Serverless protocols for inventory and tracking with a UAV

Collins Isdory Mtita, Maryline Laurent, Damien Sauveron, Raja Naeem Akram, Konstantinos Markantonakis, Serge Chaumette

Serverless Protocols for Inventory and Tracking with a UAV

Collins Mtita*, Maryline Laurent†, Damien Sauveron‡,
Raja Naeem Akram§, Konstantinos Markantonakis§ and Serge Chaumette¶
*TRAXENS S.A.S, Marseille, France
†SAMOVAR, Télécom SudParis, CNRS, Université Paris-Saclay, Évry, France
‡XLIM (UMR CNRS 7252 / Université de Limoges), Département Mathématiques Informatique. Limoges, France
§Information Security Group Smart Card Centre, Royal Holloway, University of London, Egham, United Kingdom
¶LaBRI (UMR CNRS 5800 / Université de Bordeaux), Talence, France
Email: c.mtita@traxens.com, maryline.laurent@telecom-sudparis.eu, damien.sauveron@unilim.fr,
{r.n.akram, k.markantonakis}@rhul.ac.uk, serge.chaumette@labri.fr

***Abstract*—It is widely acknowledged that the proliferation of Unmanned Aerial Vehicles (UAVs) may lead to serious concerns regarding avionics safety, particularly when end-users are not adhering to air safety regulations. There are, however, domains in which UAVs may help to increase the safety of airplanes and the management of flights and airport resources that often require substantial human resources. For instance, Paris Charles de Gaulle airport (CDG) has more than 7,000 staff and supports 30,000 direct jobs for more than 60 million passengers per year (as of 2016). Indeed, these new systems can be used beneficially for several purposes, even in sensitive areas like airports. Among the considered applications are those that suggest using UAVs to enhance safety of on-ground airplanes; for instance, by collecting (once the aircraft has landed) data recorded by different systems during the flight (like the sensors of the Aircraft Data Networks - ADN) or by examining the state of airplane structure. In this paper, our proposal is to use UAVs, under the control of the airport authorities, to inventory and track various tagged assets, such as luggage, supplies required for the flights, and maintenance tools. The aim of our proposal is to make airport management systems more efficient for operations requiring inventory and tracking, along with increasing safety (sensitive assets such as refueling tanks, or sensitive pieces of luggage can be tracked), thus raising financial profit.**

1. Introduction

Airlines carry millions of passengers all around the world. This task not only requires to take care of the passengers themselves but also of all necessary equipment, like luggage, tools, refueling vehicles and catering resources. Tracking all of these is a major challenge that cannot be achieved efficiently by hand, even though this is how it is performed today. From a passenger's perspective, luggage loss is a common occurrence; from an airline safety staff's point of view, a broken or missing safety piece of equipment, e.g. an oxygen mask, can be a major safety risk.

To improve this process, we propose a novel approach where all these assets are the subject of an inventory collated by a UAV. By doing so, we believe that the inventory can be carried out in a timely manner and performed several times if required, depending on flight and spatial constraints of a particular airport. Naturally, using UAVs in the vicinity of airports is not straightforward. Authorization by national flight control authorities and airport regulation bodies will be required, but by being situated in an area already subject to strong aerial regulations can make it easier to deal with. Furthermore the different regulation authorities are usually willing today to experiment new real world use cases of UAVs. However, this issue is out of the scope of the current paper.

1.1. Context

There exists several initiatives that support the process of luggage management in airports: a) to enable the travelers to track their luggage, e.g. at suitcase manufacturer level [1, 2] or at airline company level [3, 4], from checking/drop-off desk (and even before, to prevent theft) up to the loading in hold of the aircraft; b) to enable airline companies to improve tracking of checked luggages [5, 6]. Moreover, some major airports, such as Hong Kong, Dubai, Las Vegas, have already adopted RFID-enabled baggage handling systems to improve sorting and tracking efficiency.

Our scenario is therefore realistic because it corresponds to a real need and should contribute to improve the process, not only for luggage but also for all the assets airline companies need to deal with (for safety, repair, catering, etc.). The combination of UAVs and RFIDs for such operations can be more efficient than the standard procedures: UAVs can cover a large area, while embedded RFIDs on aircraft equipment, like oxygen generators, life vests and cabin emergency equipment, can drastically reduce inventory times. Delta Airlines, for instance, has installed more than 240,000 RFID tags on emergency pieces of equipment on all of its own and leased aircrafts. As a result, the company can check their

expiration dates aboard an aircraft in a few minutes, rather than approximately eight hours without RFID tags [7].

It is already the case that in some airports, not only luggage is equipped with RFID tags, but also maintenance tools [8, 9]. It is thus most likely to become a general approach (perhaps even subject to some regulation) because of the safety enforcement it makes it possible to support.

1.2. Problem statement

The context of operation of the UAVs and the goals to achieve raise a number of constraints and issues that must be taken into account.

1.2.1. Performance. From a functional perspective, using UAVs for inventorying implies to two main requirements. First, the inventory should be achieved in a timely manner, which means that detecting an RFID and collecting data from it should be as fast as possible. Second, the collection process and identification protocol should also be efficient to avoid several identification attempts that would waste time. Additionally, one should keep in mind that the UAVs – at least the kind of small UAV that could be used for this sort of operation – has limited resources, and the required computation should be minimised.

1.2.2. Security and privacy. Security and privacy are strong requirements. In security terms, only the supervising authority should have access to the results of the inventory and tracking processes. Privacy is also important; it should not be possible, for example, for unauthorized persons to trace pieces of luggage or safety/security-related assets.

Hence, we propose the use of lightweight secure and privacy-preserving serverless protocols as defined in article [10] for UAVs and RFIDs (on tagged assets) to perform efficient inventory and search operations. Security is achieved by means of the serverless protocols that enable centrally controlled devices to autonomously authenticate each other without the active participation of a centralized authentication or authorization server [11]. As such, they are appropriate in the airports such that UAVs and RFIDs, even if disconnected from the airport network infrastructure, may establish a mutually authenticated and secure channel among the involved communicating entities (*i.e.* among UAVs, and between UAV and RFID tags).

1.2.3. Energy consumption. In airport contexts, the UAVs ought to be of small size (for safety, security and space reasons), and so energy efficiency is paramount. The rational behind this requirement is based on the limitation of battery size (batteries have a substantial weight and a proper ratio between autonomy and weight has to be found). Airports being large areas and the number of assets to inventory and track being possibly large, energy consumption must be optimized to ensure a reasonable flight time without reloading the batteries.

1.3. Contributions

In this paper, our main goals are to propose two serverless protocols to enhance efficiency in inventory and tracking operations of RFID tagged assets in airport with support of UAVs. The proposed protocols, adapted from the Mtita et. al.'s [10] protocols for traditional RFID applications, are ideal for the UAVs in the airport environment to ensure reliable and energy-efficient inventory and search operations over some tagged assets without compromising their security and privacy.

The salient contributions of this paper are to propose suitable serverless protocols in the context of airport inventory control and tracking systems with:

a) an authentication protocol for mass identification of a group of RFID tags within a vicinity;
b) a search protocol to identify a selected group of RFID tags within the proximity.

1.4. Structure of the Paper

The remaining of this paper is organized as follows.

Section 2 presents the related work on UAV-based solutions and serverless protocols. In Section 3, we introduce the inventory and tracking system model by describing the involved entities, the requirements to ensure performance (computational and power-consumption efficiency), security and privacy, the assumptions, the threat and attack models. Section 4 details the two serverless protocols. In Sections 5 and 6, the performance, security and privacy analysis of the two protocols are conducted. Finally, Section 7 concludes the paper.

2. Related Work

As mentioned previously, there is potential the use of UAVs to facilitate the inventory of assets in airports (*e.g.* luggages, supplies required for the flights, maintenance tools) by communicating with the respective tags through authentication and search functionalities. The most feasible way is to make use of RFID technologies: *i.e.* attach RFID tags on assets and equip UAV with RFID readers. The first part of this section presents the inventory UAV-based solution, while the rest is devoted to analyzing RFID-related security protocols.

2.1. Inventory UAV-based Solutions

Since their invention, UAVs have been used for surveillance mission: *e.g.* for fire detection in forest for civilian application, for enemy detection in military application. Thanks to their capability to cover wide area in a minimal time, inventory and tracking solutions have been promptly proposed and even some proposals are currently patented. In [12], Shondel proposed an aerial inventory system for maintaining an inventory record of shipping vessels at a storage facility. In [13], McAllister claimed invention of a

mobile aerial RFID scanning platform. In [14], car dealerships claimed to save days of inventory using UAV reading passive ultrahigh-frequency (UHF) RFID tags or BLE beacons attached to cars. In 2007, Ong et al. [15, 16] proposed an RFID-equipped UAV to aid inventory automation in a warehouse. Similar ideas were developed by Bae et al. in [17] and by Andrukiewicz et al. in [18]. In [19], Longhi et al. studied electromagnetic aspects (propagation model, etc.) of the communication between an UAV and passive tags.

Recently, Greco et al. [20] proposed to use UAV to localize RFID sensors in [21] and to collect data from the RFID sensors scattered throughout the area by simply flying above them. However, in these two papers, the RFID sensors are not true RFID tags, *i.e.* they are not passive tags, but active wireless RFID nodes operating at 433 MHz. Still related to UAV and RFID, but out of the scope of the paper, in [22], Choi et al. proposed an indoor localization method for UAV using passive UHF RFID tags. It is worth noting that none of the aforementioned work deals with security aspects.

Since there is no work focusing on security and privacy issues between UAV and RFID, the two following papers related to security protocols for UAV and wireless sensors need to be mentioned. In [23], Won et al. proposed a secure communication protocol enabling a UAV to collect data from smart objects (*i.e.* wireless nodes). The closest work is the secure and trusted channel protocol proposed by Akram et al. [24] to enable in the airport environment a UAV to establish secure communication with sensors of a wireless Aircraft Data Network and other systems to collect data. The main difference with these two proposals, apart from the absence of RFID, is that the cryptographic operations used are more complex than those we use in this paper.

2.2. Serverless Protocols

RFID security protocols can be categorized into two groups: *connection-oriented* and *connectionless* (or *serverless*) protocols. Connection-oriented protocols dictate that an RFID reader – a UAV in our case – establishes and maintains a communication channel with the backend or database server during the course of authentication with the tags. Alternatively, connectionless or serverless protocols do not require an established communication between the server and the RFID reader during authentication. The latter case is more pertinent to the UAV case at hand, as it allows for greater mobility and resilience. This section focuses on the serverless authentication protocols, particularly the authentication and secure tag search protocols.

2.2.1. RFID Authentication Protocols. To the best of our knowledge, the use of serverless protocols for RFID authentication was first instigated by Tan et al. [25] in their article *Serverless search and authentication RFID protocols* published in 2008. They proposed protocols aimed at solving two fundamental problems: first, the identification of tags by readers with no persistent connection to a central database; and second, securely search tags without leaking identifying information to adversaries. In 2013, the authors of [26] found that Tan et al.'s protocols are vulnerable to traceability, impersonation and privacy attacks.

In 2009, Lin et al. [27] proposed a serverless RFID authentication protocol to improve the computational performance of Tan et al.'s [25] authentication protocol. However, Lee et al. [28] note that Lin et al.'s protocol only performs a one sided authentication, that is, the reader authenticates the tag, but the tag does not authenticate the reader. Moreover, Lin et al.'s proposed protocol is still vulnerable to impersonation attack [28].

Hoque et al. proposed a serverless, untraceable authentication, and forward secure protocol for RFID tags [29] claiming that their protocol secures both reader and tag against common attacks with no need for a central database's mediation. But, this claim was disproved by Deng et al. [30] by showing that Hoque et al.'s protocol was susceptible to data desynchronization attack. Deng et al. also improved Hoque et al.'s [29] authentication protocol in order to withstand data desynchronization attacks. However, the authors of [31] found that Deng et al.'s protocol is still vulnerable to data desynchronization attack after two protocol runs. In 2015, Abdolmaleky et al. [32] proposed a protocol to address the weaknesses found in the protocols proposed by Hoque et al. [29] and Deng et al. [30], which are tag impersonation and reader impersonation attacks. Their proposed protocol [32] solved these problems but after analysis we found that it has very limited use for mass authentication. Indeed, in their proposal, once the reader is granted access to the tag(s), the backend server can no longer access the respective tag(s). This restriction may make sense in some domains of applications, but its usability is very limited in the mass authentication scenarios where disparate readers simultaneously authenticate tags within their vicinity.

ERAP, *ECC-based RFID Authentication Protocol* [33], is a serverless protocol ensuring mutual authentication between reader and authorized RFID tags. This scheme was found vulnerable to denial of service attack by authors of [34]. The authors of [35] also proposed (HOA) *HLRO Authentication*, an ECC-based authentication scheme suitable for low-power mobile devices. However this protocol has a strong requirement that each communicating entity has prior knowledge about each other and it is too much CPU and memory demanding as tags must perform ECC and modular operations.

Timestamp is an interesting element for authentication support by constrained devices, as first suggested in 2006 by Tsudik [36]. Considering that constrained devices do not have embedded clocks, it was quite a novel idea at the time it was instigated. Tsudik's view was simple, a tag stores a static timestamp and an RFID reader periodically broadcasts timestamp of its current time. A tag, in the vicinity of a reader, receives and compares the broadcast timestamp against the stored timestamp. If the broadcast timestamp is larger than the stored timestamp, the tag updates its timestamp and replies with a keyed hash over its permanent key and the new timestamp. Otherwise, the tag sends a random value generated by a Pseudo Random Number Gen-

erator (PRNG) to confuse an adversary and avoid narrowing attacks. Narrowing attack occurs when the adversary queries a tag with a particular timestamp and then later tries to identify the same tag by querying a candidate tag with a timestamp slightly above the previous one [36].

Tsudik [36] himself noted that his proposed scheme is susceptible to Denial of Service (DoS) attacks as an adversary can easily desynchronize a tag by sending a timestamp value that is ahead of time. This idea was later improved by authors of [37] by moving the attack from the resource constrained tag to the powerful backend server. The improvement aimed at thwarting DoS attacks against the tags but it also resulted to an exhaustive search to the backend server.

The mutual authentication and search protocols adapted in this article were proposed in [10], where the authors claim that their protocols hold in resisting all common security attacks and provide the best performance by using lightweight security primitives.

2.2.2. Secure RFID Tag Search Protocols. Like serverless authentication protocols, the idea of secure RFID tag search protocols was introduced by Tan et al. [25] for the purpose of simplifying RFID readers to easily locate a target tag. Nevertheless, tag search protocols have not received the attention [38] that mutual authentication protocols received. Nonetheless, they provide a very useful functionality in efficiently locating a specific tag within a group of tags.

Tan et al. [25] proposed tag search protocol. Their protocol is found to perform unidirectional authentication [39], i.e the reader authenticates a tag but the tag does not authenticate the reader. In turn, the tag cannot be certain of the authenticity of the reader as any other entity can masquerade as a reader and fool the tag. The protocol is also susceptible to reader's identity disclosure, replay, and impersonation attacks as analyzed by Lee et al. [28].

In 2009, Lin et al. [27] proposed a search protocol by improving Tan et al.'s protocol, but Lin et al.'s protocol was found to be susceptible to replay and impersonation attacks. In 2011, Chun et al. [39] proposed an RFID tag search protocol with the goal of preserving privacy of communicating parties. However, as the authors of [40] noted, Chun et al.'s protocol is susceptible to tracking attacks due to static values sent from the reader to the tag.

In 2012, Lee et al. [28] also proposed an RFID search protocol. Their protocol uses hash function twice on the same parameter and also makes use of PRNG on the tag side. These operations consume a lot of resources with respect to the computational constraints of most RFID tags [40].

In 2014, Xie et al. [41] proposed a secure tag search protocol in their article, *RFID seeking: Finding a lost tag rather than only detecting its missing*, which is secure against common attacks such as replay, traceability and DoS. Xie et al.'s [41] protocol was later improved by Jeon et al. [42] in 2014. Jeon et al.'s protocol suffers from the reader traceability attack, which was not in the original protocol proposed by Xie et al. [41]. It is observed that the lack of context in the protocol between the reader and the tag leads to the replay attacks.

In 2017, Sundaresan et al. [43] proposed a secure search protocol for low cost passive RFID tags, which is based on quadratic residues. The authors claim that the tag running their protocol performs only simple security primitives such as XOR ($\oplus$), modular arithmetic operation (mod) and 128-bit PRNG, thus achieving compliance with EPC standards. However, the author specifically state that their protocol requires the reader must maintain a connection to the back-end server during authentication phase as the server must perform some of the critical operations; this disqualifies it as a candidate for search protocols for the scenarios in this article.

The search protocols described above make use of static authentication parameters, which do not expire. This implies that the reader is only authorized once and the parameters remain valid forever. Moreover, once the reader is compromised, the parameters cannot be revoked, hence tags can be accessed by adversaries without any remedies to the problem.

In 2016, Mtita et al. [10] proposed a secure serverless search protocol which is adapted in this article to provide a secure search functionality for the UAVs. The authors claim that their protocol is lightweight, as tags perform very few operations during the search query and only one tag responds, if the right tag is present. Likewise, they claim that the search protocol is resistant to narrowing attacks, replay and cloning attacks [36].

3. Inventory and Tracking System Model

This section outlines specifications for each player involved in the system and protocols, in addition to the performance, security and privacy requirements, assumptions, and threat and attack models.

3.1. Entities

The protocols proposed in this article involve the interaction between three parties as presented below with their respective characteristics. The definition of each parameter used in the protocols is provided in Table 1.

- **Backend Server**: denoted as S is a trusted, powerful entity with unlimited resources. S has a list of all legitimate tags and UAVs, hence it plays a role of assigning parameters to UAVs for accessing authorized tags. Note that the server is offline when the UAV is launching an authentication session with the tags.
- **Unmanned Aerial Vehicle (UAV)**: denoted as UAV_j, has finite resources for storage, computation, energy and communication. UAV_j stores a list of tags L_j, which represents all authorized tags that UAV_j can authenticate and exchange information with. UAV_j remains untrusted by the tags until the mutual authentication phase is successfully completed.
- **RFID Tag**: denoted as ρ_i, the tag is characterized by scarce resources in terms of storage, computation,

energy and communication. Each tag ρ_i has a unique identifier id_i that doubles as a secret key shared with the backend server S. Likewise, each tag ρ_i has a static timestamp T_{SYS} initialized at the time of tag's manufacture and does not need to be tag-unique.

3.2. Performance Requirements

To ensure computational and energy consumption efficiency of our protocols, the main players of the protocols, i.e. UAVs and tags, must only use lightweight operations.

3.3. Security and Privacy Requirements

The following security and privacy requirements must be present in our proposed mutual authentication and secure tag search protocols.

Mutual Authentication. Our protocols must perform mutual authentication in order to establish mutual trust between tags and UAVs, eventually avoiding impersonation.

Freshness. Protocols must enforce message freshness in order to thwart replay attacks. Our proposed protocols enforce freshness by generating each message using random values during each protocol run.

Untraceability. Non-traceability, or untraceability, entails that it should not be possible for a tag (or UAV) to be identified based solely on the exchanged messages nor to link two different sessions to the same tag (or UAV).

3.4. Assumptions

- Backend server is a trusted entity and cannot be compromised.
- Backend server allocates only a fraction of RFID tags to each UAV for authentication.
- PRNG and keyed Hash-based Message Authentication Code (HMAC) functions are considered as robust.

3.5. Threat and Attack Models

To model the security and privacy for our protocols, we consider a polynomial time adversary α attacking our proposed protocols following the games described below with the aim of gaining access to secret information or disrupting a normal protocol run. The security and privacy games are designed to show the capabilities, limitations and options of the adversary as he attempts to break the protocols. The games described hereafter can apply to the proposed protocols depicted in Figures 2 and 3.

***Game 1**: α masquerades as UAV*

- **step 1.1**: α observes and eavesdrops several exchanges between legitimate UAV_j and one or more tags.
- **step 1.2**: α sends messages *A* and *C* (respectively, only message *A* for the tag search protocol) to tag ρ_i.
  α wins if he can send valid message *C*.

***Game 2**: α creates a new counterfeit tag ρ_x*

- **step 2.1**: α physically attacks ρ_i's to access its data.
- **step 2.2**: α uses the data from valid ρ_i to create other counterfeit tags ρ_x where $x \neq i$.
  α wins if he can create counterfeit tag ρ_x and fool legitimate UAV_j.

***Game 3**: α tracks tag ρ_i*

- **step 3.1**: α is able to observe exchanges between legitimate UAV_j and tags ρ_1 and ρ_2, one after the other, for a polynomial number of times each.
- **step 3.2**: The challenger selects a tag ρ_i, $i \in \{1, 2\}$, and let it authenticate to UAV_j. α listens to the exchanges and sends a guessed value i to the challenger.
  α wins the game if value i is correct. The protocol is considered private if α cannot win the game with a probability greater than 0.5.

4. Search and Authentication Protocols

This section presents security protocols relevant to securing the communication between UAVs and the corresponding authorized tags.

Due to the high mobility of UAVs, serverless mutual authentication and search protocols seem ideal to solve the security and privacy problems. A mutual authentication protocol helps to simultaneously authenticate an UAV with a large number of tags attached to assets (*e.g.* luggages, supplies required for the flights, maintenance tools). The mass authentication is useful where a large number of assets need to be securely and quickly authenticated at once.

On the other hand, the secure search protocol is useful in efficiently locating a specific tag attached to a baggage among a number of other tags. The efficiency of the search protocol is due to its ability to narrow down the query that forces only the target tag to respond to the authentic request.

The two serverless protocols proposed in this section complement one another and share the same first phase. The first phase presented in section 4.2 involves authorization between an UAV and the central backend server. Each UAV must perform this phase prior to commencing the second phase of the protocols, which involves either authentication or search. We describe the common phase before we start explaining how each of the individual authentication and search phase work.

4.1. Protocol Notations

The protocols description and figures in the following sections will be described using notations given in Table 1.

In Table 1, AR_{ij} represents encoded access rights for UAV_j with respect to the data stored in tags $temp_{ij}$. In this article, AR_{ij} is represented in the form of a code, like Unix file permissions, with *Read, Write* and *Execute* options. Time window W_{S_j} is a 64-bit parameter represented as $[T_{0_j}||T_{Z_j}]$, where T_{0_j} is the start date and T_{Z_j} is the end date defining the time limits for the specific UAV_j to access the tags within the list L_j.

Table 1. PROTOCOL NOTATIONS WITH SIZE ESTIMATIONS

Parameter name	Symbol	Bits
Tag's Static Timestamp	T_{SYS}	32
UAV's Timestamp	t_j	32
Start date	$T0_j$	32
End date	TZ_j	32
Time window	W_{S_j}	64
Access rights	AR_{ij}	128
Tag's Random Number	r_i	128
UAV's Random Number	r_j	128
Tag's Identifier	id_i	128
Temporary Tag's Identifier	$temp_{ij}$	128
Tag's Key	K_{ij}	160
HMACs (from UAV or Tag)	H_{ij}, V_{ij}	160
Identify of UAV_j	ID_{UAV_j}	-
List of authorized tags	L_j	-
Concatenation operator	$\|\|$	-

4.2. Authorization between Backend Server and UAV

The *authorization phase*, depicted in Figure 1, involves the exchange between an UAV, UAV_j, and the backend server, S, through a secure channel, where UAV_j acquires appropriate access rights from the server to access a group of tags attached to assets.

1) S generates a key K_{ij} and a temporary identity $temp_{ij}$ corresponding to each tag ρ_i that UAV_j is authorized to access to with the given access rights AR_{ij}. The key K_{ij} and identity $temp_{ij}$ of each tag are ephemeral and derived from the time window W_{S_j} and start date T_{0_j} generated by S, respectively.

$$K_{ij} = HMAC_{id_i}(W_{S_j}||AR_{ij}) \quad (1)$$

$$temp_{ij} = HMAC_{id_i}(T_{0_j}) \quad (2)$$

2) S builds a list of authenticated tags L_j granted to UAV_j for a given time window W_{S_j} with access rights AR_{ij}. S is assumed to assign different time windows W_{S_j} and AR_{ij} to different UAVs.

$$L_j = \{(temp_{1j}, K_{1j}), ..., (temp_{ij}, K_{ij})\} \quad (3)$$

3) S securely sends L_j, AR_{ij}, and W_{S_j} to UAV_j.

4.3. Serverless Authentication between UAV and Tags

After running a mandatory preliminary phase of authorization with the backend server, depicted in section 4.2 and Figure 1, UAV_j is ready to perform mutual authentication phase with the tags in the list L_j. The mutual authentication phase, described in Figure 2, involves verification and authentication between UAV_j and a *tag* ρ_i with the purpose of guaranteeing the authenticity of UAVs and tags during communication and exchange of secret data.

As UAV_j flies over assets, it broadcasts a message A containing W_{S_j}, AR_{ij}, and r_j. All tags within the vicinity of UAV_j respond with a challenge containing r_i and $H_{ij} = HMAC_{K'_{ij}}(r_i||r_j)$, where r_i is the random number generated by a respective tag. Upon receipt of message B from multiple tags, UAV_j calculates $H'_{ij} = HMAC_{K_{ij}}(r_i||r_j)$ using the values of K_{ij} in the list L_j. If the corresponding value of H_{ij} is found, UAV_j authenticates the respective tag and replies with V_{ij} and t_j via message C.

Upon receipt of message C, ρ_i checks the validity of V_{ij}. The correct value of V_{ij} authenticates UAV_j and leads ρ_i to update its timestamp T_{SYS} with a received timestamp t_j.

Session Key Generation. The shared session key $K_S = HMAC_{K'_{ij}}(t_j||r_i||W_{S_j})$ is locally generated in both UAV_j and ρ_i using parameters exchanged during the mutual authentication phase in steps d_{26} and d_{34}, respectively. It should be noted that, a session key K_S only serves to encrypt data exchanged, if need arise. However, the generated shared key K_S plays no role during the next authentication sessions and is only valid during the respective time frame, hence a session key. The proposed protocol does not require synchronizing or updating parameters between authentication sessions.

4.4. Serverless Secure Tag Search Protocol

RFID tag search protocol allows an UAV to securely search for a particular tag among a group of tags within its vicinity, authenticate the tag and initiate a secure data exchange session. RFID tag search functionality is a basic and invaluable tool for efficiently searching among a large amounts of tags [25] without the need to authenticate all tags in the vicinity prior to finding the right one. The tag search protocol minimizes the time to search for a known tag within a group of tags.

Authentication. When UAV_j wants to search for a specific tag with a temporary identity $temp_{ij}$ from the list of tags L_j, it calculates $H_{ij} = HMAC_{K_{ij}}(t_j)$ where t_j is the UAV_j's current timestamp and K_{ij} is the key corresponding to a tag with identity $temp_{ij}$. UAV_j broadcasts message A containing W_{S_j}, AR_{ij}, H_{ij} and t_j to all tags in the vicinity.

After receiving message A, a tag ρ_i validates the parameters received, calculates its temporary key K_{ij} and checks whether it is the intended recipient tag by calculating and comparing $H'_{ij} == H_{ij}$. If it is indeed the intended tag and the values are correct, the tag authenticates the UAV_j and ρ_i updates its timestamp T_{SYS} before replying with a challenge V_{ij} and r_i to UAV_j. The other tags do not respond to the query.

Upon receipt of message B, UAV_j verifies V_{ij}. If V_{ij} is valid, UAV_j authenticates ρ_i.

Session Key Generation. UAV_j and tag ρ_i compute a shared key K_S using parameters from both parties in steps e_{23} and e_{18}, respectively. K_S is used to securely exchange data between UAV_j and ρ_i using an encryption scheme which is out of the scope of this paper.

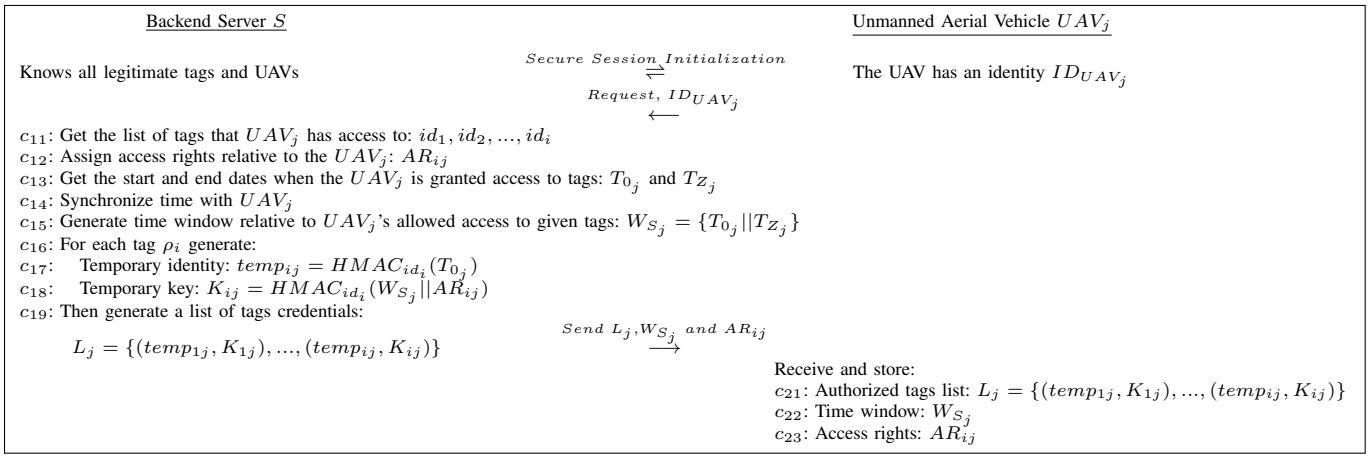

Figure 1. Authorization between a backend RFID server and a UAV supporting authentication and access rights assignment

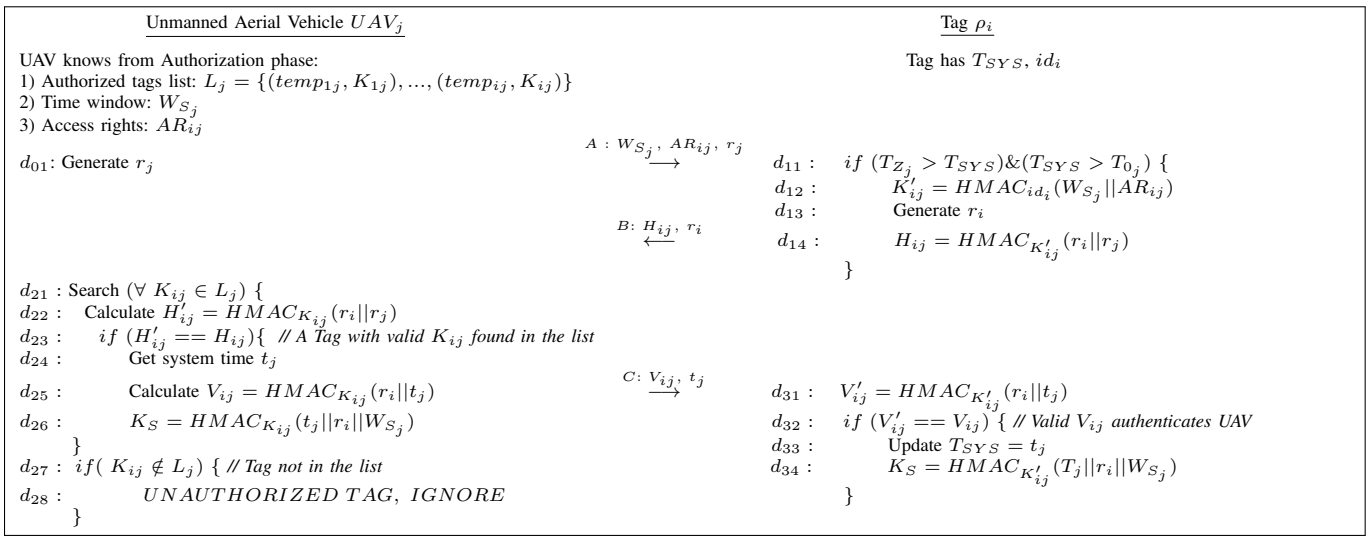

Figure 2. Our Serverless Authentication Protocol between UAV and Tag

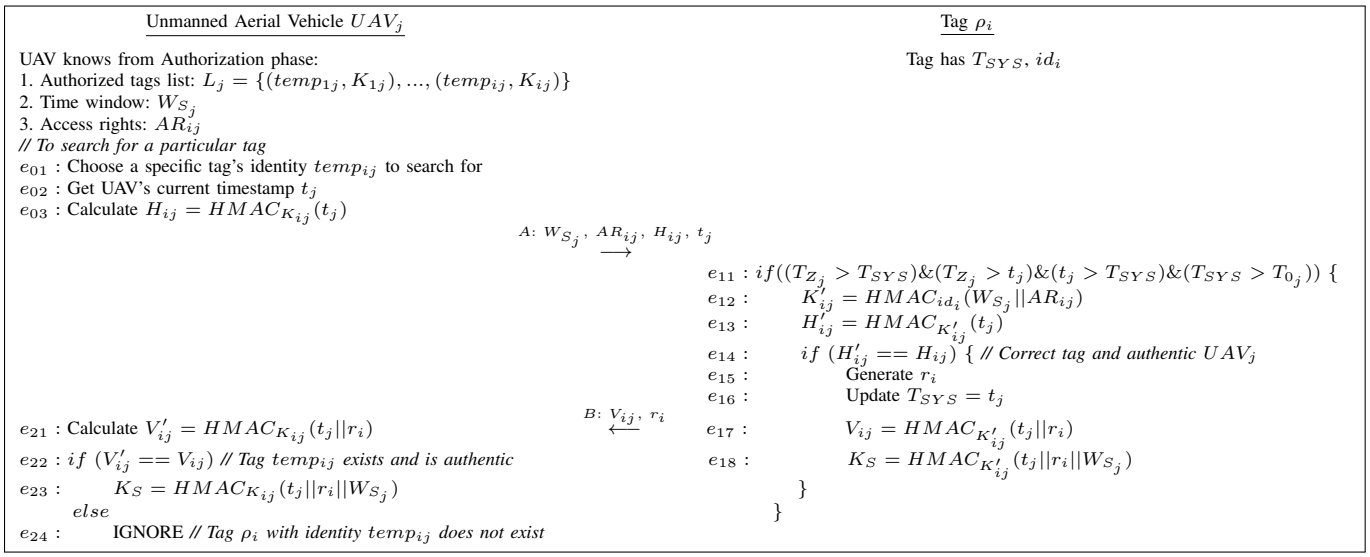

Figure 3. Our Serverless Secure RFID Tag Search Protocol

5. Performance Analysis

This section analyses the performance of our proposed authentication and search protocols relative to other protocols.
It is worth noting that the *Computational Cost* of both UAVs and tags for both protocols is lightweight and compatible with resource constrained devices since they only need to have capability to execute basic primitives such as concatenation, comparison, and HMAC.

5.1. Performance Analysis for the Authentication Protocol

Table 2 compares our mutual authentication protocol to other similar protocols. Hoque et al. [29] protocol performs authentication using four messages, this translates to energy overhead due to sending and receiving operations. Our protocol is attractive as it supports mutual authentication in three messages. Finally, while Lee et al. [28], Hoque et al. [29] and Abdolmaleky et al. [32] use hash function in their implementation, our protocol integrates a HMAC function for providing a higher security. However, the HMAC function in our protocol can be easily replaced by any secure hash or PRNG function that suit the tag's requirement and the proposed security and performance properties of our protocol will still hold.

Table 2. PERFORMANCE COMPARISON BETWEEN OUR SERVERLESS AUTHENTICATION AND SIMILAR PROTOCOLS

Criteria	Lee et al. [28]	Hoque et al. [29]	Abdolmaleky et al. [32]	Our Protocol
Computation cost	4 hash	2 hash / 1 PRNG	4 hash	3 hmac / 1 PRNG
Total messages	3	4	3	3
Storage cost (bits)	896	1024	1024	864

Communication Cost: In our protocol, the tag ρ_i sends 288 bits (36 bytes) and receives 512 bits (64 bytes) of data during communication.

Storage Cost: At the tag, our protocol uses 160 bits for storing timestamp T_{SYS} and tag's identifier id_i together with an additional 480 bits during operation for storing r_j, K_{ij} and V_{ij} which makes a total of 640 bits or 80 bytes. At the peak moment, just before sending message *B*, the tag must store a total of 864 bits or 108 bytes. The UAV_j storage demands vary depending on the number of tags it is allowed to authenticate at a time, that is the number of tag parameters contained in list L_j.

5.2. Performance Analysis for the Secure Tag Search Protocol

The similarities between RFID secure tag search protocol and mutual authentication protocol lead to similarities in performance and security properties. As such, this section discusses only a few properties that differ from those discussed in section 5.1.

The performance comparison between our secure tag search protocol with other similar protocols is given in Table 3.

Table 3. PERFORMANCE COMPARISON BETWEEN OUR TAG SEARCH PROTOCOL AND SIMILAR PROTOCOLS

Criteria	Jeon et al. [42]	Hoque et al. [29]	Xie et al. [41]	Our Protocol
Computation cost	4 PRNG	2 hash / 3 PRNG	4 hash	3 hmac / 1 PRNG
Total messages	3	4	3	2
Storage cost (bits)	896	1024	1026	896

Communication Cost: Tag search protocol exchanges only two messages, one from each party where ρ_i sends 288 bits (36 bytes) and receives 384 bits (48 bytes) of data.

Storage Cost: The peak storage for the tag search protocol is the moment just before the tag sends message *B*. The total storage space required on the tag is 896 bits or 112 bytes. This corresponds to the total size of K_{ij}, V_{ij}, W_{S_j}, AR_{ij}, t_j, r_i, id_i, T_{SYS}, and K_S.

6. Security and Privacy Analysis

This section analyses the security of our proposed mutual authentication and secure tag search protocols using relevant threat and attack models put forth in section 3.5.

6.1. Security Analysis for the Authentication Protocol

As depicted in Table 4, our protocol is the only one that guarantees the privacy of the tags and its secrets when the reader is compromised. The rest of the protocols fail to revoke or change the information granted to the reader after the initial authorization phase. Moreover, in Lee et al.'s [28] proposed protocol, the tag always responds with a constant value, which makes it traceable in all communications with the same reader. Likewise, Hoque et al.'s [29] protocol does not provide mutual authentication between the tag and UAV, hence diminishing the level of trust and security of the protocol.

Game 1 - α masquerades as UAV. : Referring to $Game\ 1$ in section 3.5, α's objective is to send legitimate messages *A* and *C*. That is, α can either crack the key K_{ij} or directly generate a valid message *C* based on sniffed messages *A*, *B* and *C* of earlier legitimate sessions.
One way to crack K_{ij} is to extract from message *B* the values of K_{ij} using public values r_i, r_j and H_{ij}. This assumes reversibility of HMAC function, which is contrary

Table 4. SECURITY COMPARISON BETWEEN OUR SERVERLESS AUTHENTICATION PROTOCOL AND SIMILAR PROTOCOLS

Security requirement	Lee et al. [28]	Hoque et al. [29]	Abdolmaleky et al. [32]	Our Protocol
Tag untraceability	No	No	Yes	Yes
Avoid tag impersonation	No	Yes	Yes	Yes
Avoid replay attack	No	Yes	No	Yes
Mutual authentication	Yes	No	Yes	Yes
Reader compromise resistance	No	No	No	Yes

to the assumption made in section 3.4.
Alternatively, α may combine messages *A, B* and *C* in order to deduce valuable information and use it to crack the key K_{ij}. However, messages *B* and *C* behave as random or pseudo-random strings because they evolve independently from each other as their inputs are different. As such, regardless of the number of sniffed messages *A, B* and *C*, it is infeasible to extract any valuable information, and the game cannot succeed.

Game 2 - α ***creates counterfeit tags.*** : In our protocol, we do not consider any hardware-based defences against physical attacks. Hence, α may physically compromise a tag ρ_i and access everything in it, including secret information and the information exchanged with UAV_j. To create a fake tag ρ_x and fool UAV_j, α must know ρ_x's identity id_x. As the identity of each tag is secret, different and unique, α cannot guess the identity of tag ρ_x by knowing the identity of ρ_i. Thus, compromising a tag ρ_i does not give α the power to derive other tags in L_j, hence α cannot win the game.

Game 3 - α **tracks** ρ_i**.** : Referring $Game\ 3$ in section 3.5, ρ_i and UAV_j use random values to generate messages *B* and *C*, respectively. During session k, ρ_i responds with messages B_{1ik} and B_{2ik}, which appear random to α. Any response from ρ_1 is semantically indistinguishable from responses of ρ_2, and even to the previously sent responses of ρ_1. As such, an adversary α is unable to guess with a probability greater than 0.5 which tag ρ_i sent message *B*.

6.2. Security Analysis for the Secure Tag Search Protocol

Table 5 gives a brief comparison between our protocol and other similar protocols. Our protocol protects tags' identities from adversaries. Moreover, Jeon et al. [42] suffers from the replay attack while Hoque et al. [29] proposed protocol does not perform mutual authentication, hence reducing trust between the communicating parties.

Our tag search protocol, like our proposed authentication protocol, is not vulnerable after reader compromise attacks i.e, the values obtained after compromising the reader cannot be used indefinitely. However, the rest of the protocols i.e., those proposed by Jeon et al. [42], Hoque et al. [29] and Xie et al. [41] give away crucial information that cannot be revoked once the reader, UAV in our case, is compromised. The adversary may continually use these values to communicate with the respective tags without the possibility of revoking them.

Table 5. SECURITY COMPARISON BETWEEN OUR TAG SEARCH PROTOCOL AND SIMILAR PROTOCOLS

Security requirement	Jeon et al. [42]	Hoque et al. [29]	Xie et al. [41]	Our Protocol
Tag untraceability	Yes	Yes	Yes	Yes
Avoid tag impersonation	Yes	No	Yes	Yes
Avoid replay attack	No	Yes	Yes	Yes
Mutual authentication	Yes	No	Yes	Yes
Reader compromise resistance	No	No	No	Yes

Game 1 - α ***masquerades as an UAV.*** : Referring to $Game\ 1$ in section 3.5, α's objective is to send a valid message *A* to ρ_i. The first idea would be that α replays a valid message *A*. However, the message is intended for one specific tag with the key K_{ij}, and processing of message *A* by the tag leads to the tag updating its timestamp. As a consequence, assuming that the target tag is in the vicinity of the legitimate UAV when transmitting a valid message *A*, replays remain useless as it will be considered by the target tag as out-of-date.

There are two other alternatives for α: cracking the key K_{ij} or generating a valid message *A* based on sniffed messages of earlier valid sessions. For cracking K_{ij}, one way is to extract the value of K_{ij} from message *A* or *B* by reversing the HMAC function with known public values t_j or r_i. However, this contradicts our assumptions of section 3.4.

Alternatively, α can analyse several valid pairs of messages *A* and *B* to generate a new valid message *A*. However, messages *A* and *B* behave as random or pseudo-random strings due to their random inputs. Thus, it is not possible to guess a new valid message *A*, and the game cannot succeed.

Game 2 - α ***creates counterfeit tags.*** : This game is similar to the one analysed in the previous authentication protocol in section 6.1.

Game 3 - α **tracks** ρ_i**.** : As our search tag protocol facilitates a legitimate UAV_j to search and communicate to a chosen tag within a group, it is also an ideal opportunity for α to track a tag and launch attacks.

However, launching a successful attack means α must link message *B* to a particular tag. As messages *B* coming from ρ_1 and ρ_2 are semantically indistinguishable due to the

random inputs r_i and r_j, an adversary α cannot guess with a probability greater than 0.5 which tag ρ_i sent message *B*, and he can not win the game.

7. Conclusion

In this paper we have addressed the problem of inventory and tracking of the RFID tagged assets from different actors (airline companies, passengers, maintenance staff, etc.) in airport scenarios, including planes and the assets they embed. We have put forward an approach that uses a UAV. To achieve this approach, we have proposed two serverless protocols:

a) an authentication protocol for mass identification of a group of RFID tags within a proximity;
b) a search protocol to interact with a specific RFID tags within the proximity.

We have presented: the inventory and tracking system model; the requirements to ensure performance in terms of computation (we are working with constrained systems); the power-consumption issue; security and privacy goals - assumptions, threat and attack models. We then have described the two serverless protocols that we propose to use and we eventually presented the associated performance, security and privacy analysis. For performance, security and privacy, we have shown that the proposed protocols compare favorably with the relevant literature. Regarding energy consumption, as proposed protocols are designed with lightweight operations, they fulfill the objective.

Following the results presented here, we intend to deploy a prototype of such inventory and tracking system to assess its resilience and real world performance.

References

[1] "Samsonite leverages bluetooth beacons for new baggage tracking solution," 2016. [Online]. Available: http://www.futuretravelexperience.com/2016/04/samsonite-leverages-bluetooth-beacons-new-baggage-tracking-solution/

[2] "Samsonite working with vodafone to develop track&go luggage tracking solution," 2017. [Online]. Available: http://www.futuretravelexperience.com/2017/02/samsonite-partners-with-vodafone-to-develop-trackgo/

[3] "Delta invests $50m in rfid baggage tracking technology," 2016. [Online]. Available: http://www.futuretravelexperience.com/2016/05/delta-invests-50m-rfid-baggage-tracking-technology/

[4] "Delta passengers offered proactive baggage tracking updates via app," 2016. [Online]. Available: http://www.futuretravelexperience.com/2016/11/delta-app-now-offers-proactive-baggage-tracking-updates/

[5] M. C. O'Connor, "Emirates rfid bag-tracking pilot takes off," *RFID Journal*, 2018. [Online]. Available: http://www.rfidjournal.com/articles/view?3930

[6] D. McFarlane, "No free lunches with rfid," *RFID Journal*, 2011. [Online]. Available: http://www.rfidjournal.com/articles/view?8190

[7] M. Roberti, "Aerospace and defense catch up on rfid," *RFID Journal*, 2016. [Online]. Available: http://www.rfidjournal.com/articles/view?14963

[8] J. Edwards, "Portuguese airline taps into rfid," *RFID Journal*, 2012. [Online]. Available: http://www.rfidjournal.com/articles/view?9688

[9] C. Swedberg, "Rfid helps milano malpensa airport to complete maintenance work on time," *RFID Journal*, 2013. [Online]. Available: http://www.rfidjournal.com/articles/view?10781

[10] C. Mtita, M. Laurent, and J. Delort, "Efficient serverless radio-frequency identification mutual authentication and secure tag search protocols with untrusted readers," *IET Information Security*, vol. 10, no. 5, pp. 262–271, 2016.

[11] C. C. Tan, B. Sheng, and Q. Li, "Secure and serverless rfid authentication and search protocols," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1400–1407, 2008.

[12] J. W. Shondel, "Unmanned aerial vehicle inventory system," Jun. 4 2014, uS Patent App. 14/295,725.

[13] C. W. McALLISTER, "Mobile aerial rfid scanner," Dec. 29 2016, uS Patent App. 15/393,499.

[14] E. Perin, "Drones reduce inventory time from days to minutes at car dealerships," *RFID Journal*, 2017. [Online]. Available: http://www.rfidjournal.com/articles/view?15663

[15] J. H. Ong, A. Sanchez, and J. Williams, "Multi-uav system for inventory automation," in *2007 1st Annual RFID Eurasia*, Sept 2007, pp. 1–6.

[16] J. Ong, "Mobile rfid system for inventory automation," Ph.D. dissertation, Massachusetts Institute of Technology, 2008.

[17] S. M. Bae, K. H. Han, C. N. Cha, and H. Y. Lee, "Development of inventory checking system based on uav and rfid in open storage yard," in *2016 International Conference on Information Science and Security (ICISS)*, Dec 2016, pp. 1–2.

[18] E. Andrukiewicz and K. Waćkowski, "Technical feasibility of the system for location and tracking goods in distribution center based on rfid and uav technologies," , no. 4, pp. 6–10, 2016.

[19] M. Longhi, G. Casati, D. Latini, F. Carbone, F. D. Frate, and G. Marrocco, "Rfidrone: Preliminary experiments and electromagnetic models," in *2016 URSI International Symposium on Electromagnetic Theory (EMTS)*, Aug 2016, pp. 450–453.

[20] G. Greco, C. Lucianaz, S. Bertoldo, and M. Allegretti, "A solution for monitoring operations in harsh environment: A rfid reader for small uav," in *2015 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, Sept 2015, pp. 859–862.

[21] ——, "Localization of rfid tags for environmental monitoring using uav," in *2015 IEEE 1st International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, Sept 2015, pp. 480–483.

[22] J. S. Choi, B. R. Son, H. K. Kang, and D. H. Lee, "Indoor localization of unmanned aerial vehicle based on passive uhf rfid systems," in *2012 9th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*, Nov 2012, pp. 188–189.

[23] J. Won, S.-H. Seo, and E. Bertino, "A secure communication protocol for drones and smart objects," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '15. New York, NY, USA: ACM, 2015, pp. 249–260. [Online]. Available: http://doi.acm.org/10.1145/2714576.2714616

[24] R. N. Akram, K. Markantonakis, K. Mayes, P. Bonnefoi, D. Sauveron, and S. Chaumette, "A secure and trusted protocol for enhancing safety of on-ground airplanes using uavs," in *Integrated Communications Navigation and Surveillance*. IEEE, 2017.

[25] C. C. Tan, B. Sheng, and Q. Li, "Serverless search and authentication protocols for rfid," in *Pervasive Computing and Communications, 2007. PerCom'07. Fifth Annual IEEE International Conference on*. IEEE, 2007, pp. 3–12.

[26] M. Safkhani, P. Peris-Lopez, N. Bagheri, M. Naderi, and J. C. Hernandez-Castro, "On the security of tan et al. serverless rfid authentication and search protocols," in *Radio Frequency Identification. Security and Privacy Issues*. Springer, 2013, pp. 1–19.

[27] L.-C. Lin, S.-C. Tsaur, and K.-P. Chang, "Lightweight and serverless rfid authentication and search protocol," in *2009 Second International Conference on Computer and Electrical Engineering*, vol. 2, 2009, pp. 95–99.

[28] C.-F. Lee, H.-Y. Chien, and C.-S. Laih, "Server-less rfid authentication and searching protocol with enhanced security," *International Journal of Communication Systems*, vol. 25, no. 3, pp. 376–385, 2012.

[29] M. E. Hoque, F. Rahman, S. I. Ahamed, and J. H. Park, "Enhancing privacy and security of rfid system with serverless authentication and search protocols in pervasive environments," *Wireless personal communications*, vol. 55, no. 1, pp. 65–79, 2010.

[30] M. Deng, W. Yang, and W. Zhu, "Weakness in a serverless authentication protocol for radio frequency identification," in *Mechatronics and Automatic Control Systems*. Springer, 2014, pp. 1055–1061.

[31] M. Pourpouneh, R. Ramezanian, and F. Salahi, "An improvement over a server-less rfid authentication protocol," *International Journal of Computer Network and Information Security (IJCNIS)*, vol. 7, no. 1, p. 31, 2014.

[32] S. Abdolmaleky, S. Atapoor, M. Hajighasemlou, and H. Sharini, "A strengthened version of a hash-based rfid server-less security scheme," *Advances in Computer Science: an International Journal*, vol. 4, no. 3, pp. 18–23, 2015.

[33] S. I. Ahamed, F. Rahman, and E. Hoque, "Erap: Ecc based rfid authentication protocol," in *Future Trends of Distributed Computing Systems, 2008. FTDCS'08. 12th IEEE International Workshop on*. IEEE, 2008, pp. 219–225.

[34] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity establishment and capability based access control (iecac) scheme for internet of things," in *Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on*. IEEE, 2012, pp. 187–191.

[35] C. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 4, pp. 1408–1416, 2008.

[36] G. Tsudik, "Ya-trap: Yet another trivial rfid authentication protocol," in *Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on*. IEEE, 2006, pp. 4–pp.

[37] C. Chatmon, T. van Le, and M. Burmester, "Secure anonymous rfid authentication protocols," *Florida State University, Department of Computer Science, Tech. Rep*, 2006.

[38] I. Erguler, "Subtle flaws in the secure rfid tag searching protocol: Srts," *Wireless Personal Communications: An International Journal*, vol. 90, no. 1, pp. 175–188, 2016.

[39] J. Y. Chun, J. Y. Hwang, and D. H. Lee, "Rfid tag search protocol preserving privacy of mobile reader holders," *IEICE Electronics Express*, vol. 8, no. 2, pp. 50–56, 2011.

[40] H. Jialiang, X. Youjun, and X. Zhiqiang, "Secure and private protocols for server-less rfid systems," *International Journal of Control and Automation*, vol. 7, no. 2, pp. 131–142, 2014.

[41] W. Xie, L. Xie, C. Zhang, Q. Wang, J. Xu, Q. Zhang, and C. Tang, "Rfid seeking: Finding a lost tag rather than only detecting its missing," *Journal of Network and Computer applications*, vol. 42, pp. 135–142, 2014.

[42] I.-S. Jeon and E.-J. Yoon, "An ultra-lightweight rfid seeking protocol for low-cost tags," *Applied Mathematical Sciences*, vol. 8, no. 125, pp. 6245–6255, 2014.

[43] S. Sundaresan, R. Doss, S. Piramuthu, and W. Zhou, "A secure search protocol for low cost passive rfid tags," *Computer Networks*, vol. 122, pp. 70–82, 2017.