Received: 1 March 2023 | Revised: 7 September 2023 | Accepted: 31 October 2023

IET Networks

DOI: 10.1049/ntw2.12108

ORIGINAL RESEARCH

FUBA: A fuzzy-based unmanned aerial vehicle behaviour analytics for trust management in flying ad-hoc networks

Sihem Benfriha[1] | Nabila Labraoui[2] | Radjaa Bensaid[1] | Haythem Bany Salameh[3,4,5] | Hafida Saidi[1]

[1]STIC Laboratory, University of Abou Bekr Belkaid, Chetouane, Tlemcen, Algeria

[2]LRIT Laboratory, University of Abou Bekr Belkaid, Chetouane, Tlemcen, Algeria

[3]Artificial Intelligence Research Center, Al Ain University, Al Ain, UAE

[4]Telecommunication Engineering Department, Yarmouk University, Irbid, Jordan

[5]College of Engineering, Staffordshire University, Stoke-in City, UK

Correspondence

Sihem Benfriha.
Email: benfriha.sihem@univ-tlemcen.dz

Abstract

Flying Ad-Hoc Network (FANET) is a promising ad hoc networking paradigm that can offer new added value services in military and civilian applications. Typically, it incorporates a group of Unmanned Aerial Vehicles (UAVs), known as drones that collaborate and cooperate to accomplish several missions without human intervention. However, UAV communications are prone to various attacks and detecting malicious nodes is essential for efficient FANET operation. Trust management is an effective method that plays a significant role in the prediction and recognition of intrusions in FANETs. Specifically, evaluating node behaviour remains an important issue in this domain. For this purpose, the authors suggest using fuzzy logic, one of the most commonly used methods for trust computation, which classifies nodes based on multiple criteria to handle complex environments. In addition, the Received Signal Strength Indication (RSSI) is an important parameter that can be used in fuzzy logic to evaluate a drone's behaviour. However, in outdoor flying networks, the RSSI can be seriously influenced by the humidity of the air, which can dramatically impact the accuracy of the trust results. FUBA, a fuzzy-based UAV behaviour analytics is presented for trust management in FANETs. By considering humidity as a new parameter, FUBA can identify insider threats and increase the overall network's trustworthiness under bad weather conditions. It is capable of performing well in outdoor flying networks. The simulation results indicate that the proposed model significantly outperforms FNDN and UNION in terms of the average end-to-end delay and the false positive ratio.

KEYWORDS

computer network security, fuzzy logic, mobile ad hoc networks

1 | INTRODUCTION

Our world has changed and is still evolving due to rapidly developing technology in sensors, communications, and networking over the past few decades [1]. Unmanned Aerial Vehicles (UAVs) have been proposed for a multitude of applications in both military and civilian domains, encompassing ad hoc networks, search and rescue missions, electronic operations in hostile zones, ground target identification and tracking, automated forest fire surveillance, wind energy generation [2], and a host of other possibilities. Furthermore, flying ad hoc networks (FANETs), a revolutionary concept, comprise a group of UAVs that cooperate to perform some crucial missions [3]. However, many cyberattacks against UAVs have emerged since 2007 [4], and their impact can be dangerous with divesting effects. Therefore, it is essential to protect FANETs from insider and outsider attacks. In FANETs, drones can leave and rejoin the network anytime, creating an opportunity for attackers to compromise a node and impersonate a legitimate one, leading to insider attacks. Insiders use their trusted access to carry out illicit actions. As a result, they are undetectable by external network security protocols (intrusion detection, firewalls, and cryptographic methods) [5]. Consequently, ensuring secure and reliable communications in FANETs is critical and continues to be an issue.

In this context, trust management is an effective and attractive technique to prevent unexpected node actions and detect malicious nodes [6]. It can improve the robustness and reliability of standard security techniques by guaranteeing that only trustworthy nodes cooperate in network missions. Nevertheless, trust depends on observation and recommendation, and some models have been proposed for FANET to calculate the trust of the drone, but they may lead to uncertainty [7]. Fuzzy logic is a popular method for representing and manipulating uncertain data, such as node behaviours. Few related works use the RSSI as an important parameter for trust evaluation, and this performs better in indoor networks. However, in outdoor networks, the RSSI can be influenced by humidity and thus impact the trust results. In addition, the drone can be detected as non-cooperative due to unintentional misbehaviour related to poor signal strength (RSSI). The main challenge in this domain is designing an efficient analytical trust model for evaluating and understanding node behaviour in FANET under poor signal (RSSI) and bad weather conditions. Without this model, there will be no effective strategy to distinguish between legitimate and malicious drone activities in FANETs. Although several trust models have recently been proposed, none have yet focused on the impact of bad weather conditions on the trust management process in FANET. The proposed work aims to address this gap using the fuzzy logic method to determine the trust of a drone based on several parameters, such as energy (battery level), weather (humidity), signal strength (RSSI), packet delivery ratio (PDR) and transmission delay (TD). Specifically, this article introduces a novel fuzzy-based UAV behaviour analytics system named FUBA for trust management in FANETs. FUBA utilises fuzzy logic methodology to assess drone trustworthiness by considering various factors such as energy levels, weather conditions, signal strength, packet delivery ratios, and transmission delays. The proposed model offers several advantages: superior performance in outdoor flying networks, effective characterisation of node behaviour, subjective evaluation of node behaviour, and the ability to make confident decisions regarding network information exchange. To comprehensively evaluate the model's performance, we implement and rigorously test the system through extensive simulation experiments conducted using the Omnet++, Xplane, and Avens frameworks. The simulation results demonstrate that our model outperforms existing ones in terms of average end-to-end delay and false positive ratio. Furthermore, we analyse the influence of RSSI and humidity on trust results through Matlab simulations, shedding light on prevailing challenges and open issues in this domain.

The rest of this paper is listed as follows: Section 2 offers an overview of the related works on trust management in FANETs. Section 3 introduces the proposed fuzzy-based UAV behaviour analytics for trust management in FANETs (FUBA). Section 4 detailed the practical aspects and limitations of FUBA. Section 5 provides the detailed implementation of FUBA. Section 6 explains the impact of RSSI and humidity on trust results. Section 7 reports and discusses the experimental results. Finally, Section 8 concludes the paper and provides possible future directions.

2 | RELATED WORK

Since UAV networks appeared, several trust models have been implemented to strengthen the trust management systems in FANET. Most of them were initially proposed for Mobile Ad hoc Networks(MANETs) [8]. The recent research on trust-based solutions is presented below:

Berka et al. [9] proposed a new energy-efficient scheme for FANET that is reputation-aware. Their approach computed the trustworthiness by considering the count of both legal and illegal node interactions to establish trust with low energy, considering the indirect trust values. However, when there is no interaction between the trustor and the trustee, the findings impact the system's accuracy. To differentiate between legitimate and malicious drone activities, the authors in ref. [8] presented a second model referred to as UNION. To eliminate man-in-the-middle threats, Barka et al. [10] proposed a comprehensive communication architecture named FNDN (Flying Named Data Networking). This architecture revolves around the integration of trust mechanisms. When propagating data, their model system uses a trust management strategy to address the network attack concern. FNDN utilises inter-UAV trust to decide whether to verify the authenticity of data for a specific node. In ref. [11], the authors suggested a new trust scheme named BUAS. BUAS is based on a blockchain technology-based inter-UAV trust evaluation method.

The Bayesian inference method was used to calculate the probability of the message's trustworthiness. Singh and Verma described a fuzzy-based trust model in ref. [12] that addresses the trustworthiness of the FANET node. A fuzzy classification has been implemented, and the quality of services and social parameters are considered to calculate trust values. They also proposed a weightage-based method that uses the genetic algorithm [13] to ascertain the trust values by simultaneously optimising the weights assigned to different parameters. In ref. [14], the authors proposed a trust-based clustering scheme using the first model to select a trustworthy cluster head that can add new nodes to the network. Zhou and Wang in ref. [15] proposed a K-means ++ clustering algorithm. This model determines the optimal number of clusters and integrates a trust value using the Bayesian model to identify malicious nodes for exclusion from the cluster selection process. Jena et al. [16] provided a methodology for filtering erroneous event messages produced by the network using event-based reputation. The impact of the node's location on detecting the genuineness of the event is considered in this model. Bhargava et al. proposed a Kalman trust estimator (KATE) in ref. [17]. KATE checks drones' misbehaviour by combining direct and indirect trust values. Kate considers the impact of historical trust values stored on the Internet on current trust values. Carlos et al. in ref. [18] suggested and assessed UAVouch, a system for identifying and locating UAVs in a group. UAVouch uses a movement plausibility check and a public-key-based authentication system to identify intruders who deviate from the group's anticipated trajectory.

In summary, several trust management solutions for FANETs have been proposed in recent years to enhance network security. Still, none have considered weather conditions' impact on node behaviour and trust computation. Therefore, this paper incorporates humidity as a novel parameter in the proposed study to demonstrate the influence of humidity on both RSSI and trust outcomes.

3 | THE PROPOSED FUBA MODEL

This section presents the network architecture and the detailed proposed FUBA model that considers the effects of climate change and poor signal strength. The major idea is to protect the network from insider attacks and differentiate between legitimate drone actions and malicious activities.

3.1 | Network architecture

FANET comprises three fundamental components: nodes (drones), ground control stations (GCS), and communication links. There are two types of communication, UAV to UAV (U2U) and UAV to Infrastructure (U2I). In FANET, the nodes can leave and join the network anytime, but this flexibility can also make the network vulnerable to attacks. During this, the hacker can compromise a normal drone and convert it into a malicious drone [14]. The intruder participates in the network as a legitimate node and potentially deletes or corrupts messages or damages the reputation of trustworthy nodes. This type of attack, known as an insider attack, can be a significant threat to the security of FANET. Figure 1 shows the network model of FANET operating under the assumption of an insider attack.

As illustrated in Figure 2, the proposed FUBA model is based on four steps: information gathering, trust score calculation, trust aggregation, and decision-making.

3.2 | Information gathering

In the proposed FUBA model, every node collects behaviour information about its neighbours, including their software and hardware performance over time. The fuzzy logic method has been used by Singh et al. [13] with four parameters. The proposed model employs five parameters: signal strength, the drone's energy, packet delivery ratio, transmission delay, and humidity. The parameters collected by each drone are shown in Figure 3.

3.2.1 | Received signal strength indicator (RSSI)

The drone can measure the received signal power of its neighbour at a specific location and time. The number obtained, known as the Received Signal Strength Indicator (RSSI) is given in dBm, which is typically a negative value [19]. The typical RSSI for most excellent signal power is greater than −50 dBm (e.g. −30 dBm). Good or acceptable signal power has RSSI ranging from −50 to −70 dBm, (e.g. −60 dBm). Poor signal power has RSSI less than −70 dbm (e.g. −90 dBm) [20].

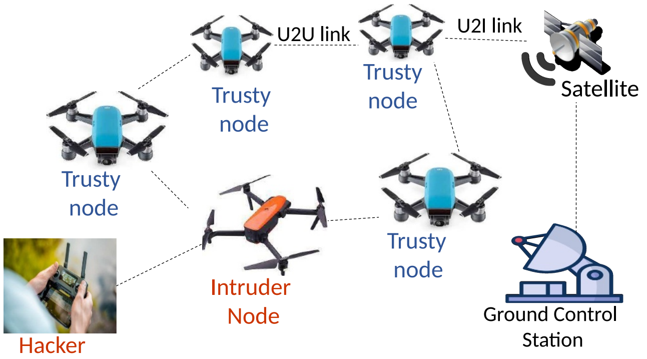


FIGURE 1 FANET model during an Insider attack.

3.2.2 | Node's energy (battery level)

The node's energy is one of the most critical factors to consider in a drone; therefore, effective power management, including wireless drone charging, solar drone charging, and even the utilisation of artificial intelligence technology [21], are required for the continuity of the applications [22]. The node can accomplish the mission when its battery level exceeds 50%. It can hardly collaborate with its neighbours when the energy level is between 20% and 50%. If the battery level falls below 20%, the node may degrade the network mission [20].

3.2.3 | Packet delivery ratio (PDR)

The packet delivery ratio is the proportion of correctly received packets to the total number of packets transmitted by the sender, represented by Equation (1) [23].

$$PDR = \frac{\sum_{i=0}^{n} ReceivedP_i}{\sum_{i=0}^{n} SentP_i} \tag{1}$$

where $ReceivedP_i$ and $SentP_i$, respectively, denote the number of correctly received packets and the number of packets transmitted by the sender. In ref. [20], it has been illustrated that if the ratio of packets sent effectively is less than 40%, then the PDR is low; if it is between 40% and 70%, then the PDR is medium; and if it is greater than 75%, then the PDR is considered high.

3.2.4 | Transmission delay (TD)

TD represents the drone sender's time to transmit the packets over the link. The following formula of TD is given as follows:

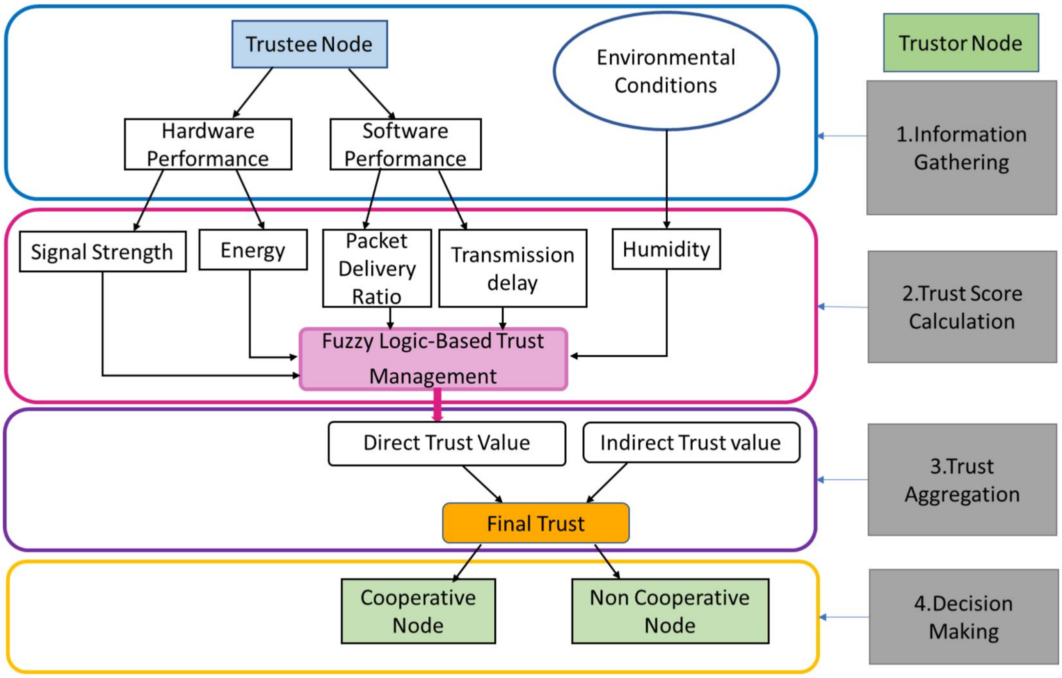


FIGURE 2 FUBA trust model.

Packet Delivery Ratio
Weather conditions
Transmission Delay
Signal Strength
Energy

FIGURE 3 The collected parameters in FANET.

$$TD = \frac{L}{R} \tag{2}$$

where L is the length of the data packet, and R is the transmission rate (bits per second). The transmission delay is judged small if its value is lower than 0.61 ms; medium if the value is between 0.96 and 1.47 ms; and large if the value exceeds 1.47 ms [20].

3.2.5 | Weather condition

The drone is equipped with many sensors that continuously measure and record information about the current environmental conditions [24], including rain sensors, wind direction sensors, wind speed sensors, air temperature, and humidity sensors. Any change in weather may be sent to the ground control station. If weather conditions significantly impact one of the collected parameters used in the assessment, it becomes challenging to differentiate between legitimate and malicious drone activities or discern intentional from unintentional drone behaviour. To address this issue, the humidity is used as an input parameter in the proposed Fuzzy Logic system.

In this particular context, extensive investigation has been carried out by the authors in ref. [25], focusing on an empirical setup based on IEEE 802.11b/g. The experimentation involves two external radio connections of varying lengths that maintain a continuous data transfer process. The findings indicate that, contrary to expectations, the shorter-distance link is found to be more susceptible to adverse weather conditions. This is attributed to the modulation strategy utilised in that specific scenario. It can be concluded that bad weather conditions may alter the UAV radio signal Propagation.

To analyse the influence of temperature and humidity on RSSI values, the authors in ref. [26] conducted measurements at a constant distance of 25 m under varying weather conditions during summer and winter. The measurement results indicate that the temperature has a relatively minor impact on RSSI compared to humidity because the RSSI values can significantly vary even under similar temperatures. It can be noticed that humidity has a significant influence on RSSI. When the humidity increases, the RSSI values decrease, thereby directly affecting the path loss exponent. It can be concluded that humidity has a greater impact on RSSI than temperature.

3.3 | Trust score calculation

After collecting the necessary information, each drone deploys a fuzzy logic method to calculate its neighbour's trust score.

The proposed system considers various input parameters, including the received signal strength indicator, packet delivery ratio, transmission delay, energy, and humidity. Triangular and trapezoidal membership functions of the input parameters are adopted to enhance the performance. Subsequently, fuzzy rules are employed within the inference engine phase to generate a final numerical value as an outcome. This resulting value signifies the direct trust assessment of the neighbouring node. The configuration of the proposed trust management model based on fuzzy logic is depicted in Figure 4.

3.4 | Trust aggregation

In this phase, the values of α and β are defined to aggregate the direct and indirect trust values. Generally, a FANET is characterised by lower node density and a small link duration between two communicating nodes. The values of α and β are determined based on these two facts, which are used to obtain the needed trust value. Table 1 represents the value of α and β according to the trust state:

a) If the output characteristic value (trust) is "Bad" or "Good," then the confidence factors $\alpha = 1$ and $\beta = 0$. This means that the $Finaltrust(i) = Directtrust(i)$.

b) If the output characteristic value is "Medium," the node requests the recommendations (indirect trust) to its neighbour nodes. Therefore, the final trust computation combines both direct and indirect trust values as shown in Figure 5. The indirect trust is given as follows:

$$IndirectTrust(i) = \frac{1}{n}\sum_{j=1}^{n} DirectTrust(i)_j \qquad (3)$$

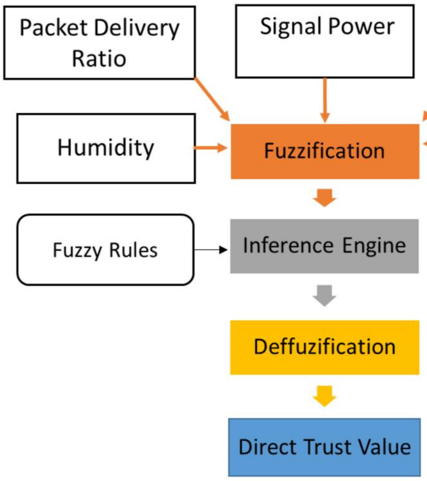


FIGURE 4 Structure of fuzzy system.

where n represents the total number of drones in the network, (i) is the index of the trustee drone, and (j) is the index of the trustor drone.

3.5 | Decision making

The main objective of the decision-making process is to respond to the following questions.

1. Is it confident to exchange information in the network?
2. Are the nodes interested in cooperating or not?

After analysing a node's behaviour and considering the climate changes, the trustor node estimates the trust score of its neighbours using Fuzzy Logic-based trust management. Subsequently, a threshold-based decision module decides whether to cooperate with the node involved in the considered operation. Specifically, the trust score of each node is then compared to a threshold value to determine if the node is trusted or malicious as follows:

$$\begin{cases} if \quad Final \quad trust \quad > \quad 30\% \quad then \quad Trust \quad node \\ if \quad Final \quad trust \quad \leq \quad 30\% \quad then \quad Malicious \quad node \end{cases}$$

4 | PRACTICAL ASPECTS AND LIMITATIONS OF FUBA

The FUBA system presents an innovative approach to enhancing trust management in FANETs by incorporating humidity as a new parameter. This section explores the generalisability and scalability of the FUBA model under various scenarios while also addressing the model's limitations and practicality.

4.1 | FUBA generalisability, applicability, and scalability

The FUBA is applicable under any weather conditions, as FUBA attempts to adapt its operating parameters according to the surrounding operating environment, which includes the incorporation of fuzzy variables of humidity, namely, Low, Medium, and Large. This adaptability ensures that FUBA's trust assessment remains relevant and effective across various environmental circumstances. Furthermore, the concept of integrating environmental parameters into trust management can be adapted to various contexts, such as agricultural robotics, environmental monitoring, border surveillance, and disaster response. On the other hand, the principles of

TABLE 1 Weight parameters.

Direct trust	α	β	Final trust
Bad/good	1	0	Final Trust(i) = direct trust(i)
Medium	0.5	0.5	Final Trust(i) = 0.5 direct trust(i) + 0.5 indirect trust(i)j

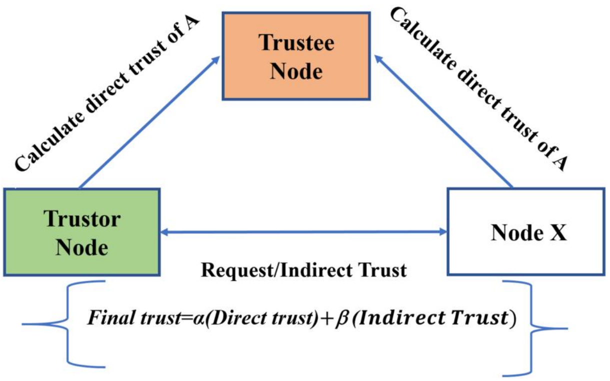

Trustee Node
Calculate direct trust of A
Calculate direct trust of A
Trustor Node
Node X
Request/Indirect Trust
Final trust=α(Direct trust)+β(Indirect Trust)

FIGURE 5 Trust aggregation.

behaviour analysis that incorporate environmental parameters could inspire diverse autonomous systems that face complex external conditions, such as wildlife monitoring, pollution detection, and habitat preservation. Finally, ethical considerations related to environmental data collection and the broader social implications of integrating natural parameters into autonomous systems such as airspace congestion, urban environments, or emergency response situations are required.

To tackle FUBA's scalability, every drone in the network evaluates the trustworthiness of its adjacent drones and subsequently relays this information to the ground control station to facilitate decision-making. This approach efficiently restricts the dissemination of trust data and evenly distributes the computational load, enabling the deployment of scalable FUBA. Thus, the scalability of the proposed FUBA model is evident in its ability to accommodate a growing number of drones.

4.2 | FUBA practicality and feasibility

Utilising FUBA in practical settings holds promise in addressing the increasing security challenges associated with drone-related threats. Fuzzy logic can be a valuable tool for identifying and responding to malicious drones, which can be used for unauthorised surveillance, smuggling, or even acts of terrorism. In what follows, we explore the implementation process of the FUBA model and its practical implications in identifying malicious drones.

- The proposed FUBA can identify anomalies in drone behaviour by comparing the detected drone's actions to predefined models of normal drone behaviour. If a drone's actions deviate significantly from the expected behaviour, the system can raise an alert and initiate appropriate response measures.
- FUBA can incorporate contextual information, such as local regulations, flight restrictions, and historical data, to make more accurate decisions about the legitimacy of a drone's presence. This ensures that harmless drones, such as hobbyists or commercial drones, are not mistakenly flagged as malicious.
- FUBA model can continuously learn from new data and adjust its rules and inference mechanisms to adapt to evolving tactics used by malicious drones.
- FUBA system can be integrated with existing aviation and security infrastructure, such as air traffic control systems, airport security, and critical infrastructure protection, to improve overall airspace security.
- FUBA can provide real-time monitoring and reporting of drone activities, helping security personnel make timely and informed decisions to mitigate potential threats.

4.3 | FUBA practical limitations

While FUBA demonstrates effective trust management in FANET under poor weather conditions, the proposed approach has the following main limitations:

- As the number of rules and fuzzy sets increases to model a large problem space, fuzzy rule bases can become very complex and difficult to manage. This affects issues such as debugging, updating, and interpretability.
- Fuzzy systems are only as good as the input features they are provided. Critical security features may be missing or noisy, limiting detection capabilities. Furthermore, security considerations around trust data exchange must be incorporated into a full system deployment.

In summary, the proposed model offers a practical and effective approach to improving security in the real world. By leveraging its ability to handle uncertain and imprecise data, the FUBA model can contribute to the development of robust and adaptive systems that safeguard against the misuse of drones for malicious purposes.

5 | IMPLEMENTATION DETAILS OF THE FUBA MODEL

Fuzzy logic is a computational approach that handles uncertain information by allowing for degrees of truth rather than rigid binary values. This section uses MATLAB to evaluate the proposed FUBA model. The fuzzy logic used to evaluate node behaviour comprises three steps: fuzzification, inference engine, and defuzzification.

5.1 | Step 1: Fuzzification

In this step, a membership function is generated to determine the degree to which the numerical data correspond to a linguistic variable, using triangular and trapezoidal functions presented in Figures 6 and 7. Typically, a triangular membership function is defined using three parameters, namely, a, b, and c, as follows:

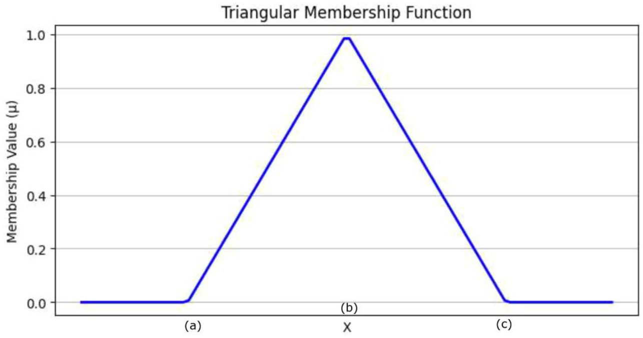


FIGURE 6 Triangular membership function.

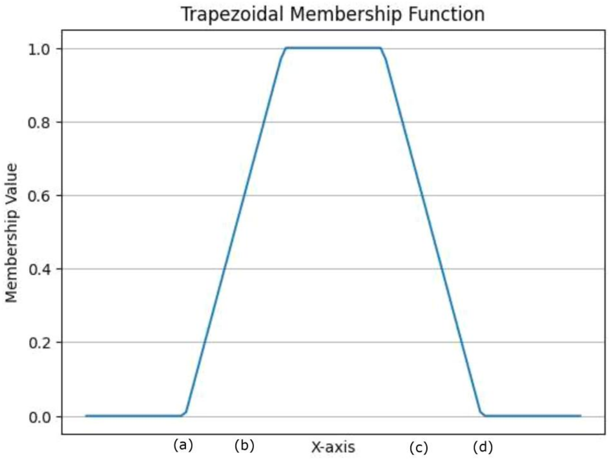


FIGURE 7 Trapezoidal membership function.

$$f(x,a,b,c) = \left\{ \begin{array}{cc} 0 & x \le a \\ \dfrac{x-a}{b-a} & a \le x \le b \\ \dfrac{c-x}{c-b} & b \le x \le c \\ 0 & c \le x \end{array} \right\} \tag{4}$$

The expression given in Equation (4) can be written in a simple form using min and max functions as follows:

$$F(x,a,b,c) = \max\left(\min\left(\frac{x-a}{b-a}\right), \left(\frac{c-x}{c-b}\right), 0\right) \tag{5}$$

$$F(x,a,b,c,d) = \max\left(\min\left(\frac{x-a}{b-a}\right), 1, \left(\frac{d-x}{d-c}\right), 0\right) \tag{6}$$

Figure 8a illustrates the membership functions of Energy: A triangular membership function for the linguistic variable *Medium* is defined by the triangle (*x*, 0.2, 0.35, 0.5). The trapezoidal membership function for the linguistic variable *High* is defined by the trapezoid (*x*, 0.5, 0.85, 1, *d*).

As shown in Figure 8a, the fuzzy variables of the energy are *VeryLow*, *Medium*, and *High* and are analysed from 0 to 1. Figure 8b shows the fuzzy variables for the packet delivery ratio, which are *Low*, *Medium*, and *High*, analysed from 0 to 1. Figure 8c shows that the fuzzy variables of the signal power are *Poor*, *Good*, and *Excellent*. They are analysed from −100 to −10 dBm. Figure 8d shows the fuzzy variables of the transmission delay: *Small*, *Medium*, and *Large*. They are analysed from 0.6 to 2.4 ms. In Figure 8e, the fuzzy variables of humidity (*Low*, *Medium*, and *Large*) are analysed from 0 to 1. Figure 8f illustrates the output trust fuzzy variables that are *Bad*, *Medium*, and *Good* and are analysed from 0 to 100.

5.2 | Step 2: The inference engine

In this step, all the rules need to be defined in the proposed fuzzy logic model and then explain those that reflect realistic situations:

The first rule illustrates the worst-case scenario. While the second rule represents the best case. The third rule requires the system to consider the node as trustworthy due to its low battery, implying that unintentional misbehaviour is considered.

Rules 4 through 7 state that if all variables have low values except for one that has a positive value. Then, the node is considered untrustworthy with a bad trust value.

Rule 8 requires the system to consider the node as trustworthy because it has a weak RSSI due to the high humidity. This implies that the system takes into account unfavourable weather conditions. Table 2 illustrates the rules when humidity is low, while Table 3 shows the rules when humidity is high.

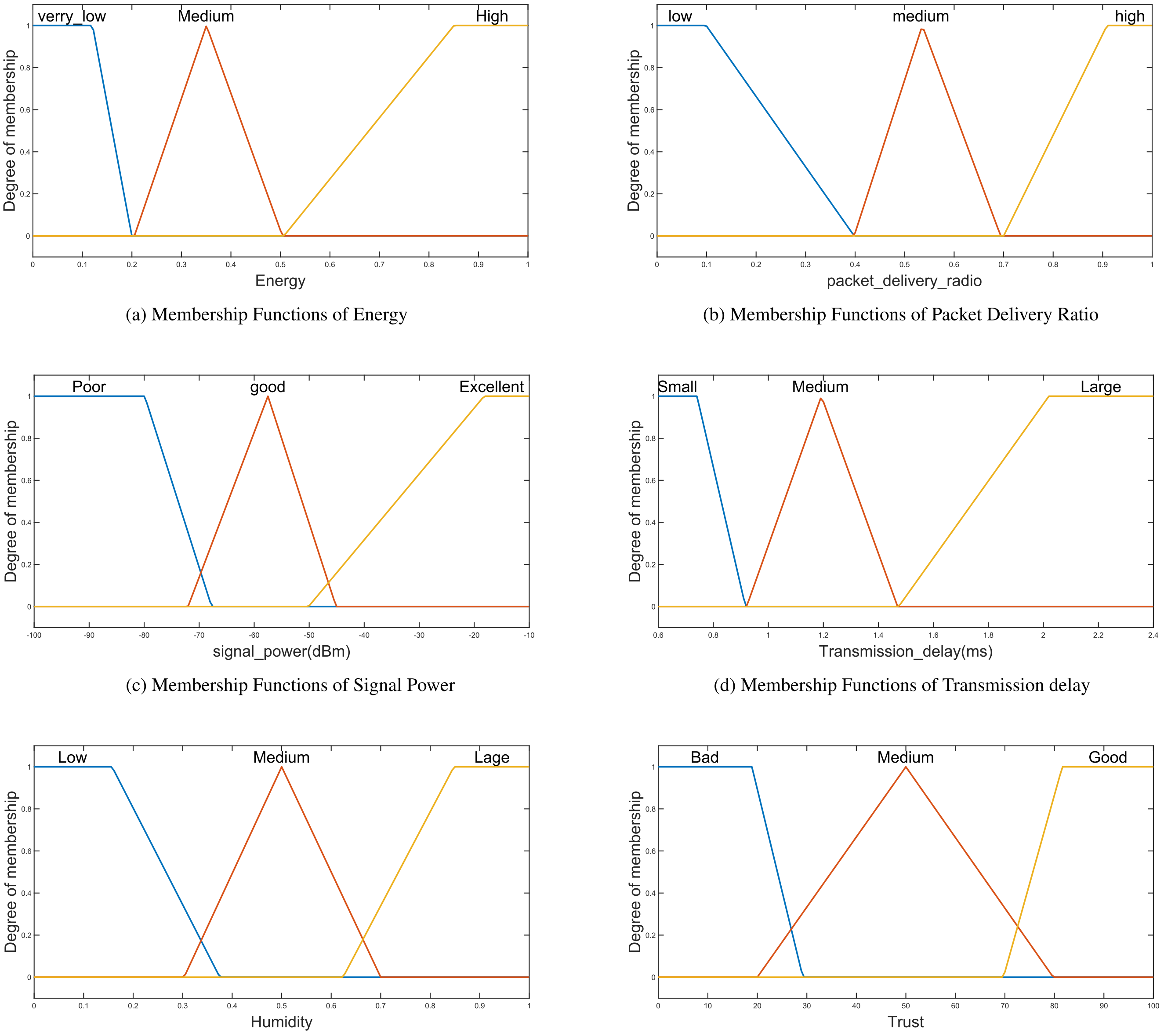
5.3 | Step 3: Defuzzification

Defuzzification is the pivotal stage within the fuzzy logic process, where the crisp output is derived from the fuzzy output generated by the fuzzy inference engine. This involves translating the fuzzy set or linguistic term (*Bad*, *Medium*, and *Good*) into a single, definite value that can be understood and utilised for drone behaviour evaluation. Various methods, such as centre of gravity, bisector, and maxima, can be employed for defuzzification to convert the fuzzy output into a clear and actionable result [27]. In the proposed model, the centroid method (COG) is considered, which is the most widely used technique and is depicted in Figure 9.

This method involves determining the centre of gravity of the obtained polygon:

$$CG = \frac{\sum_x^b = af(x) \times x}{\sum_x^b = af(x)} \tag{7}$$

where *f*(*x*) represents the aggregation of the membership functions while *a* and *b* represent the bounds of the obtained polygon.



(a) Membership Functions of Energy

(b) Membership Functions of Packet Delivery Ratio

(c) Membership Functions of Signal Power

(d) Membership Functions of Transmission delay

(e) Membership Functions of Humidity

(f) Membership Functions of Trust Score

FIGURE 8 Membership functions of the different parameters.

TABLE 2 Fuzzy rules with low humidity.

R	RSSI	PDR	Energy	TD	Output
1	Poor	Low	Very low	Large	Bad
2	Excellent	High	High	Small	Good
3	Excellent	High	Very low	Small	Good
4	Excellent	Low	Very low	Large	Bad
5	Poor	Large	Very low	Large	Bad
6	Poor	Low	High	Large	Bad
7	Poor	Low	Very low	Small	Bad

This method calculates the output by determining the abscissa of the centroid located beneath the curve's surface. The selection of the defuzzification method exerts a significant impact on the final result of the fuzzy logic model. The centre of gravity method is more flexible, as it considers the entire fuzzy output (trust) to calculate the trust result.

The functions that determine the membership of the input and output parameters must be adjusted for each iteration of the fuzzy rule base [28]. The cut-off method is depicted in Figure 10.

6 | IMPACT OF RSSI AND HUMIDITY ON TRUST RESULT

In this section, MATLAB programs are used to evaluate the performance of the proposed FUBA model. The fuzzy logic application is used for evaluating and understanding the node behaviour under the impact of bad weather conditions and poor signal strength (RSSI).

6.1 | Impact of RSSI on trust result

The bar chart in Figure 11 illustrates the trust result of 8 nodes in the network under high and low RSSI while varying the other parameters (TD, Energy, PDR) to obtain several trust values: *high*, *medium*, and *low*. The trust value dropped from 87% to 50% in nodes 1 and 3; the trust value decreased from 52% to 12% in nodes 4, 6, and 7. This figure shows that the trust level in nodes 2, 5, and 8 remained constant. However, the proportion of trust increases significantly when the RSSI is excellent. There are several possible explanations for this result, but it is essential to note that signal power (RSSI) plays a vital role in assessing drone performance in FANET. It can be concluded that trust values decrease when signal power decreases due to high humidity. Consequently, it is advisable to eliminate the node from the network to enhance network security.

TABLE 3 Fuzzy rules with high humidity.

R	RSSI	PDR	Energy	TD	Output
1	Poor	Low	Very low	Large	Bad
2	Excellent	High	High	Small	Good
3	Excellent	High	Very low	Small	Good
4	Excellent	Low	Very low	Large	Bad
5	Poor	Large	Very low	Large	Bad
6	Poor	Low	High	Large	Bad
7	Poor	Low	Very low	Small	Bad
8	Poor	High	High	Small	Good

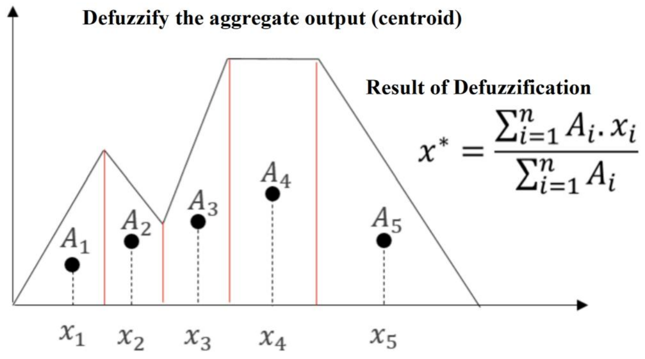

Defuzzify the aggregate output (centroid)
Result of Defuzzification
$x^* = \frac{\sum_{i=1}^{n} A_i . x_i}{\sum_{i=1}^{n} A_i}$
A_1
A_2
A_3
A_4
A_5
x_1
x_2
x_3
x_4
x_5

FIGURE 9 COG method.

6.2 | Impacts of humidity on trust result

Figure 12 illustrates the trust result for a network with 16 drones under high and low humidity while varying the other parameters (TD, Energy, PDR, RSSI) to obtain *high*, *medium*, and *low* trust values. The trust value reduced from 87.6% to 50.6% in node 9 and from 51.2% to 12.6% in node 12, then the trust values for the remaining nodes remained constant.

The most notable conclusion that can be drawn from Figure 12 is that the humidity significantly impacts the trust results in FANET. For this reason, climate change should be considered when designing a trust management system in FANET.

7 | EXPERIMENTAL RESULT AND DISCUSSION

7.1 | Simulation setup

The effectiveness of the newly introduced FUBA system is assessed through the following communication frameworks:

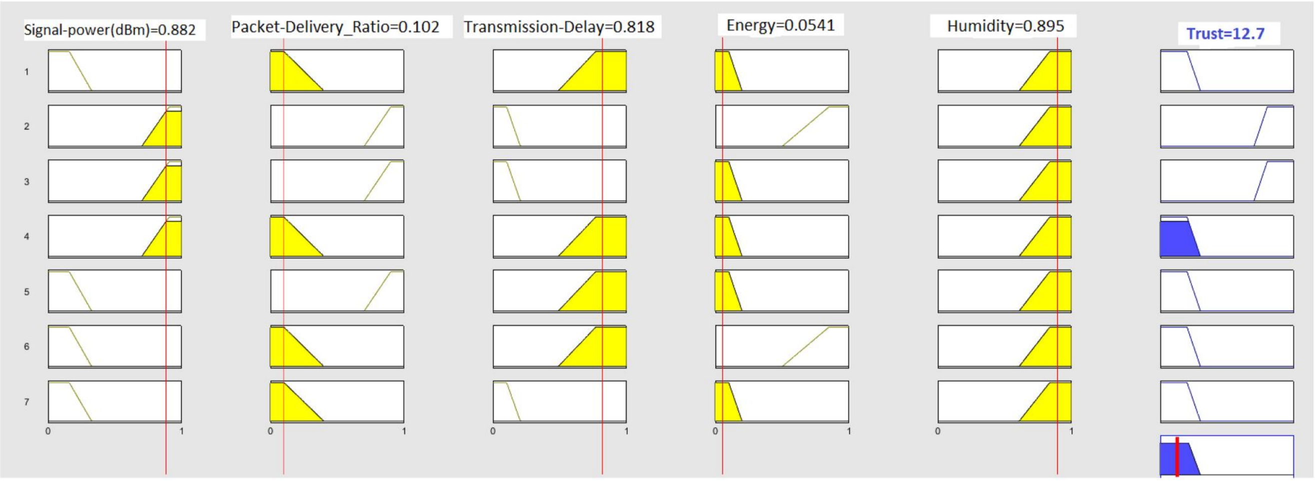


FIGURE 10 Cut-off method to combine the rules.

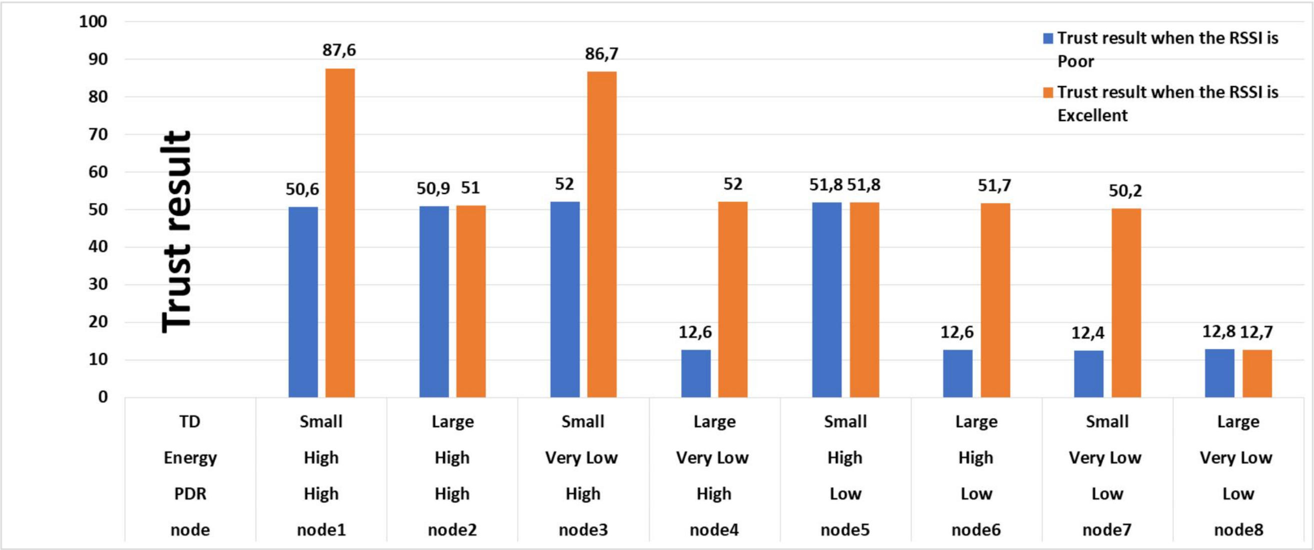


FIGURE 11 The impact of RSSI on trust result.

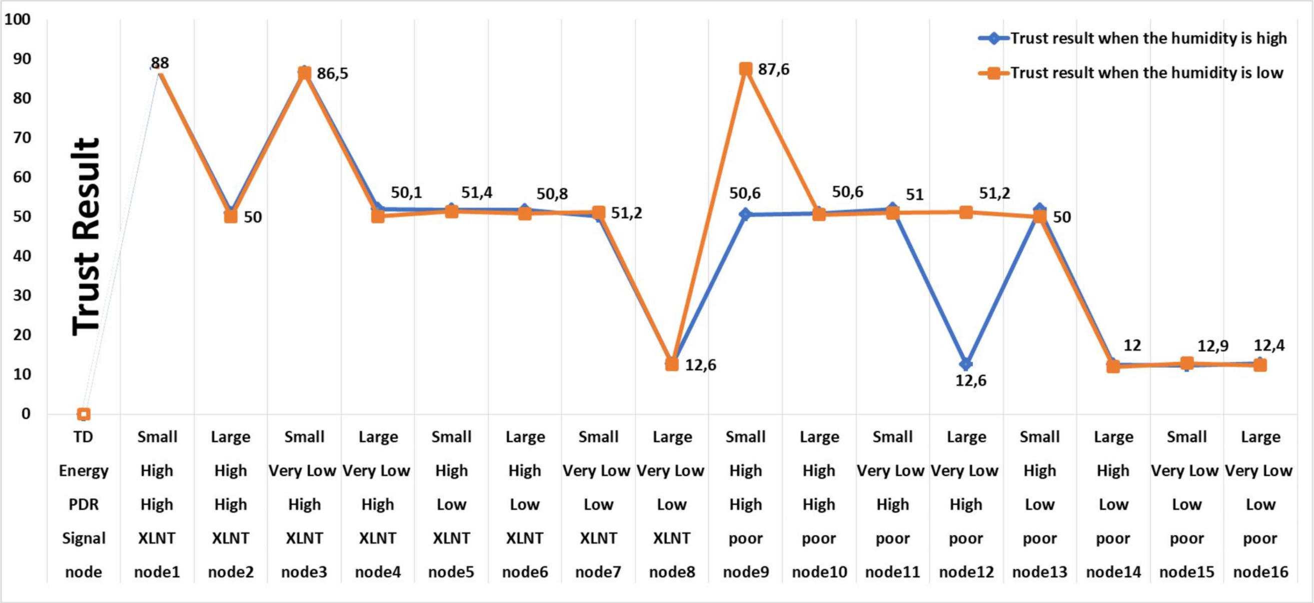


FIGURE 12 The impact of humidity on trust results.

- **OMNeT++**: It is a powerful simulation library and framework designed for building and testing complex communication networks. It is built using C++ and is highly extensible, modular, and component-based, making it a popular choice for researchers and engineers in the field [29].
- **INET Framework**: The INET Framework is integrated with OMNeT++ and provides a rich set of network models and protocols, facilitating realistic simulations of communication scenarios [30].
- **AVENS (Aerial Vehicle Network Simulator):** AVENS is designed primarily to establish a simulation testing environment that is specifically designed to conduct virtual experiments focused on evaluating the network coverage and interconnectivity of UAVs engaged in collaborative flights or coexisting within the same airspace. The integration strategy for AVENS revolves around incorporating both the XPlane Flight Simulator and the OMNeT++ network simulator [31].
- **XPlane Flight Simulator:** The XPlane Flight Simulator significantly contributes to the authenticity of the simulations by enabling the modelling of real-world flight dynamics and interactions among UAVs [32].

The simulated network uses the IEEE 802.11 communication protocol for wireless interactions among UAVs. The network area is defined as a space of 2500 m × 2500 m, accurately reflecting real-world operational conditions. To ensure a comprehensive evaluation, the simulation time is set to 3000 s, enabling observation of network behaviour and performance over an extended duration. The simulations are executed on a 64-bit PC running Windows 10. This platform offers the necessary computational resources to conduct simulations, thus effectively ensuring reliable and precise results. Table 4 summarises the different simulation parameters used in the simulation experiments.

In the simulation experiment, a scenario is designed to emulate a UAV communication network with the proposed FUBA system. The scenario initiates with 10 UAVs and a ground control station. The UAVs collaborate to share a wireless communication medium within the AVENS simulation framework. During the simulation, UAVs exchange messages and collect critical network parameters, including transmission delay, received signal strength indicator (RSSI), packet delivery ratio, and node energy. To assess scalability and performance, the number of UAVs is systematically increased from 10 to 200 in steps. The increments are chosen to comprehensively understand the proposed method's behaviour across a wide range of UAV quantities. In OMNET ++, the recording module is configured to track end-to-end delay across the network by specifying the appropriate recording intervals and enabling scalar data collection.

TABLE 4 Simulation parameters.

Simulation tools	OMNET++, Avens, Xplane10
Simulation area	2500 m × 2500 m
Node counts	10–200
Ping-transmission interval	10 s
Ping-sleep period	10 s
UDP-transmission interval	10 ms
UDP-packet size	1000 B
UDP application type name	UdP video stream SVR
UDP application video size	10 MIB
MAC address assignment	Auto
Ip process delay	10 µs
Mac Queue size	14
WLAN data rate	2 MIB
Transmission frequency	2400 Hz
Physical Tx power	100 mW
Power generation	100 MW
Simple energy storage	0.05 J
Energy generator sleep interval	Exponential (10 s)
Mobility model	Random way-point
Ground control station mobility	Stationary mobility
Mobility update rate	2 s
Wireless standard	IEEE 802.11
Simulation time	3000 s
Operating platform	64-bit Windows 10

7.2 | Simulation results

To assess the performance of FUBA, the well-established FNDN [10] and UNION [8] models are utilised as reference points. These models provide a baseline for comparison based on their inherent characteristics. Specifically, the conducted simulations focus on two key parameters: false positive rate and end-to-end delay. The false positive rate quantifies instances where the system incorrectly identifies trustworthy nodes as untrustworthy [33]. In the context of the simulation experiments, several instances of false positives relate to situations in which the FUBA system erroneously categorises a drone as a regular node despite not meeting the criteria for such classification. Furthermore, the end-to-end delay is analysed, which reflects the time taken for the data to travel from the source to the destination node in the network [34]. In the context of the conducted simulations, the end-to-end delay could be measured as the time it takes for a message or packet to be transmitted from one UAV (source) to another UAV or the ground control station (destination). It can be a critical metric for assessing real-time communication performance.

The FNDN [10] is a recent monitor-based communication architecture that uses both direct and indirect trusts for Flying Named Data Networking. Nevertheless, the UNION [8] model considers the UAV energy, mobility patterns, and enqueued packets while employing both direct and indirect trust to assess node behaviour. Comparing the proposed trust model with these two trust models is an essential step in evaluating FUBA's effectiveness and practicality.

Based on Figure 13, it can be observed that the proposed FUBA model has a significant impact on reducing the average end-to-end delay of data packets in comparison to the UNION model in high-density scenarios. Specifically, when there are 50 drones, the FUBA model reduces the delay by more than 1.4 s, unlike UNION, and in large-density scenarios with 100 drones, the enhancement is roughly 1.1 s. When the number of nodes exceeds 150, the mean end-to-end delay for FNDN and the proposed solution is nearly the same. The figure shows that the proposed FUBA model consistently results in the lowest end-to-end delay across the three models.

The false positive ratio for FUBA, FNDN and UNION as a function of the density of the UAV is shown in Figure 14. The false positive can be obtained by calculating the trusted node using the FUZZY logic application if a node (i) is not compromised. The graph curves show that for both FNDN and UNION, the calculated false positive steadily increases; however, at the beginning of the simulation experiments, no false positive instances were generated during this process.

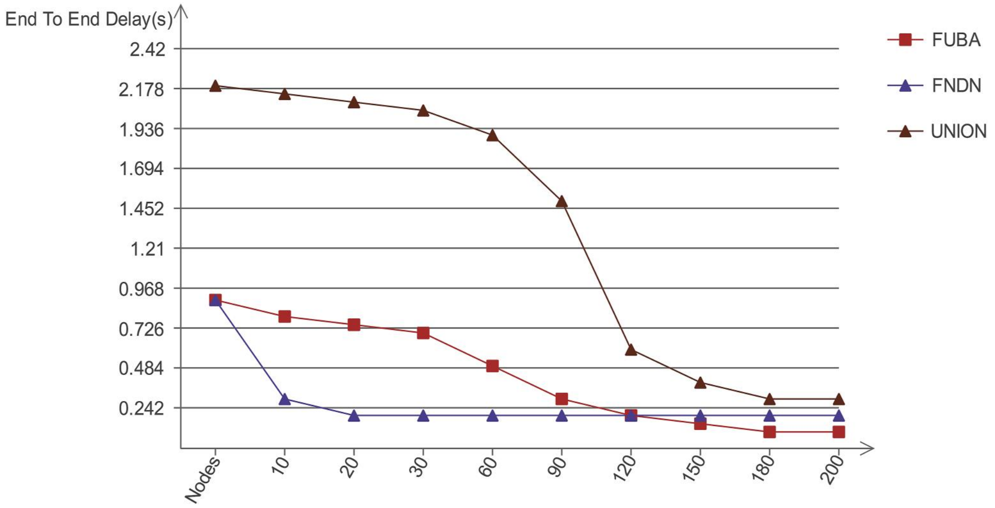


FIGURE 13 The average end-to-end delay versus the number of nodes.

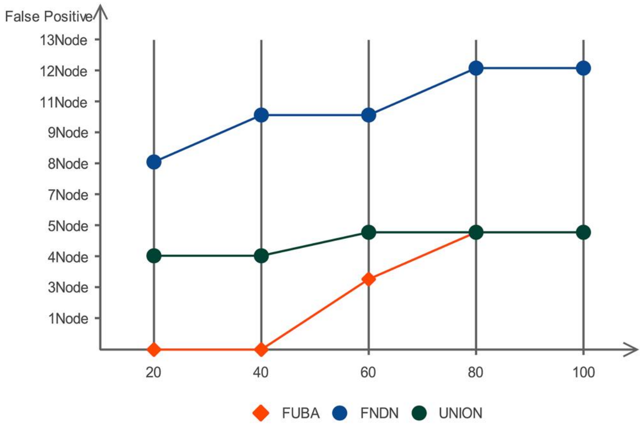


FIGURE 14 Number of false positives compared to FNDN and UNION.

Therefore, comparing the proposed model with FNDN and UNION, the proposed solution has a lower error ratio.

8 | CONCLUSIONS AND FUTURE WORK

Trust management is an effective method of detecting insider threats. The main challenge in this domain is designing a conceptual and analytical trust model for FANET that can evaluate and understand the behaviour of nodes. In the context of this article, FUBA, a Fuzzy-based UAV behaviour analytics for trust management based on direct and indirect information was introduced. Contrary to previous models, the proposed model increases the trustworthiness of the network in bad weather conditions and poor signal strength (RSSI). Furthermore, FUBA has the ability to effectively distinguish between legitimate drone actions and malicious ones. In future work, it would be valuable to incorporate machine learning (ML) and blockchain technology to enhance FUBA's capabilities. Automated tuning of the fuzzy logic rules and membership functions via machine learning may improve performance across diverse operating environments. Future research could explore more sophisticated algorithms, such as deep learning and reinforcement learning, to extract deeper insights from complex FANET data. Furthermore, federated learning presents an exciting opportunity for FANETs, where data privacy is of paramount importance. On the other hand, blockchain-based distributed ledgers could secure the sharing of trust data while providing resilience against compromised nodes. Furthermore, it can facilitate transparent and auditable trust records, reducing the reliance on centralised authorities. As these technologies continue to evolve, their integration offers the potential to create more resilient, secure, and efficient FANETs, shaping the future of aerial communication and navigation.

AUTHOR CONTRIBUTIONS

Sihem Benfriha: Conceptualization; data curation; formal analysis; investigation; methodology; project administration; resources; software; validation; visualization; writing – original draft; writing – review & editing. **Nabila Labraoui**: Conceptualization; formal analysis; investigation; project administration; supervision; validation; writing – original draft; writing – review & editing. **Radjaa Bensaid**: Formal analysis; methodology; resources. **Haythem Bany Salameh**: Formal analysis; funding acquisition; investigation; writing – review & editing. **Hafida Saidi**: Formal analysis; writing – review & editing.

CONFLICT OF INTEREST STATEMENT

We have no conflict of interest with anyone on the IET Networks Journal staff. We state that the paper is original and will not be submitted elsewhere until a decision is made by the IET Networks Journal.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

ORCID

Sihem Benfriha https://orcid.org/0000-0002-4669-6053

REFERENCES

1. Saidi, H., et al.: DSMAC: privacy-aware decentralized self-management of data access control based on blockchain for health data. IEEE Access. 10, 101011–101028 (2022). https://doi.org/10.1109/access.2022.3207803
2. Fang, Z., et al.: Age of information in energy harvesting aided massive multiple access networks. IEEE J. Sel. Area. Commun. 40(5), 1441–1456 (2022). https://doi.org/10.1109/jsac.2022.3143252
3. Benfriha, S., Labraoui, N.: Insiders detection in the uncertain IoD using fuzzy logic. In: Proceedings of the International Conference on Information Technology (ACIT), pp. 1–6. IEEE (2022)
4. Fotouhi, A., et al.: Survey on UAV cellular communications: practical aspects, standardization advancements, regulation, and security challenges. IEEE Commun. Surv. Tutorial. 21(4), 3417–3442 (2019). https://doi.org/10.1109/comst.2019.2906228
5. Yuan, F., et al.: Insider threat detection with deep neural network. In: Proceedings of the International Conference in Computational Science–ICCS 2018, Wuxi, China, June 11–13, Part I 18, pp. 43–54. Springer International Publishing (2018)
6. Labraoui, N., Gueroui, M., Sekhri, L.: A risk-aware reputation-based trust management in wireless sensor networks. Wireless Pers. Commun. 87(3), 1037–1055 (2016). https://doi.org/10.1007/s11277-015-2636-3
7. Wu, G., et al.: A fuzzy-based trust management in WSNs. J. Internet Serv. Inf. Secur. 3(3/4), 124–135 (2013)
8. Barka, E., et al.: UNION: a trust model distinguishing intentional and UNIntentional misbehavior in inter-UAV communication. J. Adv. Transport. 2018, 1–12 (2018). https://doi.org/10.1155/2018/7475357
9. Kerrache, C.A., et al.: September. Reputation-aware energy-efficient solution for FANET monitoring. In: Proceedings of the International Conference on IFIP Wireless and Mobile Networking Conference (WMNC), pp. 1–6. IEEE (2017)
10. Barka, E., et al.: A trusted lightweight communication strategy for flying named data networking. Sensors. 18(8), 2683 (2018). https://doi.org/10.3390/s18082683
11. Barka, E., et al.: Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure. Trans. Emerg. Telecommun. Technol. 33(8), e3706 (2022). https://doi.org/10.1002/ett.3706
12. Singh, K., Verma, A.K.: A fuzzy-based trust model for flying ad hoc networks (FANETs). Int. J. Commun. Syst. 31(6), e3517 (2018). https://doi.org/10.1002/dac.3517
13. Singh, K., Verma, A.K.: A trust model for effective cooperation in flying ad hoc networks using genetic algorithm. In: Proceedings of Interantional Conference Communication and Signal Processing (ICCSP), pp. 491–495. IEEE (2018)
14. Singh, K. and Verma, A.K.: TBCS: a trust-based clustering scheme for secure communication in flying ad-hoc networks. Wireless Pers. Commun., 202(4), 3173–3196 (2020). https://doi.org/10.1007/s11277-020-07523-8
15. Zhou, J., Wang, Z.: Security clustering algorithm based on integrated trust value for unmanned aerial vehicles network. KSII Trans. Internet Inf. Syst. (TIIS). 14(4), 1773–1795 (2020)
16. Jena, K.K., et al.: A trust based false message detection model for multi-unmanned aerial vehicle network. In: Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 324–329. IEEE (2019)
17. Bhargava, A., Verma, S.: Kate: Kalman trust estimator for internet of drones. Comput. Commun. 160, 388–401 (2020). https://doi.org/10.1016/j.comcom.2020.04.027
18. DeMelo, C.F., et al.: UAVouch: a secure identity and location validation scheme for UAV networks. IEEE Access. 9, 82930–82946 (2021). https://doi.org/10.1109/access.2021.3087084
19. Chen, Y., Yang, J.: Defending against identity-based attacks in wireless networks. In: Handbook on Securing Cyber-Physical Critical Infrastructure, pp. 191–222. Elsevier Inc (2012)
20. Singh, K., Verma, A.K.: FCTM: a novel fuzzy classification trust model for enhancing reliability in flying ad hoc networks (FANETs). Ad Hoc Sens. Wirel. Networks. 40(1-2), 23–47 (2018)
21. Ji, Y., et al.: Efficiency-boosting federated learning in wireless networks: a long-term perspective. IEEE Trans. Veh. Technol. 72(7), 9434–9447 (2023). https://doi.org/10.1109/tvt.2023.3250273
22. Ayass, T., et al.: Unmanned aerial vehicle with handover management fuzzy system for 5G networks: challenges and perspectives. Intell. Robot. 2(1), 20–36 (2022). https://doi.org/10.20517/ir.2021.07
23. Khan, M.K.U., Ramesh, K.S.: Effect on packet delivery ratio (PDR) & throughput in wireless sensor networks due to black hole attack. Int. J. Innov. Technol. Explor. Eng. 8(12S), 428–432 (2019)
24. Wang, J., et al.: Starling flocks-inspired resource allocation for ISAC-aided green ad hoc networks. IEEE Trans. Green Commun. Netw. 7(1), 444–454 (2023). https://doi.org/10.1109/tgcn.2023.3234165
25. Bri, D., et al.: Performance analysis of weather's impact on outdoor IEEE 802.11 b/g links using network management parameters. Mobile Network. Appl. 21(4), 603–619 (2016). https://doi.org/10.1007/s11036-016-0758-9
26. Kurt, S., Tavli, B.: Path-loss modeling for wireless sensor networks: a review of models and comparative evaluations. IEEE Antenn. Propag. Mag. 59(1), 18–37 (2017). https://doi.org/10.1109/map.2016.2630035
27. Rao, D.H., Saraf, S.S.: Study of defuzzification methods of fuzzy logic controller for speed control of a DC motor. In: Proceedings of the International Conference on Power Electronics, Drives and Energy Systems for Industrial Growth, Vol. 2, pp. 782–787. IEEE (1996)
28. Thangaraj, K., Dharma, D.: Optimized fuzzy system dependent trust score for mobile AdHoc network. Wireless Pers. Commun. 117(4), 3255–3269 (2021). https://doi.org/10.1007/s11277-020-07984-x
29. Gill, J.S., et al.: Simulation testbeds and frameworks for UAV performance evaluation. In: Proceedings of the International Conference on Electro Information Technology (IT), pp. 335–341. IEEE (2021)
30. Virdis, A., Kirsche, M.: Recent advances in network simulation. EAI/Springer Innovations in Communication and Computing (2019)
31. Marconato, E.A., et al.: Avens-a Novel Flying Ad Hoc Network Simulator with Automatic Code Generation for Unmanned Aircraft System (2017)
32. Garcia, R., Barnes, L.: Multi-UAV simulator utilizing X-plane. In: Selected Papers from the 2nd International Symposium on UAVs, Reno, Nevada, pp. 393–406. Springer Netherlands (2009–2010)
33. Marugán, A.P., Chacón, A.M., Márquez, F.P.: Reliability analysis of detecting false alarms that employ neural networks: a real case study on wind turbines. Reliab. Eng. Syst. Saf. 191, 106574 (2019). https://doi.org/10.1016/j.ress.2019.106574
34. Alaslani, M., Nawab, F., Shihada, B.: Blockchain in IoT systems: end-to-end delay evaluation. IEEE Internet Things J. 6(5), 8332–8344 (2019). https://doi.org/10.1109/jiot.2019.2917226

How to cite this article: Benfriha, S., et al.: FUBA: a fuzzy-based unmanned aerial vehicle behaviour analytics for trust management in flying ad-hoc networks. IET Netw. 1–13 (2023). https://doi.org/10.1049/ntw2.12108