Security and Privacy for the Internet of Drones: Challenges and Solutions

Chao Lin, Debiao He, Neeraj Kumar, Kim-Kwang Raymond Choo, Alexey Vinel, and Xinyi Huang

A recent trend in both industry and research is the Internet of Drones, which has applications in both civilian and military settings. However, drones (also known as unmanned aerial vehicles) are generally not designed with security in mind, and there are fundamental security and privacy issues that need study. In this article, we study the architecture and its security and privacy requirements. We also outline potential solutions to address challenging issues such as privacy leakage, data confidentiality protection, and flexible accessibility, with the hope that this article will provide the basis for future research in this emerging area.

A recent trend in both industry and research is the Internet of Drones, which has applications in both civilian and military settings. However, drones (also known as unmanned aerial vehicles) are generally not designed with security in mind, and there are fundamental security and privacy issues that need study. In this article, the authors study the architecture and its security and privacy requirements.

Introduction

Unmanned aerial vehicles (UAVs), often referred to as drones, have been the subject of focus in industry and academia. This is partly due to their potential to be deployed in a broad range of applications from civilian (e.g., package delivery, firefighting, traffic monitoring, and agriculture) to military [1–3]. Here, we use the UAV surveillance system as an example (Fig. 1). In the system, after a drone has received the control signal from the user, it collects and sends data of interest (e.g., video, photo, or other sensing data) to the closest ground control station (GCS). Then the GCS connects to the surveillance center (SC) through the private network. Finally, the SC utilizes the data from GC to analyze the behavior of interest (i.e., target).

Small drones are especially popular, as these devices have a short wingspan and light weight but are expendable and easy to operate. However, the use of drones can potentially infringe on individual privacy and data protection [4], and pose a threat to governments, national institutions, and assets such as nuclear power plants and historical sites (e.g. using drones as an improvised explosive device or to transport chemical weapon agents in a terrorist attack).

Solutions to mitigate these threats include tracking, detecting, and jamming of malicious drones, such as using drone detection and tracking algorithms, active and passive object tracking schemes, and location detection technologies and protocols. Another potential mitigation strategy is via regulation. For example, drone manufacturers should ensure that drones satisfy requirements mandated by the relevant authority, such as the United States Federal Aviation Administration's requirements:

- There must be an airworthiness certificate.
- An IFR flight plan must be registered and executed.
- It must be equipped with automatic dependent surveillance — broadcast (ADS-B) (Out) (i.e., ADS broadcasting component)
- It must meet the minimum performance and equipage requirements of the area where the operation takes place.
- There must be a flight crew, including a pilot in command who is in charge of only one drone.
- Fully autonomous operations will not be allowed.

Existing solutions are not foolproof, particularly as the use of drones and autonomous operation becomes a norm in our society [5]. Therefore, we need more effective and real-time navigation and airspace management for the finite airspace to avoid any incidents (e.g., drone collision resulting in injuries and damage to life and property). For example, drones need to be authorized (in some sense) by the relevant authority to navigate and operate in the airspace at a certain time, and drones should not deviate from the approved flight task.

The Internet of Drones (IoD) can be broadly defined as a layered network control architecture designed for coordinating the access of drones to controlled airspace and providing navigation services [3]. It consists of the following layers: airspace, node-to-node, end-to-end, services, and applications. In the layered IoD architecture, every layer can utilize services provided by all layers below it. We refer interested readers to [3] for a detailed explanation of the architecture. Although there are apparent benefits of such an architecture (e.g., avoiding airborne collisions, and guaranteeing safety and security through greater control over where drones can and cannot be), there are challenges that remain unsolved. Examples include effective routing and congestion control, in addition to the security and privacy challenges and potential solutions we focus on in this article.

Related Work

In the above mentioned infrastructure, drones are capable of conducting fully autonomous operation beyond line of sight and are equipped with technologies to help them navigate (e.g., sens-

Digital Object Identifier:
10.1109/MCOM.2017.1700390

Chao Lin and Debiao He are with Wuhan University; Neeraj Kumar is with Thapar University; Kim-Kwang Raymond Choo is with the University of Texas at San Antonio; Alexey Vinel is with Halmstad University; Xinyi Huang is with Fujian Normal University.

ing, collision avoiding, and emergency landing). Two graphs will also be needed in navigating the drones: zone graph and interzone graph (Fig. 2). The former includes airspace, zone, gate, airway, intersection, and node. The airspace is a common resource shared by the drones, partitioned into zones. Zones are connected by gates, both inbound and outbound gates. There is a path map in every zone, which consists of airways, intersections, and nodes that allow drones to fly within the zone. Airways can be associated with roads, intersections (formed by at least two airways), and nodes (the points of interest reachable through an alternating sequence of airways and intersections).

An interzone graph consists of zones, gates, and transits, and in Fig. 2b we have the interzone graph for zones 1 to 4. The directed edges between gates are referred to as transits, which are the possible paths from the inbound gate to the outbound gate for the drones. More likely, between any two zones there can be many gates, but for simplicity we show only two.

For drone navigation, we need some zone service providers (ZSPs) tasked with providing navigation information for requesting drones, and an IoD service provider (IoDSP) to help adjacent ZSPs co-manage the gates or coordinate with each other during handoff (i.e., the responsibility has to be transferred to new ZSP once a drone crosses the border). Furthermore, in the layered architecture proposed by Gharibi *et al.* [3], there are two goals:

- Guiding a drone from a source node to a target node and serving drones for coordinating their access to the airspace
- Serving as an extensible platform for other common current or future services that are needed by applications such as delivery of messages

Unlike existing large-scale networks, such as air traffic control (ATC), cellular networks, and the Internet, some of their functionalities or concerns (e.g., collision-free navigation of ATC, deployment strategies of cellular networks, the layered architecture of the Internet) can also be applicable to IoD. Here, we focus on the communication infrastructure in terms of the potential security and privacy issues that may occur during IoD interactions. IoD could be deployed via cellular networks, where the base stations can directly run the ZSP software and provide wide network coverage for the deployed IoD. In other words, utilizing mobile communication provided by the base stations, ZSPs serve as both navigation and communication channels for deployed drones. ZSPs are also capable of communicating with each other or with other authorized cloud users because there is a connection between stations and the cloud.

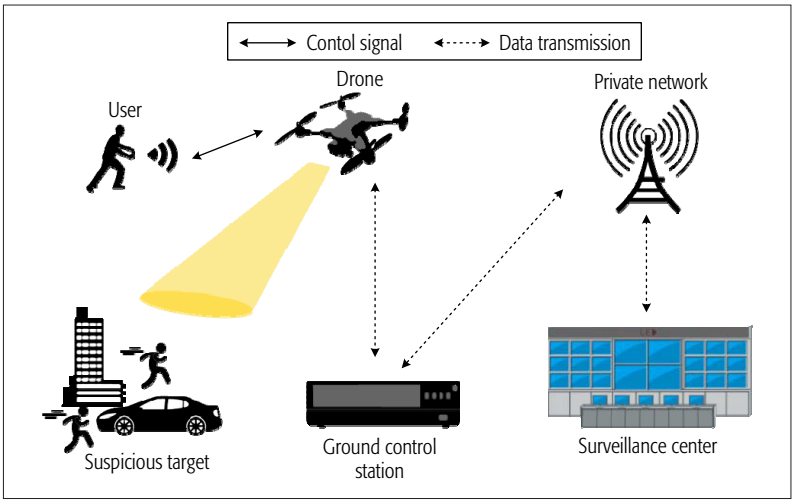

Figure 1. A typical UAV surveillance system.

When a drone flies from a node to another node, it needs to broadcast its information (e.g., geographical address) using standard open protocols to communicate with ZSPs or other drones. Instead of using an IP address to uniquely identify or locate a network node in the Internet, the use of a geographical address was suggested (i.e., each drone is assigned an evolving address according to its current geographical position, which can be obtained using GPS). An emergency (e.g., software or hardware failure, disconnection) during navigation is generally handled in the node-to-node layer; that is, the accident drone broadcasts an SOS message if possible, or the ZSP detects that a drone has stopped broadcasting and will immediately activate emergency procedures. An overview of the IoD communication system is presented in Fig. 3. In the next section, we discuss several associated security and privacy challenges.

Security and Privacy Challenges in IoD

Table 1 presents a comparative summary of IoD and traditional network characteristics. Lightweight (cryptographic) protocol designs and security solutions [6] are essential for IoD deployment due to hardware limitations, particularly for smaller and inexpensive drones (e.g., energy-constrained).

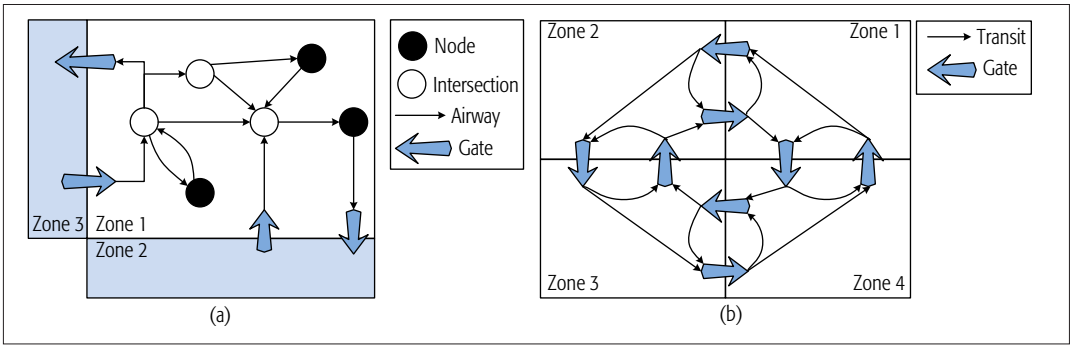

Figure 2. Structure graph of IoD: a) zone graph; b) interzone graph.

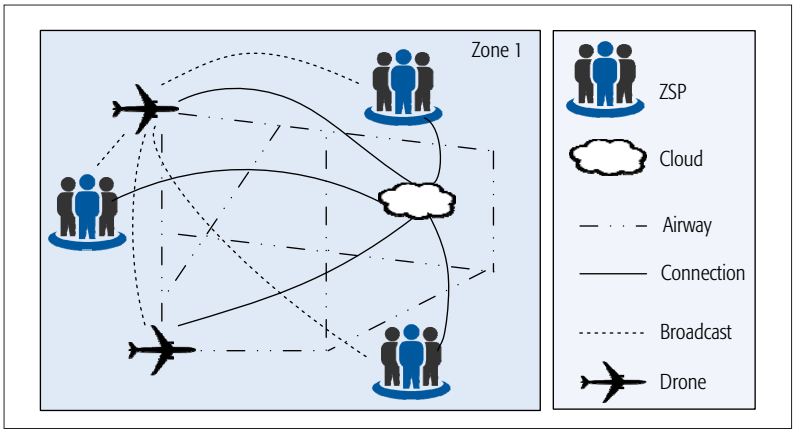

Figure 3. An overview of the communication system in IoD.

Items	Internet of Drones	Traditional networks
Energy	Constrained	Abundant
Mobility	ZSPs (stationary), drones (mobile)	Static
Architecture	Hierarchical	Hierarchical
Communication range	Limited	Long
Routing	Element-to-element connection	End-to-end connection
Packet delivery mode	Broadcast	Guaranteed delivery

Table 1. A comparative summary of IoD and traditional network characteristics.

Privacy Leakage in IoD

The increasing use of IoD will also result in more data (e.g., drones' geographical address or personally identifiable and sensitive data) being generated. Such data collectively can be used to profile any individual, and can be used in planning a physical attack on a building, installation, and so on. In this article, we focus on two types of privacy leakage, namely identity privacy and location privacy. Identity privacy requires the real/true identity of the drone to be protected. However, when a dispute occurs, it can be effectively traced and arbitrated by the relevant authority. In other words, we need to avoid having unauthenticated drones being permitted to operate in the airspace, and a mutual authentication is needed for secure communication, ensuring that drones' identity will not be leaked.

Pseudonyms [7] can be used to achieve a trade-off between authenticity and security. However, periodically updating pseudonyms and certificates will result in a high computational cost. This is not a viable option for resource-constrained drones. Moreover, this approach is vulnerable to the physically dynamic tracing attack [8], which can be used to compromise location privacy. In the proposed IoD architecture of Gharibi, Boutaba, and Waslander [3], drones are required to broadcast their addresses to ZSPs and other drones in order to avoid congestion in the navigation path. This raises location privacy concerns, since frequent broadcasting of the drone's geographical address information could lead to physical dynamic tracing attacks. Even hiding their true location through pseudonyms fails to resist such an attack.

Specifically, a set of malicious drones in IoD can collude to record the positions the target drone occasionally reaches and obtain its real identity through observing the traffic monitoring video. We suppose an adversary knows that the target drone has passed locations $L_1, L_2, ..., L_n$ with pseudonym p, and n sets of drones' real identities passing by these locations $V_1, V_2, ..., V_n$ can be observed. Then the adversary can trivially determine the target's real identity and even its private activities in other zones by the intersection.

Existing solutions for security and privacy preservation are generally designed to counter attacks by an external adversary. However, insider attackers such as a vendor and employee should not be ignored due to their level of access and ability to access sensitive data and collude with an external attacker. Therefore, mitigating insider attacks in IoD privacy leakage (e.g., authorized drones or managers of ZSP reveal drones' navigation information to an external attacker) needs to be considered in the design of a security solution or mitigation strategy.

Data Revealed and Sharing in Cloud Storage

Due to the computational limitations in drones and ZSPs, computationally intensive tasks should be outsourced to the cloud. However, the cloud service provider is always honest but curious, where it will not maliciously delete the data but may attempt to learn the contents of the drones' or ZSPs' data. If the drones' data (e.g., positions during navigation, and sensing data like surveillance images and videos) are stored in plaintext, they could be viewed by an employee of the cloud service provider. A naive solution is to encrypt the data prior to transmitting the (encrypted) data to the cloud. However, drones and ZSPs may not have the computational capability to perform encryption of large datasets (e.g., surveillance images, and videos). In addition, it is known that searching on encrypted data remains operationally infeasible or inefficient, since there is no known efficient fully homomorphic encryption scheme at the time of this research.

Apart from data confidentiality, data sharing and access control are challenges that face IoD deployment. For instance, in the application where a set of drones can collaborate to collect road traffic data of different regions, how to securely and efficiently share these collected data (e.g., in the sense that only authorized entities have access to the data) remains an ongoing challenge.

Malicious Interference in a Control Site

ZSPs are the main controllers in the architecture, where they not only provide navigation information, but also control a drone to hold, move to a new point, or land at a point. It is unsurprising that the control and feedback systems between ZSPs and drones are highly attractive targets for attackers seeking to compromise the system, often for nefarious reasons. The management, control, and operation in IoD may malfunction or be disabled in successful denial of service (DoS) attacks, spoofing attacks, malicious data injection, and so on. Most of these attacks may only be detected during third party inspection and security auditing. Data integrity and digital signatures

may work in software defined networks (where implementing a ZSP merely as software seems conceivable) to achieve data integrity, access control, and other relevant properties. While trusted computing may be used to prevent unauthorized operating system and software framework modifications/alterations, it has large latency and a high false rate; thus, it is not a suitable solution for IoD deployment (e.g., in the sense that efficient and fast detection of malicious attacks and misbehaviors are required in IoD).

In the next section, we present potential security solutions for identity privacy, location privacy, forward and backward security, insider attacks, and untrusted cloud service providers.

Proposed Solutions

In this section, we focus on privacy-preserving authentication and data security solutions for identity/location privacy protection, as well as lightweight cryptography approaches for security/privacy protection and flexible access to stored data.

Identity/Location Privacy Protection

As discussed previously, in the IoD architecture an access control and a precise navigation plan for the drones are essential. The distributed deployment of ZSPs requires a real-time navigation adjustment to avoid congestion and provides a faster route for drones. In Fig. 4 (for simplicity, we do not include the cloud by which ZSPs communicate with each other), suppose that the querying drone in the navigation services is a requester, who broadcasts a navigation query to the closest ZSPs. The query contains the current position, destination, and expiration time or maximum hops. Then this query is transmitted to the ZSP that covers the destination through the network. According to the received navigation query, the relevant ZSP will send the congestion detection task to the drones in its coverage area to find the fastest driving route for the requester. The requester retrieves a response from the ZSP when entering the coverage area of each ZSP, and finally reaches the destination.

In the above example (Fig. 4), both the querying drone and responding drones' private information (e.g., drones' original place, owners, or working companies, main travel route) may be geographically close. This private information can be linked to a specific individual and reveal his/her lifestyle information, resulting in profiling or loss of privacy, such as location-based "spam" (i.e., businesses using an individual's location information to facilitate unsolicited marketing for products or services). Moreover, an attacker can utilize the location to infer an individual's political views, state of health, or personal preferences, as well as carrying out a physical attack (e.g., stalking or robbery).

Symmetric-key cryptographic algorithms, such as lightweight and energy-efficient algorithms, should be designed for deployment on resource-constrained devices. For example, Ni *et al.* [9] used Elgamal and Advanced Encryption Standard (AES) schemes to encrypt the devices' location information. We use a similar approach to encrypt the requester's navigation information (i.e., the source location and the destination) in each query from the requester to the last ZSP to preserve the drone's query privacy.

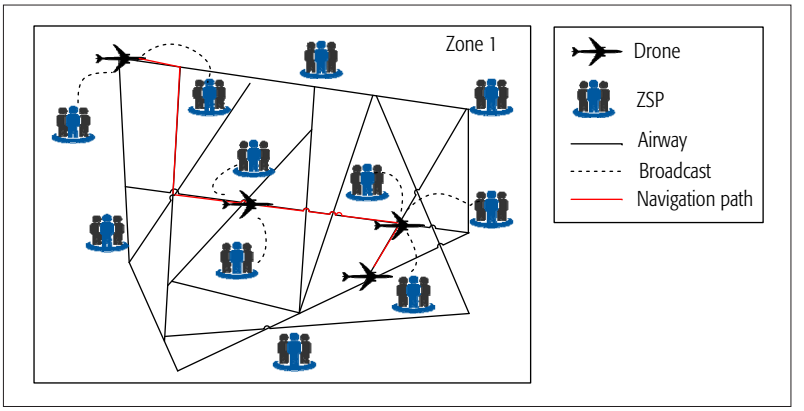

Figure 4. A simplified navigation path adjustment example in IoD.

Here, we need to point out that all drones and ZSPs are equal from a key management perspective (i.e., a common key is used between any pair or group of drones or ZSPs). We posit that a key management system [10] for sensor networks can achieve both forward and backward security while allowing drones/ZSPs to join and leave the current communication group.

In addition, each drone randomizes the credential issued by the trusted authority to generate a group signature [11] to prevent ZSPs from linking the navigation query and retrieving query to a target drone. Apart from encrypting the flying route using Elgamal and AES schemes, we suggest attaching a zero-knowledge range proof so that sensitive information (e.g., expiration time or maximum hops) in the navigation response will not be disclosed. For the traceability of group signature, the trusted authority can track any malicious drone that does not honestly follow the rules.

Security/Privacy Protection in Data Outsourcing

We also introduce a state-of-the-art security and protection protocol for data outsourced from drones to the cloud sever, but allowing flexible access to the stored data. Our design is based on identity-based encryption (IBE), and we note that IBE has been used in a wide range of applications to protect sensitive data. However, conventional IBE cannot be efficiently utilized in the resource-constrained IoD architecture. Therefore, we propose using a lightweight IBE scheme (hereafter referred to as IBE-Lite) [12] to facilitate secure sharing of drones' data. Specifically, IBE-Lite has two overlapping properties with conventional IBE: the ability to use an arbitrary string to generate a public key and the ability to generate a public key separately from the corresponding secret key. We now use the below example to demonstrate the utility of IBE-Lite.

In our example, a toxic chemical was released in an industrial accident; the goal is to locate and contain the source of the leakage [13]. To identify the chemical, multiple small drones fly in the target area to collect sensing data using onboard chemical sensors. It should be noted that different sensors may be installed on different drones from different interspaces and belonging to different collaboration owners. The users are likely required to share the data collected by drones

Since data collected by drones are outsourced to the cloud for processing, the IBE-Lite scheme ensures data confidentiality as well as providing flexible access to outsourced data. In the scheme, access control can only be controlled by the CA (i.e., acting as a trusted party and not colluding with others) since the storage site is not trusted.

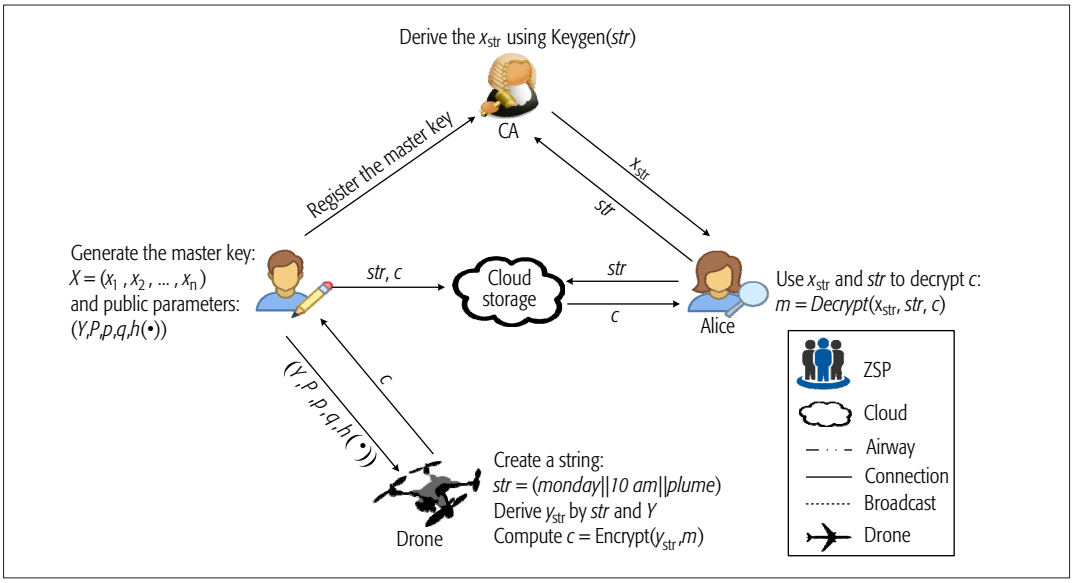

Figure 5. IBE-Lite scheme for securing outsourced drone data to the cloud storage (adapted from [12]).

(with the same chemical sensors onboard) to obtain the information required to locate and contain the source of the leakage (e.g., chemical gradients). Chemical gradients can be defined by sharing sensor data, and the users can cooperatively track boundaries or follow the gradients to the source. Since data collected by drones are outsourced to the cloud for processing, the IBE-Lite scheme ensures data confidentiality as well as providing flexible access to outsourced data. In the scheme, access control can only be controlled by the certificate authority (CA) (i.e., acting as a trusted party and not colluding with others) since the storage site is not trusted (Fig. 5).

The processes in the scheme are as follows.

Initialization. Denote p as a big prime, and P as the base point of an elliptic curve of prime order q. Let Bob be the user who wishes to store the shared data in the cloud; his corresponding partner is Alice. Bob first invokes the Setup algorithm to generate the master key $X = (x_1, x_2, ..., x_n)$ and public parameters $(Y, P, p, q, h(\cdot))$, where $Y = (y_1, y_2, ..., y_n)$, $y_i = x_i \cdot P(1 < i < n)$ and $h(\cdot)$ is a collision resistant one-way hash function: $\{0,1\}^* \rightarrow \{0, 1\}^n$. Then Bob loads the parameters to his drones' sensor and registers the master secret key together with additional instructions with the CA.

Data Encryption. After collecting the required data m, Bob's drones create a string str according to a pre-agreed syntax, such as $str = (monday||10\ am||chemical)$. Using this string, the drones can derive a public key $y_{str} = \Sigma\ h_i(str) \cdot y_i$ by the parameter Y to encrypt m, and Bob sends the cipher text to the cloud for storage and processing.

Data Decryption. When Alice wishes to access the data collected under some str (received from Bob), she needs to query the CA for permission. Upon performing the relevant checks, the CA will run Keygen(str) to derive the corresponding secret key $x_{str} = \Sigma\ h_i(str) \cdot x_i$ through the same string $str = (monday||10\ am||chemical)$. Then Alice can use x_{str} to decrypt the data encrypted by a drone using the same string. Interested readers can refer to [12] for more details of the scheme. We now discuss how this scheme can protect data privacy and achieve sharing.

First, the cloud is not able to learn the content of a drone's data because the data was encrypted using y_{st}, and the cloud does not know the corresponding secret key x_{str}. No unauthorized party can access the other drones' data, since each piece of data collected by a drone is encrypted using y_{st} derived from the string str. When Bob receives the authorization to access the data encrypted under str, the secret key x_{str} does not allow Bob to decrypt ciphertext not encrypted using y_{str}. Moreover, the drone's sensor only stores the public parameters. Thus, a compromised or malicious drone will not be able to help the adversary to obtain any useful data collected by the target drone from the storage site. Finally, using additional certificates, we can authorize another party to access the data.

In addition, Ten *et al.* [12] evaluated the performance of the proposed work using Tmote Sky[1] to demonstrate practicality for sensor deployment. Although the drones in IoD may install different sensors unlike Tmote Sky, the proposed approach could be applicable to IoD.

Conclusion and Future Challenges

IoD is a trend that is likely to stay in the foreseeable future, and there is a need to ensure the security and privacy of data collected from the drones and outsourced to the cloud (the focus of this article).

In this article, we introduce a typical IoD architecture and describe several security and privacy challenges, such as privacy leakage, and the need for secure and efficient data sharing. Then we describe potential solutions suited to the nature of IoD architecture.

Apart from the discussed potential security and privacy issues, there are a number of other security services that need to be implemented for IoD.

Intrusion Detection and Prevention. IoD is likely to be subject to intrusions; thus, designing an (energy-) efficient and effective intrusion detec-

[1] Tmote Sky is a kind of sensors with a 8MHz TI MSP430 CPU, 10KB on-chip RAM, 48KB programming ROM and 1MB permanent flash storage.

tion and prevention system to identify malicious cyber activities is crucial.

Forensic-by-Design. Ab Rahman *et al.* [14] coined the concept of forensic-by-design and emphasized the importance of integrating forensic requirements into the design of a cyber-physical system. Similarly, in [15], the authors explained that data may not always be available due to short data retention times, lack of extraction capabilities, costs associated with conducting such investigations, and so on. Hence, future IoD system and architecture designs should consider integrating forensic requirements to facilitate forensic investigation.

Secure Data Aggregation. Although we have discussed data security from the perspective of drones' data collection and sharing, data aggregation is another emerging challenge since there is a wealth of data collected by drones that are encrypted prior to transmission. Efficient secure data aggregation methods can reduce the costs of communication and energy, which may be realized by homomorphic encryption (aggregates several ciphertexts into a single ciphertext without the need of decryption). However, providing secure data aggregation that also achieves confidentiality and access control is another potential future research topic.

Acknowledgment

The work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802500, in part by the National Natural Science Foundation of China under Grant 61501333, Grant 61572379, Grant 61472287, and Grant 61772377, and in part by the Natural Science Foundation of Hubei Province of China under Grant 2017CFA007 and Grant 2015CFA068.

References

[1] Y. Ganesh, R. Ramya, and H. Rajeshwari, "Surveillance Drone for Landmine Detection," *Advanced Computing and Commun.*, 2015, pp. 33–38.
[2] F. Flammini *et al.*, "Towards Automated Drone Surveillance in Railways: State-of-the-Art and Future Directions," *Int'l. Conf. Advanced Concepts for Intelligent Vision Systems*, Springer, 2016, pp. 336–48.
[3] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of Drones," *IEEE Access*, vol. 4, 2016, pp. 1148–62.
[4] C. Pauner, K. Irene, and V. Jorge, "Drones. Current Challenges and Standardisation Solutions in the Field of Privacy and Data Protection," *ITU Kaleidoscope: Trust in the Information Society*, 2015, pp. 1–7.
[5] H. Y. Chao, Y. C. Cao, and Y. Q. Chen, "Autopilots for Small Unmanned Aerial Vehicles: A Survey," *Int'l. J. Control, Automation and Systems*, vol. 8, no. 1, 2010, pp. 36–44.
[6] S. Panasenko and S. Smagin, "Lightweight Cryptography: Underlying Principles and Approaches," *Int'l. J. Computer Theory and Engineering*, vol. 3, no. 4, 2011, p. 516.
[7] D. Forster, F. Kargl, and H. Lohr, "PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-hoc Networks (VANET)," *VNC*, 2014, pp. 25–32.
[8] M. E. Mahmoud and X. Shen, "A Novel Traffic-Analysis Back Tracing Attack for Locating Source Nodes in Wireless Sensor Networks," *IEEE ICC*, 2012, pp. 939–43.
[9] J. Ni *et al.*, "Privacy-Preserving Real-Time Navigation System Using Vehicular Crowdsourcing," *Proc. VTC-Fall*, 2016, pp. 1-6.
[10] R. Roman *et al.*, "Key Management Systems for Sensor Networks in the Context of the Internet of Things," *Computer and Electrical Engineering*, vol. 37, no. 2, 2011, pp. 147–59.
[11] X. Lin and X. Li, "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks," *IEEE Trans. Vehic. Tech.*, vol. 62, no. 7, 2013, pp. 3339–48.
[12] C. C. Tan *et al.*, "Body Sensor Network Security: An Identity-Based Cryptography Approach," *WISEC*, 2008, pp. 148–53.
[13] D. J. Harvey, T. Lu, and M. A. Keller, "Comparing Insect-Inspired Chemical Plume Tracking Algorithms Using a Mobile Robot," *IEEE Trans. Robot*, vol. 24, no. 2, 2008, pp. 307–17.
[14] N. H. Ab Rahman *et al.*, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems," *IEEE Cloud Computing*, vol. 3, no. 1, 2016, pp. 50–59.
[15] G. Grispos *et al.*, "Medical Cyber-Physical Systems Development: A Forensics-Driven Approach," *Proc. IEEE/ACM Conf. Connected Health: Applications, Systems and Engineering Technologies*, Philadelphia, PA, 17–19 July, pp. 108–14.

Biographies

Chao Lin received his Bachelor's and Master's degrees from the School of Mathematics and Computer Science, Fujian Normal University in 2013 and 2017, respectively. Currently, he is pursuing a Ph.D. degree at the Computer School of Wuhan University. His research interests mainly include authentication of graph data and blockchain security.

Debiao He received his Ph.D. in applied mathematics from the School of Mathematics and Statistics, Wuhan University, in 2009. He is currently a professor in the State Key Lab of Software Engineering, Wuhan, China. His main research interests include cryptography and information security, in particular cryptographic protocols.

Neeraj Kumar received his Ph.D. degree in CSE from Shri Mata Vaishno Devi University, Katra (J&K), India. He was a postdoctoral research fellow ay Coventry University, United Kingdom. He is currently an associate professor in the Department of Computer Science and Engineering, Thapar University, Patiala, Punjab, India.

Kim-Kwang Raymond Choo [SM] received his Ph.D. degree in information security from Queensland University of Technology, Australia, in 2006. He currently holds the Cloud Technology Endowed Professorship at the University of Texas at San Antonio, and is a Fellow of the Australian Computer Society.

Alexey Vinel received his Ph.D. degrees in technology from the Institute for Information Transmission Problems, Moscow, Russia, in 2007, and Tampere University of Technology, Tampere, Finland, in 2013. He is currently a professor of data communications at the School of Information Technology, Halmstad University, Sweden.

Xinyi Huang received his Ph.D. degree from the School of Computer Science and Software Engineering, University of Wollongong, Australia. He is currently a professor with the School of Mathematics and Computer Science, Fujian Normal University, China, and the co-director of the Fujian Provincial Key Laboratory of Network Security and Cryptology.

Efficient secure data aggregation methods can reduce the costs of communication and energy, which may be realized by homomorphic encryption. However, providing a secure data aggregation that also achieves confidentiality and access control is another potential future research topic.