Received 19 April 2021; revised 13 May 2021; accepted 23 May 2021. Date of publication 27 May 2021; date of current version 9 June 2021.

Digital Object Identifier 10.1109/OJCOMS.2021.3084532

Safeguarding Cluster Heads in UAV Swarm Using Edge Intelligence: Linear Discriminant Analysis-Based Cross-Layer Authentication

HUANCHI WANG (Graduate Student Member, IEEE), HE FANG (Member, IEEE), AND XIANBIN WANG (Fellow, IEEE)

Department of Electrical and Computer Engineering, Western University, London, ON N6A 5B9, Canada

CORRESPONDING AUTHOR: X. WANG (e-mail: xianbin.wang@uwo.ca)

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Program under Grant RGPIN2018-06254; in part by the Collaborative Research and Development Program under Grant CRDPJ533987-18; and in part by the Canada Research Chair Program.

ABSTRACT While the unmanned aerial vehicles (UAVs) swarm travels under a dynamic environment, the cluster head (CH) switching is unavoidable due to the mitigation of mobility, quality of service, and energy consumption. If an attacker becomes the new CH, the entire swarm will be controlled and the sensitive data will be leaked. Unlike the other mobile networks with constant network connectivity, the authentication in the UAV swarm suffers from intermittent connection with the ground station under a hostile environment or spectrum constraint condition. Hence, this paper proposes a novel CH safeguarding mechanism enabled by edge intelligence utilizing a situational-aware authentication scheme. This low-latency mechanism provides extra security at the CH selection and switching without cloud server support. By adopting the unique cross-layer attributes, the system security is significantly improved based on the extracted multi-dimensional information. The Linear Discriminant Analysis (LDA) algorithm fuses the authentication decision accurately by projecting the high dimensional estimations into a low dimensional space for maximum separability by only keeping the necessary attributes. A situation-aware cross-layer attribute selection algorithm is developed to select a minimum number of attributes so that the time required for attribute estimation and computation overhead of authentication can be reduced. The simulation results demonstrate that our scheme performs better under a dynamic environment compared with the physical layer authentication scheme and some existing state-of-the-art authentication techniques.

INDEX TERMS Cross layer authentication, edge intelligence, linear discriminant analysis, situation awareness, unmanned aerial vehicles (UAVs).

I. INTRODUCTION

THE UNMANNED Aerial Vehicles (UAVs) have become ubiquitous in both civilian and military fields in recent years due to the flexibility in operation and risk reduction of personal injury [1]. Consequently, the cost of the UAVs becomes lower, which enables the use of multiple UAVs in one mission to enhance the performance and broader the range of applications such as expanding wireless networks coverage, smart policing, search and rescue missions, and disaster monitoring [2]–[4]. To route, allocate resources and relay both the intra-cluster communication and down-link communication for the members, a cluster head (CH) is selected and served as the central node of the UAV swarm [5]. However, due to the vital information contained in the swarm, the attackers may target the security vulnerability and initiate attacks to acquire the sensitive information or compromise the network.

The UAV network, which is a flying ad hoc network among UAVs, can be deemed as a form of mobile ad hoc networks (MANETs) [6]. However, unlike the CH in MANETs or vehicular ad hoc networks (VANETs) whose goal is to facilitate the internal peer-to-peer connections including smart

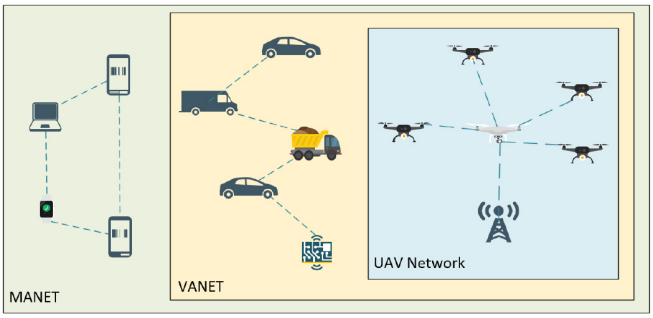

FIGURE 1. Network topology of MANET, VANET and UAV network.

infrastructures, the CH of the UAV network has to relay the sensitive transmission to the ground station [7]. This makes the CH in the UAV network carry more sensitive information than in MANETs which increases the interest of being attacked. Besides, the UAV network has unique challenges such as the high mobility in which the maximum speed of a UAV can reach 460km/h [5], [8], [9]. Typical MANET or VANETs are associated with moving human users or cars and they usually travel in the same direction [10]. Hence, the mobility of the MANETs and VANETs can be considered as 1-dimensional while the UAV network is 3-dimensional with a significantly faster changing physical topology. This dramatically increases the frequency of CH switching to accommodate the new physical topology and further rise the chance of being attacked. Moreover, the typical distances between the UAVs are also further than the nodes in the MANETs which increases the difficulty in maintaining the radio links. Hence, the frequency of the CH switching is a lot higher than the MANETs which also increases the chance of being attacked. The network topology of the MANET, VANET and the UAV network is shown in Fig. 1.

Similar to the UAV network, many wireless sensor networks (WSN) also use clustering technology and the main goal is to enhance the battery life by utilizing the CH switching techniques [11]. However, the high mobility of the UAV in the spatial domain, makes it more challenging for the CH to provide a stable network coverage where the CH switching is a lot more frequent than the WSN. This gives the attacker more chances to compromise the network and hence more challenging to safeguard the role of CH. Besides, the main power consumption factors of the UAV is on the weight and motors where a small UAV requires up to 200 watt/kg to fly [12]. On the other hand, the power consumption of the UAV management system, such as autopilots, which includes the navigation and communication module ranges from 1.5 to 5 watts which can be negligible in large UAVs [7], [12], [13]. However, the power consumption of the high-speed down-link communication between the CH and the ground station can still become a design restriction which triggers CH switching in the UAV swarm with mini UAVs [14], [15]. Hence, it is more challenging to protect the role of CH in any trajectory or environment due to the more frequent CH switching comparing to the WSN.

To handover the role of CH, the on-duty CH has to transfer the important information to the new CH and acknowledge the member UAVs to disconnect and then set up a new connection [16]. The data that transferred to the new CH may include mission-related data which is highly sensitive. Hence, if the attacker becomes the new CH by spoofing a legitimate device, the sensitive information will be leaked and the data transmission will be monitored, tampered and deleted which ultimately leads to mission failure. Moreover, the UAV swarm suffers from the spectrum constraint and radio silence in the hostile environment which limits the implementation of the cloud-based security enhancement with the base station. To resolve these challenges, a low-latency on-site safeguarding technique that enhances the security of the UAV swarm by preventing the attacker from becoming the new central node during the CH transferring is critical.

One of the traditional techniques in authentication is encryption technology such as the Advanced Encryption Standard (AES) [17]. However, the rapid computational power development increases the potential of deciphering the encryption algorithms, which makes the attacker easier to impersonate a legitimate UAV and become the new CH [18].

Another popular approach in UAV authentication enhancement is to utilize the physical layer attributes, i.e., the radio frequency (RF) fingerprinting, which has been used widely in intrusion detection, access control, cloning detection and malfunction detection [19], [20]. This method authenticates devices in the network by observing the unique channel-based attributes. The unique attributes such as the Received Signal Strength Indication (RSSI) [21], Carrier Frequency Offset (CFO) [22], Channel Impulse Response (CIR) [23], non-linear frequency domain analysis [24], and in-phase/quadrature (I/Q) imbalance [25] are related to the operating environment and the hardware condition. Therefore, individual characteristics can be extracted and used to verify the same-type UAVs within the swarm [26].

Despite its many advantages, its performance could suffer from the time-variation and imperfect estimations of the physical-layer attributes in real-world scenarios [23], [27]. The physical layer estimations can be affected severely by the decorrelated attributes caused by mobility and dynamic interference. The unstable fluctuation increases the dynamic range of the physical-layer attributes which leads to the insufficient range to distinguish the individual devices since the range of each device may overlap with each other. The overlap increases the tolerance for the attacker to imitate the legitimate UAV, thus increasing the chance of becoming the new CH. Hence, the more stable cross-layer attributes are considered in this paper since the higher layer attributes, such as the MAC layer packet error rate (PER), are more immune to the time-variance and change of communication environment [28].

To utilize the cross-layer attributes for authentication, Zhang *et al.* proposed a fast authentication scheme for dynamic sensor networks [29]. In this work, the physical

layer authentication has been used as a fast authentication process while the upper layer attributes are only used as supervision when the physical layer authentication recognizes the device as an attacker. The advantage of this fast authentication scheme is obvious when the environment is stable where the upper layer attributes supervision is not required frequently. However, the UAV swarms always work in a dynamic environment where many physical layer attributes are less stable. Hence, instead of using the upper layer attributes as two-step supervision, we need to fuse the cross-layer attributes to form a reliable and stable authentication decision.

Another solution utilizing the cross-layer attributes is proposed by Hao *et al.* where two separate decisions are formulated by using RSSI and PER [28]. The final decision is then fused based on the majority variables' decision. However, due to the fast environment change in the UAV swarm, some of the attributes are non-ideal in certain environments, e.g., the RSSI carries more information in the in-door environment compare to the clear open-air environment. The diversity of the cross-layer attributes should be improved to enhance the performance stability and robustness. Nevertheless, the overall latency needs to be considered and an attributes selection algorithm based on situational-awareness becomes critical.

To compensate for the challenges of the existing state-of-the-art cross-layer authentication algorithms, we want to achieve an accurate authentication result by fusing the most suitable cross-layer attributes based on situational-awareness. The Machine Learning (ML) techniques are taken into consideration, where techniques such as Deep Learning (DL) and Neural Network (NN) have had an extensive history in the field of authentication and testify a huge potential in performance gain [30]–[33]. However, the huge computational power enabled by the latest hardware, i.e., the graphical processing units, has become a criterion for the implementation platform which is less feasible to be implemented in the UAV network.

To mitigate the limited computational power, one of the light-weight ML techniques that can fuse the cross-layer attributes into a final decision is the tree-based ML technique [34]. The tree-based ML technique is expressed as a recursive partition of the instance space where each non-terminal node represents a predictor variable and each leaf represents a class label as the outcome [35]. However, since the tree-based ML techniques are supervised ML techniques, they require the operator to provide training data of the attackers which are not feasible under the UAV network.

Another light-weight ML technique is the non-parametric distance-based ML technique where the similarity between two instances are measured by using standard distance measurements (i.e., Euclidean distance) [36]. Since no training data and model training is required, the distance-based ML technique is more suitable to be used for a low-latency on-board authentication task.

To enhance the accuracy while minimizing the latency, a situation-aware attribute selection process becomes a dilemma which removes the excessive cross-layer attributes used to compensate the high mobility. Some of the attributes, such as the RSSI, may change significantly due to the highly dynamic physical topology in the field which may bring negative impact to the authentication decision. A potential approach is to use the sequential forward selection mechanism in which attributes are added sequentially until the criterion of selection has been reached [37]. This technique can select the minimum amount of attributes that are most relevant to the environment; however, the process of hill-climbing search requires a high computational power that is not suitable in our edge network [38].

Another approach is the Linear Discriminant Analysis (LDA) algorithm which reduces the dimensionality by applying a linear transformation that only keeps the most relevant attributes in the specific scenario. A projection of the original data is then formed such that the between-class variance is maximized and the within-class variance is minimized thereby maximizing the class separability [39]–[41]. Hence, the LDA algorithm can help to extract useful information from the high dimensional data with the maximized efficiency due to the calculation simplicity. However, the LDA algorithm needs input from the operator to specify how many attributes are needed after the attributes selection. Hence, a situational-aware attribute selection algorithm has to be developed to automatically choose the number of cross-layer attributes being selected in the LDA algorithm to forge the authentication decision.

In this paper, we propose a novel LDA-based on-site authentication scheme that safeguards the role of CH under a dynamic environment with minimum latency. The security of the UAV swarm is enhanced by adopting the more stable and unique cross-layer attributes which are difficult for the attackers to imitate. We then proposed a novel cross-layer attributes selection algorithm that selects the best combination of attributes based on situation-awareness to be used in the LDA-based authentication scheme. Unnecessary cross-layer attributes with low contribution to the LDA authentication outcome are eliminated to improve the authentication performance while minimizing the overall latency. The contributions of this paper are summarized in Fig. 2.

The paper is organized as follows: Section II introduces the system model and problem formulation. Section III overviews the principle of LDA and the adaptive cross-layer attribute selection algorithm. The performance of the LDA-aided cross-layer multi-UAV authentication is evaluated and compared to the other ML-based techniques in Section IV. Ultimately, Section V concludes this paper. The main symbols used throughout this article are summarized in Table 1.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 3, we consider a UAV swarm that consists of M member UAVs and an on-duty CH. There exists a spoofing device that aims to become the new CH to acquire

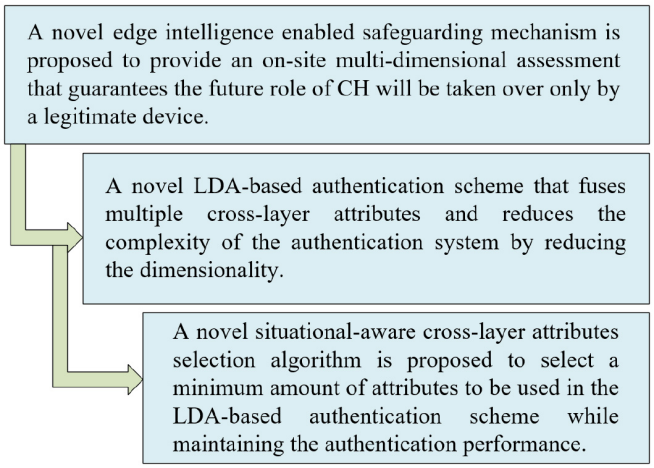

FIGURE 2. Summary of novelty and contributions of this paper.

TABLE 1. Main symbol table.

Symbol	Definition
I_m^{ini}	digital identity of the m-th UAV
M	number of member UAVs in the swarm
N	number of cross-layer attributes
t	time instance that the authentication is required
$\boldsymbol{H_m^I}$	cross-layer estimations of the m-th UAV in phase I
$\boldsymbol{H_m^{II}}$	cross-layer estimations of the m-th UAV in phase II
δ	distance threshold
ψ_0	UAV is legitimate
ψ_1	UAV is a spoofing device
R_e	authentication error level
R_e	authentication sensitivity level
$\mathcal{T}$	trust value of the authentication process
w_1	re-scaled cost of false positive case
w_2	re-scaled cost of false negative case
$\boldsymbol{h}$	a single cross-layer estimation
S_m	scatter matrix of the m-th class
$\overline{\boldsymbol{h}}_{\boldsymbol{m}}$	mean of the cross-layer estimations for the m-th class
k_m	number of cross-layer estimations for the m-th class
$\mathcal{W}$	intra-class scatter matrix
$\mathcal{B}$	inter-class scatter matrix
$\boldsymbol{\Phi}$	linear transformation matrix of the original dataset
$\boldsymbol{\lambda}$	eigenvalue of the transformation matrix
ν	the number of cross-layer estimation selected
τ	information threshold

sensitive data and control the UAV swarm. The on-duty CH aims to verify each UAV within the swarm accurately before the CH selection and CH switching to guarantee the CH candidates are legitimate, and the role of CH is being transferred to the selected UAV eventually. Hence, an accurate authentication method that continuously secures the CH selection and switching process is extremely important so that a spoofer will not become a CH candidate.

To provide multi-dimensional authentication for the new CH in the dynamic environment, cross-layer attributes are utilized in this paper. Although the physical layer attributes can be estimated quickly when needed, the upper layer attributes such as the MAC layer PER collected over time, and frequency of MAC layer probe requests [15] are more immune to the time-varying environment. The utilization of cross-layer attributes for authentication could provide multi-dimensional protections for legitimate devices as well as

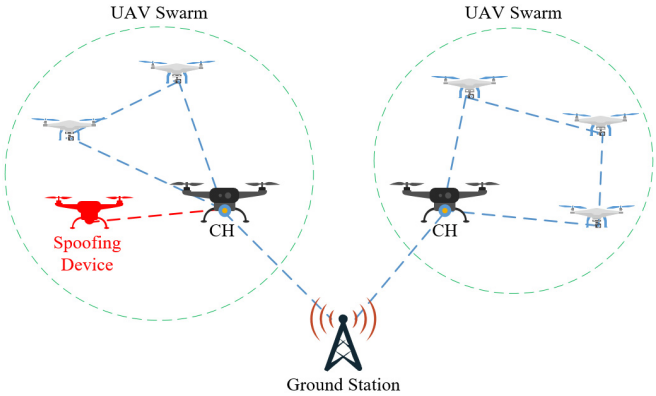

FIGURE 3. System model. *M* legitimate member UAVs exist within the UAV swarm with one on-duty CH. A potential spoofing device aims to become the new CH of the UAV swarm for illegal purposes. The on-duty CH focuses on continuously verifies all devices to prevent the spoofing device from becoming a candidate of the CH selection or substitute the selected UAV as the new CH at the switching process.

achieve robust performance in the time-varying environment. The process of authentication relying on multiple cross-layer features contains two phases.

Phase I: The on-duty CH collects the trusted cross-layer estimations from all M UAVs, when they first join the network, as $\boldsymbol{H_1^I}, \boldsymbol{H_2^I}, \ldots, \boldsymbol{H_M^I}$. These estimations are paired with their digital identities $(I_1^{ini}, I_2^{ini}, \ldots, I_M^{ini})$ during the collection. The trusted cross-layer estimation of the m-th UAV, whose digital identity is I_m^{ini}, can be denoted as:

$$\boldsymbol{H_m^I} = \left(H_{m1}^I, H_{m2}^I, \ldots, H_{mN}^I\right)^{\mathrm{T}}, \tag{1}$$

where N is the number of cross-layer attributes and $()^{\mathrm{T}}$ is the transposition of the vector. To obtain the trusted cross-layer estimations, each UAV broadcasts data packets that include its GPS location at a certain time slot. The other UAVs receive the GPS coordinates as the application layer attribute and calculates the PER of the received packets as the MAC layer attributes. The physical layer attributes can be estimated by using the embedded hardware to calculate the RSSI, I/Q imbalance, CIR, CFO and so on. The imperfect physical layer estimation is acceptable as fluctuations.

Phase II: At time t, the on-duty CH collects a set of observations from all UAVs that requires an authentication, where the cross-layer estimation of the m-th device can be written as

$$\boldsymbol{H_m^{II}} = \left(H_{m1}^{II}, H_{m2}^{II}, \ldots, H_{mN}^{II}\right)^{\mathrm{T}}. \tag{2}$$

To achieve the situation-awareness of authentication in the time-varying environment using cross-layer attributes, the cross-layer estimations should be collected periodically. Since the cross-layer attributes estimations represent the characteristic of the device, a measurement of the similarity between the estimation collected in *Phase II* and *Phase I* is critical and can be formulated as:

$$d\left(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^I}\right) = \sqrt{\left(H_{m1}^{II} - H_{m1}^I\right)^2 + \cdots + \left(H_{mN}^{II} - H_{mN}^I\right)^2}, \tag{3}$$

where $d(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^{I}})$ is the Euclidean distance between the cross-layer estimation of the m-th UAV collected in *Phase II* and the trusted estimation collected in *Phase I*. The authentication decision will be forged by judging the similarity between these collected estimations. Hence, a distance threshold δ can be introduced as the similarity judgement to separate the spoofing device from the legitimate UAVs. The authentication decision can then be written as a binary hypothesis test:

$$\begin{cases} \Psi_0, & d\left(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^{I}}\right) \leq \delta; \\ \Psi_1, & d\left(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^{I}}\right) > \delta, \end{cases} \tag{4}$$

in which Ψ_0 represents the UAV is legitimate and Ψ_1 indicates the UAV is a spoofing device. To evaluate the performance of the authentication process, three different evaluation criteria are considered:

1) *True Positive (TP):* The probability that the m-th UAV is authenticated correctly which is formulated as:

$$P_m^{\mathrm{TP}} = \Pr\left(d\left(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^{I}}\right) < \delta | \Psi_{m0}\right). \tag{5}$$

2) *False Positive (FP):* The probability that the spoofing device is authenticated as a legitimate UAV. It can be defined as:

$$P_m^{\mathrm{FP}} = \Pr\left(d\left(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^{I}}\right) < \delta | \Psi_{m1}\right). \tag{6}$$

3) *False Negative (FN):* The probability that the legitimate m-th UAV is authenticated as a spoofing device. The function can be given as:

$$P_m^{\mathrm{FN}} = \Pr\left(d\left(\boldsymbol{H_m^{II}}, \boldsymbol{H_m^{I}}\right) > \delta | \Psi_{m0}\right). \tag{7}$$

where Ψ_{m0} is the case such that the claimed m-th UAV is legitimate while Ψ_{m1} is the case such that the claimed m-th UAV is a spoofing device. To better describe the authentication performance, we define two evaluation criteria in this paper, i.e., the authentication error level (R_e) and authentication sensitivity level (R_s). To be more specific, the authentication error level is the probability that a spoofing device is authenticated as a legitimate device based on their observations of cross-layer attributes. The authentication sensitivity level presents how likely a legitimate UAV is authenticated as a spoofing device.

$$R_e = \frac{1}{M} \sum_{m=1}^{M} \frac{P_m^{\mathrm{FP}}}{P_m^{\mathrm{TP}} + P_m^{\mathrm{FP}}}, \tag{8}$$

and

$$R_s = \frac{1}{M} \sum_{m=1}^{M} \frac{P_m^{\mathrm{FN}}}{P_m^{\mathrm{TP}} + P_m^{\mathrm{FN}}}. \tag{9}$$

Then, to judge the authentication performance, the trust value ($\mathcal{T}$) is introduced as:

$$\mathcal{T} = w_1(1 - R_e) + w_2(1 - R_s), \tag{10}$$

where w_1 and w_2 are the re-scaled cost of the false positive case and the false negative case whose summation is $w_1 + w_2 = 100\%$. Ideally, if no legitimate device has been falsely rejected and no spoofing device has been ignored, the system is trust worthy and the trust value should be equal to 1. The problem formulation of this paper can then be expressed as:

$$\max_{\delta} \mathcal{T}, \tag{11}$$

where δ is the distance threshold as introduced above.

Remark 1: To solve the problem of (11), the separability between the cross-layer estimations of each device should be as far as possible. If the separability is low, the system cannot effectively distinguish the spoofing device from the legitimate device. Hence, we will propose the situation-aware LDA-based cross-layer authentication scheme which increases the separability between the estimations from different UAVs and minimize the separability from the same UAV. This gives the system more tolerance to select δ and ultimately improves the overall authentication performance.

III. SITUATION-AWARE LDA-BASED CROSS-LAYER AUTHENTICATION

To solve the problem of (11) in a small group of UAVs, it is critical to authenticate each legitimate device correctly by distinguishing the spoofing device from the legitimate UAVs under a limited computational capability. To further improve the authentication performance, the uniqueness of each UAV should be improved by enhancing the separability of the original estimations. Hence, the LDA-based authentication scheme is proposed to project the original observations into a low dimensional space with maximum separability while reduces the computational overhead and time latency. Then, a situational-aware cross-layer attribute selection algorithm is proposed to select a minimum amount of cross-layer attributes that maintain the overall performance under the dynamic environment.

A. AUTHENTICATION BASED ON LDA ALGORITHM

To extract the information from the multiple cross-layer attributes, we explore the LDA technique which transforms the initial verified cross-layer estimation into a low-dimensional space for better separability. After collecting the set of trusted cross-layer attributes ($\boldsymbol{H^I}$) in *phase I* and the cross-layer attributes ($\boldsymbol{H^{II}}$) for authentication at time t in *phase II*, all the observations are merged together to form the new set ($\boldsymbol{H}$) that are being used for the authentication. Each estimation in $\boldsymbol{H}$ is denoted as $\boldsymbol{h}$ and the estimations of the m-th UAV is I_m^{ini}. The cross-layer estimations of each UAV can be considered as a class to be further used in the LDA algorithm. To analyze the estimations, the scatter matrix of each class which estimates the covariance matrix is formulated as:

$$S_m = \sum_{h \in I_m^{ini}} \left(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}}\right)\left(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}}\right)^{\mathrm{T}}, \tag{12}$$

where

$$\bar{\boldsymbol{h}}_{\boldsymbol{m}} = \frac{1}{k_m} \sum_{h \in I_m^{ini}} \boldsymbol{h}, \tag{13}$$

represents the mean for each class and k_m is the number of samples in I_m^{ini}. The scatter matrix is fundamental to LDA since it measures the distribution of the given data. Hence, the total intra-class matrix, which describes how far each class is away from each other, is calculated as:

$$\mathcal{W} = \sum_{m=1}^{M} \sum_{h \in I_m^{ini}} \left(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}}\right)\left(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}}\right)^{\mathrm{T}}, \tag{14}$$

The inter-class scatter matrix, which describes how close the data points within a class, can be given by:

$$\mathcal{B} = \sum_{m=1}^{M} k_m \left(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}}\right)\left(\boldsymbol{h} - \bar{\boldsymbol{h}}_{\boldsymbol{m}}\right)^{\mathrm{T}}, \tag{15}$$

where $\bar{\boldsymbol{h}}$ is the total mean vector given by $\bar{\boldsymbol{h}} = \frac{1}{k}\sum_{m=1}^{M} k_m \bar{\boldsymbol{h}}_{\boldsymbol{m}}$. To find the best solution for (11), Fisher's criterion is adopted in which the means between each class after the projection should be as far as possible and the variance should be as small as possible. This criterion can be written as (16) by using the inter-class scatter matrix and the intra-class scatter matrix.

$$\max_{\delta} \frac{\boldsymbol{\Phi}^T \mathcal{B} \boldsymbol{\Phi}}{\boldsymbol{\Phi}^T \mathcal{W} \boldsymbol{\Phi}}, \tag{16}$$

where $\boldsymbol{\Phi}$ is the linear transformation matrix of the original dataset. To find the perfect linear transformation to minimize R_e of (8), (16) can be reformulated with the help of Generalized Rayleigh quotient [42] as:

$$\mathcal{B}\boldsymbol{\Phi} = \boldsymbol{\lambda}\mathcal{W}\boldsymbol{\Phi}, \tag{17}$$

where $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, \ldots, \lambda_N]^{\mathrm{T}}$ are the eigenvalues of the transformation matrix $\boldsymbol{\Phi}$. If W is non-singular, $\boldsymbol{\Phi}$ can be solved by calculating the eigenvalues and the eigenvectors of all attributes of the dataset. Each eigenvector describes one axis of the transformed space and the corresponding eigenvalue represents the ability to discriminate between different classes. The eigenvector with the highest eigenvalue carries the majority of information about the distribution of the data. Hence, the highest eigenvalues and the corresponding attributes are chosen to formulate the new space.

As described in (3), the Euclidean distance between the new estimation and the trusted estimation is calculated to verify if the characteristics of the m-th UAV has changed suddenly. In the authentication instance at time t, the cross-layer estimation can be written as $\boldsymbol{h_t}$. The Euclidean distance after the linear transformation between the new estimation and the trusted estimation can then be written as $d(\boldsymbol{h_t}\boldsymbol{\Phi}, \bar{\boldsymbol{h}}_{\boldsymbol{m}}\boldsymbol{\Phi})$.

Therefore, the binary authentication decision described in (4) after the linear transformation can be transformed to:

$$C(\boldsymbol{h_t}) = \begin{cases} \Psi_0, & d\left(\boldsymbol{h_t}\boldsymbol{\Phi}, \bar{\boldsymbol{h}}_{\boldsymbol{m}}\boldsymbol{\Phi}\right) \leq \delta; \\ \Psi_1, & d\left(\boldsymbol{h_t}\boldsymbol{\Phi}, \bar{\boldsymbol{h}}_{\boldsymbol{m}}\boldsymbol{\Phi}\right) > \delta. \end{cases} \tag{18}$$

Hence, if the cross-layer attributes between the new estimation and the record is similar ($d(\boldsymbol{h_t}\boldsymbol{\Phi}, \bar{\boldsymbol{h}}_{\boldsymbol{m}}\boldsymbol{\Phi}) \leq \delta$), the device will be authenticated as a legitimate device (Ψ_0). Similarly, if the cross-layer attributes are significantly different from the record ($d(\boldsymbol{x_t}\boldsymbol{\Phi}, \bar{\boldsymbol{h}}_{\boldsymbol{m}}\boldsymbol{\Phi}) > \delta$), the device will be authenticated as a spoofing device (Ψ_1). However, a small δ value can decrease the overall trust value of (10) since the fluctuation in the cross-layer attributes can lead to a false rejection. Similarly, a high δ value also decreases the trust value since the difference of the cross-layer attributes between the legitimate devices and the attacker can be deemed as a regular fluctuation. Hence, the choice of δ should be neither too sensitive nor too tolerant to the fluctuations and should be chosen accordingly across different scenarios. The proposed LDA-based authentication scheme is shown in Algorithm 1.

Algorithm 1 LDA-Based Authentication

Given the total number of cross-layer attributes included for the authentication for each observation by N. The estimations observed of the m-th UAV are given as $\boldsymbol{H_m} = (H_{m1}, H_{m2}, \ldots, H_{mN})^{\mathrm{T}}$, and the total number of UAVs in the network is M. The authentication happens at instance t before the new CH selection or CH switching.

1: The on-duty CH initializes the cross-layer attributes collection by broadcasting the "Initialization packet" to all UAVs in the system.
2: All UAVs constantly reply to the on-duty CH.
3: The on-duty CH collects all the "reply packets" as the initial dataset with trusted labels.
4: The on-duty CH broadcasts the "authentication request" packet to designated UAV(s) in the system at instance t before the new CH selection or CH switching.
5: The UAV(s) that receive the "authentication request" packet reply to the on-duty CH.
6: The on-duty CH adds the data into the trusted dataset.
7: The on-duty CH calculates the in-class variance and between-class variance to obtain the linear transformation of the updated dataset according to (14) and (15).
8: The on-duty CH performs the linear transformation to get the projection of the original space then calculates the Euclidean distance between the observation.
9: **if** $d(t\boldsymbol{\Phi}, \bar{\boldsymbol{h}}_{\boldsymbol{m}}\boldsymbol{\Phi}) < \delta$ **then**
10: authenticates the m-th UAV as a legitimate device.
11: **else**
12: authenticates the m-th UAV as a spoofing device.
13: **end if**
14: Update the trusted dataset by adding the new estimations at instance t if they are from legitimate UAVs.

Remark 2: To minimize R_e and R_s of (8) and (9), the cross-layer attributes between different UAVs should be separated far enough so that a correct authentication decision can be forged by using (18) with a appropriate δ value. Hence, the projection of the original space has to maximize the separation of the classes and minimize difference within the class which fulfills (16).

B. ADAPTIVE CROSS-LAYER ATTRIBUTE SELECTION ALGORITHM

Although the LDA is perfect for projecting a high dimensional data set into a low dimensional data set, it requires the parameter that states the number of attributes being left after the dimensionality reduction as an input. However, each attribute has a distinct level of significance and the optimal amount of attributes being chosen is different across the dynamic environment. Hence, a fixed amount of cross-layer attributes being used for the linear transformation is not suitable to achieve the best performance and minimize the overall latency. In this section, a situation-aware cross-layer attribute selection algorithm (see Algorithm 2) is developed to select the minimum amount of cross-layer attributes while maintaining the overall performance across different scenarios. The unique combination across different scenarios also increases the overall security of the entire system.

As shown in (17), the eigenvalue, which evaluates the level of significance of the cross-layer attributes, are required to compute the linear transformation matrix. The different choices of cross-layer attributes will result in an individual linear transformation matrix. Ideally, a minimum amount of cross-layer attributes should be selected to reduce the complexity while maintaining the maximum amount of information after the linear transformation. Hence, only the cross-layer attributes with high eigenvalues should be kept after the projection. To achieve this goal, a threshold can be set to only choose the necessary amount of eigenvalues under the dynamic environment. However, there is no upper limit for the eigenvalues ($\boldsymbol{\lambda}$), which indicates that it is impossible to set a fixed eigenvalue threshold. Therefore, we convert $\boldsymbol{\lambda}$ into a percentage scale as:

$$\boldsymbol{P}_{\lambda} = \left[P_{\lambda_1}, P_{\lambda_2}, \ldots, P_{\lambda_N}\right]^{\mathrm{T}}, \tag{19}$$

such that $P_{\lambda_1} + P_{\lambda_2} + \cdots + P_{\lambda_N} = 100\%$. In this case, P_{λ_1} has the highest eigenvalue in percentage scale and P_{λ_N} has the lowest eigenvalue in percentage scale. The information threshold (τ) can then be chosen by the users according to the specific application scenario and then be used to choose the minimum number of top cross-layer attributes as follows:

$$\tau \leq P_{\lambda_1} + P_{\lambda_2} + \cdots + P_{\lambda_\upsilon}, \tag{20}$$

where $\upsilon = 1, 2, \ldots, N-1$ and the goal of attribute selection can be rewritten as:

$$\min_{\upsilon}\left(P_{\lambda_1} + P_{\lambda_2} + \cdots + P_{\lambda_\upsilon} - \tau\right). \tag{21}$$

A higher τ value generally indicates that more attributes will be kept after the LDA process. However, a τ value that is close to 100% does not guarantee to use of all attributes since some of the attributes do not contribute or even have a negative impact on the authentication. Moreover, sometimes the authentication system does not require a highest τ value to reach the best performance; hence, the τ value should be selected based on the environment and the performance requirements accordingly. The characteristic of the τ value will be tested and shown in the performance evaluation. The detailed process is shown in Algorithm 2.

Algorithm 2 Adaptive Cross-Layer Attribute Selection Algorithm

Given the combined cross-layer attributes ($\boldsymbol{H}$) which consists of the initial verified cross-layer estimation ($\boldsymbol{H^I}$) collected in *Phase I* and the cross-layer attributes ($\boldsymbol{H^{II}}$) freshly collected in *Phase II* at time t.

1: Obtain the eigenvalue of each cross-layer attribute.
2: Covert the eigenvalues into a percentage scale $\boldsymbol{P}_{\lambda}$.
3: Rank the component of $\boldsymbol{P}_{\lambda}$ from high to low where P_{λ_1} has the highest percentage score.
4: Sum up P_{λ_1} to P_{λ_υ} such that the summation is greater or equal than τ with the minimum value of υ.
5: Use the top υ cross-layer attributes for LDA dimensional reduction.

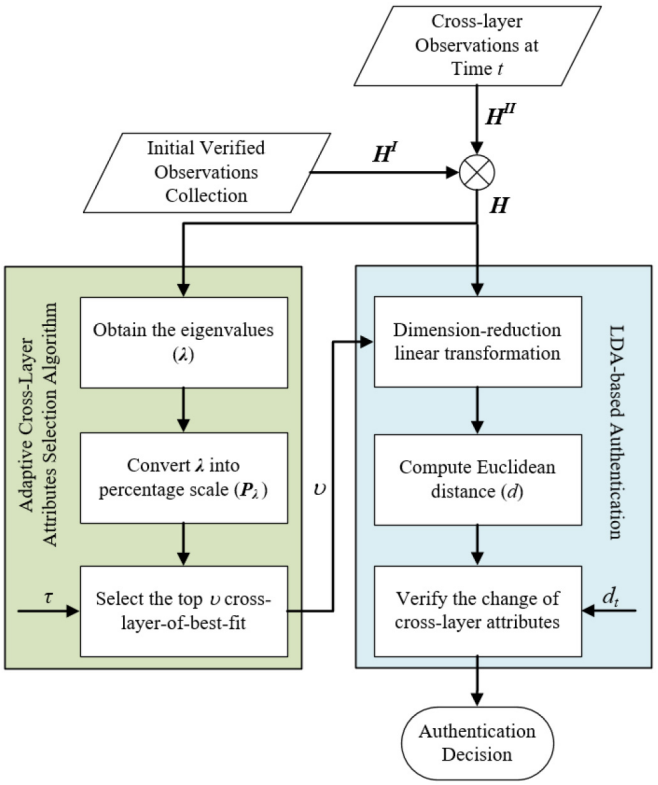

FIGURE 4. Flow chart of the adaptive LDA-based cross-layer authentication scheme.

To summarize both algorithms together, a flow chart of the authentication at instance t is shown below in Fig. 4. In this case, the cross-layer observations ($\boldsymbol{H^{II}}$) collected at instance t before the CH selection and CH switching is combined with the trusted cross-layer attributes ($\boldsymbol{H^I}$) and forms the combined cross-layer attributes set ($\boldsymbol{H}$). The adaptive cross-layer attribute selection algorithm is used to find the minimum amount (υ) of the cross-layer attributes according to τ. The top υ attributes being selected are then passed to the LDA-based authentication scheme where the authentication

TABLE 2. Properties of the testbed UAV.

Weight	3.80 kg
Motor Model	DJI 3515
Operating Frequency	2.400-2.483 GHz
Flight Control	Autopilot

output is generated by using the input $\boldsymbol{H}$ and δ. Given that under an emergency situation when an attacker becomes the new CH of the UAV swarm. One of the potential emergency countermeasures is to abort the mission and return to the base so that the sensitive data will not be compromised or leaked.

IV. PERFORMANCE EVALUATION

In this section, the performance analysis of the proposed scheme is given. A dynamic UAV swarm is constructed by using the MATLAB 2020a to simulate the cross-layer attributes data. We consider a dynamic environment that includes both the urban area and rural area to verify the situational-awareness of our proposed scheme. The flight height is between 150m to 300m in the urban area and 10m to 40m in the suburban area. We mainly consider the path-loss determined using the Friis equation, a fading channel fitting the height–dependent Rician factor in the line-of-sight-condition, and a Rayleigh fading distribution in the non-line-of-sight condition [43], [44]. The Doppler shift is also considered due to the high relative velocity in between each UAV [45]. The cross-layer attributes contain RSSI, CFO and I/Q imbalance from the physical layer, PER from the MAC layer, latitude and longitude from the application layer. The cross-layer attributes are stored into .CSV files to be analyzed in Python 3.8. The DJI Matrice 200 series UAV has been considered as the testbed UAV and the UAV properties are given in Table 2.

To study the performance of our proposed scheme, we consider 3 cases that include 4, 8 and 12 UAVs to represent the potential size of the UAV swarm. We then compare our proposed scheme to the other state-of-the-art light-weight cross-layer authentication techniques for both the accuracy performance and the computational complexity.

A. PERFORMANCE ANALYSIS OF PROPOSED LDA-AIDED AUTHENTICATION SCHEME

1) INFORMATION THRESHOLD (τ)

To understand the relationship between the proposed adaptive cross-layer attribute selection mechanism and τ, we conduct the simulation in Python by using the data harvests from MATLAB and the τ values we choose are between $\tau = 1\%$ and $\tau = 99\%$. The reason that τ cannot reach 100% is that the converted percentage eigenvalue may not add up to 100% after being rounded. Hence, we summarize the τ ranges with the corresponding amount of cross-layer attributes being kept after the dimension reduction for 4 UAVs in Table 3, 8 UAVs in Table 4 and 12 UAVs in Table 5.

TABLE 3. Information threshold range (τ) and the corresponding number of attribute(s) (4 UAVs).

τ range	Number of attribute(s) selected
$\tau < 91\%$	1
$91\% \leq \tau \leq 98\%$	2
$98\% < \tau \leq 99\%$	3

TABLE 4. Information threshold range (τ) and the corresponding number of attribute(s) (8 UAVs).

τ range	Number of attribute(s) selected
$\tau < 82\%$	1
$82\% \leq \tau \leq 98\%$	2
$98\% < \tau \leq 99\%$	3

TABLE 5. Information threshold range (τ) and the corresponding number of attribute(s) (12 UAVs)

τ range	Number of attribute(s) selected
$\tau < 73\%$	1
$73\% \leq \tau \leq 96\%$	2
$96\% < \tau \leq 99\%$	3

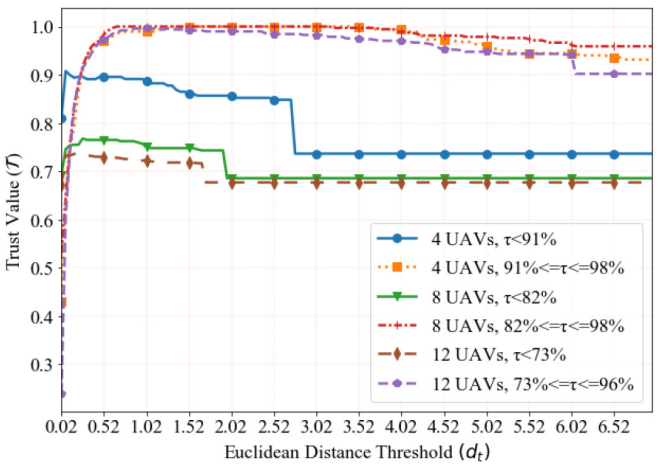

FIGURE 5. The trust value vs. the lower τ ranges.

Among the 6 cross-layer attributes contained in the dataset, only 3 attributes are selected by using our algorithm when 99% of the information is kept for analysis in all 3 scenarios. By using the LDA for dimensionality reduction, the amount of data is shrunk into half of the original data size which ultimately lowers the computational overhead when the estimations are getting bigger.

To further study the relationship between τ and the trust value, we plot all 9 cases as listed in Table 3, Table 4 and Table 5. To make it comparison more clear, we plot two separate figures as shown below.

As shown in Fig. 5, it can be observed that when τ is small, the performance is less accurate and less stable compare to the higher τ value. However, as shown in Fig. 6, it can be shown that when the τ value is at the higher range, there is not much performance increase. Therefore, it can

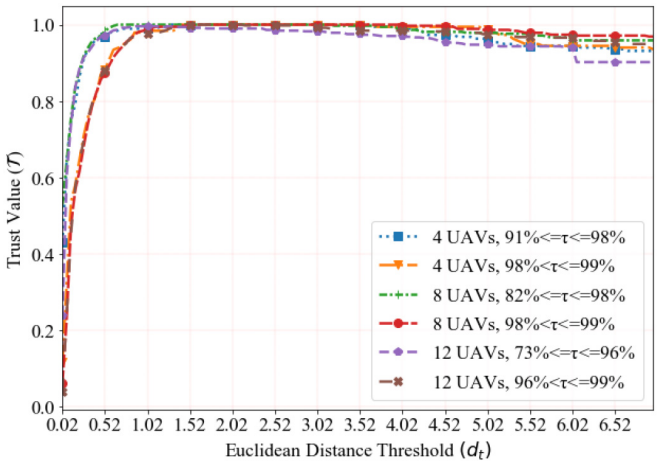

FIGURE 6. The trust value vs. the higher τ ranges.

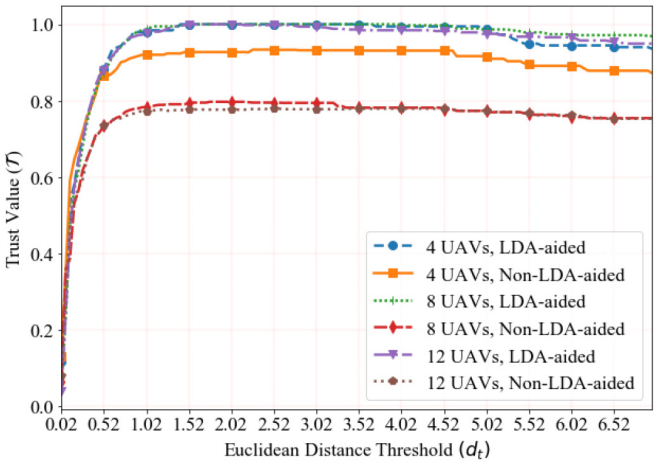

FIGURE 7. Trust Value comparison results of our LDA-based scheme and the non-LDA-based scheme.

TABLE 6. The relationship between δ and other parameters.

Swarm size	τ range	Best $\mathcal{T}$ value	δ value
4 UAVs	$\tau < 91\%$	0.907	0.07
	$91\% \leq \tau \leq 98\%$	1.000	[1.27,3.62]
	$98\% < \tau \leq 99\%$	1.000	[1.42,3.67]
8 UAVs	$\tau < 82\%$	0.765	[0.32,0.67]
	$82\% \leq \tau \leq 98\%$	1.000	[0.67,3.17]
	$98\% < \tau \leq 99\%$	1.000	[1.52,3.97]
12 UAVs	$\tau < 73\%$	0.736	0.27
	$73\% \leq \tau \leq 96\%$	0.996	[0.87,1.12]
	$96\% < \tau \leq 99\%$	1	[1.57,2.12]

be concluded that the computational overhead can be further decreased by adopting the proper τ range in each mission. However, to select the τ value safely, $\tau = 99\%$ can always be used as a starting point. The cross-layer attributes can then be collected after each mission to compute a lower τ value to minimize the computational overhead in future missions.

2) EUCLIDEAN DISTANCE THRESHOLD (δ)

As the security constraint of separating the eavesdropping device from legitimate UAVs, the choice of δ is critical. To study the impact of δ in different scenarios, we use the same Fig. 5 and Fig. 6 as shown in the previous section.

It is demonstrated that δ has a different impact on the trust value of (10) across different scenarios. From the 2 figures above, we can conclude that when δ grows, the common trend of the trust value will rise first, then become stable and decrease at the end. The reason behind this is that when δ is too small, a small change of a legitimate device will be flagged as a spoofing device which increases R_s. Similarly, when δ is too big, the difference between a spoofing device and a legitimate device will only be considered as a normal fluctuation which increases the R_e. The best result for all 3 sizes of UAV swarms are shown in Table 6.

From Table 6, it can be concluded that the optimized δ value is subjective to the environment and the size of the UAV swarm. The reason is that the cross-layer attributes are rescaled after the LDA transformation. To fulfill (11), δ should be selected within the range where the calculated trust value is maximized by using the previously collected cross-layer attributes.

3) LDA-BASED ATTRIBUTES REDUCTION

In Fig. 7, we compare the performance of the proposed LDA-based authentication scheme with the non-LDA-based authentication across the 3 cases that include 4, 8 and 12 UAVs. The non-LDA-based scheme goes through the same process for the Euclidean-distance-based authentication as the proposed scheme. It can be observed from Fig. 7 that the performance of the non-LDA-based authentication becomes less accurate when the number of UAV grows. However, our proposed scheme has stable performance across the different amounts of UAVs. Hence, it can be concluded that the accuracy performance can become more reliable and more stable across different scenarios by eliminating the unnecessary attributes with the help of the LDA.

4) CROSS-LAYER ATTRIBUTES

To test the significance of the cross-layer attributes, we extract separate physical-layer attributes based dataset from the original cross-layer dataset in all 3 scenarios. The LDA process has been applied to the physical-layer attributes only dataset for consistency. The best result of the LDA aided physical-layer attributes only dataset versus the best result of the LDA aided cross-layer attributes dataset are shown in Fig. 8 for all 3 scenarios.

It can be observed from Fig. 8 that the LDA aided physical-layer attributes based dataset carries the same trend as the cross-layer attributes dataset. The performance of the cross-layer attributes dataset is significantly better than the physical-layer attributes only dataset when the number of UAVs grows to 12. More importantly, the trust value of the cross-layer attributes dataset is significantly more stable than the physical-layer attributes only dataset across different scenarios. This proves that the cross-layer attributes are more stable under a dynamic environment and are more

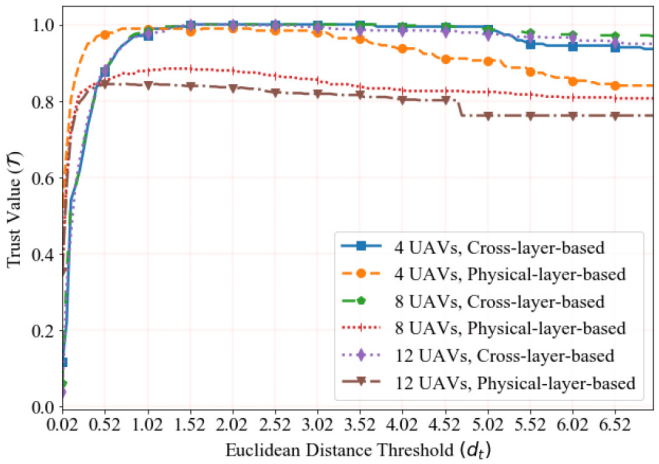

FIGURE 8. Trust Value comparison results between the cross-layer observation and physical-layer observation.

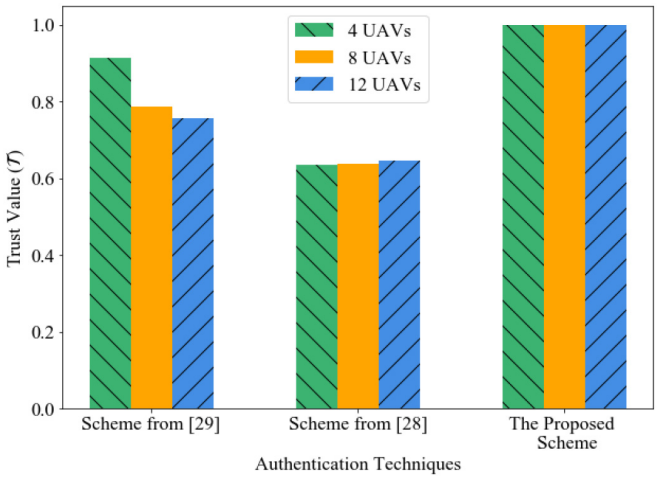

FIGURE 9. Accuracy performance comparison between different state-of-the-art cross-layer authentication techniques.

robust when the number of UAVs increases compares to the physical-layer attributes.

B. PERFORMANCE EVALUATION OF THE PROPOSED LDA-BASED AUTHENTICATION SCHEME COMPARED WITH OTHER CROSS-LAYER AUTHENTICATION TECHNIQUES

In this section, we compare our proposed scheme to the fast authentication scheme for the dynamic sensor networks proposed by Zhang *et al.* [29] and the enhanced cross-layer authentication scheme proposed by Hao *et al.* [28] We first compare the best accuracy performance and then the computational complexity by using the same data collected in the MATLAB.

Fig. 9 characterizes the trust value comparison between our LDA-based authentication scheme and the other state-of-the-art cross-layer light-weight authentication techniques. It can be observed that our proposed scheme achieves a trust value of 1 in all 3 cases which are the highest among all. This demonstrates that the other 2 techniques are not

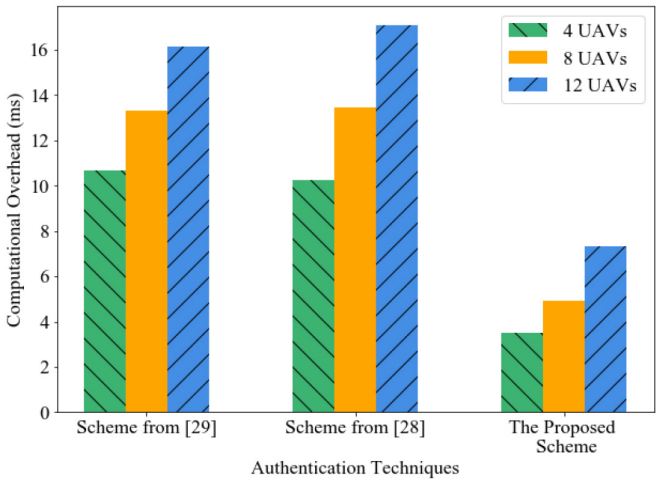

FIGURE 10. Computational complexity comparison between different state-of-the-art cross-layer authentication techniques.

suitable under the UAV network. The high mobility makes the physical layer estimation less reliable and the final decision of the fast authentication for dynamic sensor networks is still based on the physical layer estimation. Similarly, the RSSI collected in the enhanced cross-layer authentication scheme is not reliable. Since only 2 attributes are being selected, the overall stability and reliability are low in our UAV network.

To evaluate the computational complexity of our proposed scheme, the Central Processing Unit (CPU) processing time has been measured. We use an Intel Core i7 6700 CPU to simulate the Intel Core i7 8550U CPU on the DJI Matrice UAV with an on-board computer. The actual computational latency should be a little smaller than our simulation since our platform is marginally less powerful than the actual UAV. To simulate an energy constraint situation, no Graphics Processing Unit (GPU) acceleration has been implemented. The CPU processing time is measured at the nanosecond level and the result is shown in Fig. 10.

As shown in Fig. 10, it is clear that the processing time of the LDA-aided authentication methods is significantly less than the other light-weight authentication scheme. Although the computational overhead increases with respect to the number of devices, it is unlikely to have too many UAVs within the swarm due to the QoS considerations. The reason behind is that the other 2 light-weight authentication methods are still 2-step process while our proposed method forges the cross-layer attributes in a 1-step process. Hence, it is safe to conclude that our proposed scheme can not only maximize the performance but also minimize the computational latency in the UAV network.

V. CONCLUSION

An edge intelligence-enabled safeguarding mechanism has been proposed in this paper to enhance the security in the UAV swarm. This mechanism prevents the spoofing device from becoming the new CH and compromising the UAV

network by forging and deleting the data packets. This multi-dimensional authentication scheme was planted in the on-duty CH to verify that the candidate UAVs are legitimate before the CH selection process and the new CH is still legitimate before the CH switching process. The cross-layer attributes have been utilized to enhance the security by providing more reliable and unique characteristics of each UAV. Our novel LDA-aided authentication scheme increases the trust value while decreasing the computational overhead by eliminating the unnecessary attributes. Since the LDA technique could not decide the number of attributes being left after the dimensionality reduction, a situation-aware attributes selection algorithm has been proposed to select the minimum amount of attributes without jeopardizing the performance. A series of simulations were conducted to demonstrate the impact of different parameters on the authentication performance of our proposed scheme. A comparison with the other state-of-the-art light-weight cross-layer authentication techniques are also included. The results showed that our proposed scheme greatly reduces the number of cross-layer attributes and vastly improves the authentication accuracy while maintaining low computational complexity in the UAV network. In the future, we will consider to implement the proposed mechanism to other networks that involves CH switching such as WSN and VANETs to improve the overall security.

REFERENCES

[1] J. Sun *et al.*, "A data authentication scheme for UAV ad hoc network communication," *J. Supercomput.*, vol. 76, no. 6, pp. 4041–4056, 2020.

[2] C. D'Andrea, A. Garcia-Rodriguez, G. Geraci, L. G. Giordano, and S. Buzzi, "Analysis of UAV communications in cell-free massive MIMO systems," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 133–147, 2020.

[3] H. Shakhatreh *et al.*, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019.

[4] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 60–76, 2020.

[5] S. Bhandari, X. Wang, and R. Lee, "Mobility and location-aware stable clustering scheme for UAV networks," *IEEE Access*, vol. 8, pp. 106364–106372, 2020.

[6] M. Sharma, M. Singh, K. Walia, and K. Kaur, "A comprehensive study of performance parameters for MANET, VANET and FANET," in *Proc. IEEE 10th Annu. Inf. Technol. Electron. Mobile Commun. Conf. (IEMCON)*, Vancouver, BC, Canada, 2019, pp. 0643–0646.

[7] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (FANETs): A survey," *Ad Hoc Netw.*, vol. 11, no. 3, pp. 1254–1270, 2013.

[8] Y. Sun, D. Xu, D. W. K. Ng, L. Dai, and R. Schober, "Optimal 3D-trajectory design and resource allocation for solar-powered UAV communication systems," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 4281–4298, Jun. 2019.

[9] United States Department of Defense, *Unmanned Systems Roadmap* (AD-a475 002). Washington, DC, USA: Dept. Defense, 2007, pp. 2007–2032. [Online]. Available: https://books.google.ca/books?id=OHUqwwEACAAJ

[10] K. A. Hafeez, L. Zhao, Z. Liao, and B. N.-W. Ma, "A fuzzy-logic-based cluster head selection algorithm in VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, 2012, pp. 203–207.

[11] M. Alrashidi, N. Nasri, S. Khediri, and A. Kachouri, "Energy-efficiency clustering and data collection for wireless sensor networks in industry 4.0," *J. Ambient Intell. Humanized Comput.*, pp. 1–8, May 2020. [Online]. Available: https://doi.org/10.1007/s12652-020-02146-0

[12] E. Bertran and A. Sànchez-Cerdà, "On the tradeoff between electrical power consumption and flight performance in fixed-wing UAV autopilots," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 8832–8840, Nov. 2016.

[13] B. Uragun, "Energy efficiency for unmanned aerial vehicles," in *Proc. 10th Int. Conf. Mach. Learn. Appl. Workshops*, vol. 2. Honolulu, HI, USA, 2011, pp. 316–320.

[14] Y. Cai, Z. Wei, R. Li, D. W. K. Ng, and J. Yuan, "Joint trajectory and resource allocation design for energy-efficient secure UAV communication systems," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4536–4553, Jul. 2020.

[15] J. Liu *et al.*, "A weighted clustering algorithm based on node energy for multi-UAV ad hoc networks," in *Proc. 10th Int. Conf. Inf. Opt. Photon.*, vol. 10964, Nov. 2018.

[16] J. Jiménez, G. C. Gonzalez, and M. U. Pascual, "Connection mechanism for energy-efficient peer-to-peer networks," U.S. Patent 10 075 519, Sep. 11, 2018.

[17] R. B. Thompson and P. Thulasiraman, "Confidential and authenticated communications in a large fixed-wing UAV swarm," in *Proc. IEEE 15th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, 2016, pp. 375–382.

[18] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, 2016, pp. 1–6.

[19] N. Zhang *et al.*, "Physical-layer authentication for Internet of Things via WFRFT-based Gaussian tag embedding," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9001–9010, Sep. 2020.

[20] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surveys*, vol. 45, no. 1, pp. 1–29, 2012.

[21] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[22] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[23] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[24] Z. Xiao, H. Fang, and X. Wang, "Distributed nonlinear polynomial graph filter and its output graph spectrum: Filter analysis and design," *IEEE Trans. Signal Process.*, vol. 69, pp. 1725–1739, Feb. 2021, doi: 10.1109/TSP.2021.3054523

[25] P. Hao, X. Wang, and A. Behnad, "Performance enhancement of I/Q imbalance based wireless device authentication through collaboration of multiple receivers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, 2014, pp. 939–944.

[26] X. H. Cao, X. Du, and E. P. Ratazzi, "A light-weight authentication scheme for air force Internet of Things," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, 2019, pp. 1–6.

[27] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5G and beyond wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 55–61, Oct. 2019.

[28] P. Hao, X. Wang, and A. Refaey, "An enhanced cross-layer authentication mechanism for wireless communications based on PER and RSSI," in *Proc. 13th Can. Workshop Inf. Theory*, Toronto, ON, Canada, 2013, pp. 44–48.

[29] Z. Zhang, N. Li, S. Xia, and X. Tao, "Fast cross layer authentication scheme for dynamic wireless network," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Seoul, South Korea, 2020, pp. 1–6.

[30] J. Sjöberg *et al.*, *Nonlinear Black-Box Modeling in System Identification: A Unified Overview*. Linköping, Sweden: Linköping Univ., 1995.

[31] T. Wang, C.-K. Wen, H. Wang, F. Gao, T. Jiang, and S. Jin, "Deep learning for wireless physical layer: Opportunities and challenges," *China Commun.*, vol. 14, no. 11, pp. 92–111, 2017.

[32] T. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 563–575, Dec. 2017.
[33] Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou, "The individual identification method of wireless device based on dimensionality reduction and machine learning," *J. Supercomput.*, vol. 75, no. 6, pp. 3010–3027, 2019.
[34] S. Fenanir, F. Semchedine, and A. Baadache, "A machine learning-based lightweight intrusion detection system for the Internet of Things," *Revue d'Intelligence Artificielle*, vol. 33, no. 3, pp. 203–211, 2019.
[35] L. Rokach and O. Maimon, "Top-down induction of decision trees classifiers—A survey," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 35, no. 4, pp. 476–487, Nov. 2005.
[36] A. Verma and V. Ranga, "Statistical analysis of CIDDS-001 dataset for network intrusion detection systems using distance-based machine learning," *Procedia Comput. Sci.*, vol. 125, pp. 709–716, Jan. 2018. [Online]. Available: https://doi.org/10.1016/j.procs.2017.12.091
[37] A. Marcano-Cedeño, J. Quintanilla-Domínguez, M. G. Cortina-Januchs, and D. Andina, "Feature selection using sequential forward selection and classification applying artificial metaplasticity neural network," in *Proc. 36th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Glendale, AZ, USA, 2010, pp. 2845–2850.
[38] P. Bermejo, J. A. Gámez, and J. M. Puerta, "Incremental wrapper-based subset selection with replacement: An advantageous alternative to sequential forward selection," in *Proc. IEEE Symp. Comput. Intell. Data Min.*, Nashville, TN, USA, 2009, pp. 367–374.
[39] A. Tharwat, T. Gaber, A. Ibrahim, and A. E. Hassanien, "Linear discriminant analysis: A detailed tutorial," *AI Commun.*, vol. 30, no. 2, pp. 169–190, 2017.
[40] C. Wang and B. Jiang, "On the dimension effect of regularized linear discriminant analysis," *Electron. J. Stat.*, vol. 12, no. 2, pp. 2709–2742, 2018.
[41] T. Li, S. Zhu, and M. Ogihara, "Using discriminant analysis for multi-class classification: An experimental investigation," *Knowl. Inf. Syst.*, vol. 10, no. 4, pp. 453–472, 2006.
[42] R. E. Prieto, "A general solution to the maximization of the multidimensional generalized Rayleigh quotient used in linear discriminant analysis for signal classification," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, vol. 6. Hong Kong, 2003, pp. 157–160.
[43] A. A. Khuwaja, Y. Chen, N. Zhao, M.-S. Alouini, and P. Dobbins, "A survey of channel modeling for UAV communications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2804–2821, 4th Quart., 2018.
[44] D. W. Matolak and U.-C. Fiebig, "UAV channel models: Review and future research," in *Proc. 13th Eur. Conf. Antennas Propag. (EuCAP)*, Krakow, Poland, 2019, pp. 1–5.
[45] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

HUANCHI WANG (Graduate Student Member, IEEE) received the B.E.Sc degree major in electrical engineering from Western University, Canada, in 2019, where he is currently pursuing the M.E.Sc. degree with the Department of Electrical and Computer Engineering. His research interests include the intelligent authentication and distributed security provisioning.

HE FANG (Member, IEEE) received the B.Sc. and Ph.D. degrees in applied mathematics from Fujian Normal University, Fuzhou, China, in 2012 and 2018, respectively, and the Ph.D. degree in electrical and computer engineering from the Department of Electrical and Computer Engineering, Western University, Canada, in 2020.

She is currently a Postdoctoral Associate with Western University. Her research interests include intelligent security provisioning, machine learning, and distributed optimization and collaboration techniques. One focus of her current research is on the development of new machine learning enabled authentication schemes through utilization of time-varying wireless environment for security enhancement. She is also working on distributed security management in IoT and blockchain systems under practical network constraints.

XIANBIN WANG (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001.

He is a Professor and a Tier-1 Canada Research Chair with Western University, Canada. Prior to joining Western, he was with Communications Research Centre Canada (CRC) as a Research Scientist/Senior Research Scientist from July 2002 and December 2007. From January 2001 to July 2002, he was a System Designer with STMicroelectronics. He has over 450 highly cited journal and conference papers, in addition to 30 granted and pending patents and several standard contributions. His current research interests include 5G/6G technologies, Internet-of-Things, communications security, machine learning, and intelligent communications.

Dr. Wang has received many awards and recognitions, including the Canada Research Chair, CRC President's Excellence Award, the Canadian Federal Government Public Service Award, the Ontario Early Researcher Award, and six IEEE Best Paper Awards. He currently serves/has served as the editor-in-chief, an associate editor-in-chief, an editor/associate editor for over ten journals. He was involved in many IEEE conferences, including GLOBECOM, ICC, VTC, PIMRC, WCNC, and CWIT, in different roles, such as a symposium chair, a tutorial instructor, a track chair, a session chair, a TPC co-chair, and a keynote speaker. He has been nominated as an IEEE Distinguished Lecturer several times during the last ten years. He is currently serving as the Chair of IEEE London Section and the Chair of ComSoc Signal Processing and Computing for Communications Technical Committee. He is a Fellow of Canadian Academy of Engineering, Engineering Institute of Canada, and an IEEE Distinguished Lecturer.