Silva, F. Boeira, J. M. Stocchero, A. Vinel, M. Asplund, and E. P. de Freitas, "Uavouch: A secure identity and location validation scheme for uav-networks," IEEE Access, vol. 9, pp. 82 930–82 946, 2021, doi:10.1109/ACCESS.2021.3087084.

[19] E. Ghribi, T. T. Khoei, H. T. Gorji, P. Ranganathan, and N. Kaabouch, "A secure blockchain-based communication approach for uav networks," in 2020 IEEE International Conference on Electro Information Technology (EIT), 2020, pp. 411–415, doi:10.1109/EIT48999.2020.9208314.

[20] R. Liu, X. Chen, Y. Zou, and Y. Bai, "Research and application uav operation data trusted storage technology based on blockchain," 2020 IEEE 2nd International Conference on Civil Aviation Safety and Information Technology (ICCASIT, pp. 30–35, 2020, doi:10.1109/ICCASIT50869.2020.9368849.

[21] S. K. Bhoi, K. K. Jena, G. V. Maniharika, S. Muduli, R. Sahoo, and D. Bhol, "Detection of intended and unintended misbehaviors in unmanned aerial vehicle network (uavn)," in 2019 International Conference on Information Technology (ICIT), 2019, pp. 222–227, doi:10.1109/ICIT48102.2019.00046.

[22] E. E. Barka, C. A. Kerrache, N. Lagraa, A. Lakas, C. M. T. Calafate, and J.-C. Cano, "Union: A trust model distinguishing intentional and unintentional misbehavior in inter-uav communication," Journal of Advanced Transportation, vol. 2018, pp. 1–12, 2018, doi:10.1155/2018/7475357.

[23] I.-R. Chen and J. Guo, "Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection," ser. AINA '14. USA: IEEE Computer Society, 2014, p. 49–56, doi: 10.1109/AINA.2014.13.

[24] Z. Li, J. Xu, and Q. Guo, "Cooperative location method of muti-uav system under environment of communication jamming based on tri-layer trust model," 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), pp. 108–112, 2018, doi:10.1109/ITOEC.2018.8740389.

[25] X. Wang, X. Z. Gao, and S. J. Ovaska, "A hybrid optimization method for fuzzy classification systems," 2008 Eighth International Conference on Hybrid Intelligent Systems, pp. 264–271, 2008, doi:10.1109/HIS.2008.22.

[26] Z. Liu, J. Weng, J. Guo, J. Ma, F. Huang, H. Sun, and Y. Cheng, "Pptm: A privacy-preserving trust management scheme for emergency message dissemination in space–air–ground-integrated vehicular networks," IEEE Internet of Things Journal, vol. 9, pp. 5943–5956, 2021, doi:10.1109/JIOT.2021.3060751.

[27] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for vanets," IEEE Transactions on Vehicular Technology, vol. 61, pp. 4095–4108, 2012, doi:10.1109/TVT.2012.2209903.

[28] Z. Liu, J. Weng, J. Ma, J. Guo, B. Feng, Z. Jiang, and K. Wei, "Tcemd: A trust cascading-based emergency message dissemination model in vanets," IEEE Internet of Things Journal, vol. 7, pp. 4028–4048, 2020, doi:10.1109/JIOT.2019.2957520.

[29] A. Andreou, C. X. Mavromoustakis, J. M. Batalla, E. K. Markakis, G. Mastorakis, and E. Pallis, "Secure two-way communications between uavs and control center in iov 5g communication," 2022 IEEE 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 184–189, 2022, doi:10.1109/CAMAD55695.2022.9966916.

[30] I. Gupta, A.-M. Kermarrec, and A. Ganesh, "Efficient and adaptive epidemic-style protocols for reliable and scalable multicast," IEEE Transactions on Parallel and Distributed Systems, vol. 17, no. 7, pp. 593–605, 2006, doi:10.1109/TPDS.2006.85.

[31] K. Wang and M. Wu, "A trust approach for node cooperation in manet," in Proceedings of the 3rd International Conference on Mobile Ad-Hoc and Sensor Networks, ser. MSN'07. Berlin, Heidelberg: Springer-Verlag, 2007, p. 481–491, doi:10.5555/1781974.1782022.

[32] K. K. Jena, S. K. Bhoi, B. D. Behera, S. Panda, B. P. Sahu, and R. Sahu, "A trust based false message detection model for multi-unmanned aerial vehicle network," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 324–329, 2019, doi:10.1109/I-SMAC47947.2019.9032550.

[33] L.-C. Wang, W.-C. Liu, and Y.-H. Cheng, "Statistical analysis of a mobile-to-mobile rician fading channel model," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 32–38, 2009, doi:10.1109/TVT.2008.924999.

[34] A. Vosoughi and R. Katti, "Fast message authentication code for multiple messages with provable security," in 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–5, doi:10.1109/GLOCOM.2010.5684307.

[35] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for dtn protocol evaluation," in International ICST Conference on Simulation Tools and Techniques, 2009, doi:10.4108/ICST.SIMUTOOLS2009.5674.

[36] C. Ge, L. Zhou, G. P. Hancke, and C. Su, "A provenance-aware distributed trust model for resilient unmanned aerial vehicle networks," IEEE Internet of Things Journal, vol. 8, pp. 12 481–12 489, 2021, doi:10.1109/JIOT.2020.3014947.

[37] J. Xu and M. Chung, "Predicting the performance of synchronous discrete event simulation," IEEE Transactions on Parallel and Distributed Systems, vol. 15, no. 12, pp. 1130–1137, 2004, doi:10.1109/TPDS.2004.85.

Xueru Du received the B.S. degree in Computer Science and Technology from Wuhan University, Wuhan, China, in 2021. She is currently working toward the Ph.D. degree in cyber security with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. Her research interests include trust management and intrusion detection in flying Ad Hoc network.

Yue Cao received the Ph.D. degree from the Institute for Communication Systems (ICS) formerly known as Centre for Communication Systems Research, University of Surrey, Guildford, U.K., in 2013. Further to his PhD study, he had conducted a Research Fellow with the University of Surrey, and academic faculty with Northumbria University, U.K., Lancaster University, U.K., and Beihang University, Beijing, China. He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. His multidisciplinary research interest focuses on the theme of ITS, including cyber security, wireless network and service optimization. He has been also the Fellow of British Computer Society, Fellow of Royal Society of Arts and Fellow of Higher Education Academy.

Di Wang received the B.S. degree and the M.S. degree from the school of information engineering, Jiangxi University of Science and Technology, Jiangxi, China, in 2017 and 2020 respectively. She is currently pursuing the Ph.D degree with the school of Cyber Science and Engineering, Wuhan University, Wuhan, China. Her current research interests include information security, applied cryptography and IoV.

Chenchen Lv received the B.S. degree in Computer Science and Technology from Wuhan University, Wuhan, China, in 2021. She is currently working toward the M.S. degree in cyber security with the School of Cyber Science and Engineering, Wuhan University, Wuhan, China. Her research interests include trust management and intrusion detection in flying Ad Hoc network.

Celimuge Wu received his PhD degree from The University of Electro-Communications, Japan. He is currently a professor and the director of Meta-Networking Research Center, The University of Electro-Communications. His research interests include Vehicular Networks, Edge Computing, IoT, and AI for Wireless Networking and Computing.

Kezhi Wang received the PhD degree in engineering from the University of Warwick, U.K. He was with the University of Essex and Northumbria University, U.K. Currently, he is a senior lecturer with the Department of Computer Science, Brunel University London, U.K. His research interests include wireless communications, mobile edge computing, and machine learning.