Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 15 (2020) pp. 126-135
© MIR Labs, www.mirlabs.net/jias/index.html

Drone partial temporary authentication in LoRaWAN network

Sana BENZARTI, Bayrem TRIKI and Ouajdi KORBAA
University of Sousse, ISITCom, MARS Research Laboratory LR17ES05
4011, Hammam Sousse, Tunisia.
sana.benza@gmail.com, bayrem.triki@gmail.com, ouajdi.korbaa@centraliens-lille.org

Abstract: **The security of the Internet of Things (IoT) is now at the embryonic stage. In fact, unrelenting innovation has slowed down the implementation of security and made user privacy an easy target. Through this work, we propose a secure architecture dedicated to an IoT-based drone in a LoRa context. For this purpose, we focused on the drone´ s authentication process by deploying an Id-Based Signcryption method and temporary identities.**

Keywords: drone, LoRa, Id-Based Signcryption, temporary identities, partial temporary authentication.

I. Introduction

LoRa (Long-Range) networks [1] are LPWANs (Low Power Wide Area Networks) with low speed, range, and consumption created by the company SemTech. They allow battery-powered objects to transfer low amounts of information. LoRa separates communications into frequency channels and uses transmission parameters. Bandwidth channels in Europe that are at 125 kHz can circulate at a rate of a few kilobits per second. The modulation is based on a chirp frequency which evolves linearly. A LoRaWAN [2], or LoRa Wide Area Network, refers to the low-power oriented protocol layer. LoRaWAN defines three types of classes:

- Class A: represents the lowest power class and bidirectional end devices. The communication is fully asynchronous.
- Class B: The devices are synchronized by using periodic beacons.
- Class C: The class with lowest latency.

LoRaWAN is based on the LoRaMAC protocol, which defines the interaction between nodes and gateways. LoRaMAC protocol offers several useful mechanisms such as temporal node synchronization, adaptation node transmission power management through gateway exchange, and a set of node identification keys. LoRaWAN [2] network structure is represented in Figure 1. The nodes (class A) exchange data with the gateways (class B) using the LoRa radio layer and the LoRaMAC protocol. The gateways are connected to the Internet through a 3G network, Ethernet, WiFi, or other mediums . They collect messages and transfer them to the data server (class C). Unlike SigFox, it is quite possible to create a LoRaWAN private network by installing its own gateways connected to a private server.

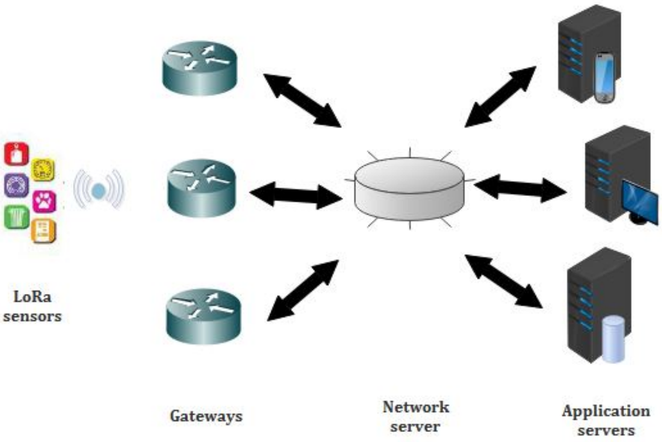


Figure. 1: LoRaWAN network architecture.

To communicate with the network server and control access from unrecognized objects, the end-devices should be activated. LoRaWAN specifies two activation methods [3]: Activation By Personalization (ABP) and Over-The-Air Activation (OTAA). - Activation By Personalization (ABP): This method is a simplified network connection; the object is quickly operational. However, the encryption keys for communication with the network are preconfigured in the object which makes security weak. If there is physical intrusion in the object, keys can be stolen, and this can lead to impersonation attacks by stealing object identities. In this case, collected data can be corrupted. - Over-The-Air Activation (OTAA): The network generates and sends encryption keys; security is thus strengthened. This is the most used method in IoT / LoRaWAN, because it is the most secure. However, the object must implement a junction mechanism which introduces additional complexity. OTAA allows a dynamic activation of the device where the keys are re-generated on every activation. ABS offers a static activation and in this case, the keys remain the same until the user changes them.

To identify an object, LoRaWAN uses [3] AppEUI, DevEUI and DevAddr. - AppEUI is a unique application identifier that allows the user to group objects. This 64-bit address is used to classify devices by application. This parameter can be edited.

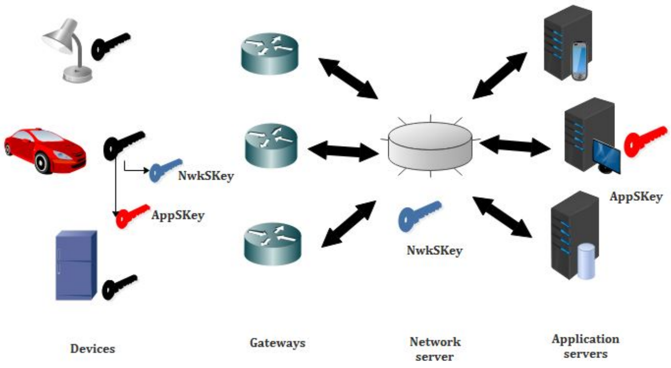


Figure. 2: NwkSKey and AppSKey.

- DevEUI is an identifier programmed in the factory that makes each object unique. This parameter is theoretically permanent.
- DevAddr is a logical address (equivalent of an IP address) to identify the object in the network. It is a non-unique device address.
LoRaWAN specifies three kinds of 128-bit security keys [4]: NwkSKey, AppSKey, and AppKey. - A Network Session Key (NwkSKey) interacts between nodes (devices) and the LoRa network server. This encryption key between the object and the operator is used for transmissions and to validate the integrity of messages.
- An Application Session Key (AppSKey) encrypts and decrypts the payload, which is fully encrypted between the node and the application servers.
- An Application Key (AppKey) is a shared secret between the device and the network, used to derive session keys. This parameter can be changed. The NwkSKey and AppSKey are unique per device and per session (see Figure 2)[4].
Using a drone in the context of LoRaWAN network seems to be interesting and helpfull especially in civilian missions. However, drones can be a source of threat when some people try to use it in a wrong way. Legal drones can be diverted to malicious drones. We distinguish two cases:
- A terrorist: a person who owns a legitimate drone, however he uses it to spy people, steal state secrets, sensitive data, spy on sensitive sites such as nuclear power plants or military bases.
- A hacker: who takes control and hijacks an authorized and a legal drone by launching attacks such as DDOS or man in the middle attack. He can for example hijack and modify collected data from a military drone in order to cause damage.
Sometimes we use drone tracking in order to avoid collisions and detect unauthorized flight, especially in limited area and when the traffic is increasing [5]. In return, this option becomes dangerous if the drone is controlled by a terrorist or a hacker.
The most relevant problems affecting the combination between drones and the LoRa network can be summarized as follows [6]: - Extending the batteries lifetime of drones, - Building reliable protocol communication between drones and base stations, - The ability to negotiate with a wide variety of heterogeneous sensors and devices ;and above all security improvement.
In order to limit the risks of drone mishandling, we propose a drone registration system. Each engine must be identified and recognized by our proposed architecture in order to know their activities such as their trajectory and the visited places. In addition, to protect the users privacy, fight against attacks like DDOS and limit the traceback risks, our architecture suggests the use of temporary identities with the partial method during renewal. In fact, each identity of a device includes several partial identities. In general, partial identities are subsets of attributes of a complete identity. In our case, partial temporary authentication is a method of authentication that uses subset of characters of an entire temporary identity which increases safety on drone's user side. Indeed, it provides less information for hackers and reduces the risk of attacks. The origin of this method is the use of partial passwords which was introduced in internet banking applications as a two-factor authentication [7].
In our article, we propose a LoRa security architecture for an IoT-based drone, also known as UAV (Unmanned Aerial Vehicle). The latter is a drone endowed with IoT devices [8] and LoRa sensors that allows users to be connected to the Internet from any place and at any time. This drone performs in a LoRa network to accomplish a special mission and may communicate with other drones. This architecture will describe the security authentication of drones in a LoRa network with the option of privacy preservation.
To the best of our knowledge, no previous research has been dedicated to the authentication and tracking process of drones using ID-based signcryption in a LoRa context. The main contribution of this work is threefold. First, thanks to the use of RFID tags, drones will be tracked whenever and wherever they go. Second, privacy preservation is managed by providing temporary identities produced and renewed upon a request. Third, the authentication process and drone communication are established using Id-Based Signcryption.
The article will be structured as follows: Section 2 presents related research. Section 3 describes our proposed architecture. Section 4 details our proposed scheme which relies on Id-Based Signcryption. Section 5 illustrates the simulation results which highlights the efficient use of temporary identities by assuming that a spy drone launches a DDOS attack to compromise the network. Finally, section 6 concludes our paper.

II. Related works

This section presents some drone and LoRa network vulnerabilities. Previous works have shown that drones are targets for different types of attacks, like DOS (Denial Of Service) attacks [9], ARP (Address Resolution Protocol) spoofing, Telnet / FTP (File Transfer Protocol) attacks [10], Man-In-The-Middle (MITM) attacks [11], hijacking [12], and packet injection [13]. Drones can be considered as simple flying assets; however, mishandling and their security vulnerabilities can cause enormous

damage and expose people to danger. In fact, security implementation poses many challenges, like data protection, privacy requirements, and compromised authentication [14][15]. Other researchers have mentioned that drones are exposed to:
- GPS jamming [16]: A pirate can generate noisy signals to interfere with the GPS receivers and disturb the real signal.
- WiFi cracking: Some drones are designed without a WiFi password, which means anyone can connect to this access point and take control of the drone. In addition, if the wireless connection is protected by a password, it is possible to crack it [17].
- Malware: Malware can be injected into drones, as proved in Maldrone, the first backdoor for drones [18]. Data extraction, data theft, and reverse engineering are all threats posed by malware in drones [19][20].
The LoRa network has interesting features and raises several challenges, which can be divided into five classes [21] :

1. Power consumption : resource allocation;

2. Communication range : channel coding, interference cancellation;

3. Multiple access : resource allocation, link coordination.

4. Error correction: channel coding, interference cancellation.

5. Security : key update, key generation , third party authentication.

Each class can have challenges in common.
LoRaWAN technology encrypts, by default, all end-to-end messages, from the connected object to the application server. All messages are also signed between the connected object and the servers of the LoRaWAN network. These operations rely on two different keys: AppSKey for encryption, and NwkSKey for signing.
According to some security researchers [22], the way in which the encryption is achieved is not optimal and opens the door to partial or total decryption attacks. In fact, the messages are not encrypted in 128-bit AES, as we had assumed. Instead, an algorithm is used to generate a succession of keys (i.e., a k̈eystream). Each block of the message is coded into XOR, an ultra-classical mathematical operation. Consequently, the encrypted message has exactly the same size as the unencrypted message. It is estimated that about 50% of devices have LoRa chips whose memory is not protected [23]. To recover all memory, including encryption keys, the serial port or the debug port must simply be connected. If these ports are not available, it is often possible to extract the keys by measuring the microcontroller consumption variations that are next to the LoRa chip [23].
In order to reduce the impact of these vulnerabilities and strengthen the security aspect, some schemes have been proposed : In [5], the authors propose a model which is based on authentication using Temporal Credential (TCALAS) in Internet of Drones context (IoD).
The TCALAS method can be considered robust, however it cannot resist the traceability and the stolen verifier attacks. The work in [24], proposes an improvement of this scheme (iTCALAS) which uses symmetric key primitives and temporal credentials.
The authors propose in [25], the use of key cryptography and symmetric key cryptography in different servers. Method named S2KG (Server Session Key Generation) in order to generate a communication key session which is not defined in the LoRaWAN specification.
The work [26] presents the implementation of AES encryption / decryption hardware in order to reduce energy consumption using the method of Three low power techniques. To enhance security, secure key updating procedure has been proposed.
The design and implementation of a LoRa gateway is proposed in [27]. The research suggests an improvement of the network server and an evaluation of performance in an urban environment.
In our work, we will propose an architecture based on the concept of drone authentication and data encryption with ID-Based Signcryption in a LoRa network. Signcryption is an innovative approach in Public Key Cryptography (PKC). It furnishes a digital signature and public key encryption in one step[28], saves time and energy costs.

III. Proposed architecture

This section describes our proposed architecture and the system model components.

A. System model

Our system model is divided into seven elements: - BS: (Base Station): Ensures the coverage area of Wi-Fi or 3G/4G networks and also used for communication between drones and gateways.
- Gateways: Forwards data.
- Network server: Provides adaptive rate management and data security while treating the redundancy of the received data.
- Application Servers: Exploits and process the received data.
- CC: (Civilian Cloud): Manages received requests from drones and synchronizes data with application servers of LoRa networks.
- DB: (Data Base): Saves the drones´ identities.
- IS: (Identity Server): Provides and manages temporary identities.

B. Development process

In this sub-section, we explain our proposed architecture based on a LoRaWAN network. Our main goal is to improve drone safety and highlight the authentication process which will be detailed in the next section. In our work, we are interested in IoT-based drones or drones with LoRa-embedded sensors that are given special missions. These drones are used to accomplish a civilian mission like fire detection, air pollution management, or road traffic management. In a LoRa context, devices should be identified before the communication process. Therefore, each object has three types of identifier: AppEUI for groups of objects, DevEUI for unique objects, and DevAddr for the IP address. However, we cannot rely on only these identifiers, given that objects connected to LoRa networks can be easily exposed to the public if they are not protected. In fact, some connected objects may be visible to search engines. For example, the most famous hackers´ search engine is ´ Shodan´ which allows people to get information on connected devices such as their location, IP address, open port, encryption method, ...etc. To reinforce our security architecture, we add RFID readers to the BS and place RFID tags on drones. The BS is the first step for drone authentication and ensures the coverage network to provide 3G/4G drone communication in a given area. Each drone is equipped with two types of interfaces: a 3G/4G interface to send big data with a high data rate and a LoRa interface to communicate with LoRaWAN networks and provide useful information from embedded sensors. As mentioned before, drones are tagged with a tamper-proof RFID that offers the unique identifier, $\mathrm{ID}_{\mathrm{RFID}}$. According to Figure 3, which illustrates our proposed architecture, drones should acquire two types of identifier: $\mathrm{ID}_{\mathrm{UNIQUE}}$ and $\mathrm{ID}_{\mathrm{temp}}$. In fact, the $\mathrm{ID}_{\mathrm{UNIQUE}}$ is composed of the $\mathrm{ID}_{\mathrm{RFID}}$ (once a drone has entered a given area, the BS identifies it with its RFID reader) and DevEUI, which is its unique and permanent identifier in a LoRaWAN network. Concerning the $\mathrm{ID}_{\mathrm{temp}}$, is an identifier obtained after a request and is renewable over time. This identity is used to protect the drone´ s privacy and maintain a higher security level, especially in the case of drone-to-drone communication or drone-LoRa object communication. Drones cannot communicate with other devices until they obtain these two identifiers. While entering a zone, the BS sends data to the Civilian Cloud (CC) and requests a temporary identifier that is provided from the Identity Server (IS) (considered as a trusted party) and saved in the Data Base (DB). The CC manages the received requests and the $\mathrm{ID}_{\mathrm{RFID}}$ is stored in the DB. Meanwhile, the IS checks the temporary identifier´ s features, like expiration time and validity. Once they are ready, the CC sends them back to the BS and assigns them to the drones. If the temporary identities are expired, then the request is renewed. The NwkSKey and the AppSKey are used after drone Id-Based Signcryption authentication. This procedure is detailed in the next section.

IV. Proposed authentication scheme

This section presents the concept of the Id Based Signcryption and describes our proposed algorithm for drone authentication.

A. Id Based Signcryption

The Id Based Signcryption (IBS) is derived from Id Based Cryptography, which was developed to employ users´ identity within a signcryption method. The IBS was proposed for the first time by Malone-Lee in the random oracle model [28]. This new paradigm furnishes a digital signature and public key encryption in one step by using object identity. This method guarantees that any authenticated entity should have a digital signature with an encrypted key. In our work, we distinguish two cases:
- Drone-to-drone communication in a LoRa context.
- Drone to LoRa object communication.

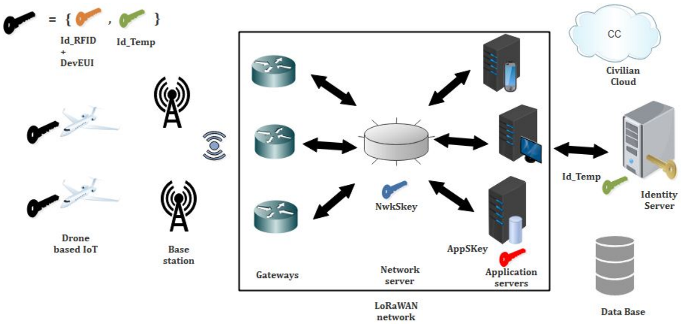


Figure. 3: Proposed Architecture

d1 identifiers			d2 identifiers		
$\mathrm{ID}_{\mathrm{UNIQUE}}$	$\mathrm{ID}_{\mathrm{temp}}$	LoRa $\mathrm{ID}_{\mathrm{temp}}$	$\mathrm{ID}_{\mathrm{UNIQUE}}$	$\mathrm{ID}_{\mathrm{temp}}$	LoRa $\mathrm{ID}_{\mathrm{temp}}$
$\mathrm{ID}_{\mathrm{RFID1}}$	$\mathrm{ID}_{\mathrm{temp1}}$	$\mathrm{NwkSKey}_1$	$\mathrm{ID}_{\mathrm{RFID2}}$	$\mathrm{ID}_{\mathrm{temp2}}$	$\mathrm{NwkSKey}_2$
DevEUI_1		$\mathrm{AppSKey}_1$	DevEUI_2		$\mathrm{AppSKey}_2$

Table 1: Identifiers of drone d1 and drone d2

B. Drone-to-drone communication

In a given area, two civilian drones d1 and d2 are given a special mission to accomplish. The BS reads their tags $\mathrm{ID}_{\mathrm{RFID}}$ and sends a request to the CC for the temporary identifier, $\mathrm{ID}_{\mathrm{temp}}$. Finally, each drone is assigned a temporary identifier, $\mathrm{ID}_{\mathrm{temp}}$ and a unique identifier, $\mathrm{ID}_{\mathrm{UNIQUE}}$ containing $\mathrm{ID}_{\mathrm{RFID}}$ and DevEUI. Table 1, groups both drones´ identifiers, if we suppose that drone d1 wants to communicate with drone d2.

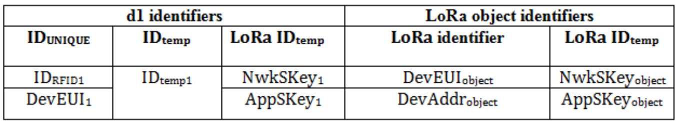
The NwkSKey and AppSKey are involved only after the authentication process and used to secure communications and message exchanges between d1 and d2. Algorithm 1 consists of six steps:

- Setup : Takes as input 1^k and generates the pair $< \lambda, \mu >$ which represent respectively the master secret and the common public parameter. The k is a security parameter.

- $\mathrm{Extract}_{\lambda\ ,\ \mu}$: Calculates the private keys $\mathrm{PrvK}_{\mathrm{d1}}$ and $\mathrm{PrvK}_{\mathrm{d2}}$ corresponding to drones´ identifiers, $\mathrm{ID}_{\mathrm{d1}}$ and $\mathrm{ID}_{\mathrm{d2}}$ under $< \lambda, \mu >$. The $\mathrm{ID}_{\mathrm{d1}}$ and $\mathrm{ID}_{\mathrm{d2}}$ contains respectively the $\mathrm{ID}_{\mathrm{temp}}$ and the $\mathrm{ID}_{\mathrm{UNIQUE}}$ of d1 and d2. The $\mathrm{PrvK}_{\mathrm{d1}}$ is used to produce the signature and encrypt the message. $\mathrm{PrvK}_{\mathrm{d2}}$ is used to decrypt the received message.

- Sign_{μ}: Generates a signature Sig and ephemeral state data E for a given input from drone1´ s private key $\mathrm{PrvK}_{\mathrm{d1}}$ and the message mes.

- $\mathrm{Encrypt}_{\mu}$: To encrypt the signed plaintext, we use this function with the given inputs $\mathrm{PrvK}_{\mathrm{d1}}$, $\mathrm{ID}_{\mathrm{d2}}$, mes, Sig and E. The output is a ciphertext CTXT that contains



d1 identifiers			LoRa object identifiers	
ID_{UNIQUE}	ID_{temp}	LoRa ID_{temp}	LoRa identifier	LoRa ID_{temp}
ID_{RFID1}	ID_{temp1}	$NwkSKey_1$	$DevEUI_{object}$	$NwkSKey_{object}$
$DevEUI_1$		$AppSKey_1$	$DevAddr_{object}$	$AppSKey_{object}$

Table 2: Identifiers of drone d1 and LoRa object

the signed message encrypted for ID_{d2} under μ.
- $Decrypt_\mu$: Decrypts the ciphertext using $PrvK_{d2}$. It uses CTXT to obtain the triple $<\widehat{ID}_{d1}$, $\widehat{mes}$, $\widehat{Sig}>$.
- $Verify_\mu$: The generated triple$<\widehat{ID}_{d1}$, $\widehat{mes}$, $\widehat{Sig}>$ is checked. If $\widehat{ID}_{d1} = ID_{d1}$ (the purported sender identity is the same drone1´ s identity), $\widehat{mes}$ = mes (the received message is the sending message) and $\widehat{Sig}$ = Sig (the received signature is the generated one) then the output is true $\top$ otherwise false $\perp$.

Algorithm 1 Id Based Signcryption drone-to-drone

```
1. Setup : $< \lambda, \mu > \leftarrow Setup[1^k]$

2. $Extract_{\lambda,\ \mu}$ : For any identities $ID_{d1}$ and $ID_{d2}$ :
   $PrvK_{d1} = Extract_{\lambda,\ \mu}[ID_{d1}]$ with $ID_{d1} = (ID_{UNIQUE1}, ID_{temp1}) = (ID_{RFID1}, DevEUI_1, ID_{temp1})$
   $PrvK_{d2} = Extract_{\lambda,\ \mu}[ID_{d2}]$ with $ID_{d2} = (ID_{UNIQUE2}, ID_{temp2}) = (ID_{RFID2}, DevEUI_2, ID_{temp2})$
   $PrvK_{d1} = Extract_{\lambda\ ,\ \mu}[(ID_{RFID1}, DevEUI_1, ID_{temp1})]$
   $PrvK_{d2} = Extract_{\lambda\ ,\ \mu}[(ID_{RFID2}, DevEUI_2, ID_{temp2})]$

3. $Sign_\mu$ : $< Sig, E > \leftarrow Sign_\mu[PrvK_{d1}, ID_{d1}$, mes]

4. $Encrypt_\mu$ : CTXT $\leftarrow Encrypt_\mu[PrvK_{d1}, ID_{d2}$, mes, Sig, E]

5. $Decrypt_\mu$ : $<\widehat{ID}_{d1}$ , $\widehat{mes}$, $\widehat{Sig}> \leftarrow Decrypt_\mu[PrvK_{d2}$, CTXT]

6. $Verify_\mu$ : $[\widehat{ID}_{d1}, \widehat{mes}, \widehat{Sig}] = \top$ if $\widehat{ID}_{d1} = ID_{d1}$, $\widehat{mes}$ = mes and $\widehat{Sig}$ =Sig
```

C. *Drone to LoRa object communication*

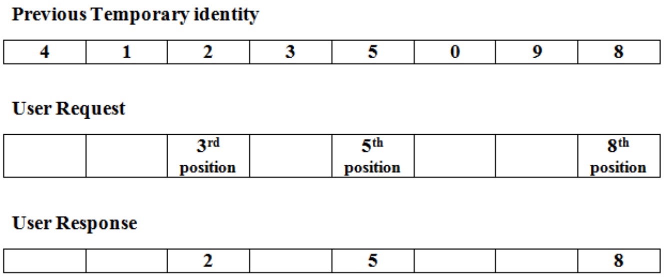
This sub-section presents the case of the communication between drone d1 and a LoRa object (any LoRa device that can connect to LoRaWAN network). We suppose that drone d1 wants to communicate and exchange information with LoRa object. The table 2 summarizes the identifiers involved in the authentication process. For LoRa object, we will use the DevEUI and DevAddr to compute the object private key $PrvK_{object}$ used later to generate the digital signature.
As mentioned in the previous sub-section, the NwkSKey and AppSKey are used after drone and object authentication. Our proposed method is exposed in Algorithm 2.

Algorithm 2 Id Based Signcryption drone-to-LoRa object

```
1. Setup : $< \lambda, \mu > \leftarrow Setup[1^k]$

2. $Extract_{\lambda,\ \mu}$ : For any identities $ID_{d1}$ and $ID_{object}$ :
   $PrvK_{d1} = Extract_{\lambda,\ \mu}[ID_{d1}]$ with $ID_{d1} = (ID_{UNIQUE1}, ID_{temp1}) = (ID_{RFID1}, DevEUI_1, ID_{temp1})$
   $PrvK_{object} = Extract_{\lambda,\ \mu}[ID_{object}]$ with $ID_{object} = (DevEUI_{object}, DevAddr_{object})$
   So we have
   $PrvK_{d1} = Extract_{\lambda,\ \mu}[(ID_{RFID1}, DevEUI_1, ID_{temp1})]$
   $PrvK_{object} = Extract_{\lambda\ ,\ \mu}[(DevEUI_{object}, DevAddr_{object})]$

3. $Sign_\mu$ : $< Sig, E > \leftarrow Sign_\mu[PrvK_{d1}, ID_{d1}$, mes]

4. $Encrypt_\mu$ : CTXT $\leftarrow Encrypt_\mu[PrvK_{d1}, ID_{object}$, mes, Sig, E]

5. $Decrypt_\mu$ : $<\widehat{ID}_{d1}$ , $\widehat{mes}$, $\widehat{Sig}> \leftarrow Decrypt_\mu[PrvK_{object}$, CTXT]

6. $Verify_\mu$ : $[\widehat{ID}_{d1}, \widehat{mes}, \widehat{Sig}] = \top$ if $\widehat{ID}_{d1} = ID_{d1}$, $\widehat{mes}$ = mes and $\widehat{Sig}$ =Sig
```

D. *Partial temporary authentication*

When the drones take off and from the communication request, our system recognizes the owner of the drone thanks to the ID_{UNIQUE} stored in our database. The generation of an ID_{temp} implies the storage of this identity in our database that will be sent to the smartphone of the drone´ s owner. When drones want to communicate with each other or with a LoRa object, the communication process is activated.
Given that the Identity Server is responsible of the temporary identities generation. Once the first request to get the IDTEMP is launched, the Identity Server checks the generation conditions (for example if this drone is authorized to have an IDTEMP or it can circulate in a specific area, ...). During a request renewal, partial temporary authentication is involved.
We will consider the following conditions where there will be certainly a renewal of ID_{temp}.:
- If the communication is interrupted,
- A technical problem occurs such that the authentication process is abnormally long,
- Changed position of the drone from one zone to another. This condition is explained in the simulation section.
To renew this identity, the user must fulfill the following condition: send a maximum of 3 digits of the previous ID_{temp}, randomly chosen by our system. This is where the partial temporary authentication method is implimented. Indeed, to maintain a fairly high level of security, we must check if the user possesses the previous



Previous Temporary identity

4	1	2	3	5	0	9	8

User Request

		3rd position		5th position			8th position

User Response

		2		5			8

Figure. 4: Partial temporary authentication

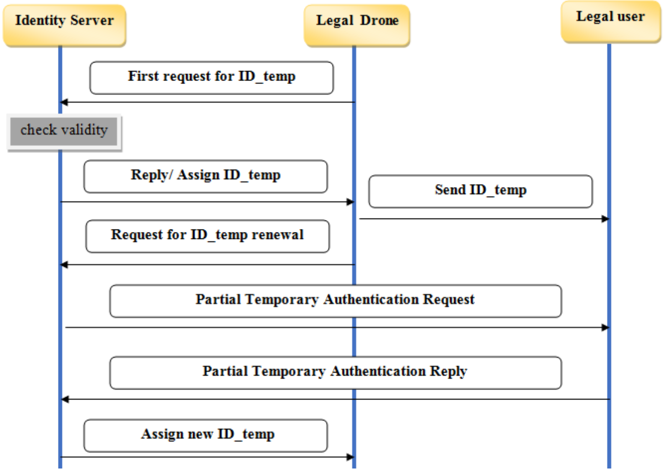

Identity Server
Legal Drone
Legal user
First request for ID_temp
check validity
Reply/ Assign ID_temp
Send ID_temp
Request for ID_temp renewal
Partial Temporary Authentication Request
Partial Temporary Authentication Reply
Assign new ID_temp

Figure. 5: Process of partial temporary authentication.

$\mathrm{ID_{temp}}$. The user has two attempts and 10 seconds for each. For example, his previous $\mathrm{ID_{temp}}$ is made up of 8 digits $< 41235098 >$, we ask him to fill in 3 boxes: we choose the 3 rd, 5 th and last position of the $\mathrm{ID_{temp}}$. The user must put 2, 5 and 8 as shown in Figure 4.

If the user reply with the correct answer, the $\mathrm{ID_{temp}}$ will be renewed, otherwise an alert will be sent to the system to warn us that there is a problem with the owner of the drone whose $\mathrm{ID_{UNIQUE}}$ is recognized.

The Figure 5 presents the process of partial temporary authentication.

The algorithm 3 explains the approach of our proposed method.

V. Simulation

A. Simulation model

The purpose of the simulation, is to highlight the efficient use of temporary identities suggested in our solution. Indeed, we will take into consideration some proposed hypotheses and study the case of a DDOS (Distributed Denial Of Service) attack launched by a spy drone. This pirate, will try to attack the LoRaWAN network by creating botnets in order to make the service unavailable. To send an extremely large number of requests to the targeted resource, the cybercriminal often establishes a zombie network of infected nodes [29]. Thus, he starts by selecting malicious nodes and extends his zombie network. Given Z , a geographical area divided into m sectors. Suppose that each zone is denoted zone 1 = 1, zone 2 = 2, ..., zone m = m. Let Z=1,2,3,4,...,m. We considered the following assumptions:

Algorithm 3 Partial temporary authentication

```
Input: Condition 1 = Interrupted communication.
Condition 2 = Changed position.
IF (condition 1 OR condition 2 == true) THEN
RQ_RNW == true (renewal request is activated)
RQ_Partial_Temporary_NUMBER (request to validate empty boxes)
WHILE ($i \leq 2$ AND $T < 10$ seconds)
IF (attempt == Corr_box) (If the numbers correspond to the correct boxes) THEN RNW (renewal)
ELSE repeat_attempt
END IF
END WHILE
IF ($i > 2$) THEN NO_RNW (No renewal )
SEND_ALERT
END IF
END IF
```

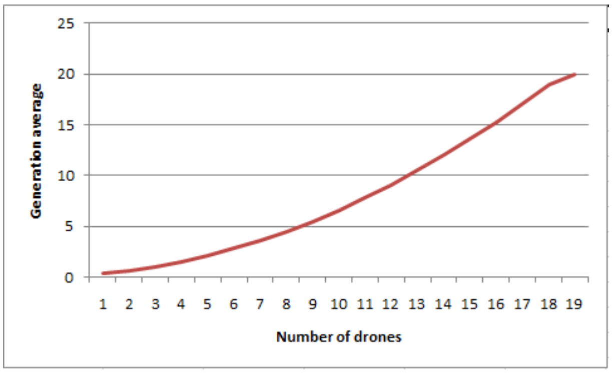


Figure. 6: Average generation for 20 drones.

1- d1: is an ordinary drone connected to the LoRaWAN network.

2- d2, d3, d4 and d5: are drones connected to the LoRaWAN network and on which we implemented our algorithm.

3- Area Z is equipped with LoRa sensors.

4- The change of position from one sector to another implies a renewal of temporary identity (d1 is not affected). In fact, each time the drone enters a new zone, a new temporary identity is assigned.

To understand the behavior of temporary identities generation, we simulated two groups of drones, one with 20 and another with 100 drones and calculated the average generation of temporary identities. The generation average for 20 drones, illustrated in Figure 6, shows a slow increase that can be considered proportional to the number of drones.

Figure 7 represents the temporary identity generation average (green) for 100 drones (red). The blue indicates the zone where the drones are randomly selected. For example, drone 1 is at position number 94. From the graph, we notice that the generation average increases slowly and reminds us of the generation graph for 20 drones. This generation is proportional to the number

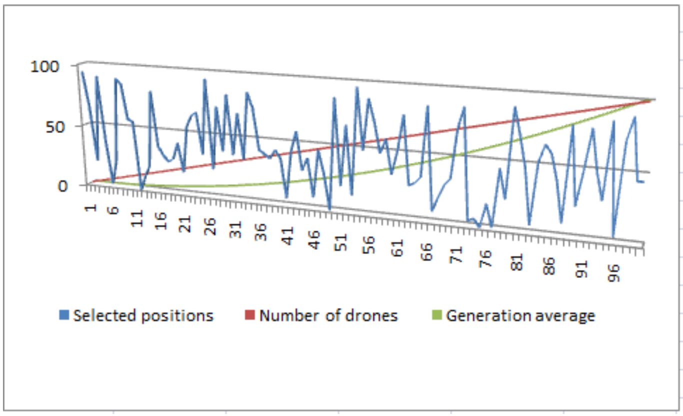


Figure. 7: Average generation for 100 drones.

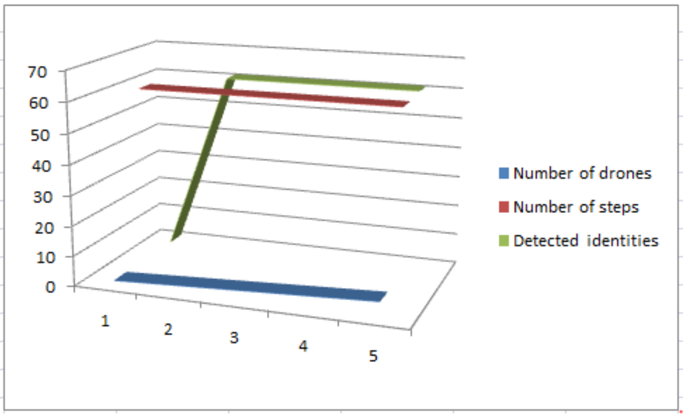


Figure. 8: Detected identities with fixed step method

	d1	d2	d3	d4	d5
Number of steps	60	60	60	60	60
Number of identity	1	62	62	62	62

Table 3: Fixed step method

	d1	d2	d3	d4	d5
Number of steps	60	30	27	80	19
Number of identity	1	32	29	82	21

Table 4: Variable step method

of drones. Whenever the number of nodes increases, the average generation of temporary identities raises too.

B. Simulation results

Consider the following scenario :
At t =t_0, five drones, d1, d2, d3, d4 and d5 get into Z. The pirate drone is somewhere in Z, observing drones activity to prepare a DDOS attack.
At t = t_1, the five drones take off to accomplish a precise civil mission and visit several sectors of Z. We will give T_{d1}, T_{d2}, T_{d3}, T_{d4} and T_{d5} the respective trajectories of d1, d2, d3, d4 and d5. In the meantime, the hacker intercepts some data to prepare the botnets. As mentioned before, d1 is an ordinary drone and the others are implemented with our algorithm. The hacker can intercept a single identity for d1 and several identities for d2, d3, d4 and d5 according to the number of changed positions. Two cases are distinguished:
- Case 1: Changed position with fixed step: (Table 3)
According to the Byzantine method [30], the network can be attacked if and only if 1/3 of the nodes are disloyal. This means 1/3 of the nodes must be compromised. In Figure 8, the blue indicates the number of drones which is five. Red stands for the number of steps which is 60. In this case, steps are fixed and all drones have changed their trajectory 60 times. Green shows the number of detected identities. For drone 1, only one identity can be intercepted. For others, the number of detected drones equals number of steps + 2. Whenever the drone moves, a temporary identity is assigned. The +2 indicates the identity of the drone in the LoRaWAN network which is formed by the DevEUI and the RFID identity. To launch a DDOS attack and to compromise this network, it is necessary for 1/3 of all nodes to be infected. All five drones can be compromised by infecting two drones. However, in our case, the pirate does not see five, but 1 + 62 * 4 = 249 drones, or one drone plus 62 * 4 for the other four. The pirate must compromise at least 249/3 = 83 drones to destroy the network.
However, these 83 compromised nodes may be fictive identities, meaning they are not real drones. The pirate believes that he attacked the network by compromising these detected drones. However, there is a high chance, he attacked fictive nodes instead. The fixed step method is effective when the moves are extended, but we must take energy consumption and battery life into consideration, which are limited.
According to the Figure 9, the spy drone will launch two DDOS attacks (one at the beginning and the other at the end of the simulation). Since the drone d1 has a single identity, the risk of compromising is very high. It is assumed that d1 became an accomplice with the pirate drone. The latter must compromise another node to control the network and expand its zombie network. We will consider that the hacker in the second attempt could compromise the node 3 and was able to steal his temporary identity $ID_{d3,p59}$ (temporary identity of drone d3 on position number 59). However, the node d3 has two other fixed identities $ID_{RFID,d3}$ and DevEUI. The attack can be effective if and only if the fixed identities have been affected. In addition, the temporary identity that has been compromised will be renewed after a time slot or if the drone changes position. Subsequently, $ID_{d3,p60}$ will be generated and even if the attacker succeeds in attacking the other nodes, he will attack fictive identities and the risk of attacking the fixed identities remains low.
Case 2: Changed position method with variable steps: (Table 4)
As shown in Figure 10, number of drones launched in area Z are in blue. Red shows the number of moves made according to variable step method. Each drone moves freely without being restricted to a fixed number of steps. For example, d4 changed position 80 times and d5 moved 19 times. Green stands for the number of de-

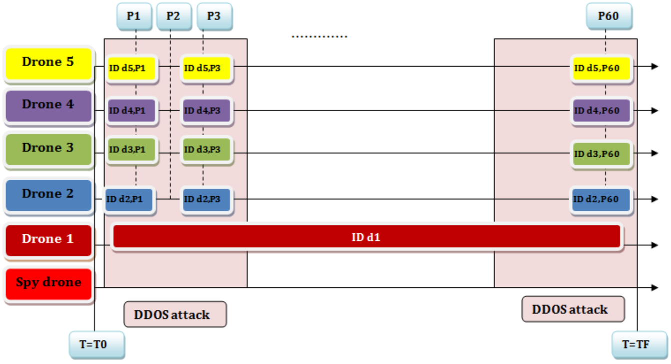


Figure. 9: Timeline attack

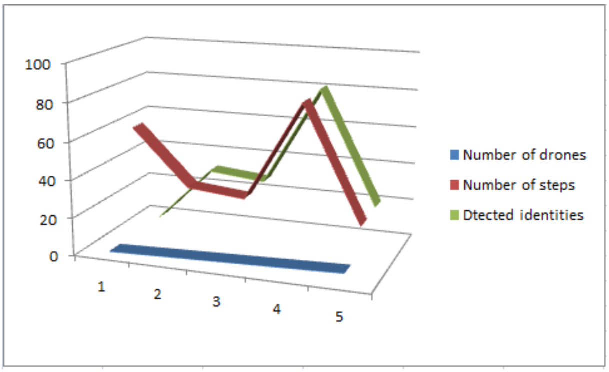


Figure. 10: Detected identities with variable step method

tected drones. Since d1 has a single identity, the hacker can easily compromise it. For the other nodes, the number of detected drones is equal to the number of steps+2. The same principle applies: to compromise this network, the pirate must attack the 1/3 of the nodes. Therefore, with 1 + 32 + 29 + 82 + 21 = 165 identities. 165 /3 = 55 nodes must be infected. The larger the number of moves, the greater the number of generated identities and the lower the probability of compromising the network.

C. Security analysis

We notice from the simulation that the drone d1 can be easily compromised and represent a threat as a botnet. However, the probability of attacking the other drones remains low thanks to the high number of temporary identities resulting from our proposed solution. In fact, the use of temporary identities can reduce the risk of attacks and fight against the traceback [31]. In addition, this method enhances the security privacy. In general, traceback is the process of determining something's trace back to its source. In a traceback attack, the hacker uses multiple monitoring nodes to passively observe requests that pass through the nodes of the network [32].
The table 5 compares some other schemes to reduce the risk of a DDOS attack (Byzantine attack) and exposes the pros and cons of each solutions. To strengthen our proposed solution, we can combine our method with the Trust-based approaches to build drones investigation and reduce the attack's risks. A combination based on watchdog and alert report to better understand the behavior of compromised nodes.

	Pros	**Cons**
Trust-based approaches [33]	- Watchdog and path rates. - Alert reports for drone's reputation.	-The way how trusted nodes can be compromised is not clear. - There is no protection against false accusations.
Cryptography Based [34]	- Strong authentication. - Trusted communications.	- Cannot defend attacks from compromised insider nodes.
Our proposed solution	- Strong authentication. -Trusted communications. - Privacy preservation. -Temporary identities renewal to fight against traceback. - Use of partial temporary authentication - Two types of methods: fixed and variable steps	- Time and energy cost can be high

Table 5: Comparative table

VI. Conclusion

Our article proposes a solution for drone authentication that relies on Id Based Signcryption in a LoRa context. We suggest the use of temporary identities to preserve privacy combined with a unique identifier in order to acquire a signed, encrypted identity for user authentication. With the partial temporary authentication method we enhance our system security and reduce the risk of attacks.

References

[1] A. Zourmand, A. L. K. Hing, C. W. Hung, M. AbdulRehman, "Internet of Things (IoT) using LoRa technology", In Proceedings of IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), Selangor, Malaysia, June 2019.

[2] M. Rizzi, P. Ferrari, A. Flammini and E. Sisinni, "Evaluation of the IoT LoRaWAN Solution for Distributed Measurement Applications", IEEE Transactions on Instrumentation and Measurement, Volume: 66 , Issue: 12 , pp 3340 - 3349, Dec 2017.

[3] X. Yang, "LoRaWAN: Vulnerability Analysis and Practical Exploitation", PhD thesis, Delft University of Technology, The Netherlands, 2017.

[4] I. ButunNuno, P. PereiraMikael, G. Gidlund, "Security Risk Analysis of LoRaWAN and Future Directions", Future Internet 11(1):3, December 2018.

[5] J. Srinivas, A. K. Das, N. Kumar, and J.J. P. C. Rodrigues, "TCALAS: Temporal Credential Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment", IEEE Transactions on Vehicular Technology, Volume: 68 , Issue: 7 , pp 6903 - 6916, July 2019.

[6] J. P. S. Sundaram , W. Du , Z. Zhao , "Survey on Collaborative Smart Drones and Internet of Things

for Improving Smartness of Smart Cities", IEEE Communications Surveys & Tutorials Volume: 22 , Issue: 1 , pp 371 - 388, September 2019.

[7] I. Praveen, M. Sethumadhavan, "Partial Password Authentication using Vector Decomposition", International Journal of Pure and Applied Mathematics, volume 118, Number 7 Special Issue, pp 381-385, 2018.

[8] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives", IEEE Internet of Things Journal, volume 3, Number 6, pp 899-922, December 2016.

[9] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza and V. Guizilini, "The impact of DoS attacks on the AR.Drone 2.0", In Proceedings of XIII Latin-American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR), pp 127-132, Recife, Brazil, October 2016.

[10] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi based UAVs from common security attacks", In Proceedings of IEEE Military Communications Conference, MILCOM, pp. 1213-1218, Baltimore, MD, USA, November2016.

[11] N. M. Rodday, R. d. O. Schmidt, and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles", In Proceedings of IEEE/IFIP Network Operations and Management Symposium (NOMS), pp 993-994, Istanbul, Turkey, April 2016.

[12] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang and M. Robinson, "Security Authentication System using Encrypted Channel on UAV Network", In Proceedings of First IEEE International Conference on Robotic Computing (IRC), Taichung, Taiwan, April 2017.

[13] J. Habibi , A. Gupta, S. Carlson, A. Panicker, and E. Bertino, "MAVR: Code Reuse Stealthy Attacks and Mitigation on Unmanned Aerial Vehicles", In Proceedings of IEEE 35th International Conference on Distributed Computing Systems, pp 642-652, Columbus, OH, USA, July 2015.

[14] A. Y. Javaid, W. Sun, V. K. Devabhaktuni and M. Alam, "Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System", In Proceedings of IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, November 2012.

[15] W. G. Voss, "Privacy Law Implications of the Use of Drones for Security and Justice Purposes", International Journal of Liability and Scientific Enquiry (IJLSE), Volume 6, Number 4, pp 171-192, January 2013.

[16] A. Purwar, D. Joshi and V. Chaubey, "GPS signal jamming and antijamming strategy A Theoretical Analysis", In Proceedings of IEEE Annual India Conference (INDICON), Bangalore, India, December2016.

[17] N. M. Rodday, R. O. Schmidt and A. Pras, "Exploring Security Vulnerabilities of Unmanned Aerial Vehicles", In Proceedings of IEEE/IFIP Network Operations and Management Symposium (NOMS), Istanbul, Turkey, April 2016.

[18] E. Dahlman, K. Lagrelius, "A Game of Drones:Cyber Security inUAVs ", PhD thesis, KTH Royal Institute of Technology, Electrical Engineering and Computer Science, 2019.

[19] N. Shashok, "Analysis of Vulnerabilities in Modern Unmanned Aircraft Systems", December 2017.

[20] V. Sharma, G. Choudhary, Y. Ko, I. You, "Behavior and Vulnerability Assessment of Drones-Enabled Industrial Internet of Things (IIoT)", IEEE Access : Security and Trusted Computing for Industrial Internet of Things, Volume: 6, pp 43368 - 43383, July 2018.

[21] J. P. S. Sundaram, W. Du, Z. Zhao, "A Survey on LoRa Networking: Research Problems, Current Solutions and Open Issues", IEEE Communications Surveys & Tutorials, Volume: 22 , Issue: 1 , pp 371 - 388 , 2020.

[22] W. Xu, S. Jha, W. Hu, "LoRa-Key: Secure Key Generation System for LoRa-Based Network", IEEE Internet of Things Journal, Volume: 6 , Issue: 4 , pp 6404 - 6416, August 2019.

[23] I. You, S. Kwon, G. Choudhary, V. Sharma, and J. T. Seo, "An Enhanced LoRaWAN Security Protocol for Privacy Preservation in IoT with a Case Study on a Smart Factory-Enabled Parking System", Sensors Journal, volume 18, issue 6, June 2018.

[24] Z. ALI, S. A. CHAUDHRY, M. S. RAMZAN, AND F. AL-TURJMAN, "Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles", Human-driven Edge Computing (HEC) , IEEE Access, Volume: 8 , pp 43711 - 43724, 2020.

[25] Kun-Lin Tsai ; Fang-Yie Leu ; Li-Ling Hung ; Chia-Yin Ko, " Secure Session Key Generation Method for LoRaWAN Servers", Secure Communication for the Next Generation 5G and IoT Networks, IEEE Access, Volume: 8, pp 54631 - 54640, 2020.

[26] K-L. Tsai , F-Y. Leu , I. You , S-W. Chang , S-J. Hu , H. Park , "Low-Power AES Data Encryption Architecture for a LoRaWAN", Security and Privacy in Emerging Decentralized Communication Environments, IEEE Access, Volume: 7 , pp 146348 - 146357, 2019.

[27] Q. ZHOU, K. Zheng , L. Hou , J. Xing , R. Xu, ”Design and Implementation of Open LoRa for IoT”, IEEE Access Volume: 7 , pp 100649 - 100657, 2019.

[28] J. M.-Lee, ”Identity-based signcryption”, Cryptology ePrint Archive, Report 2002/098, 2002.

[29] W. Luo, W. Han, ”DDOS Defense Strategy in Software Definition Networks”, In Proceedings of International Conference on Computer Network, Electronic and Automation (ICCNEA), Xi’an, China, September 2019.

[30] N. Bozic, G. Pujolle, S. Secci, ”A Tutorial on Blockchain and Applications to Secure Network Control-Planes”, In Proceedings of Smart Cloud Networks & Systems (SCNS), Dubai, United Arab Emirates, December 2016.

[31] B. Djellali, K. Belarbi, A. Chouarfia, P. Lorenz, ”User authentication scheme preserving anonymity for ubiquitous devices”, Security and communication networks, Volume 8, Issue 17, pp 3131-3141, November 2015.

[32] G. Tian, Z. Duan, T. Baumeister and Y. Dong, ”A Traceback Attack on Freenet”, IEEE Transactions on Dependable and Secure Computing, Volume: 14, Issue: 3, pp 294 - 307, June 2017.

[33] S. Buchegger and J-Y.L. Boudec, ”Performance analysis of the CONFIDANT protocol”, In Proceedings of the 3rd ACM Symposium on Mobile Ad Hoc Networking and Computing, pp. 226-236, Lausanne, Switzerland, June 2002.

[34] H. M. Deng, W. Li, D. P. Agrawal, ”Routing Security in Wireless Ad Hoc Networks”, IEEE Communications Magazine, Volume 40, Issue 10, pp70-75 , November 2002.

Author Biographies

Sana BENZARTI is currently a phd student at the Institute of Computer Sciences and Communication Techniques (ISITCOM) working on the Internet of Things security. She received her Engineering Diploma in 2013 from National Institute of Applied Sciences and Technologies (INSAT), University of Carthage.

Dr Bayrem TRIKI received the Ph.D. in Telecommunications from the Engineering School of Communications (Sup’Com), University of Carthage (Tunisia) in 2013. He is currently an Assistant Professor in Institute of Computer Sciences and Communication Techniques (ISITCOM) at the University of Sousse. Dr Triki conducting research activities in digital investigation of security incidents, intrusion detection systems, Internet of Things security and privacy issues, Cloud computing and network attacks.

Pr Ouajdi KORBAA obtained in 1995 the Engineering Diploma from the Ecole Centrale de Lille (France), and in the same year, the Master degree in Production Engineering and Computer Sciences from the University of Lille. He is Ph.D. in Production Management, Automatic Control and Computer Sciences of the University of Sciences and Technologies of Lille (France) since 1998. He also obtained, from the same university, the ”Habilitation to Supervise Researrches” degree in Computer Sciences in 2003. He is full Professor in the University of Sousse. He published around 140 research papers on scheduling, performance evaluation, discrete optimization, design, and monitoring.