Hindawi
Journal of Advanced Transportation
Volume 2018, Article ID 7475357, 12 pages
https://doi.org/10.1155/2018/7475357

Research Article

UNION: A Trust Model Distinguishing Intentional and Unintentional Misbehavior in Inter-UAV Communication

Ezedin Barka,[1] Chaker Abdelaziz Kerrache,[2,3] Nasreddine Lagraa,[2] Abderrahmane Lakas,[1] Carlos T. Calafate,[4] and Juan-Carlos Cano[4]

[1] *CIT, United Arab Emirates University, P.O. Box 17551, Al Ain, UAE*
[2] *LIM, University of Laghouat, BP 37G, route de Ghardaia, Laghouat, Algeria*
[3] *University of Ghardaia, Ghardaia, Algeria*
[4] *Department of Computer Engineering, Universitat Politècnica de València, Camino de Vera, S/N, 46022 València, Spain*

Correspondence should be addressed to Chaker Abdelaziz Kerrache; kr.abdelaziz@gmail.com

Received 9 December 2017; Revised 13 February 2018; Accepted 15 March 2018; Published 22 April 2018

Academic Editor: Nandana Rajatheva

Ensuring the desired level of security is an important issue in all communicating systems, and it becomes more challenging in wireless environments. Flying Ad Hoc Networks (FANETs) are an emerging type of mobile network that is built using energy-restricted devices. Hence, the communications interface used and that computation complexity are additional factors to consider when designing secure protocols for these networks. In the literature, various solutions have been proposed to ensure secure and reliable internode communications, and these FANET nodes are known as Unmanned Aerial Vehicles (UAVs). In general, these UAVs are often detected as malicious due to an unintentional misbehavior related to the physical features of the UAVs, the communication mediums, or the network interface. In this paper, we propose a new context-aware trust-based solution to distinguish between intentional and unintentional UAV misbehavior. The main goal is to minimize the generated error ratio while meeting the desired security levels. Our proposal simultaneously establishes the inter-UAV trust and estimates the current context in terms of UAV energy, mobility pattern, and enqueued packets, in order to ensure full context awareness in the overall honesty evaluation. In addition, based on computed trust and context metrics, we also propose a new inter-UAV packet delivery strategy. Simulations conducted using NS2.35 evidence the efficiency of our proposal, called *UNION*, at ensuring high detection ratios > 87% and high accuracy with reduced end-to-end delay, clearly outperforming previous proposals known as *RPM*, *T-CLAIDS*, and *CATrust*.

1. Introduction

Various applications emerged with the introduction of Flying Ad Hoc Networks (FANETs), including shipment of goods, home package delivery, crop monitoring, agricultural surveillance, and rescue operations [1]. Unlike traditional Mobile Ad Hoc Networks, FANET applications are generally unicast-based mainly due to energy restrictions [2].

FANETs nodes are Unmanned Aerial Vehicles (UAVs) that collaborate with each other in ad hoc mode through a Line-of-Sight (LoS) link to exchange data packets. However, they can also communicate with fixed ground stations, with an air traffic controller, or through a Non-Line-of-Sight (NLoS) link with a satellite-aided controller (see Figure 1). The problems involved in these communications are mostly related to packet loss because of both the lack of security and the unreliability of wireless communication links [3].

Many solutions have been proposed to secure inter-UAV communications. They are mostly targeting the different security services, including authentication and access control [4], data integrity and availability [5], and privacy [6]. Unlike the proposed solutions for other security services, availability insurance solutions suffer from the high error ratios in the detection process, as they do not differentiate between intentional and unintentional dishonesty of nodes.

Furthermore, the attacks against service availability are generally related to packet drops and Denial of Service (DoS). Both kinds of attacks can be faced using either cryptographic

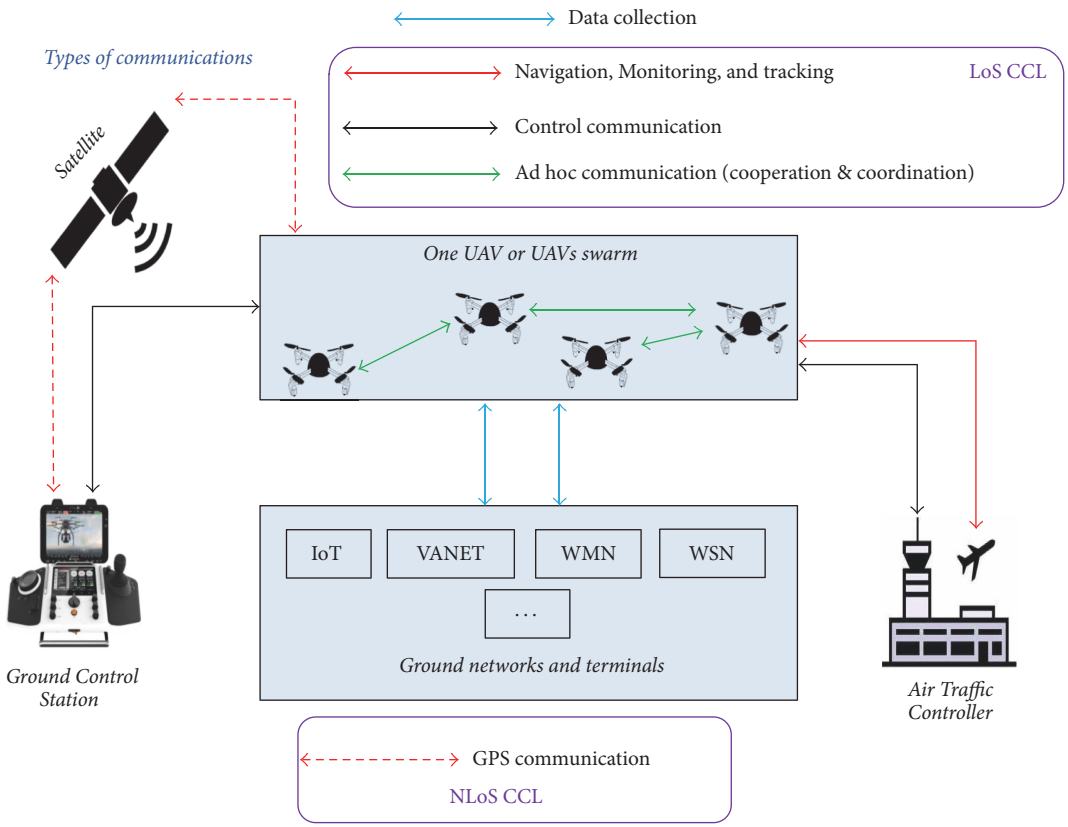

Figure 1: Communication types.

techniques [7] or trust management techniques [8]. Cryptographic techniques are the best solution against outsider unauthorized entities, but these techniques are known to require high computation overhead and consume much energy, becoming a problem for current commercial UAVs [9]. On the other hand, trust management, which is an alternative security approach dealing with insider authenticated attackers, introduces less computation and energy requirements than cryptography [10], thus being considered a more appropriate option.

In this paper, we propose a new context-aware trust-based solution called *UNION* to distinguish between intentional and unintentional dishonesty in FANETs. Our proposal establishes trust among the different UAVs, while simultaneously measuring the network and energy conditions of neighboring UAVs. Thus, if an UAV has insufficient memory, battery, or a bad communication link, thus being mostly unable to properly receive/forward packets, it will not see its trust levels decrease, and any packet drops will be considered as unintentional misbehavior (see Figure 2). Moreover, *UNION* also uses the computed trust and context-related metrics to ensure an efficient inter-UAV packet delivery.

The rest of the paper is organized as follows: in the following section, we present an overview of the main attacks that can be launched against inter-UAV communication, together with the network-related packet loss reasons. Furthermore, this section also provides a summary of the cryptography-based and trust-based inter-UAV communications. Afterwards, we detail our proposal in Section 3 and propose a new trust-based context-aware inter-UAV packet delivery strategy in Section 4. In Section 5, we present the simulation setup and discuss the obtained results compared to three existing works. Finally, Section 6 provides some concluding remarks and discusses the possible research directions.

2. Background and Related Works

Existing commercial UAVs are vulnerable to several basic security attacks, which may clearly cause inter-UAV network disruption in the context of FANETs. In fact, similarly to all Mobile Ad Hoc Networks, different kind of attacks can be launched against FANETs, including the following:

(i) *Replay attack*: in this attack, the dishonest UAV records the routing messages of legitimate nodes and resends these messages at later times, thereby building suboptimal routes or causing route loops.

(ii) *Position-based replay*: same as the previous attack, the dishonest UAV records the routing messages of legitimate nodes and resends them to another location, again building suboptimal routes or causing route loops.

(iii) *Position-based replay and gray holes*: in this kind of attack, a pair of attackers, linked via a fast transmission path (tunnel), forward routing messages between two distant nodes, thus building a route that goes through the attacker that selectively drops packets.

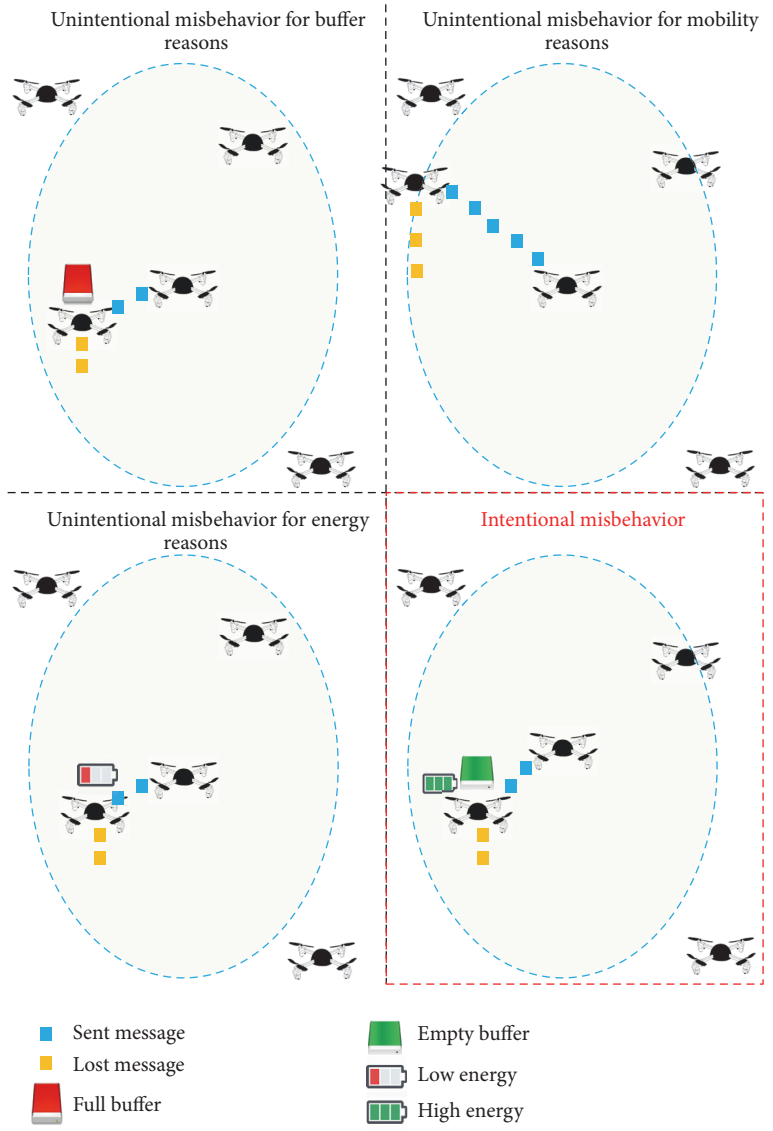

Figure 2: Intentional and unintentional misbehavior.

(iv) *Flooding*: it consists of the continuous broadcast of route requests towards nonexisting destinations, thus consuming network resources such as bandwidth.

(v) *Path diversion*: its main principle is forging routing messages generated by legitimate nodes (e.g., tampering the metric), thereby building suboptimal routes or causing route loops.

(vi) *IP impersonation*: in this case the attacker performs IP spoofing and, as a result, it can generate and propagate corrupted information on behalf of other nodes.

(vii) *Black hole*: this type of attacker does not collaborate on network operations, dropping all packets for both malicious and selfish reasons (e.g., battery saving).

The situations for which the existing security solutions do not distinguish between intentional and unintentional misbehavior are the ones related to the last category of packet dropping. This situation can occur for many reasons besides the intentional ones. Table 1 summarizes the main unintentional packet dropping reasons that an intermediate UAV may experience.

As we mentioned above, the existing security solutions do not distinguish between intentional and unintentional dishonesty. These solutions are generally classified into cryptography-based and trust-based solutions.

2.1. Main Existing Cryptography-Based Solutions. Existing security solutions for FANETs are generally falling under this category. We find that only a few ones have been specifically developed to establish trust in FANET environments.

In [11], the authors consider a game theoretic approach to avoid jamming attacks on the communications channel by computing optimal strategies within the scope of an UAV swarm. In their discussion, they have considered two

Table 1: Unintentional packet drop reasons.

Layer	Reasons
Physical layer	Signal attenuation/masking/fading/interference
	Signal reflection/diffraction/refraction
	Multipath
	Mobility
	Obstacles
	Bandwidth occupation
	...etc.
MAC layer	Collision
	Hidden-exposed station problem
	Near-far problem
	Mobility
	Energy
	Handover
	Clustering
	...etc.
Network layer	Mobility
	Queuing
	Network fragmentation/association
	ID (IP configuration)
	Time-To-Live
	Handover
	Clustering
	...etc.

approaches that are used to derive the necessary conditions to reach the saddle point strategies of the players.

In [12], a spatial secure group communication (SSGC) problem is introduced, and it deeply investigates an analytical framework for multiple UAVs. A distributed method is proposed to solve the problem, which analyzes the spatial group size, the upper bound for group members, and the stability. In particular, the communications range and the relative position are also investigated to form a closed group. The feasibility of this proposal is demonstrated with an application scenario. However, this proposal suffers from a huge communications overhead.

Different security threats for UAVs systems are analyzed, and a cybersecurity threat model has been proposed in [13]. A detailed security threat analysis is done which provides an edge to researchers, designers, and users by identifying vulnerabilities in UAVs systems, thereby helping to identify the most appropriate countermeasures.

In [7], the authors examined the cybersecurity issues associated with drone-assisted public safety networks where sensitive or critical information can be transmitted between networks. However, the authors did not propose any clear contribution.

In [14], the authors present a new secure routing protocol called SUAP (Secure UAV Ad Hoc Routing Protocol). The proposal ensures message authentication and provides detection and prevention of wormhole attacks. SUAP is a reactive protocol using public key cryptography, hash chains, and geographical leashes. However, the size of the exchanged authentication messages and the required computation power are the main drawbacks of this work.

Sharma and Kumar [15] presented an opportunistic network formation strategy using cross layer design applicable to FANETs. The service layer security of FANETs is used in the presented network model to provide parameterized input to a neural setup. The proposed design offers effective utilization of resources, high data delivery ratio, and efficient service coordination with lower delay to secure the service. Despite its efficiency for standard application services, the delay introduced by the neural network remains unacceptable when safety issues must be addressed.

2.2. Main Existing Trust-Based Solutions. Most of the existing trust-based solutions for FANETs were initially proposed for MANETs [16, 17] and VANETs [18, 19], where only a few ones are specific to FANETs.

In a previous work, we proposed a trust-based energy-efficient distributed monitoring technique for FANETs. In this proposal, UAVs trusting each other, and moving with similar mobility patterns, distribute monitoring tasks among themselves to save more energy. However, same as all the existing solutions, this solution does not distinguish between intentional and unintentional misbehavior [20].

In [8], the authors analyzed the requirements for efficient UAV communications, identifying the similarities and the differences between MANETs and UAV-based networks and protocols. They also discussed the various trust-based protocols and management schemes that can be used in UAV networks.

As we mentioned above, all the existing solutions from both categories are prone to suffer from the high packet loss ratios that are inherent to FANETs. To overcome these problems, in the following sections, we detail our proposal called *UNION*; it is able to sustain the desired security level while providing awareness of network conditions, thereby helping in minimizing the error ratios associated with detecting actual attacks.

3. UNION Details: Trust Computation and Unintentional Misbehavior Identification

To avoid signalling as malicious those UAVs who have unintentionally dropped some packet, our modular trust model illustrated in Figure 3 works as follows.

It first estimates the buffer occupation, energy, and mobility patterns of the UAVs and simultaneously computes the trust of these UAVs without considering the above three conditions. Afterward, if the system detects that any nearby UAVs have unintentionally dropped packets, it adds a trust correction factor α to the overall inter-UAV trust computation that we call $Trust(i, j)$, thus resulting in a final evaluation index called *HonestyIndex*. The latter is compared to a predefined detection threshold DTH bellow which UAVs are considered dishonest. Algorithm 1 summarizes this process.

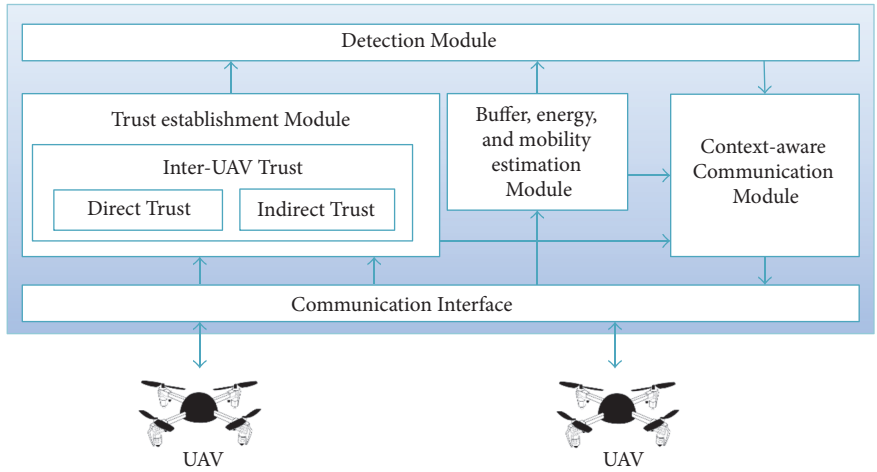

Figure 3: Proposed modular architecture.

(1) **if** ((*BufferDrop* = 1) And (*EnergyDrop* = 1) And (*MobilityDrob* > 0.5)) **then**
(2) $HonestyIndex_{(i,j)} \leftarrow Trust(i, j) + \alpha$;
(3) **else**
(4) $HonestyIndex_{(i,j)} \leftarrow Trust(i, j)$;
(5) **end if**
(6) **if** ($HonestyIndex_{(i,j)}$ < DTH) **then**
(7) $Blacklist_{(i,j)}$;
(8) **end if**

Algorithm 1: Distinguishing intentional and unintentional misbehavior.

Notice that the β factor can be dynamically adjusted using the UAVs residual energy, the duration of disconnection periods, or the buffer size.

In the following section, we first start by establishing the inter-UAV trust, and we then show how the context-related metrics are estimated.

3.1. UAV-to-UAV Trust Evaluation. Inter-UAV trust has two main metrics: (i) interaction-based trust ($DirectT^{t_x}_{(i,j)}$) and (ii) recommendation-based trust ($IndirectT^{t_x}_{(i,j)}$) in a specific time period t_x. Every UAV continuously monitors the network to evaluate the honesty of nearby UAVs. The overall trust $Trust(i, j)$ is then computed by combining both interaction-based and recommendation-based trusts. We also use factors $1 - 1/(\#action + 1)$ and $1/(\#action + 1)$ in such a way that the more direct interactions we have, the more we consider the interaction-based trust compared to the recommendation-based one, and vice versa. Since UAVs may be in the range of each other several times, over several time periods, we consider the average direct/indirect evaluation during these periods. The global inter-UAV trust is computed using

$$Trust\,(i, j) = 1 - \frac{1}{\#action + 1} \cdot \left[\frac{\sum_{x=1}^{n} Direct\,T^{t_x}_{(i,j)}}{n}\right] + \frac{1}{\#action + 1} \cdot \left[\frac{\sum_{x=1}^{n} Indirect\,T^{t_x}_{(i,j)}}{n}\right] \quad (1)$$

3.1.1. Interaction-Based Trust (Direct). The interaction-based trust ($Direct\,T(i, j)$) of an UAV j that is evaluated by another UAV i is calculated as the ratio of the forwarding actions $F^{t_x}_{(i,j)}$ to the total number of actions (both drops and forwards $All^{t_x}_{(i,j)}$) during t_x. Therefore, the interaction-based trust is calculated in the following way:

$$Direct\,T^{t_x}_{(i,j)} = \frac{F^{t_x}_{(i,j)}}{All^{t_x}_{(i,j)}} \cdot \left[1 - \frac{1}{F^{t_x}_{(i,j)} + 1}\right]. \quad (2)$$

The factor $1 - 1/(F^{t_x}_{(i,j)} + 1)$ is used in such way that several packet forwarding actions are required in order to increase the interaction-based trust. This ensures the trust property usually known as the "hard to win, easy to lose" rule.

3.1.2. Recommendation-Based Trust Computation (Indirect). In our proposal, the inter-UAV exchanged recommendations (indirect trust) are sent together with the exchanged data messages. To favor the opinions sourced by UAVs considered as trusted, the received recommendation (Rec) sourced by an UAV k concerning the behavior of UAV j ($\text{Rec}_{(k,j)}^{t_x}$) is combined with the direct trust of the recommender k during a time period t_x, as described in

$$Indirect\, T_{(i,j)}^{t_x} = \sqrt{Direct\, T_{(i,k)}^{t_x} \cdot \text{Rec}_{(k,j)}^{t_x}} \quad \text{during } t_x, \forall k \in \{\text{trusted direct neighbors of } i\}. \tag{3}$$

3.2. Unintentional Misbehavior Identification. To distinguish between unintentional dishonesty from the intentional one, in this work we study three metrics, which are (i) drops due to the limited free buffer space and data freshness, (ii) drops due to lack of energy, and (iii) drops due to the mobility patterns of the selected forwarder. The following sections detail how we estimate the current condition of each considered metric.

3.2.1. Unintentional Misbehavior for Queuing and Packet Freshness Reasons. To evaluate the buffer condition and to decide if an UAV is unintentionally dropping packets because his buffer is full, we compute the average number of received packets (RP_j) and transmitted packets (RP_j) during a time period t_x. In addition, we use factor β to give more importance to the latest period, as it is the most recent and relevant period to consider. Equations (4) show how the average number of received and transmitted packets is computed, respectively.

$$\text{RP}(j) = \frac{\beta \cdot \left[\left(\sum_{x=1}^{n-1} \text{RP}_j^{t_x}\right)/(n-1)\right] + \text{RP}_j^{t_n}}{\beta + 1}.$$
$$\text{TP}(j) = \frac{\beta \cdot \left[\left(\sum_{x=1}^{n-1} \text{TP}_j^{t_x}\right)/(n-1)\right] + \text{TP}_j^{t_n}}{\beta + 1} \tag{4}$$

Afterwards, based on the average number of received/transmitted packets, the average number of queued packets is computed as follows:

$$Queued\, P(j) = \frac{\text{RP}(j)}{\text{TP}(j) + \text{TP}(j)}. \tag{5}$$

Finally, the average waiting time of a packet within the queue of UAV j can be estimated used

$$Waiting\, T(j) = \frac{Queued\, P(j)}{\text{TP}(j)/t_n}. \tag{6}$$

Given a buffer size of $BufferSize_j$, neighboring UAVs can decide whether UAV j will unintentionally start dropping packets or not. If the number of queued packets multiplied by the standard packet size is equal to the buffer size of j, it means that the buffer is full, and so j will be dropping all received packets. In addition, if the average waiting time for the buffer of j is longer than the packet remaining life time, the packet will be also dropped. Otherwise, neither the queue nor packet freshness are causing drops by the UAV j. Algorithm 2 summarizes this process.

3.2.2. Unintentional Misbehavior for Energy Reasons. Besides the engine-related energy consumption, we have three communication-related cases causing energy depletion: (i) energy consumption due to operating in promiscuous mode, (ii) energy consumption associated with packet reception (ERP), and (iii) energy consumption related to packet transmission (ETP). Various energy models consider the energy consumption of the promiscuous mode equal to ERP, including "MEDUSA-II," designed to be ultra-low power, and "Rockwell's WINS model," representing a high-end sensor node equipped with a powerful StrongARM SA-1100 processor from Intel. For instance, in MEDUSA-II, and for any data rate, the node's ERP is 22.20 mW, and 22.06 mW is the power consumed in promiscuous mode, whereas in Rockwell's WINS the ERP is 751.6, and 727.5 mW is the power consumed in promiscuous mode [21, 22]. It is clear that, beside the device features, the ERP energy consumption is almost always equal to the one of the promiscuous mode. For the sake of simplicity, we assume in this work that the promiscuous mode consumption is equal to ERP, and the total communication-related energy is given by the following equation:

$$ConsumedEnergy = 2 * \text{ERP} + \text{ETP}. \tag{7}$$

When a node sends or receives a packet, the network interface of the node decrements the available energy according to the specific network interface card characteristics, the packets' size, and the used bandwidth. The following equations represent the energy used (in Joules) when a packet is transmitted (see (8)) or received (see (9)); notice that packet size is represented in bits [23]:

$$\text{ETP}_j = \frac{330 * 5 * PacketSize}{2 * 10^6} \tag{8}$$

$$\text{ERP}_j = \frac{230 * 5 * PacketSize}{2 * 10^6}. \tag{9}$$

Note that, when a packet is transmitted, a percentage of the consumed energy represents the radio frequency (RF) energy. This energy is used for the propagation model in $ns-2$ to determine the energy level detected by the neighbors' interface nodes upon packet reception, allowing them to consequently determine if packet reception was successful or unsuccessful.

Given an initial energy of $Energy_j$, neighboring UAVs can decide whether the UAV j will unintentionally start dropping packets or not. If $Energy_j - ConsumedEnergy_j$ is less than the minimum required communication energy represented by a predefined $Threshold$, then UAV j will not be able to communicate, and it will start dropping packets. Algorithm 3 summarizes this decision process.

3.2.3. Unintentional Misbehavior for Mobility Reasons. To evaluate UAV mobility and decide if an UAV is unintentionally dropping packets, we compute a link stability index

(1) **if** (*Queued P*(*j*) · *PacketSize* = *BufferSize*$_j$) Or (*Waiting T*(*j*) ≥ *TTL*) **then**
(2) Packet will be dropped;
(3) BufferDrop ← 0;
(4) **else**
(5) BufferDrop ← 1;
(6) **end if**

Algorithm 2: Drops for buffer size reasons.

(1) **if** (*Energy*$_j$ − *ConsumedEnergy*$_j$ ≤ *Threshold*) **then**
(2) Packet will be dropped;
(3) EnergyDrop ← 0;
(4) **else**
(5) EnergyDrop ← 1;
(6) **end if**

Algorithm 3: Drops for energy reasons.

(LSI$_{(i,j)}$). This index is derived from the work in [24]. A modification was needed to tailor the stability coefficient to our purposes. In the original work, it was used as a metric, and so its value can be any positive real number, with lower values indicating a better link stability. To compare the link stability to the trust value, we defined LSI in order to have values between 0 and 1, which represent the worst and best values, respectively.

$$\mathrm{LSI}(i,j) = \frac{d_{\max} - d_{i,j}^{\mathrm{avg}}}{d_{\max}} \cdot \frac{2 \cdot R_{i,j}\left(a_{i,j}\right)}{a_{\max} + 1}. \tag{10}$$

In (10), $d_{\max}$ is the maximum allowed distance between nodes, which corresponds to the transmission range; $d_{i,j}^{\mathrm{avg}}$ is the average distance between nodes i and j computed over the time they remain within transmission range. $a(i, j)$ is the age of the link between i and j, also referred to as link duration. $a_{\max}$ is the maximum age reached by a link from the subject node point of view. $R_{i,j}(a_{i,j})$ is the expected residual lifetime of the link between i and j, which is computed over a statistical basis, as in [24], being defined as follows:

$$R_{i,j}\left(a_{i,j}\right) = \frac{\sum_{a=a_{i,j}}^{a_{\max}} a \cdot d\,[a]}{\sum_{a=a_{i,j}}^{a_{\max}} d\,[a]} - a_{i,j}. \tag{11}$$

Vector $d[]$ stores the observed links age, and element $d[a]$ represents the number of links with age equal to a.

Finally, Algorithm 4 allows estimating the possibility of drops due to mobility. If LSI = 0 it means that there is no radio link between UAVs i and j and, hence, i will consider that the packet loss in this case is due to mobility-related problems. Otherwise, the better the link is, the fewer mobility-related drops are there.

4. Context-Aware Inter-UAV Communication

Unicast data delivery is the basis of various FANET applications, including real-time event reporting through video streaming and traffic conditions estimation. However, to have stable and permanent communication links, different factors should be taken into account. In this work, we mainly target the selection of the most trusted and stable path while achieving a load balance among the network's nodes.

We assume that packet headers include an additional field containing the selected next forwarder identity within the exchanged packets themselves.

The next forwarder for data messages (NF) is selected using the previously computed inter-UAV trust, link stability index, distance, and UAV residual energy. This way, we are able to minimize both the propagation delay and the packet loss ratio with respect to the UAVs energy.

For every neighbor j, UAV i associates a score $Score_{(i,j)}$ representing a balance between the different factors, as shown in

$$\begin{aligned} &Score_{(i,j)} \\ &\quad = HonestyIndex_{(i,j)} \\ &\qquad \cdot \frac{\dfrac{BufferSize_j - \left(Queued\,P\left(j\right) \cdot PacketSize\right)}{PacketSize} + \left(Energy_j - ConsumedEnergy_j\right) + \mathrm{LSI}_{(i,j)} + Distance\left(i, j\right)}{Distance\left(j, Distination\right)}. \end{aligned} \tag{12}$$

```
(1) if (LSI(i, j) = 0) then
(2)     Packet will be dropped;
(3)     MobilityDrop ← 0;
(4) else
(5)     MobilityDrop ← 1 − LSI(i, j);
(6) end if
```

Algorithm 4: Drops for mobility reasons.

Equation (13) represents the next forwarder selection based on the different neighbors' scores:

$$\mathrm{NF} = \frac{j}{Score_{(i,j)}} = \max\left\{Score_{(i,j)}, \forall j \in \text{Neighbors of } i\right\}, \tag{13}$$

where $\{k, \ldots, N\}$ is the set of neighbors for UAV i.

Finally, Algorithm 5 summarizes the inter-UAV data packet forwarding process.

When UAV i receives a data message forwarded by another UAV, it first checks whether it was selected as the next forwarder for that packet. If so, it continues the forwarding process. Otherwise, the processing that follows depends on the application type, thus being outside the scope of this paper. Afterward, if the data packet sender had a higher honesty index than the predefined honesty threshold, the current UAV selects the next forwarder and transmits the message to it. Otherwise, if i considers j as an untrusted UAV, the message will be dropped.

5. Performance Evaluation

To evaluate the proposed solution, simulations are conducted using the NS-2.35 simulator. UAVs are moving within a 5 km^2 area with a height from the ground varying in the range of [20, 50] meters. In addition, UAVs move within that area following the 3D random waypoint mobility model [25]. Our simulations were made using 10 source vehicles, a packet size of 256 bytes, and a rate of 4 packets per second. Our experiments are run 15 times to achieve a degree of confidence of 95%.

The remaining simulation parameters are summarized in Table 2.

Below, we first discuss how the evaluation period t_x is chosen. Second, we show the obtained detection and error ratios of *UNION*, which are also compared to the one of *RPM* [20]. Afterward, we present the resulting end-to-end delay and packet loss ratios achieved by our proposal. Finally, we show the intentional and unintentional dishonesty detection compared to *RPM* and identify the main reasons provoking unintentional dishonesty situations. We also compare our proposal against *CATrust* [26] and *T-CLAIDS* [27] trust models proposed, respectively, for MANETs and VANETs. Nodes in both *CATrust* and *T-CLAIDS* are also moving in 5 km^2 area, using random waypoint mobility model for *CATrust* and Vanetmobisim-based 5 ∗ 5 grid mobility for *T-CLAIDS*.

Table 2: Simulation parameters.

Parameters	Value
Experiment duration (s)	1000
Communication range (m)	250
Communication range (m)	802.11a
UAVs velocity (km/h)	[0, 30]
Dishonest UAVs ratio (%)	{15, 25}
Number of packet sources	10
Packet size (bytes)	256
Packet rate per second	4
Initial trust	0.5
α	0.1
β	0.6
DTH	0.5

5.1. Selecting Adequate Evaluation Periods (t_x). We studied the obtained detection performance for various periods using 100 UAVs where 20% of them are dishonest. Figure 4 shows that, for periods exceeding 35 seconds, detection performance remains nearly the same. Thus, for the experiments that follow, we used a value of $t_x = 35$ seconds. This value can also be dynamically adjusted based on the number of interactions or the number of neighboring UAVs.

5.2. Detection Performance of UNION Compared to RPM, CATrust, and T-CLAIDS. In this part, we present obtained detection performance of our proposal *UNION*. Figure 5 shows the detection ratios of *UNION* when varying the number of UAVs for dishonesty ratios of 15% and 25%, respectively. It shows that *UNION* offers high detection ratios, exceeding 87% when 25% of the UAVs are dishonest. When having a more realistic dishonesty ratio (15%), the detection performance is nearly optimal. Furthermore, for a 25% dishonesty ratio, we find that *UNION* outperforms both *RPM* by more than 15% and *CATrust* by around 5% for high density cases (see Figure 6), whereas *UNION* offer similar performance as *T-CLAIDS*.

Regarding the false positive ratio, Figure 7 shows the generated positive error ratio for both *UNION* and *RPM* when varying the UAV density. The curves of the chart evidence that, unlike *RPM*, *CATrust*, and *T-CLAIDS*, our proposal introduces a low error ratio, and this is mainly due to the accurate detection reached when distinguishing the intentional and unintentional misbehavior of UAVs.

5.3. Packet Delivery Performance of UNION Compared to RPM, CATrust, and T-CLAIDS. In this section, we present the delivery performance of *UNION* compared to *RPM*, *CATrust*, and *T-CLAIDS* through the end-to-end delay and packet loss ratio.

```
(1)  Upon receiving a data packet from j by i;
(2)  if (i is the next forwarder) then
(3)    if (HonestyIndex_(i,j) ≥ HonestyThreshold) then
(4)      NF ← Select next for warder (Equation (13));
(5)      Forward(Packet, NF);
(6)    else
(7)      Drop (msg);
(8)    end if
(9)  end if
(10) End
```

Algorithm 5: Inter-UAV packet delivery process.

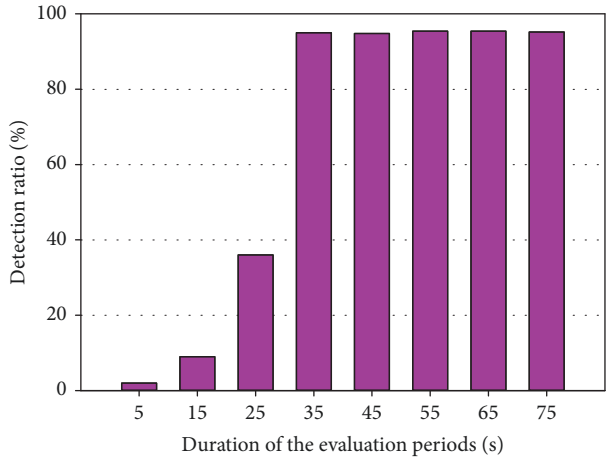

Figure 4: Selection of the adequate evaluation periods (t_x).

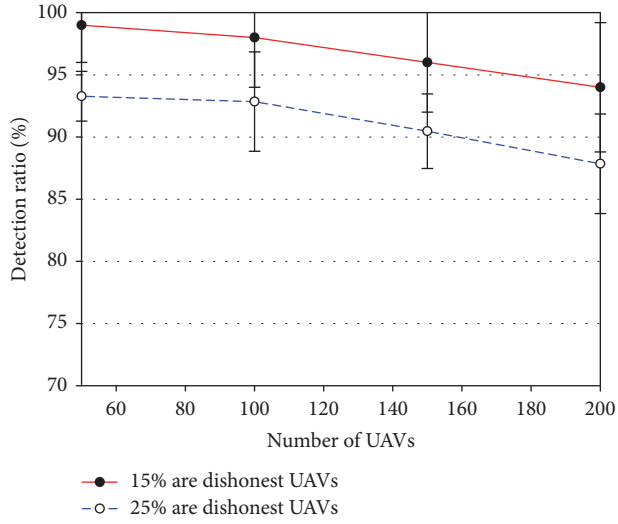

Figure 5: *UNION* detection performance for different dishonesty ratios.

Through the use of our honesty-based context-aware forwarder selection strategy, *UNION* clearly outperforms *RPM*, *CATrust*, and *T-CLAIDS* in terms of packet loss ratio. Furthermore, the loss ratios became negligible for a high UAV density, offering multiple trusted forwarding choices (see Figure 8)

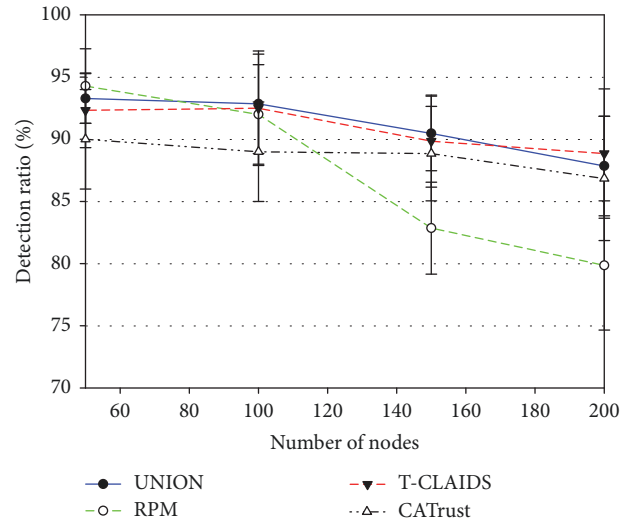

Figure 6: *UNION* detection performance compared to *RPM*, *CATrust*, and *T-CLAIDS* in the presence of 25% dishonest UAVs.

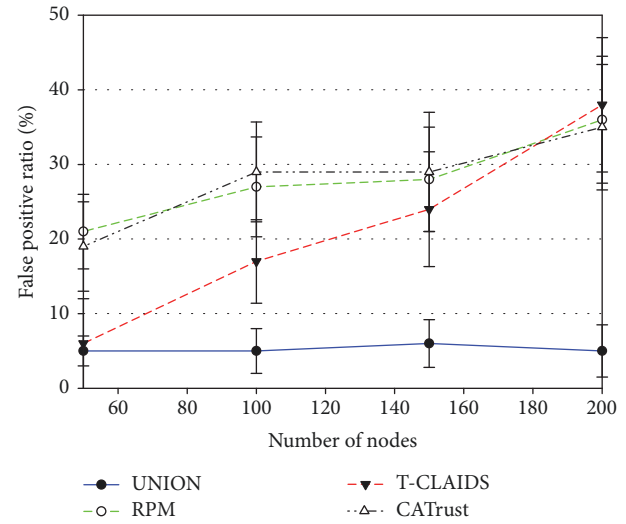

Figure 7: *UNION* false positive ratio compared to *RPM*, *CATrust*, and *T-CLAIDS* in the presence of 25% dishonest UAVs.

As a result of the reduced packet loss ratio, Figure 9 shows that, except for low density cases which are prone to cause network fragmentation, our proposal offers an acceptable

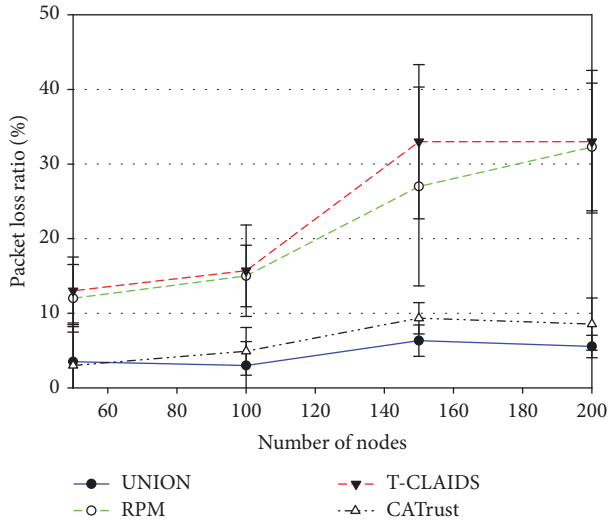

Figure 8: *UNION* packet loss ratio compared to *RPM*, *CATrust*, and *T-CLAIDS* in the presence of 25% dishonest UAVs.

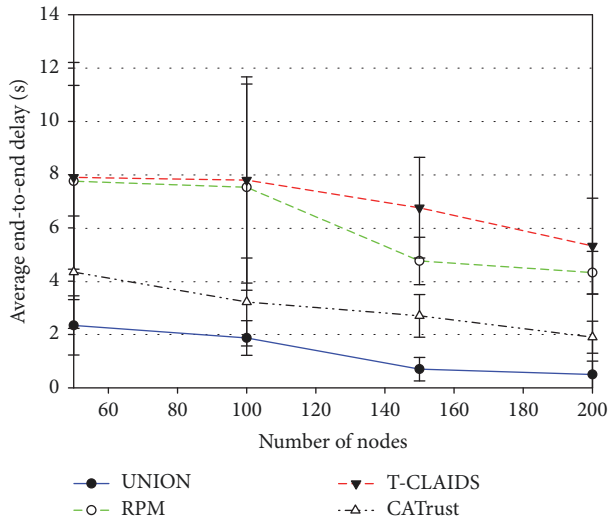

Figure 9: *UNION* average end-to-end delay compared to *RPM*, *CATrust*, and *T-CLAIDS* in the presence of 25% dishonest UAVs.

delivery delay, clearly outperforming the ones which achieved other compared proposals.

5.4. Distinguishing Intentional and Unintentional Misbehavior Using UNION. Last but not least, in this section we study how context awareness is able to improve the performance of *UNION* in terms of reducing the positive error ratios, thereby allowing us to differentiate between intentional and unintentional misbehavior in an effective manner.

Figure 10 shows the correct and wrong detection ratios for both *UNION* and *RPM*. We can see that, unlike *RPM*, *UNION* can clearly reduce the detection of unintentional misbehaving UAVs thanks to its context estimator, thereby ensuring that mostly detection decisions are correct.

Finally, we studied the most significant reasons associated with packets drops besides the security-related ones. Figure 11 shows that, for low density cases, the main reason for packet dropping is the limited size of the UAVs' buffer, and the packet

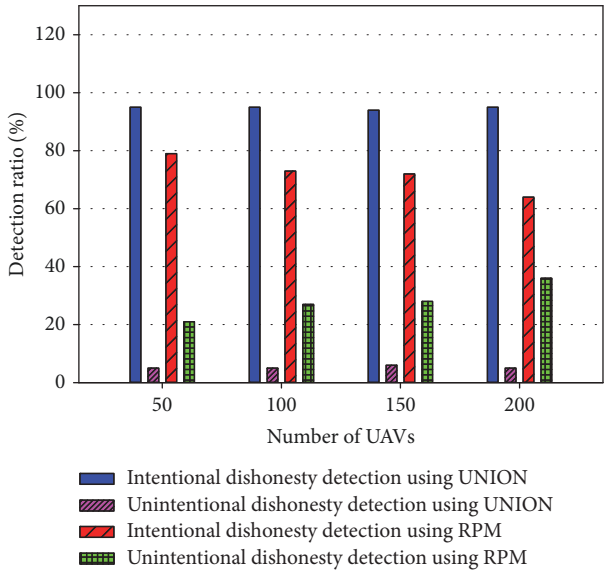

Figure 10: *UNION* intentional and unintentional dishonesty detection compared to *RPM* in the presence of 25% dishonest UAVs.

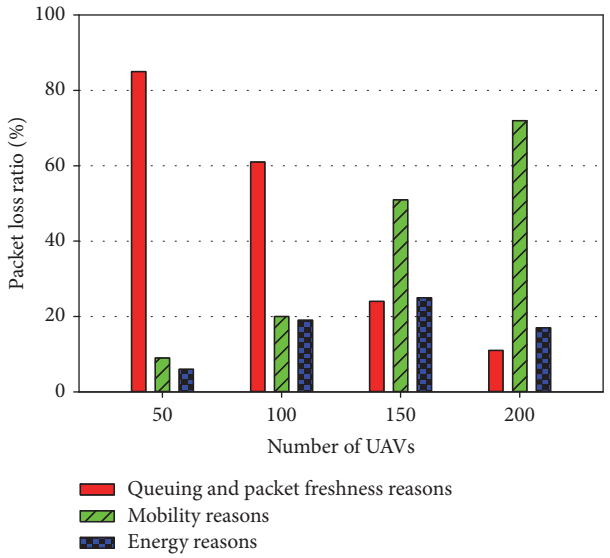

Figure 11: Reasons of unintentional dishonesty detection.

freshness. The latter is just a result of network fragmentation, as an UAV should keep packet in its buffer until it finds an adequate forwarder node. In other cases, the packet becomes too old, and it is dropped because of its TTL. On the other hand, for high density scenarios, the main reason for packet dropping is UAV mobility. Finally, we find that energy is prone to cause stable packet dropping ratios, which are mainly related to the length of flight missions more than anything else.

6. Conclusions and Future Work

Ensuring the desired security with the minimum possible errors is a major concern in all Mobile Ad Hoc Networks. In

this paper, we proposed a novel trust-based context-aware solution that is able to differentiate between intentional and unintentional misbehavior in FANETs. In addition, our proposal called *UNION* takes advantage of the different computed metrics to choose the best packet forwarders. This way, it is able to offer reliable inter-UAV communications.

Our trust-based context-aware inter-UAV communication solution can be used for various realistic applications such as rescue operations, where uncertified personal UAVs can help in delivering instant information about natural catastrophes like earthquakes, volcanoes, obstructed roads, or even car accidents in rural areas. UNION can also be beneficial for different commercial applications such as on path data delivery, and UAV-based cloud solutions.

Simulation results evidence our proposal's performance at ensuring high detection ratios with a reduced number of false positives, low packet loss ratios, and low end-to-end delay, clearly outperforming a previous solution (*RPM*).

As future work, we plan to introduce a lightweight access control strategy to be able to respond to outside attackers. We also plan to develop a technique by which we can scan and protect sensitive areas from unauthorized UAVs.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research is partially supported by the United Arab Emirates University (UAEU) under Grant no. 31T065.

References

[1] A. Bujari, C. E. Palazzi, and D. Ronzani, "FANET application scenarios and mobility models," in *Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications (DroNet '17)*, pp. 43–46, ACM, 2017.

[2] H. Ghazzai, M. B. Ghorbel, A. Kadri, M. J. Hossain, and H. Menouar, "Energy-efficient management of unmanned aerial vehicles for underlay cognitive radio systems," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 4, pp. 434–443, 2017.

[3] V. Sharma and R. Kumar, "Cooperative frameworks and network models for flying ad hoc networks: a survey," *Concurrency and Computation: Practice and Experience*, vol. 29, no. 4, 2016.

[4] W. Wang, C. Dong, S. Zhu, and H. Wang, "DFRA: demodulation-free random access for UAV ad hoc networks," in *Proceedings of the IEEE International Conference on Communications (ICC '17)*, pp. 1–6, May 2017.

[5] J. Sun, W. Wang, L. Kou et al., "A data authentication scheme for UAV ad hoc network communication," *The Journal of Supercomputing*, 2017.

[6] H. Kim, J. Ben-Othman, and L. Mokdad, "On differential privacy-preserving movements of unmanned aerial vehicles," in *Proceedings of the IEEE International Conference on Communications (ICC '17)*, pp. 1–6, May 2017.

[7] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: the security aspect," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 218–224, 2017.

[8] F. Mohammed, I. Jawhar, N. Mohamed, and A. Idries, "Towards trusted and efficient UAV-based communication," in *Proceedings of the 2nd IEEE International Conference on Big Data Security on Cloud (IEEE BigDataSecurity '16), 2nd IEEE International Conference on High Performance and Smart Computing (IEEE HPSC '16) and IEEE International Conference on Intelligent Data and Security (IEEE IDS '16)*, pp. 388–393, April 2016.

[9] K. G. Nikolakopoulos and I. Koukouvelas, "Commercial vs professional UAVs for mapping," in *5th International Conference on Remote Sensing and Geoinformation of the Environment (RSCy '17)*, vol. 10444 of *Proceedings of SPIE*, p. 1044409, International Society for Optics and Photonics, Paphos, Cyprus, March 2017.

[10] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proceedings of the 17th IEEE Symposium on Security and Privacy*, pp. 164–173, May 1996.

[11] S. Bhattacharya and T. Basar, "Game-theoretic analysis of an aerial jamming attack on a UAV communication network," in *Proceedings of the American Control Conference (ACC '10)*, pp. 818–823, IEEE, July 2010.

[12] S.-W. Kim and S.-W. Seo, "Cooperative unmanned autonomous vehicle control for spatially secure group communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 5, pp. 870–882, 2012.

[13] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Proceedings of the 12th IEEE International Conference on Technologies for Homeland Security (HST '12)*, pp. 585–590, IEEE, November 2012.

[14] J.-A. Maxa, M. S. Ben Mahmoud, and N. Larrieu, "Extended verification of secure UAANET routing protocol," in *Proceedings of the IEEE/AIAA 35th DASC Digital Avionics Systems Conference (DASC '16)*, pp. 2155–7209, IEEE, September 2016.

[15] V. Sharma and R. Kumar, "An opportunistic cross layer design for efficient service dissemination over flying ad hoc networks (FANETs)," in *Proceedings of the 2nd International Conference on Electronics and Communication Systems (ICECS '15)*, pp. 1551–1557, IEEE, Coimbatore, India, February 2015.

[16] A. Singh, M. Maheshwari, Nikhil, and N. Kumar, "Security and trust management in MANET," *Communications in Computer and Information Science*, vol. 147, part 3, pp. 384–387, 2011.

[17] A. B. C. Douss, R. Abassi, and S. G. El Fatmi, "A trust management based security mechanism against collusion attacks in a MANET environment," in *Proceedings of the 9th International Conference on Availability, Reliability and Security (ARES '14)*, pp. 325–332, IEEE, September 2014.

[18] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: an adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[19] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[20] C. A. Kerrache, E. Barka, N. Lagraa, and A. Lakas, "Reputation-aware energy-efficient solution for FANET monitoring," in *Proceedings of the 10th IFIP Wireless and Mobile Networking Conference (WMNC '17)*, pp. 1–6, Valencia, Spain, September 2017.

[21] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, "Energy-aware wireless microsensor networks," *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 40–50, 2002.

[22] L. M. Feeney, "An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks," *Mobile Networks and Applications*, vol. 6, no. 3, pp. 239–249, 2001.

[23] J.-C. Cano and P. Manzoni, "A performance comparison of energy consumption for mobile ad hoc network routing protocols," in *Proceedings of the 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS '00)*, pp. 57–63, IEEE, September 2000.

[24] F. De Rango, F. Guerriero, and P. Fazio, "Link-stability and energy aware routing protocol in distributed wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 4, pp. 713–726, 2012.

[25] E. Hyytia, P. Lassila, and J. Virtamo, "Spatial node distribution of the random waypoint mobility model with applications," *IEEE Transactions on Mobile Computing*, vol. 5, no. 6, pp. 680–694, 2006.

[26] Y. Wang, I.-R. Chen, J.-H. Cho et al., "CATrust: context-aware trust management for service-oriented ad hoc networks," *IEEE Transactions on Services Computing*, 2016.

[27] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1981–1996, 2014.