Secure proxy MIPv6-based mobility solution for LPWAN

Hassan Jradi, Fabienne Nouvel, Abed Ellatif Samhat, Jean-Christophe Prévotet, Mohamad Mroue

Secure Proxy MIPv6-Based Mobility Solution for LPWAN

Hassan Jradi[1,2], Fabienne Nouvel[1], Abed Ellatif Samhat[2], Jean-Christophe Prévotet[1], and Mohamad Mroue[2]

[1]Institut National des Sciences Appliquées de Rennes — IETR, Rennes, France.
[2]Lebanese University — Scientific Research Center in Engineering, Hadath, Lebanon.
[1]Email: firstname.lastname@insa-rennes.fr
[2]Email: samhat@ul.edu.lb, mohamad.mroue@ul.edu.lb

Abstract

With the advancement and the wide deployment of the Internet of Things (IoT), Low Power Wide Area Network (LPWAN) technologies will respond to applications requiring low power and long range features. In this context, mobility is an additional requirement needed by several applications including supply chain monitoring and health-care supervision. Proxy Mobile IPv6 (PMIPv6) as an extension of Internet Protocol (IP) is used in the LPWAN protocol stack since it provides mobility management. But PMIPv6 does not provide secure access for mobile nodes joining to the network. In this paper, we propose a new mobility solution for LPWAN based on PMIPv6 and we provide a new authentication mechanism to achieve secure access to the network. Thereafter, we evaluate the performance of the proposed solution by simulation using the Network Simulator 3 (NS-3) and by theoretical analysis. Moreover, the security of the proposed authentication mechanism is assessed using an informal security analysis as well as using the AVISPA validation tool. Finally, we compare the performance of our solution with other proposed solutions where we show the improvements made by our solution with respect to several parameters and requirements.

Keywords – IoT, LPWAN, Mobility, PMIPv6, Security, Authentication.

1 INTRODUCTION

The Internet of Things (IoT) is the global network of interconnected devices serving various functions by which people have the ability to monitor, make decisions and control devices placed in faraway locations [1]. The primary considerations for IoT deployment are network hierarchy, link management and association security. To attain these considerations, several IoT communication technologies are invented and can be categorized according to the link characteristics. The three major categories for IoT technologies are: Low Rate Wireless Personal Area Network (LR-WPAN) [2] like ZigBee [3] and Bluetooth [4], Low Power Wide Area Network (LPWAN) [5] like LoRaWAN [6] and Sigfox [7], cellular-based technologies like the Fifth Generation (5G) technology standard for broadband cellular networks [8]. However, LPWAN technologies are suitable for applications that need long range and low data rate communications [9].

Several applications based on LPWAN such as supply chain monitoring, healthcare supervision and transportation system tracking require mobility and dynamic change of location [10, 11]. In this context, several existing proposals based on IPv6 adopt Mobile IPv6 (MIPv6) as a solution to address the mobility in LPWAN. This is convenient with the adoption of IPv6 over constrained LPWAN networks as stated in the IETF LPWAN workgroup [12]. How-

ever, adding Internet Protocol (IP) to LPWAN protocol stack leads to overhead and additional signaling. Thus, suitable countermeasures should be used to overcome these drawbacks. For that, several compression mechanisms are proposed to compress the IPv6 headers such as 6LoWPAN [13], Robust Header Compression (ROHC) [14] and Static Context Header Compression (SCHC) [15].

Furthermore, Proxy Mobile IPv6 (PMIPv6) [16] is one of IPv6 extensions providing network-based mobility since the Mobile Node (MN) does not contribute to the signaling procedure, where a new network entity is added to perform the mobility update procedure on behalf of the MN.

In addition to the part related to the network hierarchy and the link management, security is an imperative requirement to ensure secure access to the network, and secure communication with the network and the corresponding node. The establishment of a secure connection necessitates a secure authentication mechanism that should take into consideration the LPWAN limitations such as the payload length, the number of messages sent per day, the memory capacity, and the processing power. Secure access can be provided at link-layer by the underlying technology like the join procedure in LoRaWAN [17], or at network layer using a security protocol like IPsec [18], or at transport and application layers.

In this context, the main contributions of this paper are the following:

- We propose a new mobility solution for LPWAN based on PMIPv6 and using SCHC compression algorithm, with a light authentication mechanism for secure access.
- We evaluate the solution performance by theoretical analysis and we validate it by simulation using Network Simulator 3 (NS-3).
- We evaluate the solution security according to common and mobility-related security issues as well as using AVISPA validation tool.
- We compare our solution with several existing solutions in terms of performance and security, in addition to other parameters.

The rest of this paper is organized as follows. In Section 2, we define mobility and its different types, then we present several existing works that aim to provide mobility in LPWANs. In Section 3, we explain PMIPv6 mobility management protocol along with MN attachment and handoff process, then we focus on the protocol security. In Section 4, we present our mobility management solution in LPWAN including an authentication mechanism to provide secure access, focusing also on network architecture and different mobility scenarios. In Section 5, we present the solution implementation using NS-3, then we evaluate the performance and the security of our solution. In Section 6, we compare our solution to several proposed solutions, and Section 7 concludes the paper.

2 BACKGROUND AND RELATED WORKS

In this section, we define mobility and the types of mobility, then we show existing solutions that improve mobility in LPWAN. As a definition of mobility, it is the movement of an MN (which is the End Device (ED) in LPWAN) that causes the release of the established radio link with the current point of attachment, and the establishment of a new radio link with the next point of attachment. Thus the MN will regain access to the previously established session with the corresponding node. To achieve decent mobility management with pre-qualified requirements, suitable mobility management protocols should be adapted, developed and deployed. We use also the term "handoff" which reflects the part of mobility-related to the switching from the previous to the new radio link. In other words, mobility management can be seen as a combination of handoff management [19] and location management [20], where the latter is related to location tracking and paging. Based on mobility requirements and handoff scenarios, several types of mobility could be identified. Therefore, we define the types of mobility based on the types of handoff:

- **Homogeneous Intra-Domain:** when the MN mo- ves from the coverage of a point of attachment to another that belongs to the **same operator** and has the **same link-layer technology**.

- **Heterogeneous Intra-Domain:** when the MN mo- ves from the coverage of a point of attachment to another that belongs to the **same operator** and has **different link-layer technology**.

- **Homogeneous Inter-Domain:** when the MN mo- ves from the coverage of a point of attachment to another that belongs to **different operator** and has the **same link-layer technology**.

- **Heterogeneous Inter-Domain:** when the MN mo- ves from the coverage of a point of attachment to another that belongs to **different operator** and has **different link-layer technology**.

An important requirement in particular mobility scenarios is session continuity, where the mobility solution should ensure the continuity of the established session between the MN and the Correspondent Node (CN). In addition, a minimum handoff delay should be respected to consider the cases of MNs with high mobility rates and velocities. Furthermore, LPWAN technologies are considered independent technologies, since there is no framework aggregating the different technologies to work together, which complicates the link-layer handoff. In the literature, several solutions are proposed to remedy the lack of mobility feature in LPWANs, each trying to achieve a certain type of mobility. Right away, we briefly present several LPWAN mobility solutions.

Distribution servers-based mobility solution for LoR- aWAN is proposed by Lamberg-Liszkay and Lisauskas [21]. The authors propose to add a new entity called the distribution server in each LoRaWAN network which acts as a broker entity to achieve a distributed mobility system instead of the centralized mobility system relying on the join server in LoRaWAN [22]. Each two distribution servers collaborate together and have four services used to manage device mobility: registration service, database service, message distribution service, and information exchange service. The registration service is used to register either new devices which the distribution server will handle their mobility management later, or new distribution servers to collaborate with them. Information related to these devices or distribution servers are conserved in the database using the database service. The message distribution service is responsible for packet routing based on the network identifier field included in the packet. This field is processed by the service to check if the ultimate destination belongs to a distribution server having an active collaboration with the help of database service. The information service is used to regularly update collaboration information between distribution servers. This solution contributes mainly to homogeneous inter-domain handoff for LoRaWAN technology, but the limitation is in the peer-to-peer communication approach between distribution servers, as there is no routing algorithm for the collaboration between multiple distribution servers at the same time which adds a lot of redundant traffic.

In another work carried out by Durand et al. [23], the authors propose the use of blockchain and smart contracts to attain a blockchain-based join procedure in LoRaWAN. In the smart contract, they define two functions. The first is the registration function executed by the Network Server (NS) which binds the device JoinEUI with its home NS address, thereafter adds this binding to the blockchain using the smart contract. The second is the address getter function executed by any NS that needs to know the home NS address of a device trying to connect through its GWs. Thus after receiving a join request from a device containing a JoinEUI, the visited NS executes this smart contract function and obtains the home network address of the device, and if a collaboration agreement exists between the two servers, the join procedure is completed as defined in LoRaWAN specifications [17]. This solution contributes to homogeneous inter-domain handoff for LoRaWAN technology, but the disadvantage is in the time needed to verify transactions and its deployment has a cost since transaction validations are not free.

The omnipresence of IP in typical network architectures and the features provided by IP networks encourage Ayoub et al. [24] to integrate IP in LoRaWAN. However, an overhead of 40 bytes is caused by the use of IPv6. Thus, a suitable variant of a compression algorithm called SCHC [15] is used to overcome this drawback. The authors propose an optimization of SCHC called Mobile SCHC (MSCHC) which is integrated with the mobility feature provided

by Mobile IPv6 (MIPv6). This solution comes with the benefit of integrating IPv6 in LPWAN, hence the solution provides a heterogeneous inter-domain handoff for LoRaWAN and NB-IoT technologies. The challenge in this solution is the network discovery since the used technologies are different.

In order to improve the previous solution, the authors Ayoub et al. [25] propose a media-independent solution providing seamless handoff and session continuity by proactively initiating handoff independently of the used link-layer technology. This solution is based on IEEE 802.21 framework called the Media Independent Handoff (MIH) framework [26]. The exchanges expected to take place between the device, the home network, the visited network and the mobility management server are initiated by either the device or the network according to the used configuration. As key features, this solution leverages the three features of MIPv6 networks with low overhead due to the use of MSCHC recalled Dynamic Context Header Compression (DCHC), and the session continuity provided by the MIH.

Although the mentioned solutions provide different capabilities and application requirements, they did not focus on the security side. The last two mobility solutions [24, 25] are based on MIPv6. However, several IPv6-based mobility protocols exist like Proxy MIPv6 [16], Fast MIPv6 [27], Hierarchical MIPv6 [28], etc. Nonetheless, PMIPv6 is more suitable for IoT networks since it provides network-based mobility and low power consumption for MNs [29]. In the next section, we provide an overview of how PMIPv6 protocol assists in providing light mobility for MN and the security in PMIPv6.

3 PROXY MOBILE IPV6

3.1 Protocol Overview

Proxy Mobile IPv6 (PMIPv6) [16] is a network-based mobility management protocol. PMIPv6 belongs to network based category [30] because new entities responsible for the tracking of MN movement and initiating signaling procedures on the behalf of MN are added to the network, therefore network modification is needed to support PMIPv6. The newly added entities are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). PMIPv6 is also considered a local mobility management protocol since it is designed to manage device mobility within the same domain.

MAG is the entity responsible for tracking the MN movements and initiating the binding update procedure on its behalf. LMA is the entity responsible for maintaining MN accessibility to the CN and operates with MAG to perform the handoff and binding update procedure.

Two fundamental procedures are defined in PMIPv6, the first is the MN attachment where it attaches for the first time to the PMIPv6 domain controlled by the LMA through one of the MAGs. The second is the MN handoff when it moves between different MAGs connected to the same LMA, i.e., the same PMIPv6 domain or network operator.

The first procedure is shown in Figure 1. After the MN attachment at the lower layer, usually link-layer like LoRaWAN and Zigbee, the MAG fetches the MN unique identifier in the PMIPv6 domain, either from information saved in its database, or by other ways for authentication. The MN sends a Router Solicitation (Rtr Sol) message to MAG in order to configure its network layer interface, then the MAG sends a Proxy Binding Update (PBU) message to LMA which replies with Proxy Binding Acknowledgement (PBA) to MAG including the MN Home Network Prefix (MN-HNP) used by the MN to configure its network layer interface, and LMA creates a bidirectional tunnel with the MAG used for packet routing and a BCE for this MN. Finally, the MAG replies with Router Advertisement (Rtr Adv) message to the MN containing the MN-HNP.

The second procedure is shown in Figure 2. When the previous MAG detects the MN detachment at the lower layer, it sends a DeRegistration PBU (DeReg PBU) message to LMA which accepts the deregistration after a certain duration and sends back PBA to the previous MAG to delete the established tunnel. When the MN attaches to the next MAG, the latter performs the first procedure again and finally sends the Rtr Adv message. This message is detected by the MN which finds the same HNP in the message,

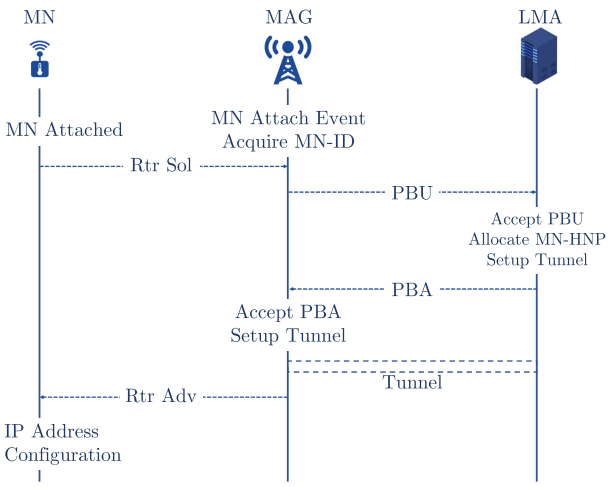

Figure 1: Mobile node attachment to PMIPv6 domain.

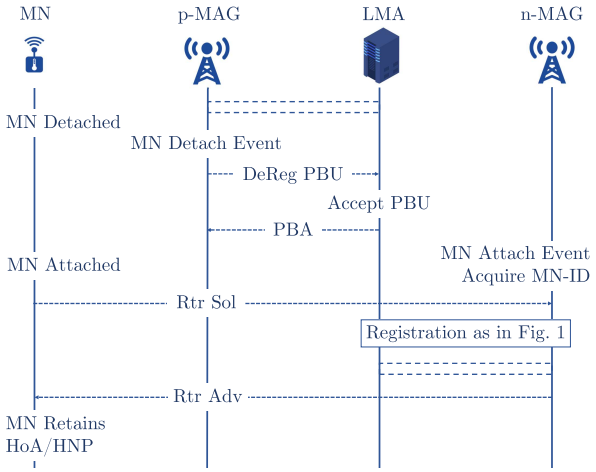

Figure 2: Mobile node handoff from previous MAG to next MAG in the same PMIPv6 domain.

therefore it retains the same network layer address. In other words, this procedure is completely transparent to the MN network layer interface.

Regarding the packet routing, any packet sent by the MN to the CN is intercepted by the MAG which encapsulates it in another packet having the MAG address as the tunnel source point address (also called the Proxy Care-of Address) and the LMA address as the tunnel endpoint address. Upon packet arriving at LMA, it decapsulates the packet and sends it to the CN. The inverse applies for packets sent by the CN to the MN.

3.2 Protocol Security

There are two essential security aspects to review in PMIPv6. First, we have to consider the security of signaling messages exchanged during MN attachment and MN handoff between the MAG and LMA. According to PMIPv6 specification, the security of signaling messages exchanged is ensured using IPsec [31] between MAG and LMA. In this way, signaling message confidentiality, integrity and authenticity are ensured.

Second, the MN identification using the MN identifier is a difficult challenge. When the MN attaches to the point of attachment, the MAG should be able to obtain the MN identifier in order to check its authenticity and its right to access network services. The specifications for how MAG achieves this truth are not given in PMIPv6 which assumes to have a pre-established mutual trust between MN and MAG. Therefore, we focus on this part of authentication required to provide secure access to PMIPv6 domain.

Several security solutions are proposed to solve this problem. A little far from LPWAN, an important work integrating the power of PMIPv6 with MIH is done by Sharma et al. [32]. The authors also redress the problem of secure access to PMIPv6 domain by the proposition of an authentication mechanism. This solution is designed to operate for IoT devices in 5G networks. Another work achieved by Shin et al. [33] proposes a route optimization for PMIPv6 and an authentication mechanism for smart home IoT networks. Chuang and Lee [34] tries also to provide secure access along with the integration of Fast MIPv6 to provide low handoff latency and resolve the packet loss problem. However, these solutions do not fit LPWAN requirements, thus we propose a new mobility solution with an appropriate authentication mechanism.

4 PROPOSED SOLUTION

In this section, we present our proposed mobility solution for LPWANs. In Subsection 4.1, we cite the main requirements taken into consideration to develop the mobility solution. In Subsection 4.2, we show the MN protocol stack. In Subsection 4.3, we show the evolved network architecture. In Subsection 4.4, we show how the solution reacts in different cases of mobility. The authentication scheme that aims to ensure legal MN access to the PMIPv6 domain is presented in Subsection 4.5. In Subsection 4.6, we show a complete mobility scenario to provide a better understanding of entities' collaboration.

4.1 Requirements

In order to propose an efficient mobility solution, several requirements should be taken into consideration as shown below:

- ✓ *Minimum signaling:* the number of signaling messages exchanged to perform the handoff procedure in the mobility solution should be minimized as much as possible, since the increase in the number of signaling messages leads to an increase in the overall handoff latency and power consumption.
- ✓ *Minimum overhead:* which is the header added by signaling messages to perform the handoff procedure. This overhead should be minimized since several LPWAN technologies have limitations in the payload length and the number of messages sent per day.
- ✓ *Operational with current protocols:* the proposed mobility solution should be able to work smoothly with current protocols at different stack layers.
- ✓ *Global accessibility:* the proposed mobility solution should ensure MN accessibility by the CN wherever the device is located.
- ✓ *Energy-efficient communication:* the proposed mobility solution should give particular care to the power consumption of MNs since we deal with resource-limited devices in terms of battery lifetime, bandwidth efficiency and embedded resources.
- ✓ *Secure access and authentication:* the authentication of an MN trying to perform the handoff procedure should be properly secured since the violation of the authentication mechanism leads to severe security issues.

4.2 Protocol Stack

The protocol stack implemented in the MN is represented in Figure 3. The layers presented in the figure are discussed below.

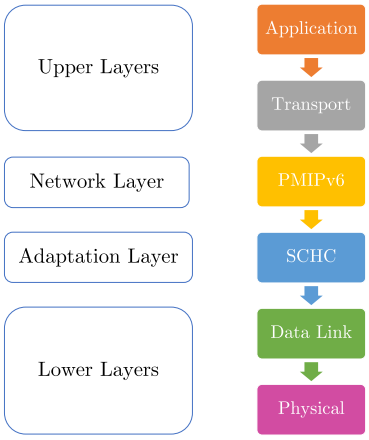

Figure 3: Mobile node protocol stack.

4.2.1 Upper Layers

These layers contain the application and transport layers used to exchange the intended data with the CN or the Application Server (AS). These layers are dependent on the deployment purpose of the MN. Thus they are user-specific and independent of the rest of the layers needed to realize the mobility solution described below.

4.2.2 Network Layer

In this layer, we propose to use IPv6 for packet routing, and PMIPv6 to support node mobility when the

MN carries out intra-domain mobility. We focus on LoRaWAN and NB-IoT technologies since they are the two leading technologies in LPWAN [35].

As we deal with LPWAN, LoRaWAN is considered as a link-layer technology, i.e., the protocol stack describing it contains physical, data link, and application layers. Thus adding a network layer for LoRaWAN is achieved by adding IPv6 between data link and application layers. Adding PMIPv6 to LoRaWAN requires adding the required infrastructure entities which are the LMA and the MAG.

For NB-IoT, the network layer is formerly existing in the protocol stack and is initiated by user or control plane network attachment mode. The Serving Gateway (S-GW) in the user plane mode or the Mobility Management Entity (MME) in the control plane mode take the role of the MAG, and the Packet Data Network Gateway (PDN-GW) takes the role of the LMA as described in [36].

The exact details of the adapted network architecture are explained in Subsection 4.3.

4.2.3 Adaptation Layer

This layer is added to overcome the drawbacks of adding IPv6 for LPWANs. As discussed before, LoRaWAN has payload length constraints, and adding IPv6 leads to an overhead of 40 bytes per packet. Therefore, we propose to add this adaptation layer located between the network and the data link-layer for LoRaWAN in order to perform the necessary compression/decompression of IPv6 packets. This one is carefully examined in other works as in [37] and [38].

For NB-IoT, the protocol stack already contains an adaptation layer named the Protocol Data Convergence Protocol (PDCP), which contains the compression/de- compression mechanisms along with the ciphering/de- ciphering mechanisms. For both technologies, we propose SCHC [12] to be the packet compression mechanism.

4.2.4 Lower layers

At this level, we find the data link and the physical layers of LPWAN technologies. Figure 4 illustrates the proposed protocol stack over LoRaWAN and NB-IoT technologies.

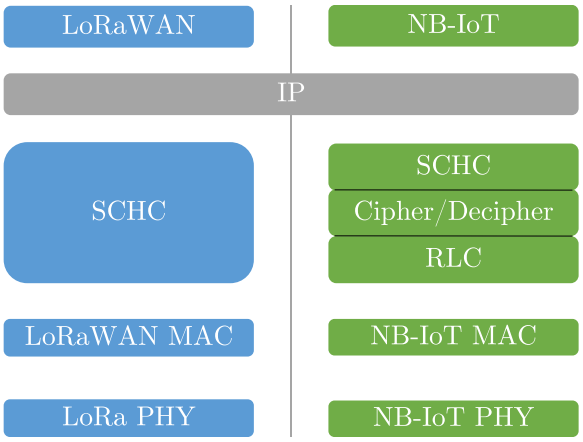

Figure 4: Protocol stack for LoRaWAN and NB-IoT technologies.

4.3 Network Architecture

4.3.1 Evolved LoRaWAN Architecture

In LoRaWAN, the main entities are the Gateway (GW), the Network Server (NS) and the Join Server (JS). In PMIPv6, the main entities are the MAG and the LMA. In the following, we propose a network architecture to integrate PMIPv6 with LoRaWAN.

The proposed network architecture is shown in Figure 5. Since NS is the anchor point of LoRaWAN devices, where any data to be sent/received by a device should pass through the NS, we propose to place the NS and the PMIPv6 LMA at the same functional entity.

The challenge is in the deployment of MAG in LoRaWAN, as we should take into consideration that uplink data sent by the device to the NS are received and forwarded by one or more GW at the same time, whereas, downlink data sent by the NS to the device are routed through only one GW, which has the best channel conditions. Besides, the device should authenticate itself each time it attaches to a MAG which adds a lot of unnecessary signaling if the MAG is placed with each GW. Therefore, placing the MAG

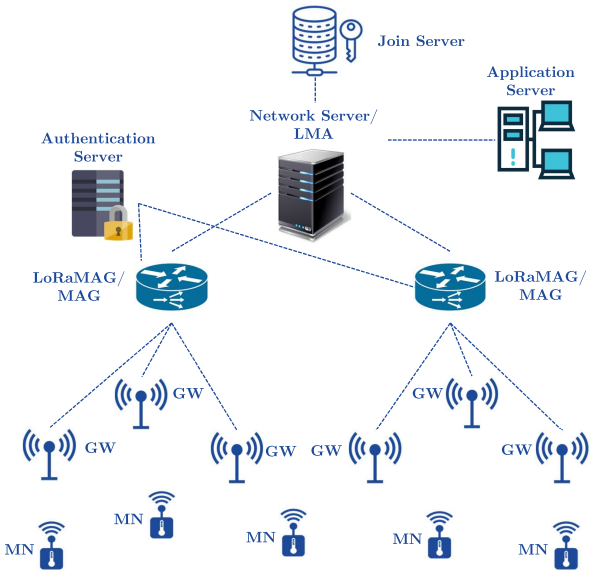

Figure 5: Evolved LoRaWAN network architecture.

with the GW is not efficient.

For the aforementioned reasons, we propose to add a new entity called LoRa Mobile Access Gateway (LoRaMAG) topologically placed between the NS and the GWs. LoRaMAG has the MAG functions, and responsible for the communication between the NS and a predetermined set of GWs. Consequently, an MN attached to LoRaWAN network through a set of GWs can still move and send data without any additional mobility mechanisms. At the same time, this will reduce the NS processing to select the best downlink path since downlink data should be simply tunneled to LoRaMAG. The exact specifications of how to select the GW sets are beyond the scope of this work.

In addition, a new entity called the Authentication Server (AuS) is added to the LoRaWAN network. The role of AuS is to authenticate the MN with the MAG in some mobility cases as described in Subsection 4.4. Authentication is achieved by the execution of the authentication mechanism described in Subsection 4.5.

In case of mobility between different LoRaMAGs, the previous and next LoRaMAGs should execute the PMI- Pv6 MN handoff procedure described in Section 3, to update the NS Binding Cache Entry (BCE). This leads to the redirection of the new data through the new tunnel established with the next LoRaMAG and to delete the old tunnel with the previous LoRaMAG. Regarding the MN, this process is wholly transparent and does not need any new mobility mechanisms.

4.3.2 NB-IoT Architecture

In NB-IoT, the main entities involved to establish an Evolved Packet System (EPS) bearer with PDN-GW are the eNB, S-GW, MME and the Home Subscriber Server (HSS). For the operation of NB-IoT with PMIP- v6, the architecture enhancements for non-3GPP accesses release 16 [36] details the integration of NB-IoT with PMIPv6. In the specifications, S-GW plays the role of MAG of PMIPv6 domain, PDN-GW plays the role of the LMA, and the MME in conjunction with HSS contributes to the MN authentication. Network architecture for NB-IoT is shown in Figure 6.

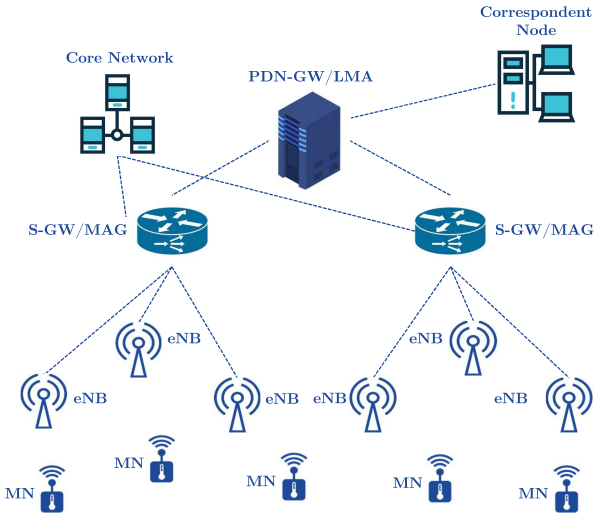

Figure 6: NB-IoT network architecture.

We note that the proposed architecture has a little impact on the NB-IoT architecture, and much more

impact on LoRaWAN architecture.

4.4 Mobility Scenarios

According to the handoff type, several mobility scenarios can happen as summarized in Table 1. In Table 1, we focus on 5 parameters: PBU, authentication, link-layer identifier, IPv6 address and SCHC context. In all cases, we consider the mobility inside the same operator coverage, i.e., intra-domain mobility. However, the use of PMIPv6 adds a level to the network hierarchy. Thus, two new types of handoff can happen, intra-MAG and inter-MAG handoff, where the handoff is between the same or different MAG entities.

Regarding the PBU message, it is not sent in homogeneous intra-MAG handoff, since the link-layer identifier, the IPv6 address and the SCHC context do not change, thus there is no need for any information update in the MN BCE stored in the LMA. However, inter-MAG handoff needs PBU since there is a handoff between two MAGs, and heterogeneous intra-MAG handoff needs a PBU to update the MN BCE where the link-layer technology and identifier are changed.

Regarding the authentication with the MAG, it is not needed in intra-MAG handoff, since the handoff is between several GW or eNB coverages connected to the same MAG. In addition, authentication is not needed in case of homogeneous inter-MAG handoff since the link-layer identifier of the MN is conserved and the MAG can verify its identity using the technology-specific security protocol. However, in case of heterogeneous inter-MAG handoff, since both link-layer identifier and MAG are changed, it is not possible to directly identify the MN and authentication is needed.

Regarding the link-layer identifier, it does not change in homogeneous handoff since the used technology does not change, and the handoff is confined inside the same operator coverage. However, heterogeneous handoff will lead necessarily to the change in the link-layer identifier as it is assigned by the underlying technology.

Regarding the compression/decompression context of the SCHC algorithm [12], the version, differential service, flow label, next header, hop limit and destination address fields are usually static. In addition, the use of PMIPv6 makes the source address quasi-static, except in some cases when the MN obtains a new address, thus the context will be altered slightly.

4.5 Proposed Authentication Scheme for LoRaWAN

The proposed authentication scheme is used to solve the authentication problem between the MN and LoRaMAG described in Section 3 in case of inter-MAG mobility. This scheme belongs to hash-based authentication schemes, since we use a hash function to achieve the authentication, without the need for encryption/de- cryption, public/private keys, certificates and signatures.

In the first place, AuS holds two secret keys X and Y, and a database containing records that contain:

- ID_i : identifier of MN_i.
- n_i : attachment try.
- X_i : key 'X_i' of MN_i.
- Y_i : key 'Y_i' of MN_i.

This scheme consists of two phases: the registration phase executed at the time of device deployment, and the authentication phase executed when the device performs the handoff procedure and needs to authenticate with the next LoRaMAG.

4.5.1 Registration Phase

During this phase, the MN associated with K LPWAN technologies generates its $ID_i = H(\ \|\ _{j=1}^{K}\ ID_{Tech_j})$. For example, if MN_i uses only LoRaWAN and NB-IoT, its identifier will be $ID_i = H(DevEUI \parallel IMSI)$.

Therefore, AuS generates two secret keys and preshares them securely with the MN. These two keys are:

- $X_i = H(H(X) \oplus ID_i)$.
- $Y_i = H(H(Y) \oplus ID_i)$.

Table 1: Mobility scenarios.

#	Handoff type	MAG	PBU	Authentication	L2 ID	IPv6 Address	SCHC Context
1	Homogeneous	Intra	✗	✗	Invariable	Invariable	
2		Inter	✓	✗		May vary	
3	Heterogeneous	Intra	✓	✗	Variable	Invariable	
4		Inter	✓	✓		May vary	

4.5.2 Authentication Phase

The authentication exchanges between the MN, the LoRaMAG and the AuS are shown in Figure 7.

(1) MN_i gets the current timestamp T_1, calculates the hash key of the current attachment try $K_i = H(X_i)$
$\oplus H(Y_i)$ and the message integrity code $MIC_1 = H(ID_i \parallel T_1 \parallel K_i)$, then sends an authentication request to AuS containing $M_1 = \{ID_i \parallel T_1 \parallel MIC_1\}$ through LoRaMAG.

(2) LoRaMAG receives the authentication request then forwards it to AuS.

(3) AuS checks the timestamp T_1 if it is within the acceptable time range. Based on the ID_i, AuS gets X_i, Y_i from the database then calculates the hash key $K_i = H(X_i) \oplus H(Y_i)$ and $MIC'_1 = H(ID_i \parallel T_1$
$\parallel K_i)$. If $MIC'_1 = MIC_1$, the MN message is authenticated by the AuS. The AuS generates a random number V and sends it over the secure link to the LoRaMAG along with ID_i.

(4) AuS calculates $W = V \oplus H(K_i)$ then AuS gets the current timestamp T_2, calculates
$MIC_2 = H(ID_i \parallel T_2 \parallel W \parallel K_i)$ and sends the request response for the MN containing $M_2 = \{ID_i$
$\parallel T_2 \parallel W \parallel MIC_2\}$ through LoRaMAG.

(5) LoRaMAG receives the random number V and the authentication response which is forwarded to the MN.

(6) The MN checks the timestamp T_2 if it is within the acceptable time range. Then it calculates $MIC'_2 = H(ID_i \parallel T_2 \parallel W \parallel K_i)$. If $MIC'_2 = MIC_2$, the AuS message is authenticated by the MN. After that, to get the random number V, the MN calculates $V = W \oplus H(K_i)$.

(7) LoRaMAG gets the current timestamp T_3, calculates $MIC_3 = H(ID_i \parallel T_3 \parallel V)$ and sends $M_3 = \{ID_i \parallel T_3 \parallel MIC_3\}$ to MN.

(8) The MN checks the timestamp T_3 if it is within the acceptable time range. Then it calculates $MIC'_3 = H(ID_i \parallel T_3 \parallel V)$. If $MIC'_3 = MIC_3$, LoRaMAG is authenticated by the MN.

(9) The MN gets the timestamp T_4, calculates $MIC_4 = H(ID_i \parallel T_4 \parallel V)$ and sends for LoRaMAG $M_4 = \{ID_i \parallel T_4 \parallel MIC_4\}$.

(10) LoRaMAG checks the timestamp T_4 if it is within the acceptable time range. Then LoRaMAG calculates $MIC'_4 = H(ID_i \parallel T_4 \parallel V)$. If $MIC'_4 = MIC_4$, the MN is also authenticated by LoRaMAG.

(11) The AuS updates the database record $\{ID_i, n_i \longleftarrow n_i + 1, X_i \longleftarrow H(X_i), Y_i \longleftarrow H(Y_i)\}$. At the same time, the MN updates the two memory registers containing the secret keys by saving $X_i \longleftarrow H(X_i)$, $Y_i \longleftarrow H(Y_i)$.

4.5.3 Resource Considerations

LPWANs have limitations in terms of storage, payload length, message exchange and energy consumption. These limitations mainly concern the MN. The other entities in the network do not have such limitations.

Regarding the payload length, the maximum payload length is 115 bytes for LoRaWAN (for a spreading factor = 9 and a bandwidth = 125 kHZ), and

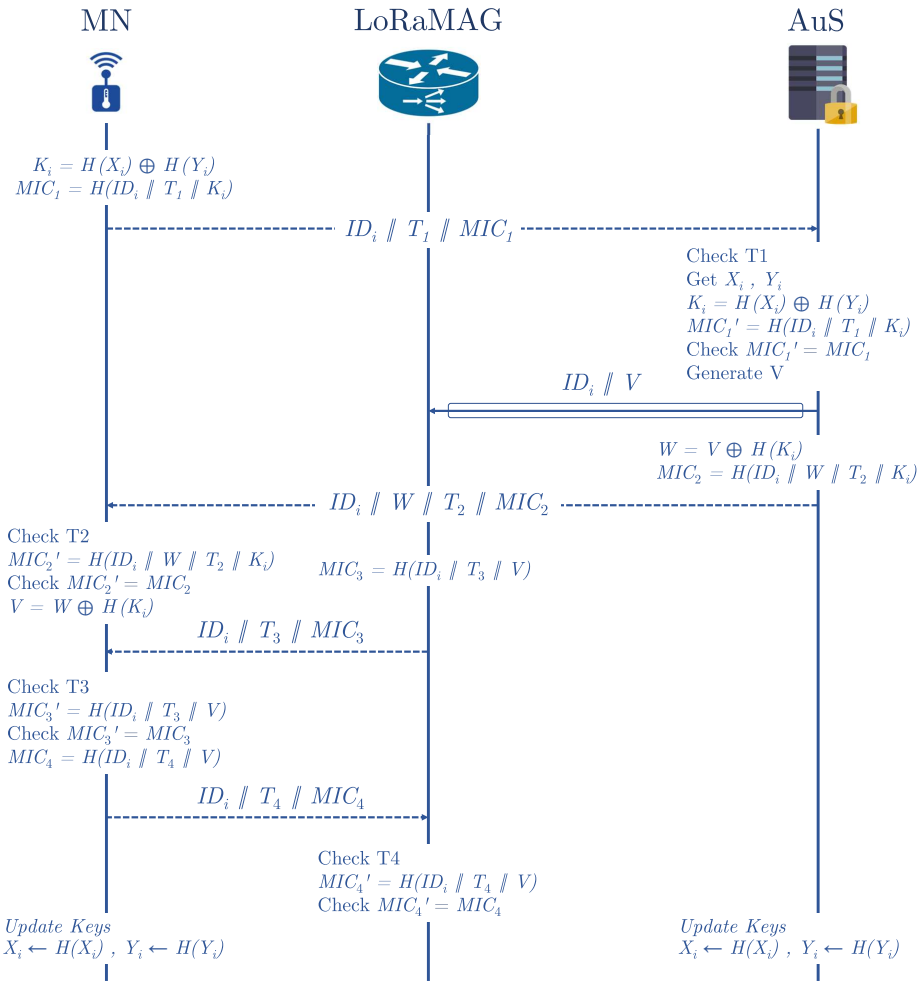

Figure 7: Message exchange during the authentication phase.

1600 bytes for NB-IoT. In the authentication scheme, the longest message is the authentication response M_2 sent by the AuS to MN, where we have ID_i, W, T_2, and MIC_2. The timestamp length (L_{TS}) should be between 7 to 13 bytes [39], we choose $L_{TS} = 10$ Bytes. We propose that ID_i length (L_{ID}) is equal to 4 Bytes. W and MIC_2 lengths are equal to hash length (L_H). Therefore, the L_H chosen should fit the following condition:

$$4 + 10 + 2 \times L_H < 115\ Bytes \Rightarrow L_H < 50\ Bytes.$$

This condition can be met easily with any kind of secure hash algorithm (SHA-1, SHA-224, SHA-256, SHA-384). SHA-1 and SHA-224 are not considered secure, thus we propose to use SHA-256 or SHA-384. Taking into account the energy consumption limitation, we propose to use SHA-256 hash algorithm, thus the hash length is $L_H = 256\ Bits = 32\ Bytes$.

Regarding the storage needed, MN has to hold its ID_i, X_i and Y_i at long term. At the runtime of the authentication scheme, the MN should hold V and K_i. Thus the needed storage is equal to L_{ID}, and two times L_H at the long term, and two times L_H at the runtime. Thus the needed storage is 132 $Bytes$.

Regarding the message exchange, the MN sends in total 2 uplink messages and receives 2 downlink messages which is appropriate for LPWAN.

4.6 NB-IoT to LoRaWAN Mobility Scenario

In Figure 8, we show detailed message exchanges for an MN performing heterogeneous inter-MAG mobility scenario, i.e., moving from NB-IoT eNB to LoRaWAN GW connected to different MAGs. All these MAGs are connected to the same LMA or operator.

The PMIPv6 domain consists of:

- NB-IoT network containing mainly: eNBs, S-GW acting as a MAG, PDN-GW and MME.
- LoRaWAN network containing: GWs, JS, LoRaMAG and NS.
- AuS and LMA.

At the first time, the MN is under the coverage of the NB-IoT network, thus it sends an attach request and completes the attach procedure described in [36]. During this procedure, the MN is attached to PMIPv6 domain, and obtains its link-layer identity, its IPv6 address, and the compression context for SCHC algorithm used to compress the headers of IPv6 packets. If the MN sends application data to the CN, these data are encapsulated in IPv6 packets which are compressed by the SCHC algorithm. These data are sent over radio bearer to eNB which forwards them to S-GW using S1 interface. S-GW having the decompression context, decompresses the packet header and rebuilds the original IPv6 header, then S-GW tunnels data to PDN-GW. PDN-GW removes the tunnel header, then forwards the original packet to the CN.

At this level, the MN moves away from the coverage of NB-IoT network, thus S-GW will detect the detachment and send DeReg PBU to PDN-GW. At the same time, the MN tries to attach with another network, and as it is supporting LoRaWAN technology, it sends a join request to GWs which forward it to NS through LoRaMAG. After that, MN completes the LoRaWAN attachment procedure described in [17]. Right away, the MN obtains its LoRaWAN identity which is a link-layer identity. The LoRaMAG detects MN attachment, which also tries to rejoin the PMIPv6 by sending a Rtr Sol message, this needs to authenticate the MN with LoRaMAG. The authentication mechanism described in Subsection 4.5 is executed between AuS, MN and LoRaMAG. If the MN is authenticated, LoRaMAG sends PBU that updates the BCE fields in LMA (which is the NS in this case). The updated fields are the link-layer identifier, the tunnel interface identifier, the access technology type, and the timestamp value. The link local address may be updated later if the MN obtains a new address. In this way, the NS will reply with PBA to LoRaMAG, which replies with Rtr Adv to MN which in turn can retain or reconfigure its IPv6 address. The SCHC context may vary in this case if the MN changes its IPv6 address. After finishing this procedure, data can be sent from MN to LoRaMAG encapsulated and compressed in packets, which tunnels them to NS. The NS removes the tunnel headers, and finally forwards them to the CN.

5 IMPLEMENTATION AND EVALUATION

In this section, we evaluate the proposed solution based on the performance and provided security features. Performance is evaluated according to several network metrics, and verified by simulation using NS-3. Security evaluation is realized based on common attacks, mobility-related attacks, and by using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [40].

Abbreviations used in the following sections are described in Table 2.

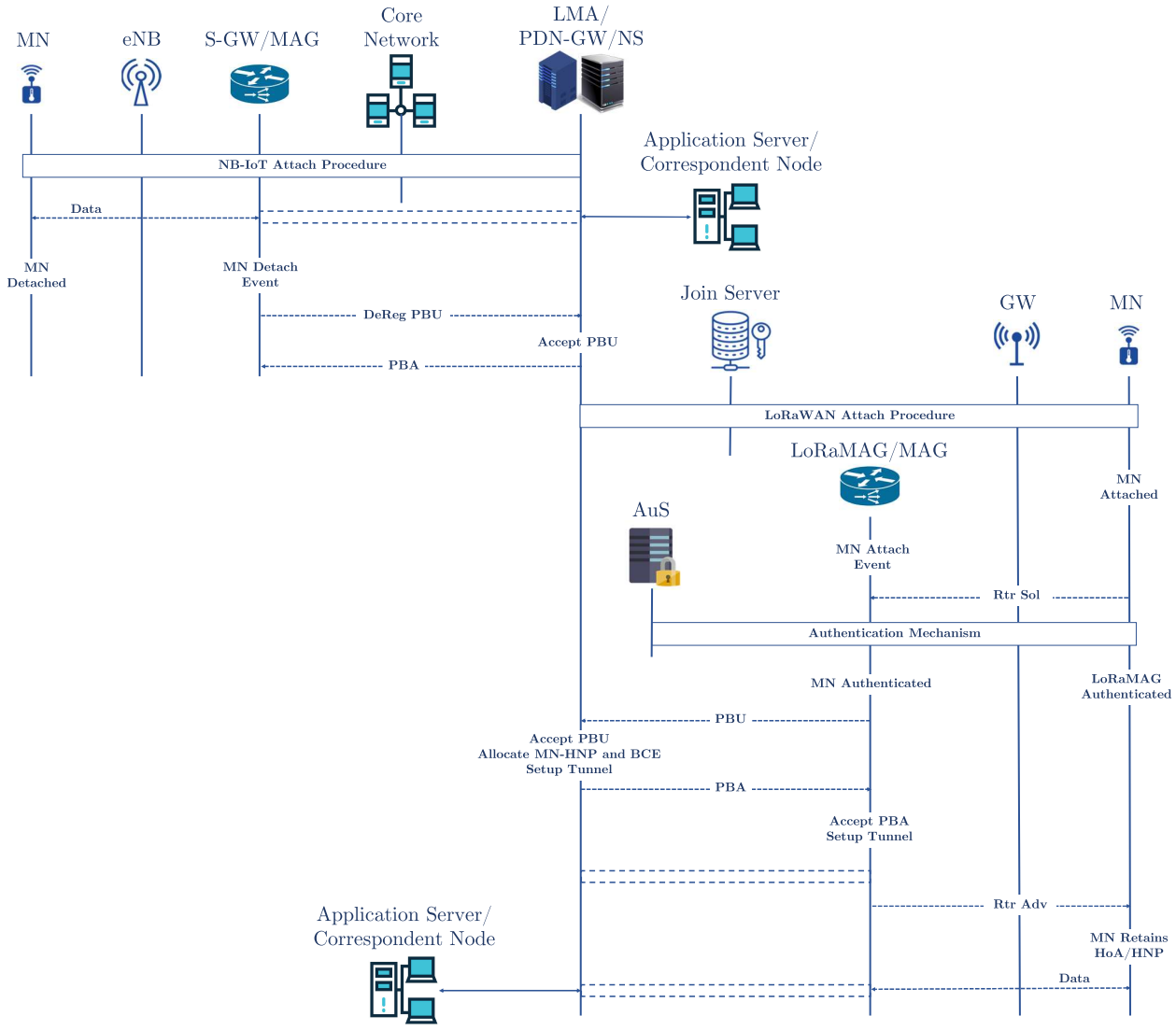

Figure 8: NB-IoT to LoRaWAN mobility scenario.

5.1 Performance Evaluation

5.1.1 Cost Analysis

We consider three main metrics to evaluate the performance of our solution: the handoff latency, the number of operations performed by the MN and the signaling overhead. Our solution consists of three main adopted methods: PMIPv6 for mobility management, SCHC for IPv6 header compression, and the authentication mechanism to provide secure access to PMIPv6 domain.

The handoff latency introduced by our solution compared to PMIPv6 solution is the authentication time T_{Auth}. The compression/decompression time is

Table 2: Abbreviations and descriptions.

Abb.	Description
L_{TS}	Timestamp length
L_H	Hash length
L_{ID}	Mobile node identity length
T_{Auth}	Time of the authentication mechanism
T_P	Processing time
T_{IP}	Time over IP link
T_R	Time over radio link
T_H	Time of one hash operation
$T_{\oplus}$	Time of one xor operation
$T_{\|\|}$	Time of one concatenation operation
R_b	Data rate over radio link
τ	Channel Delay
SO_{Auth}	Signaling overhead
N	Number of gateways per LoRaMAG
O_{L2}	Link layer overhead

included when sending/receiving data thus it does not contribute to handoff latency.

As described before, several steps are executed to complete the authentication mechanism. The overall authentication mechanism time is expressed in equation (1). T_P, expressed in equation (2), is the time needed to perform the hash, xor and concatenation operations which is highly dependent on the used processor. T_{IP} is the time needed to transmit the messages over the IP link between the MAG and the AuS and is considered to be constant as it is related to the established link. T_R is the time needed to transmit the messages over the radio link between the MN and the MAG. T_R is expressed in function of R_b in equation (3). Equation derivations are shown in appendix A.

$$T_{Auth} = T_P + T_{IP} + T_R \quad (1)$$

$$T_P = 16T_H + 4T_{\oplus} + 26T_{||} \quad (2)$$

$$T_R = \frac{2368}{R_b} + 4\tau \quad (3)$$

However, the operations performed by the MN are $9T_H$, $2T_{\oplus}$, and $13T_{||}$.

Regarding the signaling overhead added by the authentication mechanism over the network, we suppose a network with N GWs connected to LoRaMAG, and a direct link between LoRaMAG and the AuS. Uplink data in LoRaWAN are forwarded through N GWs to LoRaMAG. SO_{Auth} is the overhead added by the authentication mechanism and expressed in equation (4).

$$SO_{Auth} = (2N+7)L_{ID} + (2N+6)L_{TS} + (2N+8)L_H \quad (4)$$

In Table 3 below, we show the signaling overhead for several values of N.

Table 3: Signaling overhead for several values of N.

N	SO_{Auth} **(Bytes)**
2	528
3	620
4	712
5	804

$L_{ID} = 4\,Bytes,\ L_{TS} = 10\,Bytes,\ L_H = 32\,Bytes$

5.1.2 NS-3 Simulation

We used NS-3 to evaluate the performance by simulation. The simulation scenario consists of three entities: MN, LoRaMAG and AuS. Between the MN and the LoRaMAG, we tried to establish a LoRaWAN radio link while an IP link is set up between the LoRaMAG and the AuS. We considered direct links between LoRaMAG and connected GWs that forward uplink and downlink data. The IPv6 protocol stack is installed for all nodes in the network, thus the MN communication with the AS is IP-based. MN is trying to authenticate itself to the PMIPv6 domain using the previously described authentication mechanism.

The evaluation of the performance is dependent on several link-layer characteristics, thus we tried to assess the impact of the change in these characteristics which are the data rate (R_b) used for the radio communication between the MN and the LoRaMAG,

and the channel delay (τ) introduced when performing the authentication. The considered R_b are that used in LPWAN technologies which are in the range of 20 and 200 kbps. τ is considered between 10 and 100 ms [41]. The source codes of the implementation can be found in [42].

To be more adequate, we checked the burden of each step of the authentication mechanism. For that, we logged the time needed to execute each step by running the simulation 100 times at each R_b from 20 to 200 kbps. Then we calculated the mean of each step duration over 100 times, after that, we traced the plots of each step duration for the R_b range. The results are shown in Figure 9.

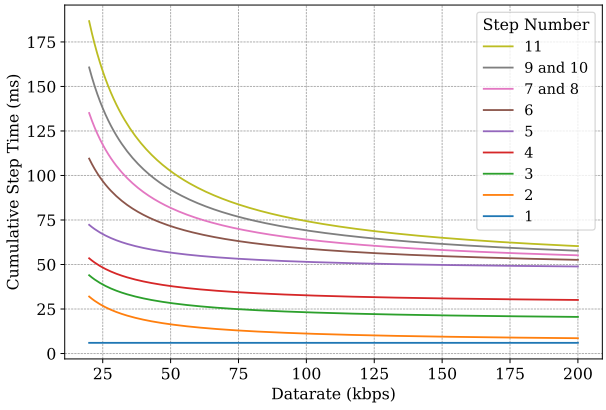

Figure 9: Duration of each authentication step for variable data rates.

From the results shown in Figure 9, we note that at low R_b, the T_{Auth} reaches 186 ms. The most occurring steps over time are steps 2 and 6 through 11 which consist the mutual authentication between MN and LoRaMAG, and between the MN and AuS, and the key update mechanism. This is due to three reasons. The first is that the MN is contributing essentially to these steps which have low processing power. The second is due to the fact that the communication is performed over radio link which is considered slower than the IP link between the LoRaMAG and the AuS. For the last, these steps require performing hashing which needs more time than forwarding messages as in other steps. At higher R_b supported by LPWANs, T_{Auth} goes below 65 ms which is considered affordable for LPWAN handoff.

To validate our simulation results with equation 1, we consider that T_{IP} and T_P are independent of the radio link. T_{IP} changes according to the IP link between LoRaMAG and AuS, and T_P is dependent on the processing power of the used processor. Therefore, we consider essentially T_R expressed in equation 3. We logged the total time over the radio link which is the time to transmit M_1, M_2, M_3 and M_4 over the radio link between MN and LoRaMAG. Thus, T_R by simulation is the sum of these logged times. Then we plot the simulation results along with equation 3 in Figure 10. The figure shows the validity of the obtained results.

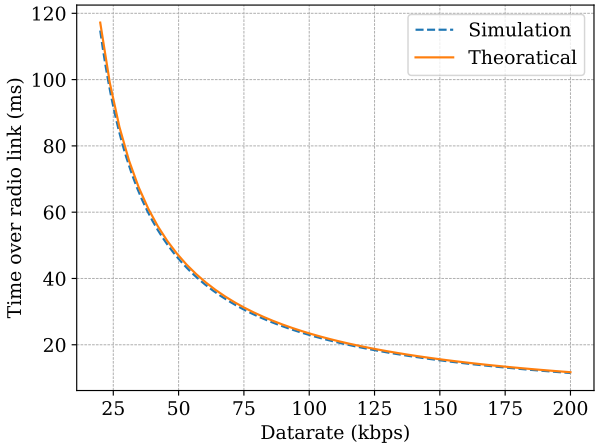

Figure 10: Results validation for radio link delay: theoretical versus simulation results for variable data rates.

Regarding the channel delay τ, we run the same simulation but we varied τ which is the delay added by the channel when transmitting/receiving data by the MN. The only considered time in this simulation is the T_{Auth} (shown in the last step in Figure 9). Thus we varied τ between 10 to 100 ms and we logged the T_{Auth} for R_b between 20 to 200 kbps, the results are shown in Figure 11. The results show that the τ is linearly added to T_{Auth} as shown in equation 1. This is because we have 4 messages exchanged over the

radio link, and from equation 3, τ is added to T_R multiplied by a factor of 4, thus adding 10 ms of τ increases the T_R by 40 ms which increases T_{Auth} by 40 ms.

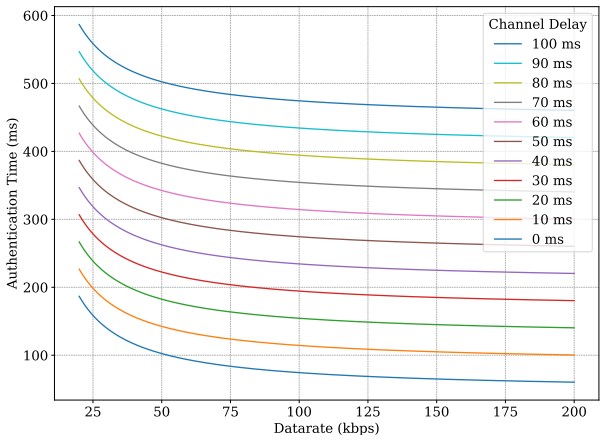

Figure 11: Authentication time for variable data rates and channel delays.

5.2 Security Evaluation

5.2.1 Security Analysis

We evaluate the security of our proposed solution according to several security issues as shown below:

1. *Confidentiality:* We distinguish between two elements of confidentiality: data confidentiality and signaling message confidentiality. For data confidentiality, we rely on the application or higher layers for data encryption, as in LoRaWAN we have the key established between the MN and the AS (or the CN) to secure the session data. In NB-IoT, the PDCP consists of a sub-layer for data ciphering/deciphering where key agreement is performed at the network attachment phase. Thus data confidentiality is provided by the used technology. For signaling message confidentiality, this is related to mobility and discussed later. In the authentication scheme, although there is no encryption mechanism used, confidential data such as the hash key and long term keys are never revealed to any entity other than the MN and the AuS, and the secret variable V is still secret in all exchanged signaling messages.

2. *Message integrity:* integrity of each message of the authentication mechanism is ensured by the added MIC field. MIC_1 and MIC_3 use the hash key K_i only known by the MN and the AuS. MIC_2 and MIC_4 use V as hash key, which is known by the LoRaMAG since AuS sends it, and known by the MN performing the xor of W with $H(K_i)$, and since K_i is only known by the MN and the AuS, no one is able to reveal the value of V. Thus, all signaling messages are integrity protected.

3. *Mutual authentication:* entities participating in the authentication mechanism authenticate each other on the MIC generated from a certain hash key. Three security associations needing mutual authentication exist: between MN and AuS, AuS and LoRaMAG, MN and LoRaMAG. The first is ensured by K_i only known to MN and AuS. The second is considered an assumption as specified in PMIPv6 specification. The third is ensured using V exchanged securely, thus when the MN checks MIC_3 and verifies that the same V sent by AuS is used by LoRaMAG, MN authenticates LoRaMAG, and the same is performed with MIC_4 to authenticate the MN by LoRaMAG.

4. *Key freshness:* at the end of each attachment try n_i, the MN and the AuS update the registers and database records containing X_i and Y_i For that, in the next attachment try $(n_i + 1)$, the hash key used K_i is quite different from the previous K_i. This protect the key generation if a LoRaMAG becomes malicious, which will be able to extract $H(K_i)$ from the received V and the listened W. LoRaMAG is not able to get K_i as hash functions are irreversible. In any case, if current K_i is revealed, next K_i cannot be deduced, since $K_i = H(X_i) \oplus H(Y_i)$ which is $\neq H(K_i) = H(H(X_i) \oplus H(Y_i))$. Thus an attacker should reveal X_i and Y_i separately, which is computationally infeasible.

5. *Replay attack:* briefly, each exchanged signaling message contains a timestamp field, thus each receiver should check the message freshness before processing it to prevent replay attacks.

6. *Denial of service:* to prevent an MN to send randomly, AuS exploits the attachment try number n_i associated with each MN identified by its ID_i. AuS can deploy an algorithm that takes as input several parameters like the MN velocity, network coverage and other parameters to calculate the mobility frequency which will be used as a threshold. If the increase of n_i, i.e., the authentication request frequency is greater than the excepted mobility frequency, AuS can consider it a malicious device and stop responding to its authentication requests. The exact specifications of the aforementioned algorithm are outside the scope of this paper.

7. *Spoofing signaling message:* signaling messages are ensured to be integrity protected by the sender and origin authenticated by the receiver. An attacker cannot send a signaling message on behalf of any entity in the network.

8. *Address squatting, spoofing, and old address control:* since the MN authenticates itself when moving in the PMIPv6 domain, the network is aware of its address using the BCE saved in the LMA. This prevents an MN to squat and spoof other node addresses, and an MN retains its old address when moving in the same domain.

9. *Context alteration:* In this solution, the SCHC compression/decompression context is saved and managed by the SCHC algorithm and considered to be tamper-resistant [12].

5.2.2 AVISPA Evaluation

To evaluate the security of our authentication scheme, we used AVISPA software which performs automated validation of internet security protocols. AVISPA contains four sub-components to derive the results regarding the implemented protocol using the High Level Protocol Specification Language (HLPSL). These four sub-components are On-the-Fly Model-Checker (OFMC), CL-based Attack Searcher (CL-AtSe), SAT-based Model -Checker (SATMC) and Tree Automata-based Protocol Analyser (TA4SP). AVISPA implementation of our authentication mechanism can be found in [43]. Running AVISPA using the implemented codes shows that our mechanism is secure as illustrated in Figure 12.

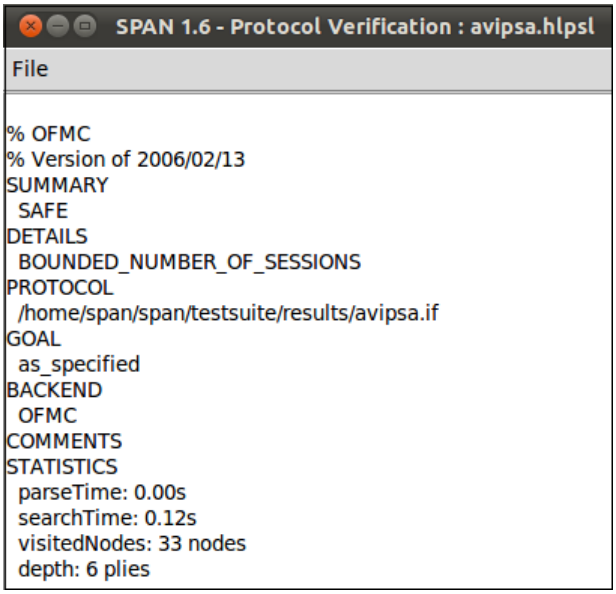

Figure 12: AVISPA validation of the authentication mechanism.

6 SOLUTIONS COMPARISON AND REQUIREMENTS FULFILMENT

In this section, we compare our mobility solution with the solutions proposed by Sharma et al. [32], Ayoub et al. [24] and Ayoub et al. [25] introduced in Section 2, in addition to the comparison with PMIPv6 [16]. Furthermore, we show how our solution fulfills the requirements presented in Section 4. The main parameters evaluated in the comparison are: adopted

methods, performance evaluation and security features.

In [32], the adopted methods was to provide secure cross-layer handover protocol for Fast PMIPv6 in conjunction with the use of MIH for heterogeneous handoff scenarios in 5G communications. While in [24], the adopted methods was to provide session continuity for device mobility using MIPv6-based communication in addition to the use of a variant of SCHC compression algorithm with route optimization to reduce latency in LPWAN technologies. The work described in [25] was the extension of [24] to provide media-independent handoff between different LPWAN technologies by introducing the adaptive layer services and the mobility management server.

Regarding the performance evaluation, the handoff latency in PMIPv6 is between 100 and 160 ms for $\tau = 10\ ms$ channel delay [32] and reaches 350 ms at $\tau = 60\ ms$ [44]. In [32], the added handoff latency is between 50 ms at low τ and reaches 120 ms at high τ which will lead to an average handoff latency between 150 and 470 ms at $R_b = 8\ Mbps$. In [24], the use of MSCHC and MIPv6 with route optimization for packets after the handoff leads to high handoff latency that reaches 7.41 seconds, but the used R_b was about 100 kbps, which is used in LPWANs. The performance is optimized in the work extension [25] to reach about 2.6 seconds using the media-independent handoff functions. However, in our solution, the added handoff latency was the authentication time which is about 110 ms at $R_b = 100\ kbps$ and decreases to about 100 ms at $R_b = 200\ kbps$ for $\tau = 10\ ms$. Thus, the overall handoff latency is the authentication time added to PMIPv6 latency which is between 200 ms and 210 ms for $\tau = 10\ ms$. Thus we achieved competitive results with [32] where the used R_b is 80 times our R_b. Moreover, signaling is affordable in our solution where it grows linearly with the number of gateways per LoRaMAG, and is comparable to [32] where it is linear to the number of hops used but more signaling messages are used.

Regarding security features provided in each solution, [24] and its extension [25] did not consider security issues that can confront their solutions. However, in [32] and in our work, we provide secure access to the PMIPv6 by the proposition of an authentication mechanism which is evaluated using Burrows–Abadi–Needham (BAN) [45] logic and AVISPA for [32], and using security analysis for common security attacks and AVISPA for our work. Table 4 summarizes the different features of each mobility solution.

Finally, our proposed solution met the requirements presented in Section 4. **Signaling is minimized** in our solution as already shown, and **overhead is reduced** using SCHC algorithm to compress the IPv6 header. Besides, our solution is **operational with current protocols** since it is based on IPv6, which ensures also **global accessibility**. **Secure access and authentication** are provided by the authentication mechanism.

7 CONCLUSION

In this paper, we proposed a new secure mobility solution for LPWANs based on PMIPv6 to manage intra-domain mobility. In addition, we used a packet compression algorithm called SCHC to overcome the drawbacks of adding IPv6 over LPWANs having strict resource constraints. Moreover, a new proposed authentication mechanism is deployed to provide secure access to PMIPv6 domain. After the proposition of the solution, we evaluated its security and performance using several tools that prove the improvements brought by our solution compared to others proposed in the literature. Improvements include the low handoff latency, the reduced signaling overhead and the compatibility with LPWAN. Future work may study the deployment of LoRaMAG and the selection of GWs set connected to each LoRaMAG. In addition, inter-domain authentication is not covered in this paper, thus future work may study the problem of inter-domain authentication based on the current scheme.

References

[1] Gianluca Aloi, Giuseppe Caliciuri, Giancarlo Fortino, Raffaele Gravina, Pasquale Pace, Wilma Russo, and Claudio Savaglio. En-

Table 4: Comparison of mobility solutions.

Solution	**Ayoub et al. [24]**	**Ayoub et al. [25]**	**Sharma et al. [32]**	**Our Solution**
Technology	LPWAN	LPWAN	4G - 5G	LPWAN
Model Type	Host Based	Host/Network Based	Network Based	Network Based
Handoff Category	Reactive	Proactive	Reactive	Reactive
Adopted Methods	MIPv6, MSCHC	MIPv6, DCHC, MIH	FPMIPv6, MIH, Secure Access	PMIPv6, SCHC, Secure Access
Additional Entities	No	Mobility Management Server	PMIPv6 Infrastructure	PMIPv6 Infrastructure, AuS
Handoff Latency	7.41 s	2.6 s	150 — 470 ms	200 — 210 ms
Operating Datarate	50 — 200 kbps	50 — 200 kbps	4 — 8 Mbps	20 — 200 kbps
Security	Default Network Security		Secure PMIPv6 Access	

abling iot interoperability through opportunistic smartphone-based mobile gateways. *Journal of Network and Computer Applications*, 81:74–84, 2017.

[2] Abdul Saboor, Adeel Mustafa, Rizwan Ahmad, Muneeb Ahmed Khan, Muhammad Haris, and Rashid Hameed. Evolution of wireless standards for health monitoring. In *2019 9th annual information technology, electromechanical engineering and microelectronics conference (IEMECON)*, pages 268–272. IEEE, 2019.

[3] C Muthu Ramya, M Shanmugaraj, and R Prabakaran. Study on zigbee technology. In *2011 3rd International Conference on Electronics Computer Technology*, volume 6, pages 297–301. IEEE, 2011.

[4] Robin Heydon and Nick Hunn. Bluetooth low energy. *CSR Presentation, Bluetooth SIG https://www. bluetooth. org/ DocMan/handlers/ DownloadDoc. ashx*, 2012.

[5] Benny Vejlgaard, Mads Lauridsen, Huan Nguyen, István Z Kovács, Preben Mogensen, and Mads Sorensen. Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. In *2017 IEEE 85th vehicular technology conference (VTC Spring)*, pages 1–5. IEEE, 2017.

[6] N Sornin and A Yegin. Lorawan backend interfaces 1.0 specification. *Lora Alliance Standard Specification*, 11, 2017.

[7] R Yugha and S Chithra. A survey on technologies and security protocols: Reference for future generation iot. *Journal of Network and Computer Applications*, page 102763, 2020.

[8] Shancang Li, Li Da Xu, and Shanshan Zhao. 5g internet of things: A survey. *Journal of Industrial Information Integration*, 10:1–9, 2018.

[9] J. Santos, T. Wauters, B. Volckaert, and F. Turck. Towards end-to-end resource provisioning in fog computing over low power wide area networks. *J. Netw. Comput. Appl.*, 175: 102915, 2021.

[10] Wael Ayoub, Abed Ellatif Samhat, Fabienne Nouvel, Mohamad Mroue, and Jean-Christophe Prévotet. Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility. *IEEE Communications Surveys & Tutorials*, 21(2):1561–1581, 2018.

[11] João Santos, Joel JPC Rodrigues, Bruno MC Silva, João Casal, Kashif Saleem, and Victor Denisov. An iot-based mobile gateway for intelligent personal assistants on mobile health environments. *Journal of Network and Computer Applications*, 71:194–204, 2016.

[12] Ana Minaburo, Laurent Toutain, Carles Gomez, Dominique Barthel, and Juan-Carlos Zúñiga. Schc: Generic framework for static context header compression and fragmentation. Technical report, RFC 8724, April, 2020.

[13] Zach Shelby and Carsten Bormann. *6LoWPAN: The wireless embedded Internet*, volume 43. John Wiley & Sons, 2011.

[14] K Sandlund, G Pelletier, and Jonsson LE. The robust header compression (rohc) framework. Technical report, RFC 5795, March, 2010.

[15] CGDBJZA Minaburo and L Toutain. Lpwan static context header compression (schc) and fragmentation for ipv6 and udp draft-ietf-lpwanipv6-static-context-hc-17, 2018.

[16] Sri Gundavelli, Kent Leung, Vijay Devarapalli, Kuntal Chowdhury, Basavaraj Patil, et al. Proxy mobile ipv6. *IETF*, 2008.

[17] Nicolas Sornin, Miguel Luis, Thomas Eirich, Thorsten Kramp, and Olivier Hersent. Lorawan specification. *LoRa alliance*, 2015.

[18] Naganand Doraswamy and Dan Harkins. *IPSec: the new security standard for the Internet, intranets, and virtual private networks*. Prentice Hall Professional, 2003.

[19] Ibrahim Al-Surmi, Mohamed Othman, and Borhanuddin Mohd Ali. Mobility management for ip-based next generation mobile networks: Review, challenge and perspective. *Journal of Network and computer Applications*, 35(1):295–315, 2012.

[20] Ashutosh Dutta and Henning Schulzrinne. *Mobility Protocols and Handover Optimization: Design, Evaluation and Application*. John Wiley & Sons, 2014.

[21] János Lamberg-Liszkay and Tadas Lisauskas. An alternative roaming model in lorawan, 2018.

[22] Hassan Jradi, Abed Ellatif Samhat, Fabienne Nouvel, Mohamad Mroue, and Jean-Christophe Prévotet. Overview of the mobility related security challenges in lpwans. *Computer Networks*, 186:107761, 2021.

[23] Arnaud Durand, Pascal Gremaud, and Jacques Pasquier. Decentralized lpwan infrastructure using blockchain and digital signatures. *Concurrency and Computation: Practice and Experience*, 32(12):e5352, 2020.

[24] Wael Ayoub, Fabienne Nouvel, Abed Ellatif Samhat, Mohamad Mroue, and Jean-Christophe Prevotet. Mobility management with session continuity during handover in lpwan. *IEEE internet of things journal*, 7(8):6686–6703, 2020.

[25] Wael Ayoub, Abed Ellatif Samhat, Fabienne Nouvel, Mohamad Mroue, Hassan Jradi, and Jean-Christophe Prévotet. Media independent solution for mobility management in heterogeneous lpwan technologies. *Computer Networks*, 182:107423, 2020.

[26] Antonio De la Oliva, Ignacio Soto, Albert Banchs, Johannes Lessmann, Christian

Niephaus, and Telemaco Melia. Ieee 802.21: Media independence beyond handover. *Computer Standards & Interfaces*, 33(6):556–564, 2011.

[27] Rajeev Koodli and Charles Perkins. Mobile ipv6 fast handovers. Technical report, RFC 5568, July, 2009.

[28] Hesham Soliman, Claude Castelluccia, Karim El Malki, and Ludovic Bellier. Hierarchical mobile ipv6 mobility management (hmipv6), 2005.

[29] Safwan M Ghaleb, Shamala Subramaniam, Zuriati Ahmed Zukarnain, and Abdullah Muhammed. Mobility management for iot: a survey. *EURASIP Journal on Wireless Communications and Networking*, 2016(1):1–25, 2016.

[30] Feng Zhong, Chai Kiat Yeo, and Bu Sung Lee. Enabling inter-pmipv6-domain handover with traffic distributors. *Journal of Network and Computer Applications*, 33(4):397–409, 2010.

[31] Stephen Kent and Randall Atkinson. Rfc2401: Security architecture for the internet protocol, 1998.

[32] Vishal Sharma, Jianfeng Guan, Jiyoon Kim, Soonhyun Kwon, Ilsun You, Francesco Palmieri, and Mario Collotta. Mih-spfp: Mih-based secure cross-layer handover protocol for fast proxy mobile ipv6-iot networks. *Journal of Network and Computer Applications*, 125:67–81, 2019.

[33] Daemin Shin, Vishal Sharma, Jiyoon Kim, Soonhyun Kwon, and Ilsun You. Secure and efficient protocol for route optimization in pmipv6-based smart home iot networks. *IEEE Access*, 5:11100–11117, 2017.

[34] Ming-Chin Chuang and Jeng-Farn Lee. Sf-pmipv6: A secure fast handover mechanism for proxy mobile ipv6 networks. *Journal of Systems and Software*, 86(2):437–448, 2013.

[35] Kais Mekki, E. Bajic, F. Chaxel, and Fernand Meyer. A comparative study of lpwan technologies for large-scale iot deployment. *ICT Express*, 5:1–7, 2019.

[36] ETSI. *LTE, Architecture enhancements for non-3GPP accesses (3GPP TS 23.402 version 16.0.0 Release 16)*. ETSI, 2020. URL `www.etsi.org/deliver/etsi_ts/123400_123499/123402/16.00.00_60/ts_123402v160000p.pdf`.

[37] Wael Ayoub, Mohamad Mroue, Abed Ellatif Samhat, Fabienne Nouvel, and Jean-Christophe Prévotet. Schc-based solution for roaming in lorawan. In *International Conference on Broadband and Wireless Computing, Communication and Applications*, pages 162–172. Springer, 2019.

[38] Wael Ayoub, Mohamad Mroue, Fabienne Nouvel, Abed Ellatif Samhat, and Jean-Christophe Prévotet. Towards ip over lpwans technologies: Lorawan, dash7, nb-iot. In *2018 sixth international conference on digital information, networking, and wireless communications (dinwc)*, pages 43–47. IEEE, 2018.

[39] IBM, 2020. URL `https://www.ibm.com/support/knowledgecenter/SSFMBX/com.ibm.swg.im.dashdb.sql.ref.doc/doc/r0008474.html`.

[40] Luca Vigano. Automated security protocol analysis with the avispa tool. *Electronic Notes in Theoretical Computer Science*, 155:61–86, 2006.

[41] Dimitrios Zorbas, Khaled Abdelfadeel, Panayiotis Kotzanikolaou, and Dirk Pesch. Ts-lora: Time-slotted lorawan for the industrial internet of things. *Computer Communications*, 153:1–10, 2020.

[42] Hassan Jradi, 2021. URL `github.com/Hassan Jradi/secure-mobility-secure.git`. ns-3 Implementation source codes.

[43] Hassan Jradi, 2021. URL `github.com/Hassan Jradi/AVISPA-Validation-Code.git`. AVISPA HLPSL codes.

[44] Seonggeun Ryu, Gye-Young Kim, Byunggi Kim, and Youngsong Mun. A scheme to reduce packet loss during pmipv6 handover considering authentication. In *2008 International Conference*

on Computational Sciences and Its Applications, pages 47–51. IEEE, 2008.

[45] Michael Burrows, Martin Abadi, and Roger Michael Needham. A logic of authentication. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 426(1871):233–271, 1989.

A Cost Analysis

$$T_R^{M1} = \frac{L_{M_1}}{R_b} + \tau = \frac{L_{ID} + L_{TS} + L_H + O_{L2}}{R_b} + \tau$$
$$T_R^{M2} = \frac{L_{M_2}}{R_b} + \tau = \frac{L_{ID} + L_W + L_{TS} + L_H + O_{L2}}{R_b} + \tau$$
$$T_R^{M3} = T_R^{M4} = \frac{L_{ID} + L_{TS} + L_H + O_{L2}}{R_b} + \tau$$
$$T_R = T_R^{M1} + T_R^{M2} + T_R^{M3} + T_R^{M4}$$
$$T_R = \frac{4L_{ID} + 4L_{TS} + 5L_H + 4O_{L2}}{R_b} + 4\tau = \frac{2368}{R_b} + 4\tau$$

Table 5: Numerical values

Variable	**Length (Bytes)**
L_{ID}	4
L_{TS}	10
L_H	32
O_{L2}	20