PMAKE: Physical Unclonable Function-based Mutual Authentication Key Exchange Scheme for Digital Aeronautical Communications

Nils Mäurer and Thomas Gräupl
Institute of Communication and Navigation
German Aerospace Center (DLR)
Wessling, Germany
{nils.maeurer, thomas.graeupl}@dlr.de

Corinna Schmitt and Gabi Dreo Rodosek
Research Institute CODE
Bundeswehr University Munich
Neubiberg, Germany
{corinna.schmitt, dreo}@unibw.de

***Abstract*—Growth of civil air traffic and new entrants into the air transportation sector such as Unmanned Aeronautical Vehicles (UAV) pose a great challenge for air traffic management and its supporting Communication, Navigation and Surveillance (CNS) infrastructure. Analogue systems have to be replaced by digital systems to optimize spectrum efficiency, and automation needs to be introduced to support human decision making at scale. As safety and security are strongly intertwined in aviation, cybersecurity is one key enabler for digitalization in civil aviation. However, few deployed digital aeronautical communications systems incorporate dedicated cybersecurity measures. Link requirements of low latency, low bandwidth, and long range make aeronautical datalinks especially challenging in terms of security design. Further, challenging are the nature of wireless communication itself and the political boundaries in international air transportation concerning unique communication participant identification. Thus, this paper proposes a concept for a challenge-response (CR) based Physical Unclonable Function (PUF) Mutual Authentication Key Exchange scheme, short PMAKE, binding communication identity and radio device together. Initial evaluations showed its suitability for the digital aeronautical communications system LDACS.**

***Index Terms*—Cybersecurity, Mutual Authentication and Key Exchange (MAKE), Physical Unclonable Function (PUF), Digital Aeronautical Communications, L-band Digital Aeronautical Communications System (LDACS)**

I. Introduction

The ongoing digitization process nowadays has also spillovers in the civil aeronautical industry, especially affecting Communication, Navigation and Surveillance (CNS) infrastructure. The Single European Sky Air Traffic Management Research (SESAR)[1] program in the European Union (EU) and NextGEN[2] in the US have been tasked with the development of new technologies to create an aeronautical Future Communications Infrastructure (FCI). Wireless technology candidates for the FCI are the Aeronautical Mobile Airport Communication System (AeroMACS) for airport communications, the satellite communications for oceanic, polar and remote domains, and the L-band Digital Aeronautical Communication System (LDACS) for long-range terrestrial aeronautical communications [29]. In this paper we focus on LDACS.

As safety and security are strongly interrelated in aviation, strong cybersecurity is the foundation and precondition for digitization in aviation [14]. However, cybersecurity for CNS is unfortunately not realized in most deployed systems [9], [27], [31]. One of the few systems in the ecosystem, which has a dedicated cybersecurity architecture is AeroMACS as it was based on the IEEE 802.16 WiMAX standard [19]. Central to the security of AeroMACS lies its Public Key Infrastructure (PKI) building a chain of trust originating from a root Certificate Authority (CA) [21]. This turned out to be problematic, since a root of trust has to be declared that all ICAO state actors can trust directly or via cross certification. Security infrastructure becomes therefore entangled with the political reality of aviation, which is a small number of dominant state actors capable of securing critical infrastructure with limited trust towards others. For these others a PKI becomes a less attractive solution for an aeronautical trust framework. AeroMACS is therefore not widely deployed. Besides the mentioned situation with AeroMCS, we also have to consider the technical requirements for aeronautical datalinks representing the highest challenges for security support in aeronautic: (1) The low additional security latency and (2) the low additional security overhead as prompted by the long range and limited available bandwidth of aeronautical wireless systems. Further, political boundaries in international transportation concerning unique communication participant identification must be respected.

With these challenges in place, it is clear that traditional certificate-based authenticated key exchange schemes might be too expensive in terms of political issues, security overhead, and maintenance expense on digital aeronautical links [2]. Tackling the issue of certificates, trust, and low security data overhead, the Internet of Things (IoT) sector and solutions like Physical Unclonable Function (PUF)-based Challenge-Response (CR) Mutual Authentication and Key Exchange

[1]https://www.sesarju.eu/, Oct. 14, 2020
[2]https://www.faa.gov/nextgen/, Oct. 14, 2020

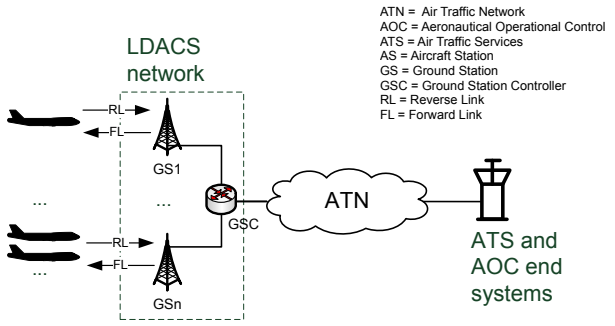

Fig. 1. Network architecture of LDACS [22]

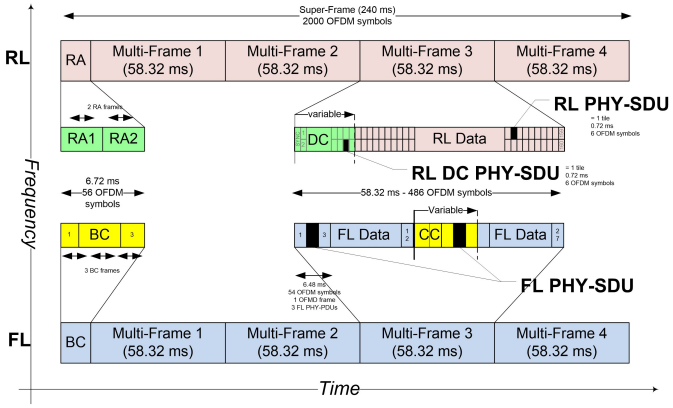

Fig. 2. Frame structure of LDACS [13]

(MAKE) schemes [7], [8], [18] come into focus. These solutions offer ways for binding communication entity and radio device together without the need for centrally managed certificates.

Thus, the objective of this paper is to investigate the combination of PUF, key exchange methods such as Diffie-Hellman Key Exchange (DHKE) and CR-based mutual authentication and Authenticated Key Exchange (AKE) protocols for application in the aeronautical domain. The outcomes lead us to our proposed PUF-based Mutual Authentication Key Exchange scheme called PMAKE.

The paper is structured as follow: Section II presents insides to LDACS together with its frame structure, PUF theory, and DHKE theory. Security assumptions and detailed objectives are presented in Section III. PMAKE itself is discussed in detail in Section IV followed by the respective evaluation in Section V. Finally, the paper is concluded in Section VI.

II. Background on LDACS, PUF and DHKE

As stated in Section I an efficient security solution needs to be designed and developed in order to establish cybersecurity support in CNS infrastructure, especially in aeronautics. First investigations were undertaken by specifying a cybersecurity architecture for LDACS proposing several security solutions [22], [24]–[26]. As digitization goes onward and attackers become more inventive the defense strategies and protocols need to improve further. Thus, the idea came up to combine PUF and DHKE methods with each other, as realized by our PMAKE scheme. Before diving into the solution we present here background information to make our taken design and implementation decisions (cf. Section IV) understandable.

A. LDACS Theory

LDACS is a ground-based digital communications system for flight guidance and communications related to the safety and regularity of flight. It has been developed in Europe and is currently under standardization by ICAO.

Figure 1 depicts involved components and communication links. Up to 512 Aircraft Station (AS) communicate to an LDACS Ground Station (GS) in the Reverse Link (Reverse Link (RL)), GS communicate to AS in the Forward Link (Forward Link (FL)). GSs are controlled by a Ground Station Controller (GSC). The GSC connects the LDACS sub-network to the global Air Traffic Network (Air Traffic Network (ATN)) to which the corresponding Air Traffic Services (Air Traffic Services (ATS)) and Aeronautical Operational Control (Aeronautical Operational Control (AOC)) end systems are attached. As we will need a detailed understanding of LDACS frame structure design in the evaluation Section V, we will briefly discuss this here.

In the FL direction, each Super Frame (SF) starts with a Broadcast (BC) slot, where the GS announces its existence to the AS and sends physical parameters for link establishment. The rest of the FL SF is split into four Multi Frames (MFs), each containing nine Orthogonal Frequency-Division Multiplexing (OFDM) frames and each frame comprises three FL Physical Layer Service Data Units (PHY-SDUs). Every FL PHY-SDU can be used to transmit FL user data or Common Control (CC) data, in which GS can allocate resources to an AS. In the RL, a SF starts with a Random Access (RA) slot, where AS can request access to an LDACS cell, and continues with four MFs. Each RL MF is constructed from 162 RL PHY-SDUs equivalent to Orthogonal Frequency-Division Multiple Access (OFDMA) tiles. They are used for two purposes, namely (1) to transmit Dedicated Control (DC) data, which are used by an AS to request the allocation for resources allowing them to send on the RL and (2) to transmit RL user data.

Those details are depicted in Figure 2. For more details of LDACS framing, we refer to [13].

LDACS covers current ATS, AOC data and also future applications, enables new concepts (e.g., sectorless Air Traffic Management (ATM)) and has at least an order of magnitude more net capacity than the currently used terrestrial links like the VHF Digital Link Mode 2 (VDLm2) system [13]. Instead of kilobits per second, LDACS offers up to 2 Mbps. By enabling not only communication but also navigation and surveillance at the same time, it is the world's first integrated CNS system [29].

Over time several security algorithms were integrated into the initial LDACS cybersecurity architecture [24]–[26]. However, aeronautical systems in general and LDACS in particular

do not offer high data rates as depicted in [23]. In order to address this problem we recommend

1) to reduce security message exchanges between GSC, GS and AS,
2) to eliminate the need of the integration of a PKI into the LDACS security framework, and
3) to uniquely bind identification and radio device, respectively the actual physical aircraft.

These three recommendations are followed by our proposed PMAKE scheme and is presented in Sections IV and V.

B. PUF's Theory

A silicon PUF is a mapping $f : \{0,1\}^n \rightarrow \{0,1\}^m$ with n challenge bits and m response bits. The response is derived when applying the n challenge bit onto the intractably complex instance-specific unique system behaviour [30]. PUFs use device unique random patterns, which are introduced in the manufacturing process to differentiate chips and make them uniquely identifiable. Hence, a PUF can be interpreted as a unique device's fingerprint, an enabler to create a unique set of CR pairs and a strong random number generator.

PUFs have been used for the identification, key-generation phase and as basis for encryption schemes [8]. The remarkable feature is the ability of the protocol to mutual authenticate entities, without storing Challenge-Response-Pairs (CRPs) at the verifier. As data links for IoT based networks share some similarities with the aeronautical sector such as low latency and low bandwidth with a fast changing network, solutions here are of particular interest. For example, there exist PUF-based mutual authentication schemes for IoT [5] and end-to-end AKE schemes [7] already.

Our PMAKE scheme picks up the concept of so called Static Random-Access Memory (SRAM) PUFs [16]. The underlying idea is that the physical properties of every transistor in an integrated circuit differs from another due to small, submicron variations in the production process. Electronic properties such as transistor threshold voltages or gain factor are different and unique per chip and as the variations during production are not controllable, this creates unique, unclonable physical properties per chip. An important fact to note is, that SRAM PUF derived keys are only extracted from the chip when needed and thus no key is present when the chip is powered off.

Thus the PUF can be combined with an arbitrary amount of arbitrary challenges to produce an arbitrary amount of device unique responses without the responses being available and accessible to an adversary when the chip is powered down. This capability will be used in the proposed PMAKE solution in Section IV.

C. DHKE's Theory

The original DHKE was first published in 1976 and is based on the discrete logarithm or Diffie-Hellman problem [10]: Given a cyclic group G of prime order n, a generator g of G and elements $g^x, g^y \in G$, find g^{xy}. A Man-in-the-Middle attack is possible when no authentication or additional security features are used [3], which is why authenticated DHKE schemes (e.g., Station to Station (STS), Internet Key Exchange (IKE) and IKE version 2 (IKEv2) protocols [4] were invented.

In order to reduce key sizes, other abelian groups [20] were investigated. One cryptographic platform here was the use of elliptic curves over finite fields, resulting in the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol [1], [20]. Hardening cryptographic protocols for quantum resistance follows the idea of quantum-resistant public-key cryptosystems based on the conjectured difficulty of finding isogenies between supersingular elliptic curves was formulated in 2006 by Rostovtsev et al. [28] and extended for key exchange applications by Jao et al. in 2011 [17]. This scheme is called Supersingular Isogeny Diffie–Hellman (SIDH) and represents a post-quantum robust version of the DHKE.

For our PMAKE scheme we will use the basic principle of any of the three previously mentioned DHKE. We assume that each communicating party chooses a secret key and performs any DHKE type specific mathematical operation to derive a public key to be used in further message exchanges. This allows the Physical Unclonable Function based Mutual Authentication Key Exchange (PMAKE) scheme to use different DHKE types, depending on the situation.

III. Security Assumptions and Objectives

Our proposed PMAKE scheme was influenced by following four **security assumptions** from [4], which uphold for the main phase of PMAKE:

- S1: The adversary is able to eavesdrop on all messages sent in a cryptographic protocol.
- S2: The adversary is able to alter all messages sent in a cryptographic protocol using any information available. In addition the adversary can re-route any message to any other principal. This includes the ability to generate and insert completely new messages.
- S3: The adversary may be a legitimate protocol participant (an insider), or an external party (an outsider), or a combination of both.
- S4: An adversary is able to obtain the value of the session key K_{AB} used in any sufficiently old previous run of the protocol.

We design the PMAKE scheme in the context of the Dolev and Yao model [11]. To be able to prove security properties of communication protocols, one has to additionally model the attacker, since he or she (possibly) plays an active part in each run of the protocol. Following the works of Dolev and Yao, the ideal and most powerful attacker is assumed, who can create, intercept or modify any message in the network, spoof any identity and even compromise long term keys.

Bilzhause et. al identified five objectives to secure LDACS [2]. These five objectives were later extended to nine objectives in the LDACS Standards and Recommended Practises

(SARPS) endorsed by International Civil Aviation Organization (ICAO) [15], namely (1) to protect availability and continuity of service, to protect (2) integrity, (3) authenticity for user and control plane messages in transit, (4) provide non-repudiation of origin, (5) confidentiality for user plane messages in transit, (6) mutual entity authentication, (7) authorize explicitly permitted actions of users or entities, (8) prevent the propagation of intrusions within LDACS domains and towards external domains and (9) protect against service attacks to a level consistent with the application service requirements.

Overall, to fulfill any of these objective, some key exchange and mutual authentication procedure must take place at the very beginning of connection establishment. The objective of the LDACS's PMAKE scheme is to establish a shared session key K between any two parties AS and GSC, in which they can have "mutual belief", following the definition of Boyd [4]: "Mutual belief in the key K is provided for B only if K is a good key for use with A, an A wishes to communicate wit B using key K which A believes is good for that purpose." Following the hierarchy of authentication and key establishment goals of Boyd, this mutual belief goal can be split up into the sub-goals *entity authentication*, *key confirmation* and *good key*. Additionally, we want to address the issue of compromised long-term keys.

Summarizing this we define the following three **objectives O1-O3 for PMAKE**:

O1: *Mutual Authentication* means, both parties can be sure of each others identity and that both participated in this interaction.

O2: *Secure Key Agreement* assumes, both parties have established a shared session key that is fresh and can be use for a certain time between them only.

O3: *Perfect Forward Secrecy* means, the established session key remains secret, even when long term keys of the involved parties have been compromised after the session.

IV. The PMAKE Scheme

Assuming a verifier wants to authenticate i nodes using traditional PUF-based authentication protocols (e.g., A and B) he needs to store j numbers of k-bit long challenges and l-bit long corresponding responses, accumulating to a space complexity of $O((k+l) \times i \times j)$. Reducing this number, we loosely orient ourselves on the HMAC-based RFID PUF mutual authentication protocol (HPK), as it has already reduced space complexity to $O((k+l) \times i)$ [18]. This means, for every node only one CRP has to be maintained. With every protocol run a new CRP is securely exchanged, making the amount of protocol runs independent of the stored amount of CRPs.

A. Notations and Prerequisites

The notations for the following PMAKE scheme are listed in Table I following the notation by [4] for the key exchange part of the protocol.

Following previous works in designing MAKE protocols for LDACS [26], we aim to build a secure connection between GSC and AS, with the GS just being the intermediary, forwarding all messages over the air gap to the AS and via the ground based backbone back to the GSC. Every mobile node (aircraft) is equipped with a SRAM PUF during the construction process of the specific LDACS radio device. Communication partners AS and GSC will have to have previously agreed upon the chosen DHKE variation and respective public parameters. Similar to previous works [25], [26], the ground based entities GSC and GS will have established a secure connection prior to a PMAKE scheme run. Note, it is essential for PMAKE's success that the setup phase where the initial generation of a CRP happens (cf. Section IV-B) will have to remain secure. Compromise of the first CRP renders the protocol insecure. Further, the public ephemeral keys of the DHKE requires to fulfill two purposes, namely (1) being key material, (2) serving as nonces. Thus for every run of the protocol r_A will have to be chosen anew.

TABLE I
NOTATIONS USED IN THE PMAKE SCHEME

Notation	Definition
msg1 $\oplus$ msg2	XOR operation on msg1 with msg2
msg1 $\mid$ msg2	Concatenation operation on msg1 with msg2
PUF_A	Physical Unclonable Function of entity A
$\text{HMAC}_K(msg)$	Hash-based Message Authentication Code with key K and input data msg
$\text{HKDF}(K)$	HMAC Key Derivation Function (HKDF) with input K
C_{A_i}	i-th Challenge for PUF from entity A
R_{A_i}	i-th Response from PUF from entity A
ID_A	Identifier of entity A
r_A	Random integers of entity A "Ephemeral private key"
t_A	Ephemeral public key of entity A
g	Public Diffie-Hellman parameters
$S_{AS,GSC}$	Static Diffie-Hellman key shared between AS and GSC
$K_{AS,GSC}$	Session key for AS-GSC communications
$\{msg\}_K$	Encrypted data msg with key K

B. The Setup Phase

PMAKE's **Setup Phase** starts with an agreement between GSC and AS as illustrated in Figure 3. They need to have agreed upon a choice of a DHKE method and its public parameter g, HMAC, HKDF and on a suitable symmetric encryption algorithm. Next, the GSC sends a challenge C_{AS_0} to the AS. Then the AS calculates a response making use of the SRAM PUF and the challenge C_{AS_0} producing R_{AS_0}. The response is send back to the GSC. As last step in this phase, the GSC securely stores $< C_{AS_0}, R_{AS_0} >$ and the AS stores $< C_{AS_0} >$.

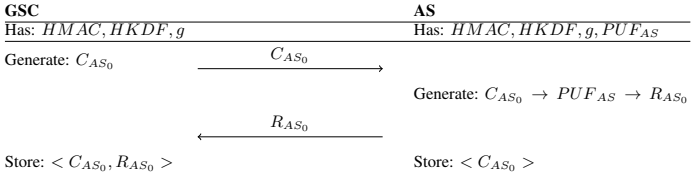

Fig. 3. PMAKE's Setup Phase

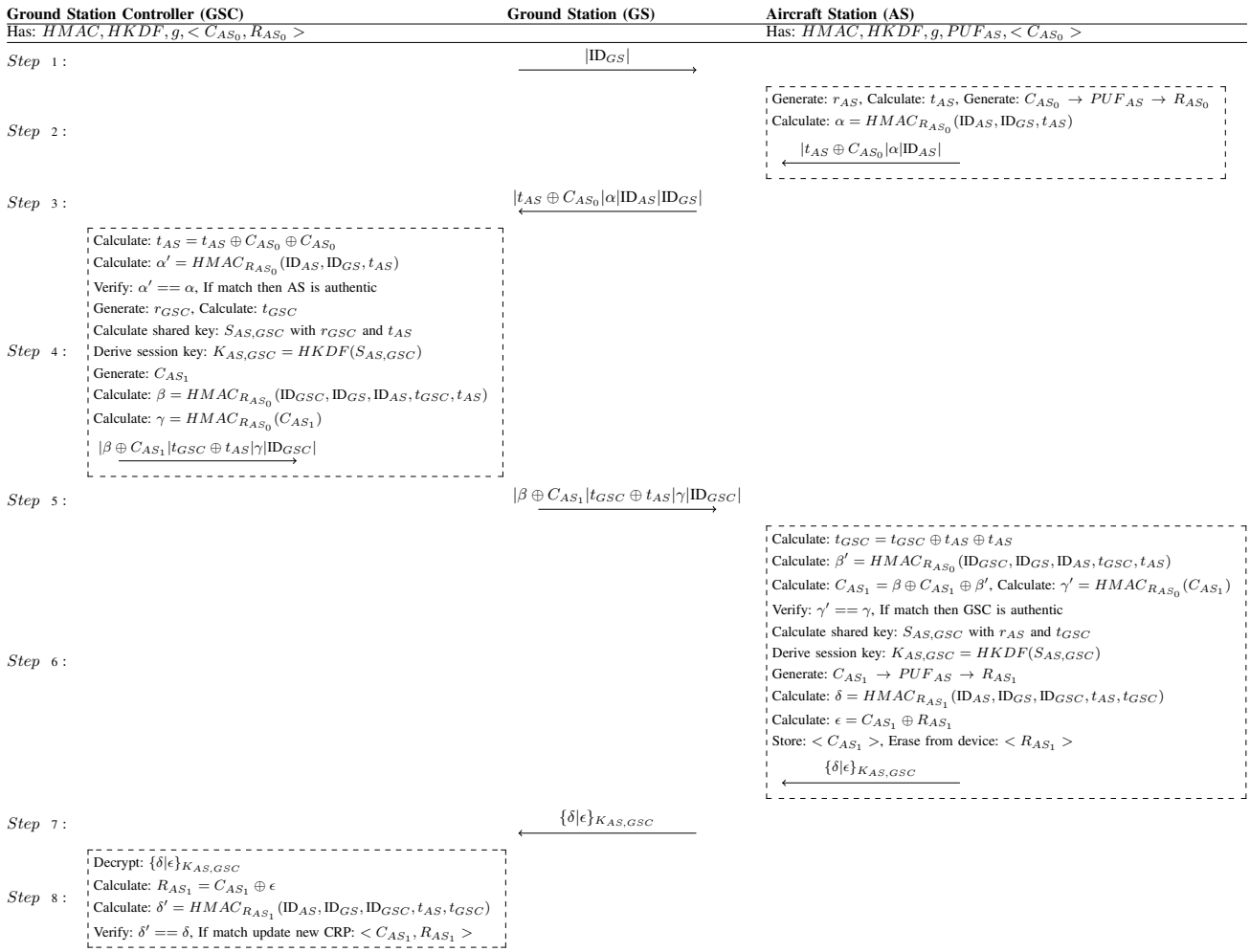

Fig. 4. PMAKE's Main Phase

C. The Main Phase

In case the setup phase was passed successful PMAKE continues with its **Main Phase**. Figure 4 illustrates required steps and message exchanges that are:

1) After GSC and GS have established a secure connection, the GS starts broadcasting its identity ID_{GS} regularly.
2) The AS, upon receiving such a beacon, generates a random number r_{AS} and depending on the respectively chosen DHKE procedure calculates t_{AS} and $\alpha = HMAC_{R_{AS_0}}(\text{ID}_{AS}, \text{ID}_{GS}, t_{AS})$. It then responds with $|t_{AS} \oplus C_{AS_0}|\alpha|\text{ID}_{AS}|$.
3) Once the GS receives the response to the beacon message, it appends its ID to the message and forwards $|t_{AS} \oplus C_{AS_0}|\alpha|\text{ID}_{AS}|\text{ID}_{GS}|$ to the GSC.
4) With the help of the previously stored tuple $< C_{AS_0}, R_{AS_0} >$, the GSC can compute the public key of the AS $t_{AS} = t_{AS} \oplus C_{AS_0} \oplus C_{AS_0}$ and $\alpha' = HMAC_{R_{AS_0}}(\text{ID}_{AS}, \text{ID}_{GS}, t_{AS})$. It then checks whether $\alpha' == \alpha$ match. If that is the case, the AS has authenticated to the GSC. Then the GSC generates a random number r_{GSC} of its own and again in dependence on the previously agreed DHKE procedure, calculates t_{GSC}. Now the shared AS-GSC key $S_{AS,GSC}$ can be calculated via the secret of the GSC r_{GSC} and the public key of the AS t_{AS}. With that, the GSC calculates the session key $K_{AS,GSC}$ via the HKDF and $S_{AS,GSC}$. Finally a new challenge C_{AS_1} is chosen by the GSC and two new MAC tags are calculated. β is used to conceal C_{AS_1}, while γ serves as authenticity proof about the GSC for the AS. It finally sends $|\beta \oplus C_{AS_1}|t_{GSC} \oplus t_{AS}|\gamma|\text{ID}_{GSC}|$ to the GS.
5) The GS forwards that message to the AS.
6) First the AS calculates the public key of the GSC via $t_{GSC} = t_{GSC} \oplus t_{AS} \oplus t_{AS}$. To be able to decipher C_{AS_1}, β' is calculated by the AS by reconstructing R_{AS_0} and using previously established values t_{GSC}, t_{AS}, ID_{GSC}, ID_{GS}, ID_{AS}. As $C_{AS_1} = \beta \oplus C_{AS_1} \oplus \beta'$ the AS successfully received the new challenge C_{AS_1}. It then calculates its own value for $\gamma' = HMAC_{R_{AS_0}}(C_{AS_1})$ and compares $\gamma' = \gamma$. If they match, the GSC has authenticated to the AS. Furthermore the verifiable integrity and

return of t_{AS} proves to the AS, that the GSC actually participated in the protocol. Now the AS calculates the shared key $S_{AS,GSC}$ with r_{AS} and t_{GSC} and derives the session key $K_{AS,GSC} = HKDF(S_{AS,GSC})$. Via the AS PUF a new response R_{AS_1} is generated to the new challenge C_{AS_1} via $C_{AS_1} \rightarrow PUF_{AS} \rightarrow R_{AS_1}$. It then calculates $\delta = HMAC_{R_{AS_1}}(\text{ID}_{AS}, \text{ID}_{GS}, \text{ID}_{GSC}, t_{AS}, t_{GSC})$ that will be used by the GSC as proof for the authenticity and correctness of the new response R_{AS_1}. $\epsilon = C_{AS_1} \oplus R_{AS_1}$ is used to conceal the response R_{AS_1} during transport. At this point, the AS securely stores C_{AS_1} and erases R_{AS_1} from memory. As AS and GSC have previously agreed upon suitable encryption algorithms, the AS sends δ and ϵ encrypted with $K_{AS,GSC}$ back to the GSC.

7) The GS forwards that message to the GSC.
8) The GSC decrypts the message with the agreed upon encryption algorithm and key $K_{AS,GSC}$. It then computes $R_{AS_1} = C_{AS_1} \oplus \epsilon$. It then calculates $\delta' = HMAC_{R_{AS_1}}(\text{ID}_{AS}, \text{ID}_{GS}, \text{ID}_{GSC}, t_{AS}, t_{GSC})$ and checks whether $\delta' == \delta$. If that is the case, the GSC can be sure of the authenticity of the response R_{AS_1} and the participation of AS in the protocol. It updates the current tuple for that AS to $< C_{AS_1}, R_{AS_1} >$.

Assuming everything went fine, Secure user data communication between AS and GSC can now commence with the session key $K_{AS,GSC}$. After a successful encrypted user data message exchange between AS and GSC, also key confirmation is achieved. If during PMAKE's Main Phase anything went wrong the total process must be performed again.

V. LDACS BASED EVALUATION OF PMAKE

In this section we will evaluate our proposed PMAKE scheme using a special latency emulation model, which is first introduced here. PMAKE itself is assumed to meet our security assumptions and objectives from Section III. Thus, we evaluate used message sizes and introduced data/latency overhead due to the new security implementation.

A. Latency Model

In 2015, Gräupl et al. [12] presented a full methodology on how to emulate latencies for user data in the forward and reverse link (FL/RL) of LDACS depending on the bit error rate and message size, which was updated in [26]. Taking retransmissions into account, FL latency can be calculated as

$$L_{FL}(t) = m_{FL}(t) + (1 + \delta_{RX}(1 + n)) \times d_{MF} \quad (1)$$

and RL latency as

$$L_{RL}(t) = m_{RL}(t) + (2 + \delta_{RX}(N + 3)) \times d_{MF}. \quad (2)$$

In Equation 1, we use $m_{FL}(t)$ to classify the time until the start of the next CC frame, $\delta_{RX} \in \{0, 1\}$ to indicate a retransmission, d_{MF} to denote the length of a MF and n is derived from the length of the reverse link medium access cycle from forward link perspective. In Equation 2, we use $m_{RL}(t)$ to denote the time until the start of next DC slot, $\delta_{RX} \in \{0, 1\}$ to indicate a retransmission, d_{MF} to denote the length of a MF and N is derived from the length of the reverse link medium access cycle from reverse link perspective.

TABLE II
PARAMETER VALUES FOR LATENCY TIMING FOR THE LDACS MEDIUM ACCESS LAYER (MAC) PROTOCOL.

Forward Link Model $L_{FL}(t) = m_{FL}(t) + (1 + \delta_{RX}(1 + n)) \times d_{MF}$		**Reverse Link Model** $L_{RL}(t) = m_{RL}(t) + (2 + \delta_{RX}(N + 3)) \times d_{MF}$	
Parameters	**Values**	**Parameters**	**Values**
d_{MF}	60ms	d_{MF}	60ms
$m_{FL}(t)$	Time until start of next FL MF: Every 1 to 60ms modelled by $U(1, 60)$	$m_{RL}(t)$	Average time until start of next MAC cycle: $\#\text{AS}/32 \times d_{MF} + wait$ $wait$ modelled by $U(1, 60)$
n	Average amount of MF after transmission until next DC slot is scheduled for AS in MAC-cycle: $n = \#\text{AS}/32$	N	Average amount of MF after transmission until next DC slot scheduled for AS in MAC-cycle: $N = (\#AS/32 - 3) \mod \#\text{AS}/32$
BER	$0, 10^{-6}, 10^{-5}$		
P	$P(\{\text{no error in packet}\}) = (1 - BER)^l$ $P(\{\text{error in packet}\}) = 1 - ((1 - BER)^l)$		

We model $\delta_{RX} \in \{0, 1\}$ as stochastic process, based on the packet error rate. Given a Bit Error Rate (BER), we can calculate the packet error rate based on the length of a packet l: $P(\{\text{no error in packet}\}) = (1 - BER)^l$. Thus the opposite event, that a packet indeed contains an error is: $P(\{\text{error in packet}\}) = 1 - ((1 - BER)^l)$. These two probability decide the value of δ_{RX}, whether a retransmission is necessary and, thus, an error appeared in the packet, or not. For more details on this model we refer to [12] and [26]. In Table II we list the used parameters for LDACS's MAC protocol, necessary for the PMAKE's evaluation.

For the upcoming evaluation here, we will first assign bit sizes to each message and then calculate data overhead and latency based on that. We will use the notions $ClientHelloKeyExchange$ (Step 2), $ServerKeyExchangeFinished$ (Step 4) and $ClientKeyExchangeFinished$ (Step 6) for the AS-GSC exchanged PMAKE messages. Please note, steps are referred to according to Figure 4 and that the first message exchanged in Step 1 is part of regular control broadcast messages by the GS and thus not part of our evaluation.

B. Message Sizes

Every LDACS message has to have a header at the beginning of a user data message, which is 48bit long. Sizes of t_{AS}, t_{GSC} vary depending on the choice of DHKE procedure. The following recommended bit sizes for cryptographic material are all taken from [6], Diffie-Hellman public keys lengths are

chosen similar to [26] leading to:
$t_{GSC} : \{DHKE = 3072|ECDH = 256|SIDH = 2624\}$ and $t_{AS} : \{DHKE = 3072|ECDH = 256|SIDH = 2640\}$.
As recommended in [6] a challenge "should have a minimum entropy of 100bits" we decided that the Message Authentication Code (MAC) tag's length is 128bit for PMAKE. A MAC is derived from any operation in PMAKE that involves the HMAC function, as the result of HMAC is a MAC tag (e.g., α is a MAC tag with $\alpha = HMAC_{R_{AS_0}}(\text{ID}_{AS}, \text{ID}_{GS}, t_{AS})$ from step 2, together with β, γ, δ and ϵ).
Identities are already specified in the official LDACS specification [13] for AS and GS: ID_{AS} is 28bit and ID_{GS} 12bit long. For the length of ID_{GSC} we assume another 28bit.

C. Data Overhead

If we assign the aforementioned message sizes now to every PMAKE message, we get the following sizes, depending on the chosen DHKE procedure (c.f. Section IV-B):
A $ClientHelloKeyExchange$ consists of a $header = 48$, $t_{AS} = \{DHKE = 3072, ECDH = 256, SIDH = 2640\}$ xored with the challenge C_{AS_0} (resulting in the same bit lengths as t_{AS}), a MAC tag $\alpha = 128$ and the aircraft ID $\text{ID}_{AS} = 28$, totalling in $\{3276, 460, 2844\}$bits.
A $ServerKeyExchangeFinished$ consists of a $header = 48$, a MAC tag xored with the new challenge $\beta \oplus C_{AS_1} = 128$, both t_{GSC} and t_{AS} xored together resulting in $\{DHKE = 3072, ECDH = 256, SIDH = 2624\}$, another MAC tag $\gamma = 128$ and the GSC ID $\text{ID}_{GSC} = 28$, totalling in $\{3404, 588, 2972\}$bits.
Finally the $ClientKeyExchangeFinished$ consists of a $header = 48$ and two MAC tags $\delta = 128$ and $\epsilon = 128$ totalling in 304bits.
Overall this amounts to the total message sizes for PMAKE shown in Table III.

TABLE III
TOTAL MESSAGE SIZES FOR PMAKE IN *bit*

PMAKE-DHKE	PMAKE-ECDH	PMAKE-SIDH
6984	1352	6120

D. Latency Overhead

Now we use the latency evaluation methodology introduced in Section V-A and calculate LDACS latencies for the PMAKE, depending on the BER on the link and the amount of AS in an LDACS cell. We will use the three BER levels mentioned in Table II, namely 0 BER for getting a baseline authentication latency, BER of 10^{-6}, the working point of LDACS, and a BER of 10^{-5} for a worst case BER.

Authentication Latency Baseline: With $BER = 0$, the different sizes of the DHKE variations have no impact on the latency times as no retransmission due to lost packets is necessary. In Figure 5 we see that minimum PMAKE authentication latency values range from 300ms with few AS in a cell to 2200ms when the LDACS cell is full. For maximum values, we see ranges from 480ms for few aircraft to 2400ms for a full LDACS cell.

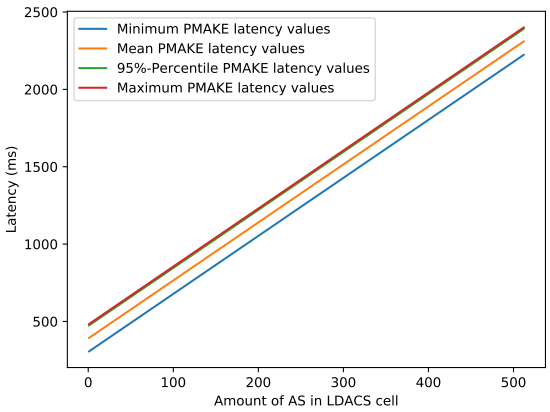

Fig. 5. Baseline authentication latency of PMAKE depending of the amount of AS in an LDACS cell at BER= 0.

Authentication Latency with realistic BER: For the evaluation under realistic BER, we emulated 10,000 authentication attempts per AS in the LDACS cell to get a realistic view on the authentication latency times, following the same argumentation as in [26]. At a BER of 10^{-6}, retransmissions and thus the choice of DHKE flavor does not play a large role for the authentication latency. Thus independent of the choice of DHKE procedure, mean PMAKE authentication latency ranges from 420ms for 1 AS in a cell to 2300ms for 512 AS in a cell. The 95%-Percentiles range from 480ms to 2360ms. At a BER of 10^{-5}, retransmissions and thus the choice of DHKE flavor do play a large role. Figure 6 reveals, that the bigger key sizes of DHKE and SIDH trigger more reliably retransmissions in the 95%-Percentiles cases and thus PMAKE-ECDH turns out to be about 1000ms faster in the worst case with a full LDACS cell. Apart from that, we see that on average all procedures take again between 480ms to 2400ms.

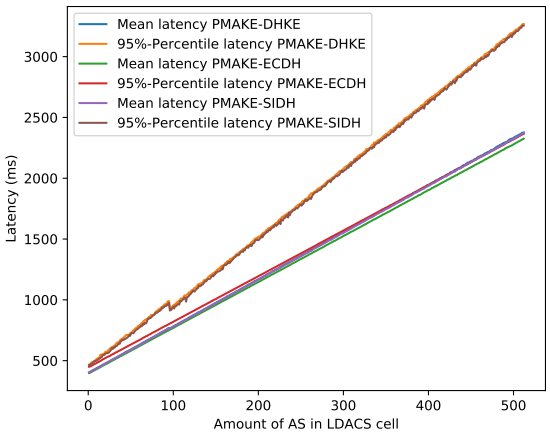

Fig. 6. Authentication latency of the PMAKE scheme depending of the amount of AS in an LDACS cell and DHKE at BER=10^{-5}. Note that the small peaks in the result for less than 3×32 AS are caused by the DC slot falling into an unfavorable position for retransmissions as calculated by N in Table II.

E. Evaluation Findings

Overall PMAKE allows for mutual authentication and key exchange capabilities between ground and aircraft without the use of a PKI or digital certificates. The only prerequisite is that a CRP is exchanged previously to the main phase of the protocol and is kept secret until the next CRP is used in which case the previous pair can even be disclosed as no relevant information can be derived. Furthermore, via the use of a PUF, the physical entity of the aircraft and respectively the LDACS radio can be tied to the respective aircraft identity.
Now we want to put the results of the latency and data overhead evaluation into perspective. In [25], [26], a STS based MAKE scheme for LDACS was introduced and evaluated.
Comparing data overhead values from PMAKE to the scheme of [26], we see that PMAKE requires 6% (DHKE), 23% (ECDH), 6% (SIDH) less data for the entire MAKE procedure. In terms of latency duration, PMAKE takes roughly the same amount of time, when few aircraft are in an LDACS cell. However, as the number of AS in a cell goes up, PMAKE can take up 800ms longer. The reason for that is, PMAKE uses one FL messages and two RL messages, while the proposed STS scheme in [26] takes two FL messages and one RL message and FL latency is usually smaller than RL latency. Here the benefit of PMAKE is, an unauthorized AS can be ruled out quicker, as the first message in the PMAKE scheme comes from the AS.

VI. Conclusions

In this paper the applicability of PUF, CR and DHKE based AKE protocols was investigated. The goal was to derive a new security paradigm for securing digital aeronautical communications systems while taking LDACS's architecture and communication flows as example application.

It turned out that modifications of the HPK mutual authentication scheme can improve the existing cybersecurity architecture of LDACS. The scheme was extended with a key exchange addition, leading to the proposed PMAKE scheme offering a PUF-based mutual authentication key exchange. As the CRPs are central to the security of the protocol, the currently used CRP must not be disclosed to any unauthorized party, as otherwise the security of the protocol is compromised. Based on LDACS's architecture and communication flows, we evaluated the PMAKE scheme in terms of data and latency overhead compared to previously proposed MAKE procedures for LDACS. The results show that PMAKE requires less data but can take more authentication latency times then previous schemes.

For future research, we are going to model the proposed PMAKE scheme in the symbolic model checker Tamarin and proof its security properties. Another open question is how to make the CRPs securely available for a certain GSC at the time when an AS, matching those pairs, enters the LDACS cell served by that GSC. This will also be part of future work.

Appendix

AeroMACS	Aeronautical Mobile Airport Communication System
AKE	Authenticated Key Exchange
AOC	Aeronautical Operational Control
AS	Aircraft Station
ATN	Air Traffic Network
ATM	Air Traffic Management
ATS	Air Traffic Services
BC	Broadcast
BER	Bit Error Rate
CA	Certificate Authority
CC	Common Control
CNS	Communication, Navigation and Surveillance
CR	Challenge-Response
CRP	Challenge-Response-Pair
DC	Dedicated Control
DHKE	Diffie-Hellman Key Exchange
ECDH	Elliptic Curve Diffie-Hellman
FCI	Future Communications Infrastructure
FL	Forward Link
GS	Ground Station
GSC	Ground Station Controller
HKDF	HMAC Key Derivation Function
HPK	HMAC-based RFID PUF mutual authentication protocol
ICAO	International Civil Aviation Organization
IKE	Internet Key Exchange
IKEv2	IKE version 2
IoT	Internet of Things
LDACS	L-band Digital Aeronautical Communication System
MAC	Medium Access Layer
MAKE	Mutual Authentication and Key Exchange
MF	Multi Frame
OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
PHY-SDU	Physical Layer Service Data Unit
PKI	Public Key Infrastructure
PMAKE	Physical Unclonable Function based Mutual Authentication Key Exchange
PUF	Physical Unclonable Function
RA	Random Access
RL	Reverse Link
SARPS	Standards and Recommended Practises
SESAR	Single European Sky Air Traffic Management Research
SF	Super Frame
SIDH	Supersingular Isogeny Diffie–Hellman
SRAM	Static Random-Access Memory
STS	Station to Station
VDLm2	VHF Digital Link Mode 2

REFERENCES

[1] G. Baumslag, B. Fine, M. Kreuzer, and G. Rosenberger, *A Course in Mathematical Cryptography*. Berlin, Germany: Walter de Gruyter GmbH & Co KG, 2015.

[2] A. Bilzhause, B. Belgacem, M. Mostafa, and T. Gräupl, "Datalink Security in the L-band Digital Aeronautical Communications System (LDACS) for Air Traffic Management," *Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, pp. 22–33, Nov. 2017.

[3] S. Blake-Wilson and A. Menezes, "Authenticated Diffe-Hellman Key Agreement Protocols," in *International Workshop on Selected Areas in Cryptography*. Heidelberg, Germany: Springer, Aug. 1998, pp. 339–361.

[4] C. Boyd, A. Mathuria, and D. Stebila, *Protocols for Authentication and Key Establishment*. Heidelberg, Germany: Springer, 2020.

[5] A. Braeken, "PUF Based Authentication Protocol for IoT," *Symmetry*, vol. 10, no. 8, pp. 1–15, Aug. 2018.

[6] BSI, "Cryptographic Mechanisms: Recommendations and Key Lengths," Federal Office for Information Security Germany, Tech. Rep. BSI TR-02102-1, Mar. 2020.

[7] J. Byun, "End-to-End Authenticated Key Exchange Based on Different Physical Unclonable Functions," *IEEE Access*, vol. 7, pp. 102 951–102 965, Jul. 2019.

[8] U. Chatterjee, V. Govindan, R. Sadhukhan, D. Mukhopadhyay, R. Chakraborty, D. Mahata, and M. Prabhu, "Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifier Database," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 3, pp. 424–437, May 2018.

[9] A. Costin and A. Francillon, "Ghost in the Air(Traffic): On Insecurity of ADS-B protocol and Practical Attacks onADS-B Devices," *Black Hat USA*, pp. 1–10, Aug. 2012.

[10] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[11] D. Dolev and A. C. Yao, "On the Security of Public Key Protocols (Extended Abstract)," in *22nd Annual Symposium on Foundations of Computer Science*. New York, NY, USA: IEEE Computer Society, Oct. 1981, pp. 350–357.

[12] T. Gräupl and M. Mayr, "Method to Emulate the L-band Digital Aeronautical Communication System for SESAR Evaluation and Verification," in *34th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Oct. 2015, pp. 1–18.

[13] T. Gräupl, C. Rihacek, and B. Haindl, "LDACS A/G Specification," German Aerospace Center (DLR), Oberpfaffenhofen, Germany, SESAR2020 PJ14-02-01 D3.3.030, 2019.

[14] A. Hall, J. Wingfield, G. De Moura, and K. Tiscareno, "Advancing Cyber Resilience in Aviation: An Industry Analysis." Davos, Switzerland: World Economic Forum, 2020, pp. 1–28.

[15] International Civil Aviation Organization (ICAO), "Finalization of LDACS Draft SARPs - Working Paper WP05 including Appendix," ICAO, Montreal, Canada, Tech. Rep., Oct. 2018.

[16] Intrinsic ID, "SRAM PUF: The Secure Silicon Fingerprint," pp. 1–6, 2018 (accessed Feb. 20, 2020). [Online]. Available: https://pdfs.semanticscholar.org/e823/f6078233b3f9e826f7570e794689b354f1a1.pdf

[17] D. Jao and L. De Feo, "Towards Quantum-Resistant Cryptosystems From Supersingular Elliptic Curve Isogenies," in *International Workshop on Post-Quantum Cryptography*. Heidelberg, Germany: Springer, Nov./Dec. 2011, pp. 19–34.

[18] S. Jung and S. Jung, "HRP: A HMAC-Based RFID Mutual Authentication Protocol Using PUF," in *International Conference on Information Networking*. New York, NY, USA: IEEE, Jan. 2013, pp. 578–582.

[19] B. Kamali, *AeroMACS: An IEEE 802.16 Standard-based Technology for the Next Generation of Air Transportation Systems*. Hoboken, NJ, USA: John Wiley & Sons, 2018.

[20] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, Jan. 1987.

[21] O. Marcia, "AeroMACS PKI," in *Integrated Communications, Navigation, Surveillance Conference*. New York, NY, USA: IEEE, Apr. 2018, pp. 1–15.

[22] N. Mäurer and A. Bilzhause, "Paving the Way for an IT Security Architecture for LDACS: A Datalink Security Threat and Risk Analysis," in *18th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, Apr. 2018, pp. 1A2/1–1A2–11.

[23] N. Mäurer, T. Gräupl, and C. Schmitt, "Evaluation of the LDACS Cybersecurity Implementation," in *38th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Sept. 2019, pp. 1–10.

[24] N. Mäurer and C. Schmitt, "Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- and Risk Analysis," in *19th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, Apr. 2019, pp. 1A2/1–1A2–13.

[25] Mäurer, N. and Bilzhause, A., "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)," in *37th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Sept. 2018, pp. 1–10.

[26] Mäurer, N., Gräupl, T. and Schmitt, C., "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS," in *39th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Oct. 2020, pp. 1–10.

[27] M. Niraula, J. Graefe, R. Dlouhy, M. Layton, and M. Stevenson, "ATN/IPS Security Approach: Two-way Mutual Authentication, Data Integrity and Privacy," in *Integrated Communications, Navigation, Surveillance Conference*. New York, NY, USA: IEEE, Apr. 2018, pp. 1–17.

[28] A. Rostovtsev and A. Stolbunov, "Public-Key Cryptosystem Based on Isogenies," *IACR Cryptology ePrint Archive*, pp. 1–19, May 2006.

[29] M. Schnell, "Update on LDACS - The FCI Terrestrial Data Link," in *19th Integrated Communications, Navigation and Surveillance Conference (ICNS)*. New York, NY, USA: IEEE, Apr. 2019, pp. 1–10.

[30] G. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *44th ACM/IEEE Design Automation Conference*. New York, NY, USA: IEEE, Jun. 2007, pp. 9–14.

[31] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A Practical and Compatible Cryptographic Solution to ADS-B Security," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3322–3334, Nov. 2018.