ACCEPTED FROM OPEN CALL

Security Challenges and Potential Solutions in Aerial-Terrestrial Wireless Networking

Keshav Sood, Dinh Duc Nha Nguyen, Youyang Qu, Lei Cui, Kallol Krishna Karmakar, and Shui Yu

Abstract

Integration of unmanned aerial vehicles (UAVs) with terrestrial networks form an aerial-terrestrial wireless networking concept. Particularly, the UAVs are composed of Internet of Things sensors (IoTs) and they also are typically known as flying IoTs. These are used to collect real-time data for diverse network's applications in order to make optimal network performance and secure management decisions. In this networking domain, cyber-attacks on UAVs sensors are rapidly increasing and the attacks on sensors inevitably raise the data sparsity issue, means the recorded data, by drones or UAVs, could be often incomplete and even sparse enough too. This impacts the performance evaluation of this networking composed of flying and ground base stations. This paper explores the *data sparsity* issue in context of the integration of aerial-terrestrial wireless networks. Critical challenges and potential high-level solutions are also proposed to enhance the security and performance of networks.

Introduction

The unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UASs), both are widely known as Drones. UAVs are now new emerging flying Internet of Things (IoTs). Flying IoTs is the new form of emerging new IoT devices essentially called cognitive drone platform with the full network connectivity and intelligent cognitive computing capabilities to fly in the sky to recognize and track objects to control them [1]. The coexistence of drones with terrestrial networks complements the capabilities of the current terrestrial wireless communication networks in many ways [2]. For example, drones are used as flying aerial base stations to facilitate rapid information dissemination among ground devices to improve the reliability of wireless links in device-to-device (D2D) and vehicle-to-vehicle (V2V) communications. Overall, in many ways UAVs alleviate the load on the terrestrial networks. A typical high-level architecture of aerial-terrestrial wireless networking concept is shown in Fig. 1.

The rapid evolution of UAVs and terrestrial networks has been made possible due to smart sensors based IoT technology and its applications as well as intelligent nodes using Artificial Intelligence (AI) on the networks. For any real-time effective decision-making the time series data collection and analysis of that real-time data series is the first step. There are many sensors installed in UAVs or UAVs swarm networks which carry large streams of data which can be used in performing various analytical tasks in real time applications. Unfortunately, the data collected by a diversity of sensors cannot be guaranteed for its availability all the time due to several factors which include unexpected weather, power supply, fault in hardware, etc. Also, cyber-attacks on UAVs are another critical factor due to which data cannot be available (or available but maliciously manipulated) all the time. This leads to missing information, i.e., inaccurate reading, missing values, etc. which produces a difference in standard deviation for a selected data. Also, this leads to the problem of being left with sparse and incomplete data which makes the dataset too complicated to be used for scientific purposes. This is known as *data sparsity* issues.

To better comprehend this in aerial-terrestrial wireless networking, we start the concept with an example. It is known that the terrestrial base stations cannot be deployed in rural areas, deserts, harsh environment, etc. hence the concept of integrating them with wireless networks essentially gives birth to the concept the ground-to-air wireless networks and vice versa [3]. This fulfilled the envision of the concept of anytime and anywhere network access in wireless domains via Vertical Heterogeneous Network (VHetNet) concept. However, due to the co-existing of various wireless connectivity, hardware and software variations, etc. this integrated network creates a multi-tier topology, with heterogeneous entities, which is vulnerable to malicious attacks [4, 5]. For example, the wireless data link contains vital information such as location/position of a drone, distance and location to target, payload information, etc. A potential threat is to break down the data link connection between the Ground Control Station (GCS) and backbone UAV. Further this connection could be eavesdropped and hence can be maliciously controlled or infected with malware [2]. In such cases the attacker could alter the data samples received by the remote server for data processing or the remote server received very little data means the received data is sparse. Also, mmWave signal propagations may be prone to some impairments including channel fluctuations eventually the channel sparsity occurs as a nature of channels [6]. This can affect the accurate positioning of the UAVs (to accurately determine the geo-location of UAVs) and the detection of unauthorized intrusion (via AI models) into the airspace in the presence of data sparsity.

We note that the combination of mmWave communication and massive MIMO-based approaches are used to optimize the UAVs positioning by optimizing the link capacity which optimiz-

Keshav Sood and Dinh Duc Nha Nguyen are with the School of Information Technology Deakin University, Australia.
Youyang Qu is with Data61, Australia.
Lei Cui is with Shandong Computer Science Center (National Supercomputer Center in Jinan), China.
Kallol Krishna Karmakar is with The University of Newcastle, Australia.
Shui Yu is with the University of Technology Sydney, Australia.

Digital Object Identifier: 10.1109/IOTM.001.2300024

es the physical layer security of UAV swarms as well [7]. The authors in [8] utilized the uniqueness of beam pattern features in mmWave–enabled devices and proposed a scalable physical layer security mechanism for the detection of wireless spoofing attacks. When a new node enters the network, the proposed algorithm uses the unique beam pattern features to determine the anomaly. We believe the similar approach can be adopted in UAVs domain to accurately determine the UAVs positioning. However, it does not address the data sparsity issue at all. Eventually, this could also lead to a problem of data protection and leakage of confidential information, especially on large data sets. Also, it impacts the network resilience and reliability of coexisting drone and terrestrial networks.

Our contributions in this article are below.

1. To better comprehend the data sparsity issue, multiple threat scenarios are shown to prove that the data sparsity is a critical issue (causing both due to cyber-attacks and in other legitimate network failure cases) which affects the decision-making process of such network's applications. Critical challenges and potential solutions, related to network security, are explored with high level discussion is given.
2. Using a real data set, results have been given to demonstrate that the data sparsity impacts the decision making of AI models. Potential solution is also validated.

In network security, the intelligent machine learning models are used for authentication and intrusion detection. The data sparsity causes problems like overfitting and suboptimal results in learning models impacts the accuracy and reliability of the machine learning models. The article proposes a reasonable theoretical approach to recovering missing data that will be fed into AI models. UAVs extensively use AI models for data analytics; hence the proposed work has numerous advantages in this domain. Furthermore, the high-level UAV-IoT architecture is shown in [4]. The authors discussed critical challenges in multi-UAV-based heterogeneous flying ad hoc networks (FANET), including the formulation of a stable network structure. We identified that this architecture can be considered as a reference architecture to investigate the data sparsity issue following which our work can be aligned and integrated.

UAV's Security in General

The formation of aerial-terrestrial wireless networks, with the complementary technologies like 5G, enhances the coverage, scalability, and other network performance KPIs, however, on the other hand this introduced new security vulnerabilities (example, the end customer's smart device unknowingly can be used as botnet). The adversaries can intercept the signal or data being transmitted between the drone and a base station, to a great extent the adversaries could use the UAVs to capture physical control of a smart device, using it as a backdoor into a company's network. Further from one base station to another, this hack can be easily propagated. Also, in flight the hackers can inject misleading or phishing sensor streams/information to change the content which disrupt the autonomous decision-making capability of the applications/UAVs.

Take a critical example of drones without any active involvement of pilots in battlefield or disastrous situations. The UAVs fly with GPS-aided navigation, but the loss of GPS signal have a great impact to disruption of the drone operation. Although it can be addressed by using different localization and mapping algorithms, however these algorithms do not work optimally as they have limitations based on environment texture, reflectivity, types, and the quality of sensors used, eventually these algorithms cannot work which can lead to drones getting lost or colliding. Nevertheless, to periodically convey the location and extract activity of the drone, the wireless radio beacon signal remains a necessary requirement. In totality, network services also have an impact on cost and operations and therefore to be able to handle all these factors is a significant challenge.

Furthermore, the applications of Drones in both industrial

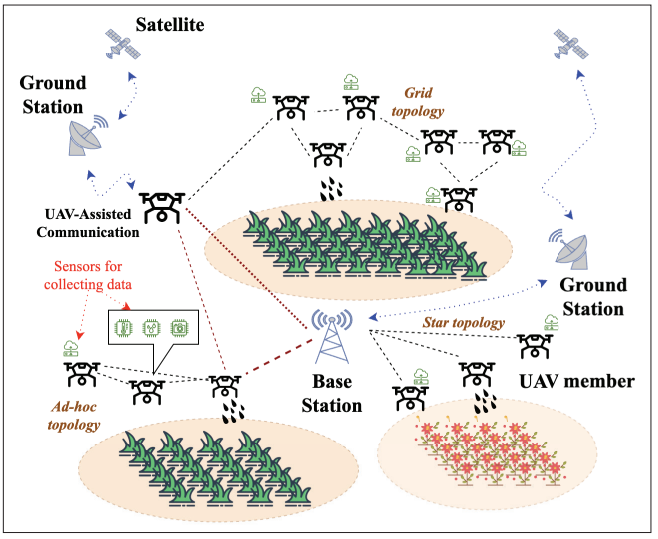

FIGURE 1. A typical illustration of aerial-terrestrial (UAV-terrestrial) networks.

(operational technology or OT networks) and military operations are growing at a fast pace. In the former domain, drones can be used by adversaries for surveillance, capture data or cause infrastructure damage by collision. In the military domain, the widespread use of militarized drones (in global warfare) pushed researchers to investigate advanced tools and methods to attack drones (potentially enemy's drones). Note that the industrial drones have lower security controls than military drones therefore the OT sector is more vulnerable where, for example, hacking drones in flight is common. Drones carry payload to conduct surveillance. In worst case scenarios the compromised drones carry malicious payload and easily can fetch the victims' sensitive information via Bluetooth sniffing. Also, drones or UAVs can be routed to a wrong destination with GPS spoofing. On top of this, a malicious WiFi network can be set up which imitates an organization's WiFi network. With this way adversaries can take control of all the traffic. Although there are some solutions (such as Geofencing, Sound Wave detection like radar, or other scanning methods) to counter drones from cyber-attacks, it seems that the vision of drone attacks on OT sectors is far-fetched and needs to be considered in an effective security architectures. This can be achieved easily with more transparency into the network from regulators side.[1]

Functional Decomposition and Data-Flow of UAVs or UASs

Firstly, in Fig. 2 we present a general operational illustration to understand the Functional Decomposition and Dataflow of UAVs. It is decomposed into four parts: a) Navigation module (analyze sensory data for autopilot decisions), a) Data Collection (collect raw data for mission and UAVs status), c) Communication (send and receive the control signal and UAS data), and d) Flight Control (interact with other modules to preserve correct UAVs flight state).[2]

1. *Navigation module:* This is responsible for correctly stabilizing and navigating the UAS along a predefined path. This is performed either by the auto-pilot function in an autonomous way or by a manual control using a handheld controller over a wireless network setting. For accurate navigation, the auto-pilot function uses sensing data generated by the navigational sensors to accomplish its mission. Whereas in manual control operation, line of sight communication is used by a user. Further, a central flight controller is used to control both these modes of navigational operation. The central flight controller is mainly responsible for processing sensory data. Some potential attacks on navigational modes are forced

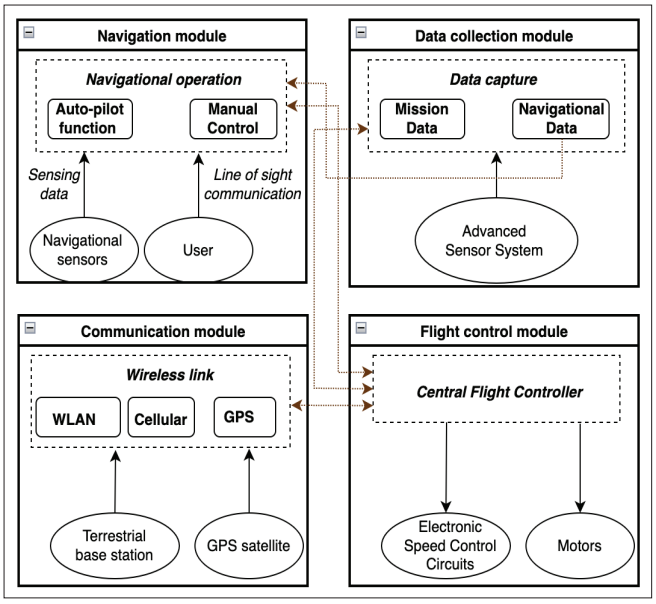

FIGURE 2. Functional decomposition and data-flow. Here, the sensors are capturing information and the attackers can also collect and analyze the information and can affect any service attribute. Some common countermeasures are use of strong encryption methods, use of physical unclonable features (PUF) based systems, checking metadata along with the data is another option. However, autonomous solutions are needed to predict the missing sensor values which will not impact the decision-making ability of controllers. This is a critical research issue and related threats are discussed below.

deadlock, fault injection, and authentication bypass. For example, the malicious sensory data injected by any means can corrupt the navigational data which greatly lead to a forced deadlock. Eventually, the navigation mechanism may be affected by this attack which may lead to disastrous consequences such as failure of the autopilot software, resulting in a crash or fly-away.

2. *Data Collection Module:* This acquires raw data from sensors during the mission and processes that data into necessary control data to accomplish the drone objective. The sensor interacts with the environment to sense its surroundings. Sensor data is divided into two categories, navigational and mission specific related data categories. For navigational measurements sensors such as magnetic, accelerometers, and gyroscope sensors provide an environmental perception for the real-time UAVs navigation such as position, stabilization, orientation, etc. Further to accomplish the drone's objective sensors are used in infrared or night vision cameras to take video and still images. Many other sensors are used for different purposes and the data is then sent to the navigational and flight control unit for further processing. Potential attacks, due to sensor stream failures, are malicious logic insertion, exploiting trust in clients, etc. leads to autopilot error/fail or crash.
3. *Communication Module:* This is responsible for transmitting and receiving information, either from the user or from GPS satellites or terrestrial base stations. The three primary wireless communication links used for communication are:
   –Wireless network link based on IEEE 802.11 2.4GHz channel for line-of-sight communication with the UAVs
   –Cellular network to control the UAVs remotely
   –Finally links via GPS satellites. Potential attacks can be replay attack, spoofing, cross layer attack, interception (eavesdropping), authentication bypass, etc. which leads to resource leakage and failure of control systems.
4. *Flight Control Module (or central flight controller):* The module is responsible for processing the data received from multiple sensors as well as any wireless communication sensor data into electrical signals for the UAVs control circuits. This is also responsible for bidirectional communication between all modules (data collection, communication, and navigation modules).

Critical Threats or Solutions

Threat Scenario 1 (faulty, legitimate and attack sensor streams): UAVs work in diverse and dynamic environmental conditions which affects the UAVs sensor behaviors to the mission critical operation. Also, these sensors are vulnerable to malicious attacks and can be compromised which eventually increases the risk of cyber-attacks, threats and introduces vulnerabilities. For example, in UAVs, these faulty sensor measurements or computation of faulty or compromised data may mislead the behavior and operation of the navigation module. Hence, guaranteeing the sensor's correct operation and predicting malfunctions, etc. is essential. To better comprehend this, three possible events where sensors may generate faulty and compromised malicious sensor streams are discussed below.

In the first case, faulty readings or measurements can come through from genuinely faulty sensors, this is typically known as legitimate behavior, but sensor failure condition. In the second case, any unprecedented change may be recorded, for example, the temperature sensor to monitor the temperature is capturing the temperature of any other object sitting in its path. This is termed as faulty behavior which also impacts the intelligent decision-making ability of UAVs sensing system. In the third case, any malicious activity or event such as: attacks on UAVs or sensors, tampering the sensor device etc. will transmit conflicting information which also greatly impacts the intelligent decisions making ability of drones, e.g., the path diversions or poor navigation due to cyber-attacks impacts the autonomous decision making via drones. Therefore, it is vital to accurately differentiate the UAVs sensors' behavior. This is more critical when UAVs work in critical operational sectors (example military) and have a high degree of autonomy.

Potential solution: Researchers have proposed an approach based on Spatial Correlation and Moran *I* index theory [9]. The approach calculates the correlation of sensor from neighboring sensors. The approach works on a natural phenomenon of data, means that if any sensor is legitimately faulty will generate faulty data and the system will generate an outlier, however, data readings or measurement from its neighbors' sensors will not be the same. This is because it is highly unlikely that at the same time the neighbors' IoT sensors will be faulty too. In scenarios where neighbors' sensors are faulty too there would be more outliers detected. Finally, in attack scenarios, several neighborhood sensors placed near or next to the victim node will generate outliers at significant levels. Although the approach works better in both static and mobile sensor scenarios, there are key limitations of this work. Fundamentally, the solution is not applicable in scenarios where co-location of sensors may not be the criteria for all sensor domains. This assumption needs to relax to enable the approach out of this research setting.

Threat Scenario 2 (forecasting with missing data): UAVs are widely used for real-time monitoring of data. The generated time series data is used for forecasting or prediction in many fields such as traffic flow forecasting, monitoring disastrous situations, and other fields. The integration of terrestrial networks sparks additional heterogeneity which impacts multiple areas in security such as authentication while roaming or in static mode. Due to cyber-attacks or any event discussed in threat 1, it is possible that the collected time series data include missing values. If the computational model cannot correctly deal with this missing data information, there will be errors accumulated during the training process, resulting in incorrect, false, or misleading, or low prediction outcomes. Consider a scenario where the navigation module takes signals from the data collection module (Fig. 2) for autopilot to work or navigate the

device accurately. The accurate classification by machine learning model drops dramatically in the presence of incomplete or imbalanced data, known as dataset with missing data values. The problem is more challenging in high dimensional data classification scenarios. This issue is more challenging when the UAVs do not have autonomy or only have partial autonomy and hence, they pass the sensor streams (with missing values) to ground base stations via terrestrial network. The terrestrial network communication further adds path loss which further degrades the signal quality and makes the process at remote data server much more challenging.

Potential solution: A Fuzzy-based Information Decomposition (FID) algorithm is proposed by the authors in [9]. The algorithm recovers the missing values as well as redistributes the imbalanced training data. The workflow is decomposed into two parts: weighting and recovery, the former part quantifies the data contribution, and the later part estimates the missing values considering the contribution of the observed data. FID employs the fuzzy membership function approach. Based on the observed data, the discrete universe values are computed relies on the minimum values, maximum values, and the number of recovered data. Then, the fuzzy set theory is applied to determine the membership degree of recovered data and the contribution weight. Finally, the missing data values are estimated. The proposed work can be improved in many ways. Firstly, the classification accuracy can be improved by considering the correlation among different column vectors, further the degree of the imbalance and percentage of missing values across multi-class datasets is a challenging direction.

Threat Scenario 3 (authentication during roaming): The next generation networks, due to SDN-NFV, are more flexible and add attractive features to authenticate a User Equipment (UE) or UAV in this case. In certain mobile scenarios UAVs capture data from large geographical areas. It is possible that UAVs leave one network or terrestrial network zone and enter into the another terrestrial network zone. In such a case offloading or handover is needed but even before that it should be ensured that the legitimate UAV is entering in the new network zone. The authentication and/or authorization should be performed independently by the external network operators even before the primary network allows a UAV to connect to the external network to request the external network perform a secondary authentication/authorization and only permit connectivity after the external network approves [11].

It can be seen from Fig. 3 that to provide seamless network connectivity to mobile UAVs, the offloading of traffic is needed in certain cases, for example drones fly from one zone to another, etc. The offloading is essential within the same network cells as well as when a drone moves from one network domain to another network domain/s. It is typically termed a horizontal and vertical handover/roaming, respectively. The first one is understood as UAVs mobility across different cells/zones administered by the same organization. Whereas vertical network roaming is understood as end-device mobility across different administrative domains, regardless of whether it is in the same country or not. In critical scenarios such as military operations in fields during war or while disaster management, seamless connectivity is the fundamental requirement. Drones are often used for continuous surveillance and monitoring of humans and assets in multiple scenarios and roaming is inevitable. As seen in Fig. 3, a UAV is moving from Zone *A* to Zone *B*. The service provider *A* provides the channel connectivity to this vehicle via base station using cellular technology. Whereas Zone *B*'s service provider provides connectivity to this vehicle via satellite links (note the technologies as well as service providers are different).

It is worth noting that before the network providers allow successful offloading the drones should only be allowed to enter from home to foreign networks after validating their authenticity. The authentication sessions were exchanged for seamless offloading/mobility management between a home

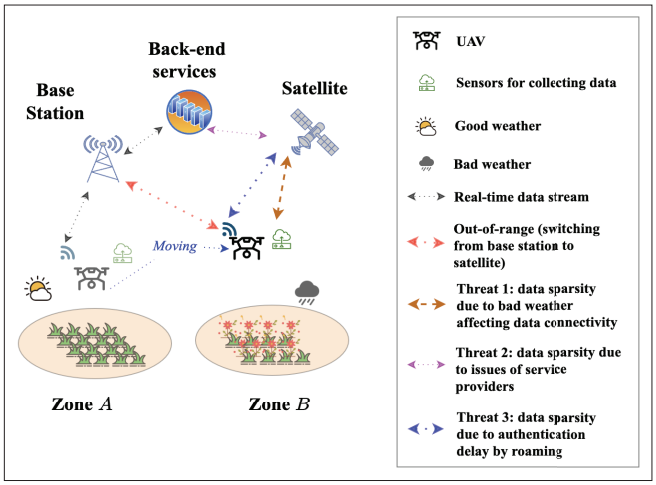

FIGURE 3. Critical scenarios of UAV's mobility and data sparsity.

network and a foreign network. The heterogeneous network connectivity such as drones connect to terrestrial networks, also drones and terrestrial networks use multiple technologies, protocols, multi-administrative domains etc. impacts on the authentication process, i.e. increases the authentication time. Further due to the path loss and data sparsity issue, drones cannot seamlessly operate and perform autonomous mission critical operations. The drone may simply lose the connectivity which may have devastating impacts in certain critical situations.

Potential solution: Unfortunately, initiatives particularly related to data sparsity in drones as well as authentication while roaming are not well explored. Nevertheless, some ongoing efforts in the IoT domain by the IETF working group IPv6 over LP-WAN are reported. This group deals with the IoT operations in inter-operability, to establish trust, across various heterogeneous communication networks. Further, the LoRaWAN architecture (version 1.1) also provides handover support while nodes are roaming across multiple networks, however, needs critical agreement negotiations between multiple organizations or sectors in an ad-hoc manner, case by case, to exchange data in a secure manner. Therefore, roaming in itself is very difficult in multi-operator-based communication networks practice, let alone the authentication challenge in drone-terrestrial networks due to data sparsity. The existing literature does not fully cover the issue of authentication of UAVs device during vertical roaming. Further the issue of data sparsity can fuel the fire, particularly in inter-domain communication, to a great extent from both roaming and authentication aspects [12, 13].

Threat Scenario 4 (channel-less authentication): For accurate identification and tracking of drones, for reliable and secure drone network operation, many ongoing research efforts are reported in the existing literature. The researchers argue the necessity of a tamper resistant unique identifier for drones for various purposes such as identity and location validation for UAV-Network, etc. [14]. This unique identifier is expected to have unique features such as details of drone owner as well as pilot details. These details strengthen the security as well as they established a trust, i.e., responsibility and liability. The FAA's ARC committee (Aviation Rule-making Committee)[3] mentioned that this could be the responsibility of cellular networks to complete and broadcast identification and network tracking capabilities as they can easily provide or assist with drone identification, authorization, and geofencing. Interestingly, the cellular network uses International Mobile Equipment Identity (IMEI) to identify the mobile device. Further to determine the user, they use the International Mobile Subscriber Identity (IMSI) number. These details are embedded in the SIM card and ensures a tamper resistant solution for drone identification. Further, authorization and authentication based on

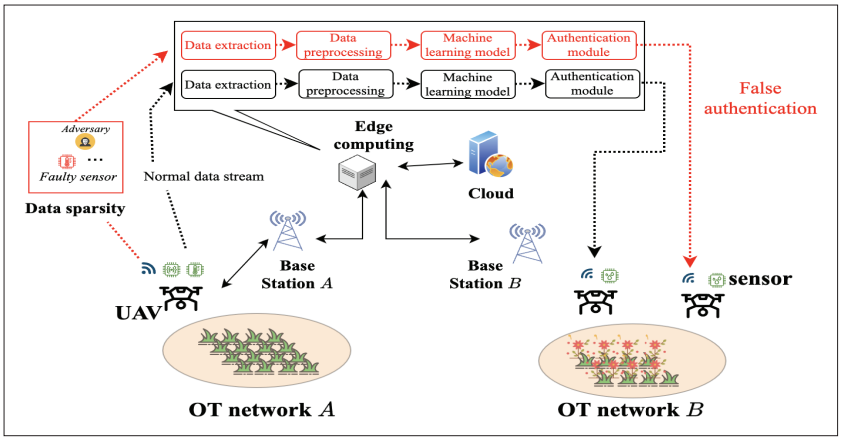

FIGURE 4. The impact of missing sensor stream on authentication.

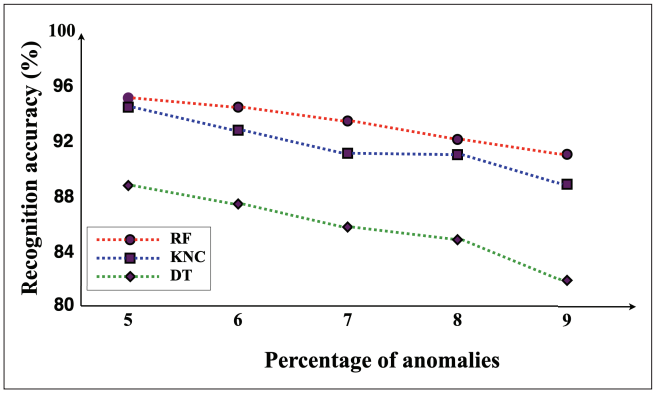

FIGURE 5. Machine learning models' performance at varying degree of data sparsity. It is seen that the increase of noise level or data sparsity reduces the model's accuracy of anomaly detection. At lower values of noise, the detection accuracy is 94.77% of the RF and KNN and 89.32% of DT. Now, as the noise percentage increases, the three machine learning models performance dropped significantly. The DT algorithm shows the highest decrease around 7.41%, while the KNN still has the better performance (approximately 3%).

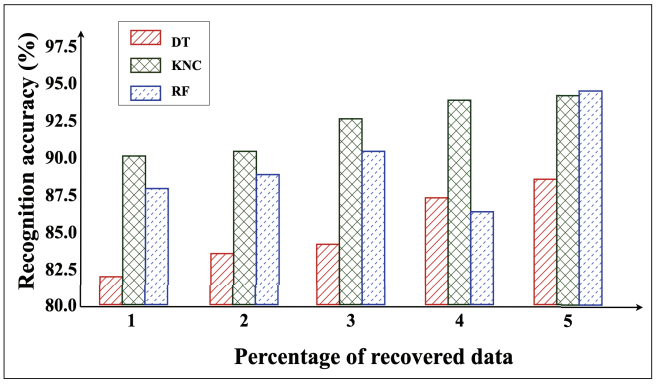

FIGURE 6. The performance of FID scheme to recover missed data values. The result shows that FID calculates the contribution weight based on observed data and predicts the compromised data values. The recovered data is tested with three machine learning models to evaluate the effectiveness of the FID approach. The FID has successfully recovered the sparse data at varying degree of sparsity, the detection accuracy is also calculated.

these unique features can provide a robust and secure way to bootstrap certificate-based solutions to identify drones, pilots, and individual drone operations.

For drone identification, the solution can be divided into two categories; local broadcast solutions and network publishing solutions, both can be supported by cellular networks without the need of any specialized receivers. In the first category, LTE sidelink V2X communication capabilities that can be integrated into mobile chipsets, and in the solutions in the second category are often supported by the data connectivity provided to mobile subscribers. This is an effective way to use secure channels as well as to keep the information encrypted. For drone tracking, the commonly used approach is the use of GNSS systems or mobile positioning system (MPS) through which UAVs obtain their positional information with high accuracy and precision. This is then communicated to a central server for whole network application management. However, from a security aspect, adversaries can easily alter the telemetry data. Consider a scenario, due to data sparsity, in which the communication between the UAVs and IT network is broken, but it is critical to authenticate a remote UAV (Fig. 4). In this case, the need for channel-less authentication schemes are expected.

Potential solution: Recently, in [15] the authors have proposed a solution which can effectively work in authentication of nodes in the absence of a communication channel. The work is not in the aerial-terrestrial domain, but could be an interesting base for researchers in the domain of authentication of remote nodes in an is-landed scenario.

Experiments and Evaluations

We demonstrate that

- The data sparsity impacts the decision making of AI models
- FID based approach is a promising solution

The testing platform is set up on Google Colab, Python 3.7.13 and Tensorflow 2.8.0, (Tesla T4, CUDA version 11.2, single CPU, 26GB RAM, dual cores Intel(R) Xeon(R) CPU @ 2.30GHz on a socket with 2 threads per core). We used Random Forest Classifier (RF) with *n*_estimators = 10 $, *random_state* = 0, K-Neighbors Classifier (KNN or KNC) with *n*_neighbors = 5, and Decision Tree Classifier (DT) with *random_state* = 0. The real dataset used is a collection of Spanish road traffic images captured by UAVs for the purpose of training artificial intelligence algorithms.[4] Due to resource constraints, only a portion of the dataset is used in the experiments which contains 461 images.[5] The data set, source code, and the detailed description of FID model is shared via the GitHub link.[6]

The Gaussian noise values are added in the data values to simulate that an adversary attacks the data. This data is considered as sparse data which varies from 5% to 9%. Then, machine learning models classify these data values. The result is shown in Fig. 5. This simple experiment validates that the sparse data set has clear impact on this UAVs application domain means that the attacked UAVs sensor data impacts the normal cyber-security defense operations.

To demonstrate the effectiveness of the FID method, the approach is employed to estimate/recover the compromised data values. The implementation result is shown in Fig. 6. It is seen that RF achieves the highest detection accuracy (94.55%) at 5% of recovered data. The results show that the performance of three models has increased with FID, even with the sparse data. It proves that the FID can recover the faulty/attack data and ensure the cyber-security defense abilities.

Summary and Future Work

In this article, we highlighted the data sparsity problem and threats in UAVs context. Although our early work addressed this issue; still there are many unexplored areas for researchers to investigate. In future, it is vital to investigate the performance of

the proposed method in different context such as mobility management, trajectory optimization, interference management, etc.

In our method the faulty data is equated to outliers means that the system ignores the case where an adversary manipulates data by replacing valid data with other valid data (non-outliers). The assumption appears to be that attackers will always affect the system in a way that can be detected by the "compromised data detection" algorithm. Yet if this were possible and reliable, then the attack does not always succeed. The detailed evaluation of this assumption is essential in future.

Further, how the proposed solution will cope-up the multi-domain scenarios, for example the cooperation of different types of UAVs is still an open issue. In our opinion the solution could be considered in the case of an in-country scenarios (both in single and multi-domain), if at all allowed by the regulator.

References

[1] H. Genc *et al.*, "Flying IoT: Toward Low-Power Vision in the Sky," *IEEE Micro*, vol. 37, no. 6, 2017, pp. 40–51.

[2] B. Li, Z. Fei, and Y. Zhang, "UAV Communications for 5G and Beyond: Recent Advances and Future Trends," *IEEE Internet of Things J.*, vol. 6, no. 2, 2019, pp. 2241–63.

[3] F. A. Dicandia *et al.*, "Space-Air-Ground Integrated 6G Wireless Communication Networks: A Review of Antenna Technologies and Application Scenarios," *Sensors*, vol. 22, no. 9, 2022, p. 3136.

[4] J. Wang *et al.*, "Taking Drones to the Next Level: Cooperative Distributed Unmannedaerial-Vehicular Networks for Small and Mini Drones," *IEEE Vehic. Tech. Mag.*, vol. 12, no. 3, 2017, pp. 73–82.

[5] C. F. E. de Melo *et al.*, "Uavouch: A Secure Identity and Location Validation Scheme for UAV-Networks," *IEEE Access*, vol. 9, 2021, pp. 82,930–46.

[6] R. He *et al.*, "Wireless Channel Sparsity: Measurement, Analysis, and Exploitation in Estimation," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 113–19, 2021.

[7] Z. Xiao *et al.*, "A Survey on Millimeter-Wave Beamforming Enabled UAV Communications and Networking," *IEEE Commun. Surveys & Tutorials*, vol. 24, no. 1, 2021, pp. 557–610.

[8] M. R. Nosouhi *et al.*, "Towards Spoofing Resistant Next Generation IoT Networks," *IEEE Trans. Information Forensics and Security*, vol. 17, 2022, pp. 1669–83.

[9] K. Sood *et al.*, "Accurate Detection of IoT Sensor Behaviors in Legitimate, Faulty and Compromised Scenarios," *IEEE Trans. Dependable and Secure Computing*, 2021, pp. 1–1.

[10] S. Liu *et al.*, "Fuzzy-Based Information Decomposition for Incomplete and Imbalanced Data Learning," *IEEE Trans. Fuzzy Systems*, vol. 25, no. 6, 2017, pp. 1476–90.

[11] Y. Zhang *et al.*, "Robust and Universal Seamless Handover Authentication in 5G Hetnets," *IEEE Trans. Dependable and Secure Computing*, vol. 18, no. 2,, 2021 pp. 858–74.

[12] M. Mozaffari *et al.*, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," *IEEE Commun. Surveys Tutorials*, vol. 21, no. 3, 2019, pp. 2334–60.

[13] Y. Mekdad *et al.*, "A Survey on Security and Privacy Issues of UAVs," arXiv preprint arXiv:2109.14442, 2021.

[14] A. Rugo, C. A. Ardagna, and N. E. Ioini, "A Security Review in the UAVNet era: Threats, Countermeasures, and Gap Analysis," *ACM Computing Surveys (CSUR)*, vol. 55, no. 1, 2022, pp. 1–35.

[15] H. Mahmood and F. Blaabjerg, "Autonomous Power Management of Distributed Energy Storage Systems in Islanded Microgrids," *IEEE Trans. Sustainable Energy*, 2022.

Biographies

Keshav Sood (keshav.sood@deakin.edu.au) received the Ph.D. degree from Deakin University, Melbourne, VIC, Australia, in 2018. Following his Ph.D. degree, he worked as a Research Fellow with the Advanced Cyber Security Engineering Research Centre (ACSRC), The University of Newcastle, NSW, Australia. He is currently a Lecturer at Deakin University. He worked on the project funded by the Defence Science and Technology Group. Some of his work is funded by the Department of Defense, Australia, and the Cyber Security Cooperative Research Centre (CSCRC), Australia.

Dinh Duc Nha Nguyen (dinh.nguyen@deakin.edu.au) received his Bachelor's degree from the Posts and Telecommunications Institute of Technology, Vietnam, and his Master's degree from Queensland University of Technology, Australia. He has been awarded a place on the Dean's list of excellent academic performance two consecutive times in 2020. He has more than six years of industry experience, mainly as a network analyst and software engineer. He is currently pursuing a Ph.D. degree at Deakin University, Melbourne, Australia.

Youyang Qu (youyang.qu@data61.csiro.au) received his B.S. degree in mechanical automation in 2012 and his M.S. degree in software engineering in 2015 from Beijing Institute of Technology. He received his Ph.D. degree from the School of Information Technology, Deakin University in 2019. His research interests focus on dealing with security and customizable privacy issues in blockchain, social networks, machine learning, and IoT. He has over 50 publications, including high-quality journals and conferences papers, including IEEE TII, IEEE TNSE, IEEE IOTJ, and more. He is active in IEEE Communication Society and has served as an organizing committee member in SPDE 2020 and BigSecurity 2021.

Lei Cui (lei.cui@tyust.edu.cn) received the Ph.D. degree from Deakin University, Melbourne, VIC, Australia, in 2021. He has authored or coauthored more than 30 publications, including monographs, book chapters, and journal and conference papers. Some of his publications have been published in the top venues such as IEEE TII, IEEE TNSM, and IEEE TPDS. His research interests include security and privacy issues in IoT, social networks, and machine learning. He is active in communication society and was a reviewer for many Q1 journals and the TPC Member for international conferences.

Kallol Krishna Karmakar (kallolkrishna.karmakar@newcastle.edu.au) is working as a Research Lecturer with the Advanced Cyber Security Engineering Research Centre, University of Newcastle, Callaghan, NSW, Australia. He is also working closely with DST and Data61, CSIRO, Australia, on SDN and IoT-related projects. His research interests include SDN, NFV, IoT security, and malwarereverse engineering.

Shui Yu (shui.yu@uts.edu.au) is a professor in the School of Computer Science, University of Technology Sydney, Australia, and a guest professor at Zhengzhou University, China. He is currently serving on a number of prestigious Editorial Boards, including *IEEE Communications Surveys & Tutorials* (Area Editor) and *IEEE Communications Magazine*. He is a member of AAAS and ACM, and a Distinguished Lecturer of IEEE Communication Society.

Footnotes

[1] https://dronelife.com/2019/10/17/drones-and-cybersecurity-an-expert-opinion-on-protecting-industry-against-drone-and-data-attacks/

[2] https://www.mass.gov/doc/volume-2-task-f-drone-cyber-security-assurance-methods-and-standards/download

[3] https://www.ericsson.com/en/reports-and-papers/white-papers/drones-and-networks-ensuring-safe-and-secure-operations}

[4] https://zenodo.org/record/5776219

[5] The data is divided into 70% and 30% for training and validation, respectively. In classification tasks like outlier detection, class labels may not have an equal number of instances. To preserve the proportion of samples in each class as seen in the original dataset, it is recommended to split the dataset into train and test sets using a stratified approach. To achieve this, the "stratify" option is applied to the y component of the original dataset. The train_test_split() function is then used to ensure that both the train and test sets contain a similar proportion of samples from each class.

[6] https://github.com/ndducnha/uav_awn