future internet

MDPI

Review

Securing UAV Flying Base Station for Mobile Networking: A Review

Sang-Yoon Chang [1,*], Kyungmin Park [2], Jonghyun Kim [2] and Jinoh Kim [3]

[1] Computer Science Department, University of Colorado Colorado Springs, Colorado Springs, CO 80918, USA
[2] Electronics and Telecommunications Research Institute, Daejeon 34129, Republic of Korea; kmpark@etri.re.kr (K.P.); jhk@etri.re.kr (J.K.)
[3] Computer Science Department, Texas A&M University-Commerce, Commerce, TX 75428, USA; jinoh.kim@tamuc.edu
* Correspondence: schang2@uccs.edu

Abstract: A flying base station based on an unmanned aerial vehicle (UAV) uses its mobility to extend its connectivity coverage and improve its communication channel quality to achieve a greater communication rate and latency performances. While UAV flying base stations have been used in emergency events in 5G networking (sporadic and temporary), their use will significantly increase in 6G networking, as 6G expects reliable connectivity even in rural regions and requires high-performance communication channels and line-of-sight channels for millimeter wave (mmWave) communications. Securing the integrity and availability of the base station operations is critical because of the users' increasing reliance on the connectivity provided by the base stations, e.g., the mobile user loses connectivity if the base station operation gets disrupted. This paper identifies the security issues and research gaps of flying base stations, focusing on their unique properties, while building on the existing research in wireless communications for stationary ground base stations and embedded control for UAV drones. More specifically, the flying base station's user-dependent positioning, its battery-constrained power, and the dynamic and distributed operations cause vulnerabilities that are distinct from those in 5G and previous-generation mobile networking with stationary ground base stations. This paper reviews the relevant security research from the perspectives of communications (mobile computing, 5G networking, and distributed computing) and embedded/control systems (UAV vehicular positioning and battery control) and then identifies the security gaps and new issues emerging for flying base stations. Through this review paper, we inform readers of flying base station research, development, and standardization for future mobile and 6G networking.

Keywords: security; telecommunications networking; 5G networking; 6G networking; base station; UAV drone; distributed networking

check for updates

Citation: Chang, S.-Y.; Park, K.; Kim, J.; Kim, J. Securing UAV Flying Base Station for Mobile Networking: A Review. *Future Internet* **2023**, *15*, 176. https://doi.org/10.3390/fi15050176

Academic Editors: Alessandro Raschellà and Michael Mackay

Received: 16 April 2023
Revised: 4 May 2023
Accepted: 5 May 2023
Published: 9 May 2023

1. Introduction

Mobility has traditionally been implemented and enabled for the mobile user. However, recent research and proposals introduce mobility to the telecommunications network service provider infrastructure. The unmanned aerial vehicle (UAV) drone-based flying base station (called UxNB in 3rd Generation Partnership Project or 3GPP [1,2]) improves the telecommunications connectivity provision. While the traditional stationary terrestrial base station has a fixed cell for its connectivity coverage, the flying base station's mobility and its strategic location for connectivity enable more flexible, dynamic, and adaptive connectivity coverage. The flying base station can also improve the channel quality to the mobile user by approaching or securing the line-of-sight path to the mobile user (which is especially important for mmWave communications, which do not penetrate physical barriers as well as lower-band communications). The improved connectivity coverage and communication channels enable greater bandwidth/data rates and reduced latency for the next-generation wireless applications, including sensor applications (e.g., surveillance, personal, body, and environmental monitoring) and those based on holographic and haptic operations (e.g., virtual reality/VR or augmented reality/AR).

Securing a UAV flying base station is critical because it is a part of the cellular service provider infrastructure and the mobile users rely on it for connectivity. Its disruption and manipulation represent high security risks, as our everyday lives increasingly depend on reliable connectivity. In addition, the advancements and developments in wireless/mobile implementations, including software-defined radio (SDR) and open-source mobile networking softwares such as srsRAN, reduce the threat implementation barrier and increase the attack feasibility (even though these enabler tools and technologies provide longer-term benefits in securing the system, including improving the transparency, vendor interoperability, and security awareness). We therefore treat the networking provider infrastructure as a critical infrastructure and focus on the integrity of flying base station operations (execution is as designed, and the unauthorized attackers cannot manipulate or change the protocol execution) and availability (the connectivity is provided when needed and requested).

The UAV drone flying base station system combines a telecommunications base station (for its application and purpose of connectivity provision) and UAV drone (for mobility implementation and control). While there has been research and development to secure the component technologies of the flying base station system (communications for base station, embedded control for UAV drone, and distributed computing for the base station's coexistence with other base stations and the rest of the infrastructure), research and developments taking a systems approach to secure the flying base station as a system have been lacking. In this review paper, we therefore identify the unique properties of a flying base station distinct from its component technologies, review the related research in the component technologies (based on which we can draw the initial reference designs for the security solutions before adapting and advancing them for flying base station), and discuss future work directions. We envision that this paper will inform, encourage, and facilitate further research to advance the security of flying base stations.

This review paper surveys the existing research literature on UAV flying base station security, identifies research gaps for the flying base station system built on its component technologies, and informs readers about future research directions. To the best of our knowledge, this is the first review paper focusing on the security of UAV flying base stations. Wang et al. [3] use UAV to enable physical-layer security but lack the systems approach, i.e., they do not consider the flying base station system aspects of UAV/drone control, battery, and digital security. Other survey or review papers focus on the individual component technology or lack a security focus, e.g., UAV/drone sensing and monitoring (e.g., [4,5]), communications to enable UAV/drone operations (e.g., [6,7]), the security of UAV drones (e.g., [8–11]), security of wireless communications, and security of wireless and mobile applications (e.g., [12,13]).

The rest of the paper is organized as follows. Section 2 describes the telecommunications networking background involving base stations focusing on the most recent 5G New Radio (NR) standardized protocol. Our treatment of the background information on telecommunications is brief and of a high level as we describe those factors needed for flying base station research as opposed to providing significantly longer and more detailed coverage of the 5G NR protocol. Section 3 discusses the unique properties of a UAV flying base station distinct from its component technologies of a stationary ground base station and UAV drone, which establishes the focuses of this review paper. Based on the unique properties and the component technologies of the stationary ground base station and UAV drone, Section 4 reviews the security research in base station control communication security, authentication and cryptography (the digital security mechanisms), mobility control security (traditionally been studied in embedded, cyber-physical, and vehicular systems), battery integrity security, and distributed network security. Section 5 discusses future work to facilitate and encourage future research and development to secure flying base stations. Section 6 concludes this paper.

2. Mobile Networking Background

This paper focuses on the most recent 5G New Radio protocol as standardized and specified by the Third Generation Partnership Project (3GPP) [14–16]. 3GPP standardizes and specifies the technologies for the radio access, backend core network, and service capabilities for mobile telecommunications, thus guiding mobile networking research and development and enabling interoperability between the different cellular service provider services. While 6G's protocol design and standardization are currently ongoing, 5G will provide a building base for 6G as 6G will inherit most of the existing technologies, including those described in this section.

Section 2.1 provides a high-level overview of the current mobile networking focusing on 5G, including the different protocol steps for the wireless/RF communication channel setup vs. the digital setup and the critical messages and identifiers/credentials used for the channel setup (which can become the targets for security protection in future security research). Building on the 5G architecture, Section 2.2 describes the incorporation of the UAV flying base station to the 5G architecture.

2.1. Existing Telecommunications Networking Protocol: 3GPP Standardization Protocol and User vs. Base Station vs. Core Network

The connectivity provider infrastructure to provide connectivity to the mobile user includes the base station, the core network, and the intermediate routers/switches (which forward the networking packets across the physical distances after the base station). The lower row in Figure 1 depicts these entities from the user (left) to the cloud (right), where those between the base station and the core network are within the cellular service provider infrastructure. Beyond the core network is outside of the cellular service provider infrastructure and relies on the collaborations and agreements with other service provider entities.

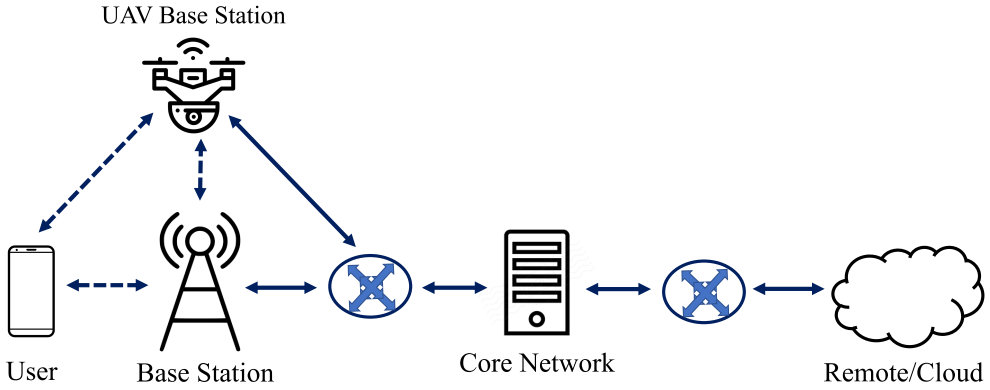

Figure 1. Telecommunications networking architecture and entities, including the UAV flying base station in the upper row.

The base station connects to the mobile user wirelessly and serves as the bridge gateway to transition to the wireless communications for the mobile users in telecommunications networking. Because the mobile user uses a wireless communication link, while the networking from the base station to the internet and cloud are in the form of wired communications, the base station serves as the gateway between wireless vs. wired networking. The user and the base station communicate via radio-frequency (RF) wireless communications, while communication from the base station to the core network and then to the cloud is via wired communications involving other nodes such as routers and switches. Therefore, the base station is the first and the last hop to the mobile users communicating in RF. Beyond the base station, the core network is responsible for much of the digital processing to set up the connectivity services to the mobile user, including user registration, security setup, and service as well as access control. The communications and packets from the user are processed by the core network before it leaves, e.g., to the public internet.

Figure 2 describes the logical interactions for the control communications between the user, base station, and core network. The brief description abstracts from the telecommunications implementations and details from [14–16] and focuses on the information needed to understand this review paper. The user and the base station require radio resource control (RRC) and a wireless channel for setting up the RF wireless communications, where the communication resources are shared with multiple other users coexisting in the nearby air medium. The RRC begins with the broadcasting messages by the base stations, including the master information block (MIB) and system information block (SIB). The MIB and SIB messages are publicly broadcasted and advertised as the base station is a public entity for serving the cellular connectivity, often serving a large number of mobile users freely entering and exiting the cell. Receiving and decoding the MIB and SIB enable the mobile user to attach to the base station and set up a communication channel, resulting in the user-dedicated cell radio network temporary identifier (C-RNTI). This wireless channel setup is followed by digital control including the registration and authentication verification as well as the security setup between the user and the core network. From the user and (universal) subscriber identity module (SIM or USIM) registration (which occur in advance before the user activation to receive the connectivity service and not drawn in Figure 2), the core network derives the mobile subscriber identification number (MSIN) and the more temporary ID of the temporary mobile subscription identifier (TMSI) and shares that with the user and the base station. The MSIN is not communicated in plain-text and rather is processed by an encryption function E, thus exchanging $E(\text{MSIN})$. Afterward, the user can use the established RF and digital channel for data communications and networking applications.

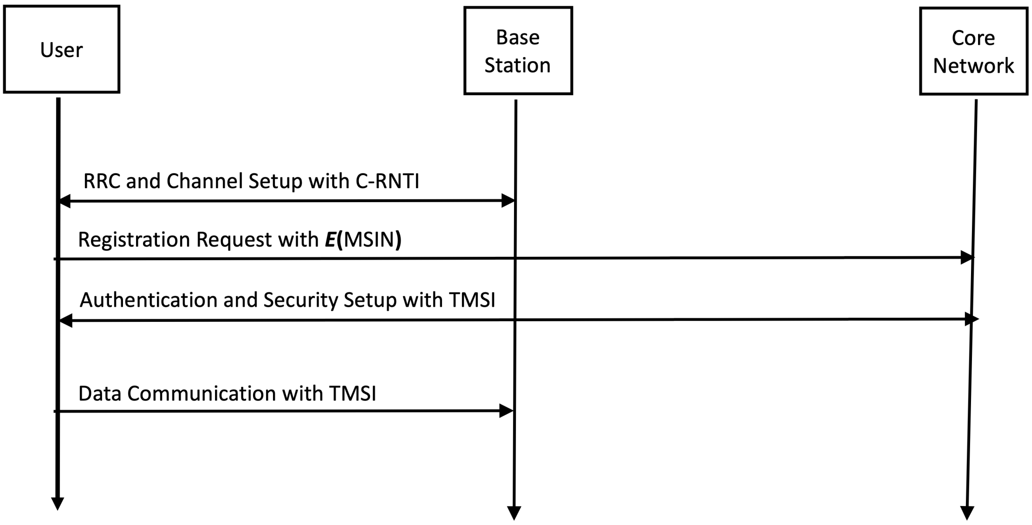
User
Base Station
Core Network
RRC and Channel Setup with C-RNTI
Registration Request with ***E*(MSIN)**
Authentication and Security Setup with TMSI
Data Communication with TMSI

Figure 2. Control communication protocol interactions between the user, base station, and core network to set up the data channel.

2.2. Incorporating Flying Base Station

Sixth-generation networking introduces the UAV flying base stations to improve the base station coverage and the channel link qualities to mobile users. As is typical with new technologies in mobile networking, the incorporation of the flying base station to mobile networking should support backward-compatibility to the 5G networks described in Section 2.1. For example, a flying base station can provide the connectivity service even if the mobile user only supports 5G or even lower-generation telecommunications, e.g., 2G for emergency applications.

Figure 1 therefore builds on the traditional cellular/5G architecture (lower row) and introduces the flying base station (upper row). In Figure 1, the flying base station connects to the mobile user and to the stationary ground base station (to access the backend and the internet), and these communications are in wireless/RF communications, as drawn in dotted arrow lines. While mobile, the flying base station connects to the stationary ground base station to access the rest of the network. In addition, the flying base station can sometimes connect directly to the cellular provider infrastructure via a switch, e.g., when it is recharging its battery, requiring physical connections as drawn in solid arrow lines.

The flying base station can be multiple physical entities (multiple flying base stations), although drawn as one logical entity in Figure 1. These flying base stations can network with each other (forming their own network) for coordination and connectivity-provision control (involving ad hoc networking capabilities, e.g., flying ad hoc network or FANET), while maintaining the connections with the rest of the connectivity provider infrastructure including the ground base station. The collaborative network of flying base stations can extend the connectivity range by forming a relay network.

The emerging flying base station has the purpose of serving connectivity to mobile users, requiring connectivity in an on-demand basis or dynamically entering/exiting the flying base station's cellular range. To serve the public's mobile devices, the flying base station will be publicly accessible and broadcast and advertise RRC messages, similarly to the stationary terrestrial base stations described in Section 2.1. This makes the flying base station distinct from some other flying/UAV applications requiring privacy and/or having dedicated communication targets.

3. UAV Flying Base Station Properties

A UAV flying base station combines the functionalities of a base station (to provide the last-mile hop wireless communication link to the user equipment) and UAV drone (to move its location). However, a UAV flying base station is distinguishable from each of these underlying technologies and introduces novel security vulnerabilities and threats previously unseen in stationary base stations and generic UAV drones.

3.1. Controlling Mobility and Positioning

A UAV flying base station implements the mobility functionality to better serve mobile users, while the traditional base stations are stationary and have a fixed location. While this mobility presents an opportunity to better serve the user (approaching the user for greater channel reliability and data communication rate/bandwidth), it also presents unique engineering problems and risks. Because flying base station research and development is in its infancy, its user-dependent mobility control is new.

Security implications: New security risks can involve a malicious user, including those violating the integrity of the positioning control, to misplace the base station and launch a denial-of-service (DoS) of the base station's connectivity provision. The vulnerabilities for such security threats are due to the mobility capability of the flying base stations and therefore do not apply to the stationary base stations.

3.2. Operation on Battery

Because the UAV flying base station is mobile and cannot afford wired connections hindering its mobility, a UAV flying base station operates on the battery energy resource to supply the electrical power supply. The UAV flying base station requires the battery energy for both its connectivity provision (i.e., it cannot support the connectivity to the user if it does not have electrical energy) and its mobility (move and re-position its location to improve the connectivity provision to the mobile user), as depicted in Figure 3. Because of the battery's finite energy amount, the flying base station operation requires regular re-charging when the battery is running low in energy. The re-charging phases interfere with the flying base station operations because of the fixed locations of the recharging stations, reducing the flying base station to stationary base station operations.

Security implications: Such finite resources in battery energy and their direct impact on the connectivity provision lead to vulnerabilities against battery-draining DoS threats. In addition to the more traditional DoS channels focusing on networking bandwidth and processing resources, the battery energy provides a new channel for the DoS attacker to interfere with and disrupt the base station operations. Because the battery/energy resource is shared by both the base-station communication and the drone mobility, as depicted in Figure 3, there are greater DoS vulnerabilities than having either communication or mobility but not both. For example, the attacker manipulating the base station location can trigger greater power consumption for the signal transmission; requiring greater reliability and jamming resistance can incur greater bandwidth and thus power consumption, e.g., the code-division multiple access (CDMA) spread spectrum; and bogus injection messages can cause greater re-charging, disabling the optimal control of the mobility and location of the base station.

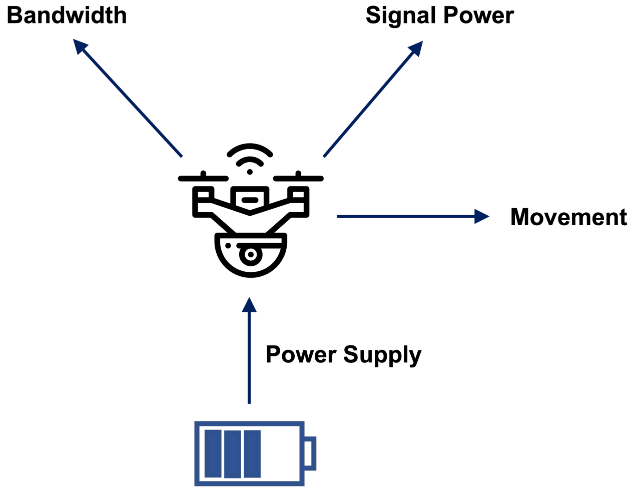

Figure 3. Flying base station control parameters affecting its power consumption. The UAV flying base station shares the power from a singular source of a battery to support multiple functionalities of the UAV drone (movement) and the base station (wireless communication).

3.3. Providing Communication and Connectivity to Users

The generic UAV drones have many applications and purposes, including sensing and collecting information and the delivery/moving of physical objects. The generic UAV drones typically use communications to facilitate and optimize their goals (communications for UAV); they are the beneficiary of communication service provider infrastructure, assuming the mobile user's role in cellular architecture. In contrast, the UAV flying base station's goal and purpose is to provide connectivity and networking to the users (UAV for communications) and is a part and enabler of the communication service provider infrastructure.

Security implications: Due to the networking application's reliance on the communications and networking provided by the cellular infrastructure (including the UAV flying base station), the flying base station has significant security risks, i.e., the integrity and availability threats on its operations have significant impacts.

3.4. Involving Distributed and Edge Computing

A UAV flying base station is inherently smaller than the stationary terrestrial base station because of its mobility and battery requirements. The smaller size and the energy constraint of a flying base station limits the number of users that a flying base station can serve, compared to a stationary terrestrial base station, which in turn increases the number of flying base stations on the edge and reduces the cell coverage size per base station. The architecture and control involving a group of base stations require greater sophistication on the networking edge and involve greater distributed computing and networking to enable dynamic, adaptive, and agile control for the improved connectivity provision of base stations. Therefore, flying base station control involves distributed networking to support the ad hoc and peer-to-peer networking, in addition to the centralized backhaul-accessible networking. Such capabilities forgoing the centralized backhaul networking can enable networking redundancy to control the flying base station operations (so that the flying base station control and operations have higher reliability) and can implement wireless relay to enable greater geographical coverage for the connectivity.

Security implications: The dynamic, flexible, and ad hoc communications to control the flying base stations' operations are high-risk communications because such operations are high-impact and mission-critical. The failure of such communications in terms of availability and integrity can disable and disrupt the cellular connectivity provision to the user. Therefore, the flying base station's communications present a higher security risk than many other UAV ad hoc communication applications.

4. Related Work

4.1. Base Station Control Communication Security

The base station provides connectivity to many users utilizing multiple-antenna/MIMO and channelization/multiplexing technologies (where the channels coexist but are separate in frequency, time, code, and/or space-direction) and the medium access control (MAC) protocol (which sets up and synchronizes such wireless channel resources to use for data communications across multiple users). Previous research secured the integrity of the MAC and control communications for the availability of data channel resources, which is especially important because the DoS on the flying base station's channel resources can disrupt and disable the channel connectivity to the other legitimate users. Such research includes securing MAC protocol and radio-control handshaking in the dynamic and sophisticated dynamic spectrum environment against the channel control against insider, credential-compromising, and dynamic jamming [17–19], against MAC injection and handshaking-manipulating threats [20,21], and against the threats on channel-state-information (CSI) feedback [22,23]. While these research use models are abstracted from the 5G protocol details and generally applicable to wireless communications, the threats apply to the concrete protocols of 5G NR RRC protocol standardized by 3GPP [24–26]. However, the research solutions for securing the specific 5G RRC protocol between the user and the base station have been lacking; rather, the 5G security research has focused on incorporating and implementing security on the backend core network beyond the base station, e.g., [27–30].

4.2. Authentication and Cryptography

Telecommunications networking, including 5G NR by 3GPP, includes digital security protection mechanisms both for key establishment and the security functionality derivations based on that. In contrast to the research in Section 4.1, these digital security mechanisms are implemented after the RRC/radio channel establishment and after the core network is involved to verify the user registration. In 5G, the USIM described in Section 2.1 includes the core network's public key in advance, i.e., when it registers for the cellular service and before the user gets activated for receiving the connectivity service. These security functionalities relying on the established public key (as the root of digital security) include the standard cryptographic techniques, including Diffie–Hellman Key Exchange to agree on the symmetric keys, the use of the symmetric key for message authentication code (MAC) for source/transmitter and message authentications, the symmetric encryption for message confidentiality, and pseudo-random number generation for random TMSI and nonces. In addition to the digital credentials for authentication, e.g., the core network's public key, previous research has suggested physical-layer and radio-based authentication credentials against malicious users [31–33].

Another threat model against base station security involves the attacker compromising or acting as the base station (as opposed to a user), hence acting as a malicious or rogue base station [34–36]. Previous research studied such malicious and rogue base station threats in the standardized cellular/telecommunications protocols, including attacks on the authentication and key agreement (AKA) [37], bidding-down to the less-secure 2G/3G protocol [38], and SMS phishing attacks [39,40]. Despite the known threats of malicious and rogue base stations, the defense solutions have been relatively lacking although recent research has proposed secure bootstrapping with a newly encountered base station based on incorporating cryptographic techniques in the 5G/4G RRC phases [41,42].

4.3. Mobility Control Security

The mobility control of a UAV flying base station relies on location and position awareness. The flying base station utilizes its component technology of a UAV/drone to provide mobility, as discussed in Section 1. For a flying base station building on a UAV drone, because of its purpose of serving the users, the mobility control depends on the flying base station's relative location to the user. For example, the flying base station moves to the line-of-sight path and closer to the user equipment to provide better wireless channel quality. Misplacing the flying base stations or the UAVs, e.g., via GPS spoofing [43–45], can disrupt the UAV flying base station's operations by triggering abnormally frequent battery re-charging [11,46]. To counter such misplacement and to defend the relative location integrity, previous research has included securing ranging to measure the distance between the nodes against signal-injection threats [47,48], including advancing distance or time-of-arrival measurements for ranging [49,50] and the detection of the distance-manipulation/DoS threats [51–53].

4.4. Battery Integrity Security

Unlike a stationary terrestrial base station, the UAV base station operates on battery energy. The battery energy introduces a unique denial-of-service (DoS) vulnerability, beyond targeting the more traditional networking and computing resources (such as those exhausting the networking bandwidth or the networking connections/states), which can be exploited by an energy-targeting DoS threat to drain the battery. Previous research includes battery-depletion DoS threat studies against drones or UAVs [11,46,54–56], which are especially related to our work in the hardware platform (flying base station is based on the UAV drone for mobility control and implementation). Because the mobility is constrained to the battery re-charging stations, disrupting the optimal connectivity provision, a DoS can disrupt the availability of the flying base station's operations. The battery-draining DoS has been more widely been studied in other wireless computing/networking contexts (wireless applications beyond the flying base station control), including in implantable medical/health devices [12,57,58], wireless charging [59,60], and standardized protocols of WiFi and Bluetooth [59–62].

4.5. Distributed Networking Security

Adding distributed, ad hoc, peer-to-peer networking capabilities beyond the centralized backend-infrastructure-accessible networking can enable greater connectivity coverage and implement redundancy in controlling the flying base stations to improve the connectivity provision reliability, as described in Section 3.4. Previous research studied the flying ad hoc network (FANET) or UAV ad hoc network to implement communications between the UAV drones, e.g., [63–65].

The Blockchain can also enable the secure dissemination of security-critical information to secure integrity and message authenticity against base-station threats. These threats are described in Section 4.2 although in a more centralized environment. The Blockchain can replace the centralized key management to enable/share the networking root of trust (from which other security functionalities and properties can be derived). Blockchain-based designs have implemented distributed key management and establishment in other computing/networking applications, e.g., general digital networking [66–69], vehicular communications [70,71], electronic voting system [72,73], and software-defined networking or SDN [74–76]. The previous research can provide initial building references for designing such solutions for the applications of securing ground/terrestrial and flying base stations. More specifically, as demonstrated by the previous research in other computing applications, the Blockchain can be used for the following security purposes: disseminating the public key while replacing the centralized-server-based public-key infrastructure (PKI) to authenticate the base station; identifying/detecting a malicious or rogue base station; and using the public-key to construct channels with message authenticity (e.g., the Blockchain can be used to securely disseminate the core network's public key, which can be used for the source integrity protection of the delivery of the core-network generated credentials, such as E(MSIN) or TMSI in Section 2.1).

5. Future Work Discussions

5.1. Systems Approach and Building on the Component Technologies

Section 4 describes the security research into the component technologies of the UAV flying base station (Section 1 surveys the review or survey articles of the component technologies to distinguish our contributions from them). While the previous research can provide the bases for securing flying base stations in principle, security solutions supporting the unique challenges and characteristics of future flying base stations require further work. This also requires a systems approach with an understanding of how the different components and requirements affect all of the security solutions. For example, an effective security solution can introduce overheads prohibitive for the flying base station system (such as delaying the RRC, introducing additional vulnerabilities for DoS, or requiring frequent re-charging of the battery) to limit its utility and practicality. Furthermore, the security challenges can be prioritized differently because of the new security impact implications introduced by the flying base station operations, e.g., a flying base station has severe and critical impact implications because of the telecommunications mobile users' reliance on the base station.

5.2. Prototype Implementation

Prototype implementation can inform and enable the systems approach described in Section 5.1. The implementation-based approach can expand our understanding of the system beyond the theoretical models and thus improve the practicality and utility of the system modeling. This is especially important for the UAV flying base station, which is a relatively novel concept and is currently undergoing engineering development, dynamically affecting our knowledge of the system.

For such research benefits, we built a UAV flying base station prototype based on a DJI Matrice 300 RTK drone for the mobility functionality and USRP B210 software-defined radio for the base station functionality. Figure 4 shows the hardwares and the corresponding simulated entities in 5G networking for our prototype. From left to right (loosely), the UAV flying base station connects to the stationary ground/terrestrial base station (the traditional base station), which in turn connects to the core network at the backend, as described in the 5G architecture in Figure 1. Our prototype also includes a monitoring system for digital networking analysis. The ground base station and the core network are connected via a switch, not shown in Figure 4. We plan to use such a prototype to better model the flying base station system and validate and test our security solutions. For example, based on a preliminary prototype-based study, for a rotor-based drone, the hovering operation dominates the lateral movements of the drone in energy, and most of the power consumption from the hovering operation is significantly larger than the marginal power consumption from adding lateral movement. We only made this observation after our prototype implementation, and the observation informed our modeling and research afterward. The observation also motivates the flying base station to land while serving as a base station as frequently as possible (as opposed to hovering in the air) and discretize and separate between the movement vs. stationary phases due to the overhead of launching itself into the air (as opposed to hovering and moving continuously).

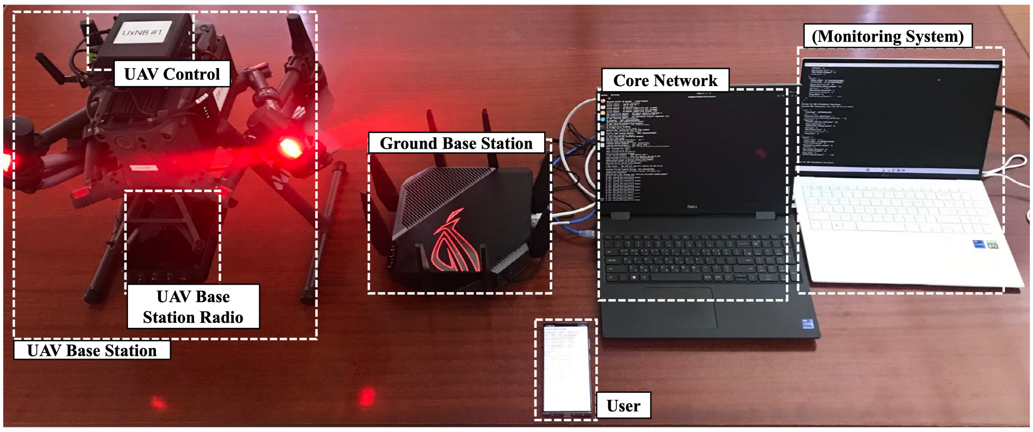

Figure 4. Our prototype implementation of UAV flying base station.

5.3. Flying Base Station for Security Opportunities

While this paper reviews the issues and gaps that challenge the security of flying base stations, flying base stations can provide unique opportunities to aid the security of base station operation. Such opportunities include advancing channel reliability and jamming resiliency by using the mobility of the flying base station, using the line-of-sight path securing to provide additional security properties (which can especially be important for mmWave communications as it gets block on the physical barriers), improving reliability by jointly processing the communications with line-of-sight sensing, and creating unique physical-layer signatures based on the mobility and the corresponding channel variations.

5.4. Hardening the Infrastructure and Ecosystem

Hardening the ecosystem including the rest of the connectivity-provision infrastructure (e.g., the backend core network, the stationary terrestrial base station, the other UAV flying base stations, the LEO satellite or HAPS base station) can improve reliability and security. The connectivity-provision infrastructure system can provide redundancy coverage and connectivity to mitigate the DoS threat and continue to provide availability/service to users by utilizing other base stations and by forming a service-provision network of base stations. For example, a mobile user can select between a flying base station and a stationary terrestrial base station, or a mobile user can have two flying base stations available.

5.5. Transition to Standardization and Practice

The telecommunications networking R&D prioritizes standardization for the implementation compatibility and interoperability across the vendors and the mobile service providers, c.f., OpenRAN. Securing the UAV flying base stations in 6G standardization facilitates the transition from security/engineering research to practice, as the standardization enables the compatibility with the systems/application requirements and drives the incorporation to the current practices and implementations. Therefore, the standardization incorporation of flying base station security research and the research community's effort to facilitate such incorporation remains an important future direction.

5.6. Security by Design

A UAV flying base station is a relatively new concept, and its prototypes and protocols are currently being developed. 3GPP introduces the notion (termed UxNB base station) and its requirements [1,2] but lacks the concrete standardization of the protocol and operations. Because the flying base station protocols are under development and a concrete and well-adopted protocol is lacking (anticipated for the upcoming 6G standardization), we encourage researchers to being addressing the misplacement threat and securing the flying base station against it. Practicing security by design and embedding security mechanisms during UAV-flying-base-station protocol design and standardization can enable security properties that would be more difficult if the protocol were already fixed and the security built as an afterthought. Security by design can also reduce the mechanisms' overheads compared to having to build modular, wrap-around security mechanisms after the rest of the functionality and performance mechanisms have been fixed. This review paper motivates such security-by-design practices as the UAV flying base stations are developed and standardized.

6. Conclusions

This paper intends to motivate and inform further research and development to secure the availability and integrity of UAV flying base station operations. We therefore identify the unique properties of the flying base station while describing and building on its component technologies, including the traditional telecommunications networking (including the stationary ground base station), UAV drone, embedded and battery control, authentication, and distributed networking. We review the related literature in securing the component technologies that would be especially useful in addressing the unique properties and the corresponding gaps for securing the flying base station. This paper ends with discussions of future works to facilitate future research and highlights important remaining challenges to secure UAV flying base stations. The future research directions highlighted in this review paper include taking a systems approach to study the security of the flying base station and its surrounding infrastructure, practicing and incorporating security-by-design as the flying base station technology is developed, using the flying base station for security opportunities, and transitioning to practice, implementations, and standardization.

Author Contributions: Conceptualization, S.-Y.C., J.K. (Jonghyun Kim) and J.K. (Jinoh Kim); methodology, S.-Y.C. and K.P.; software, K.P.; validation, S.-Y.C. and K.P.; investigation, S.-Y.C. and K.P.; writing—original draft preparation, S.-Y.C.; writing—review and editing, S.-Y.C., K.P., J.K. (Jonghyun Kim) and J.K. (Jinoh Kim); visualization, S.-Y.C. and K.P.; supervision, S.-Y.C. and J.K. (Jonghyun Kim); project administration, S.-Y.C., J.K. (Jonghyun Kim) and J.K. (Jinoh Kim); funding acquisition, S.-Y.C., J.K. (Jonghyun Kim) and J.K. (Jinoh Kim). All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by an Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korean government (MSIT) (No.2021-0-00796, Research on Foundational Technologies for 6G Autonomous Security-by-Design to Guarantee Constant Quality of Security).

Data Availability Statement: No new data were created.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. 3rd Generation Partnership Project. Enhancement for Unmanned Aerial Vehicles. 2019. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3557 (accessed on 15 April 2023).
2. 3rd Generation Partnership Project. Uncrewed Aerial System (UAS) Support in 3GPP. 2022. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3545 (accessed on 15 April 2023).
3. Wang, H.M.; Zhang, X.; Jiang, J.C. UAV-Involved Wireless Physical-Layer Secure Communications: Overview and Research Directions. *IEEE Wirel. Commun.* **2019**, *26*, 32–39. [CrossRef]
4. Yao, H.; Qin, R.; Chen, X. Unmanned Aerial Vehicle for Remote Sensing Applications—A Review. *Remote Sens.* **2019**, *11*, 1443. [CrossRef]
5. Fascista, A. Toward Integrated Large-Scale Environmental Monitoring Using WSN/UAV/Crowdsensing: A Review of Applications, Signal Processing, and Future Perspectives. *Sensors* **2022**, *22*, 1824. [CrossRef] [PubMed]
6. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [CrossRef]
7. Shrestha, R.; Bajracharya, R.; Kim, S. 6G Enabled Unmanned Aerial Vehicle Traffic Management: A Perspective. *IEEE Access* **2021**, *9*, 91119–91136. [CrossRef]

8. Lykou, G.; Moustakas, D.; Gritzalis, D. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. *Sensors* **2020**, *20*, 3537. [CrossRef]
9. Nassi, B.; Bitton, R.; Masuoka, R.; Shabtai, A.; Elovici, Y. SoK: Security and Privacy in the Age of Commercial Drones. In Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 1434–1451. [CrossRef]
10. Kim, S.G.; Lee, E.; Hong, I.P.; Yook, J.G. Review of Intentional Electromagnetic Interference on UAV Sensor Modules and Experimental Study. *Sensors* **2022**, *22*, 2384. [CrossRef]
11. Tlili, F.; Fourati, L.C.; Ayed, S.; Ouni, B. Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures. *Ad Hoc Netw.* **2022**, *129*, 102805. [CrossRef]
12. Rushanan, M.; Rubin, A.D.; Kune, D.F.; Swanson, C.M. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014; pp. 524–539. [CrossRef]
13. Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. SoK: Security Evaluation of Home-Based IoT Deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1362–1380. [CrossRef]
14. 3GPP. TS 23.003. Numbering, Addressing and Identification, 2021. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729 (accessed on 15 April 2023).
15. 3GPP. TS 36.321. Medium Access Control (MAC) Protocol Specification. 2021. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3194 (accessed on 15 April 2023).
16. 3GPP. TS 36.331. Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC). 2021. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2440 (accessed on 15 April 2023).
17. Chang, S.Y.; Hu, Y.C.; Laurenti, N. SimpleMAC: A jamming-resilient MAC-layer protocol for wireless channel coordination. In Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, Istanbul, Turkey, 22–26 August 2012; pp. 77–88.
18. Vo-Huu, T.D.; Vo-Huu, T.D.; Noubir, G. Interleaving Jamming in Wi-Fi Networks. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Darmstadt, Germany, 18–20 July 2016; WiSec '16; pp. 31–42. [CrossRef]
19. Chiang, J.T.; Hu, Y.C. Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks. In Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking, Montreal, QC, Canada, 9–14 September 2007; MobiCom '07; pp. 346–349. [CrossRef]
20. Kulkarni, R.V.; Venayagamoorthy, G.K. Neural network based secure media access control protocol for wireless sensor networks. In Proceedings of the 2009 International Joint Conference on Neural Networks, Atlanta, GA, USA, 14–19 June 2009; pp. 1680–1687. [CrossRef]
21. Chang, S.Y.; Hu, Y.C. SecureMAC: Securing wireless medium access control against insider denial-of-service attacks. *IEEE Trans. Mob. Comput.* **2017**, *16*, 3527–3540. [CrossRef]
22. Tung, Y.C.; Han, S.; Chen, D.; Shin, K.G. Vulnerability and Protection of Channel State Information in Multiuser MIMO Networks. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; CCS '14; pp. 775–786. [CrossRef]
23. Hou, T.; Bi, S.; Wang, T.; Lu, Z.; Liu, Y.; Misra, S.; Sagduyu, Y. MUSTER: Subverting User Selection in MU-MIMO Networks. In Proceedings of the IEEE INFOCOM 2022-IEEE Conference on Computer Communications, Virtual Event, 2–5 May 2022; pp. 140–149. [CrossRef]
24. Hussain, S.R.; Echeverria, M.; Karim, I.; Chowdhury, O.; Bertino, E. 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; CCS '19; pp. 669–684. [CrossRef]
25. Ettiane, R.; Chaoub, A.; Elkouch, R. Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions. *J. Inf. Secur. Appl.* **2021**, *61*, 102943. [CrossRef]
26. Raavi, M.; Wuthier, S.; Sarker, A.; Kim, J.; Kim, J.H.; Chang, S.Y. Towards Securing Availability in 5G: Analyzing the Injection Attack Impact on Core Network. In Proceedings of the Silicon Valley Cybersecurity Conference: Second Conference, SVCC 2021, San Jose, CA, USA, 2–3 December 2021; Revised Selected Papers; Springer: Cham, Switzerland, 2022; pp. 143–154.
27. Park, S.; Kim, D.; Park, Y.; Cho, H.; Kim, D.; Kwon, S. 5G Security Threat Assessment in Real Networks. *Sensors* **2021**, *21*, 5524. [CrossRef]
28. Sarker, A.; Byun, S.; Raavi, M.; Kim, J.; Kim, J.; Chang, S.Y. Dynamic ID randomization for user privacy in mobile network. *ETRI J.* **2022**, *44*, 903–914. [CrossRef]
29. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G Security Challenges and Solutions. *IEEE Commun. Stand. Mag.* **2018**, *2*, 36–43. [CrossRef]
30. Samarakoon, S.; Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Chang, S.Y.; Kim, J.; Kim, J.; Ylianttila, M. 5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network. *arXiv* **2022**, arXiv:2212.01298. [CrossRef]
31. Brik, V.; Banerjee, S.; Gruteser, M.; Oh, S. Wireless Device Identification with Radiometric Signatures. In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, San Francisco, CA, USA, 14–19 September 2008; MobiCom '08; pp. 116–127. [CrossRef]

32. Yu, P.L.; Baras, J.S.; Sadler, B.M. Physical-Layer Authentication. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 38–51. [CrossRef]
33. Wang, W.; Sun, Z.; Piao, S.; Zhu, B.; Ren, K. Wireless Physical-Layer Identification: Modeling and Validation. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2091–2106. [CrossRef]
34. Shaik, A.; Borgaonkar, R.; Park, S.; Seifert, J.P. On the impact of rogue base stations in 4g/lte self organizing networks. In Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Stockholm, Sweden, 18–20 June 2018; pp. 75–86.
35. Hussain, S.; Chowdhury, O.; Mehnaz, S.; Bertino, E. LTEInspector: A systematic approach for adversarial testing of 4G LTE. In Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego, CA, USA, 18–21 February 2018.
36. Yang, H.; Bae, S.; Son, M.; Kim, H.; Kim, S.M.; Kim, Y. Hiding in plain signal: Physical signal overshadowing attack on {LTE}. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 55–72.
37. Kim, H.; Lee, J.; Lee, E.; Kim, Y. Touching the untouchables: Dynamic security analysis of the LTE control plane. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–22 May 2019; pp. 1153–1168.
38. Shaik, A.; Borgaonkar, R.; Park, S.; Seifert, J.P. New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 15–17 May 2019; pp. 221–231.
39. Mulliner, C.; Golde, N.; Seifert, J.P. {SMS} of Death: From Analyzing to Attacking Mobile Phones on a Large Scale. In Proceedings of the 20th USENIX Security Symposium (USENIX Security 11), San Francisco, CA, USA, 8–12 August 2011.
40. Zhang, Y.; Liu, B.; Lu, C.; Li, Z.; Duan, H.; Hao, S.; Liu, M.; Liu, Y.; Wang, D.; Li, Q. Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, 9–13 November 2020; pp. 521–534.
41. Hussain, S.R.; Echeverria, M.; Singla, A.; Chowdhury, O.; Bertino, E. Insecure connection bootstrapping in cellular networks: The root of all evil. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 15–17 May 2019; pp. 1–11.
42. Singla, A.; Behnia, R.; Hussain, S.R.; Yavuz, A.; Bertino, E. Look before you leap: Secure connection bootstrapping for 5g networks to defend against fake base-stations. In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, Virtual Event, 7–11 June 2021; pp. 501–515.
43. Tippenhauer, N.O.; Pöpper, C.; Rasmussen, K.B.; Capkun, S. On the Requirements for Successful GPS Spoofing Attacks. In Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; CCS '11; pp. 75–86. [CrossRef]
44. Kerns, A.J.; Shepard, D.P.; Bhatti, J.A.; Humphreys, T.E. Unmanned aircraft capture and control via GPS spoofing. *J. Field Robot.* **2014**, *31*, 617–636. [CrossRef]
45. Davidovich, B.; Nassi, B.; Elovici, Y. Towards the Detection of GPS Spoofing Attacks against Drones by Analyzing Camera's Video Stream. *Sensors* **2022**, *22*, 2608. [CrossRef]
46. Chang, S.Y.; Park, K.; Kim, J.; Kim, J. Towards Securing UAV Flying Base Station: Misplacement Impact Analyses on Battery and Power. In Proceedings of the Sixth International Workshop on Systems and Network Telemetry and Analytics (SNTA 2023), Orlando, FL, USA, 20 June 2023.
47. Poturalski, M.; Flury, M.; Papadimitratos, P.; Hubaux, J.P.; Le Boudec, J.Y. The cicada attack: Degradation and denial of service in IR ranging. In Proceedings of the 2010 IEEE International Conference on Ultra-Wideband, Nanjing, China, 20–23 September 2010; Volume 2, pp. 1–4. [CrossRef]
48. Moser, D.; Leu, P.; Lenders, V.; Ranganathan, A.; Ricciato, F.; Capkun, S. Investigation of Multi-Device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures. In Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, New York, NY, USA, 3–7 October 2016; MobiCom '16; pp. 375–386. [CrossRef]
49. Capkun, S.; Hubaux, J.P. Secure positioning of wireless devices with application to sensor networks. In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, USA, 13–17 March 2005; Volume 3, pp. 1917–1928. [CrossRef]
50. Leu, P.; Singh, M.; Roeschlin, M.; Paterson, K.G.; Čapkun, S. Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020; pp. 500–516. [CrossRef]
51. Singh, M.; Leu, P.; Abdou, A.; Capkun, S. UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 73–88.
52. Vo-Huu, T.D.; Vo-Huu, T.D.; Noubir, G. Spectrum-Flexible Secure Broadcast Ranging. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Virtual Event, United Arab Emirates, 28 June–2 July 2021; WiSec '21; pp. 300–310. [CrossRef]
53. Sharma, A.; Jaekel, A. Machine Learning Approach for Detecting Location Spoofing in VANET. In Proceedings of the 2021 International Conference on Computer Communications and Networks (ICCCN), Virtual Event, 19–22 July 2021; pp. 1–6. [CrossRef]
54. Desnitsky, V.; Rudavin, N.; Kotenko, I. Modeling and evaluation of battery depletion attacks on unmanned aerial vehicles in crisis management systems. In Proceedings of the International Symposium on Intelligent and Distributed Computing, Saint-Petersburg, Russia, 7–9 October 2019; pp. 323–332.

55. Khan, M.A.; Ullah, I.; Kumar, N.; Oubbati, O.S.; Qureshi, I.M.; Noor, F.; Ullah Khanzada, F. An Efficient and Secure Certificate-Based Access Control and Key Agreement Scheme for Flying Ad-Hoc Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4839–4851. [CrossRef]
56. Desnitsky, V.; Kotenko, I. Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures. *Simul. Model. Pract. Theory* **2021**, *107*, 102244. [CrossRef]
57. Halperin, D.; Heydt-Benjamin, T.S.; Ransford, B.; Clark, S.S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W.H. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 18–21 May 2008; pp. 129–142. [CrossRef]
58. Siddiqi, M.A.; Strydis, C. Towards Realistic Battery-DoS Protection of Implantable Medical Devices. In Proceedings of the 16th ACM International Conference on Computing Frontiers, Alghero, Italy, 30 April–2 May 2019; CF '19, pp. 42–49. [CrossRef]
59. Chang, S.Y.; Kumar, S.L.S.; Tran, B.A.N.; Viswanathan, S.; Park, Y.; Hu, Y.C. Power-positive networking using wireless charging: Protecting energy against battery exhaustion attacks. In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Boston, MA, USA, 18–20 July 2017; pp. 52–57.
60. Chang, S.Y.; Kumar, S.L.S.; Hu, Y.C.; Park, Y. Power-Positive Networking: Wireless-Charging-Based Networking to Protect Energy against Battery DoS Attacks. *ACM Trans. Sen. Netw.* **2019**, *15*, 1–25. [CrossRef]
61. Moyers, B.R.; Dunning, J.P.; Marchany, R.C.; Tront, J.G. Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices. In Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 5–8 January 2010; pp. 1–9. [CrossRef]
62. Fobe, J.; Nogueira, M.; Batista, D. A New Defensive Technique Against Sleep Deprivation Attacks Driven by Battery Usage. In Proceedings of the Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Porto Alegre, RS, Brazil, 12–15 September 2022; pp. 85–96. [CrossRef]
63. Bekmezci, I.; Sen, I.; Erkalkan, E. Flying ad hoc networks (FANET) test bed implementation. In Proceedings of the 2015 7th International Conference on Recent Advances in Space Technologies (RAST), Istanbul, Turkey, 16–19 June 2015; pp. 665–668. [CrossRef]
64. Islam, N.; Hossain, M.K.; Ali, G.G.M.N.; Chong, P.H.J. An expedite group key establishment protocol for Flying Ad-Hoc Network(FANET). In Proceedings of the 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV), Dhaka, Bangladesh, 13–14 May 2016; pp. 312–315. [CrossRef]
65. Maxa, J.A.; Ben Mahmoud, M.S.; Larrieu, N. Secure routing protocol design for UAV Ad hoc NETworks. In Proceedings of the 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Prague, Czech Republic, 13–17 September 2015; pp. 4A5-1–4A5-15. [CrossRef]
66. Matsumoto, S.; Reischuk, R.M. IKP: Turning a PKI around with decentralized automated incentives. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 410–426.
67. Al-Bassam, M. SCPKI: A smart contract-based PKI and identity system. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, United Arab Emirates, 2 April 2017; pp. 35–40.
68. Yakubov, A.; Shbair, W.; Wallbom, A.; Sanda, D. A blockchain-based PKI management framework. In Proceedings of the First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) Colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23–27 April 2018.
69. Fan, W.; Hong, H.J.; Zhou, X.; Chang, S.Y. A Generic Blockchain Framework to Secure Decentralized Applications. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–18 June 2021; pp. 1–7.
70. Sarker, A.; Byun, S.; Fan, W.; Chang, S.Y. Blockchain-based root of trust management in security credential management system for vehicular communications. In Proceedings of the 36th Annual ACM Symposium on Applied Computing, Virtual Event, 22–26 March 2021; pp. 223–231.
71. Didouh, A.; Labiod, H.; Hillali, Y.E.; Rivenq, A. Blockchain-Based Collaborative Certificate Revocation Systems Using Clustering. *IEEE Access* **2022**, *10*, 51487–51500. [CrossRef]
72. Sarker, A.; Byun, S.; Fan, W.; Psarakis, M.; Chang, S.Y. Voting credential management system for electronic voting privacy. In Proceedings of the 2020 IFIP Networking Conference (Networking), Virtual Event, 22–26 June 2020; pp. 589–593.
73. Alvi, S.T.; Uddin, M.N.; Islam, L.; Ahamed, S. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *J. King Saud-Univ.-Comput. Inf. Sci.* **2022**, *34*, 6855–6871. [CrossRef]
74. Fan, W.; Chang, S.Y.; Kumar, S.; Zhou, X.; Park, Y. Blockchain-based Secure Coordination for Distributed SDN Control Plane. In Proceedings of the 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Tokyo, Japan, 28 June–2 July 2021; pp. 253–257.
75. Fan, W.; Park, Y.; Kumar, S.; Ganta, P.; Zhou, X.; Chang, S.Y. Blockchain-Enabled Collaborative Intrusion Detection in Software Defined Networks. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December–1 January 2020; pp. 967–974. [CrossRef]
76. Hameed, S.; Shah, S.A.; Saeed, Q.S.; Siddiqui, S.; Ali, I.; Vedeshin, A.; Draheim, D. A Scalable Key and Trust Management Solution for IoT Sensors Using SDN and Blockchain Technology. *IEEE Sens. J.* **2021**, *21*, 8716–8733. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.