Secure PMIPv6-Based Mobility Solution for LoRaWAN

Hassan Jradi*†, Abed Ellatif Samhat*, Fabienne Nouvel†, Mohamad Mroue*, Jean-Christophe Prévotet†
*Lebanese University — CRSI, Hadath, Lebanon.
email: {samhat, mohamad.mroue}@ul.edu.lb
†INSA de Rennes — IETR, Rennes, France.
email: firstname.lastname@insa-rennes.fr

***Abstract*—The widespread use of Internet of Things (IoT) has stimulated the invention of new communication technologies like Long Range Wide Area Network (LoRaWAN) and Narrow Band-Internet of Things (NB-IoT) belonging to Low Power Wide Area Network (LPWAN) technologies. The wide use of these technologies brings new requirements like mobility management. Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol. However, integrating PMIPv6 in LPWAN rises a special challenge due to LPWAN constraints. In addition, PMIPv6 does not provide secure access to the operator domain. In this paper, we propose a new PMIPv6-based mobility solution for LoRaWAN boosted with an authentication scheme to access the operator domain and make this solution resist several types of attacks. In addition, we evaluate the performance of our scheme and we compare it with other works. Finally, we evaluate the security of the new scheme using Automated Validation of Internet Security Protocols and Applications (AVISPA) tool.**

Keywords – IoT; LPWAN; LoRaWAN; Mobility; Authentication.

I. INTRODUCTION

The Internet of Things (IoT) is the novel era of wireless communication carrying out several services ranging from data sensing to command execution [1]. New communication technologies designed to meet the needs of long communication range with low data rates and power consumption are invented and categorized under Low Power Wide Area Network (LPWAN) [2]. Long Range Wide Area Network (LoRaWAN) is one of the most prominent LPWAN technologies operating in the unlicensed Industrial, Scientific, and Medical radio band (ISM band) [3].

However, several applications like healthcare supervising and supply chain monitoring, require a secure mobility management protocol to ensure session continuity and secure access to the operator network [4]. Proxy Mobile IPv6 (PMIPv6) [5] is one of IPv6 protocol extensions designed to provide network-based mobility protocol. The mobility procedure is executed by an entity on behalf of the Mobile Node (MN) which minimizes the power consumed by it.

However, PMIPv6 does not deploy an authentication mechanism which is essential in case of an MN wishing to join the network. Several authentication schemes are proposed to be used in PMIPv6 as in [6][7]. Nonetheless, the used solution should be well adapted to work in LoRaWAN environment taking into consideration LPWAN constraints like payload length, data rate range, and number of messages per day.

Contribution. The main contribution of this paper is the proposal of a new mobility solution based on PMIPv6 protocol with an authentication scheme providing both intra-domain and inter-domain authentication for LoRaWAN.

Paper Organization. In Section II, we present some related work and we describe the problem. In Section III, we present the proposed mobility solution along with the authentication scheme. Section IV shows the results and the comparison with related work and Section V concludes the paper.

II. BACKGROUND AND RELATED WORK

Mobility is the movement of an MN leading to the release of the connection with the current Point of Attachment (PoA) and the establishment of the connection with a new PoA [8]. The deployed mobility management protocol has a major role in the connection release/establishment procedures from performance and security points of view.

Several types of mobility can be identified according to the handoff scenario. Handoff is the process of release of the old connection and establishment of the new connection. Thus, mobility can be homogeneous or heterogeneous if the previous and the new PoAs use the same or different link layer technologies, respectively. Mobility can be also intra-domain or inter-domain (also known as roaming) if the previous and the new PoAs belong to the same or different network operators, respectively. Consequently, several schemes are proposed to deal with the mobility challenge in LPWANs taking into consideration the security aspect.

The work done by Moosavi *et al.* [9] aims to provide a mobility management solution for IoT by splitting the network into two virtual layers. The intermediate processing layer consists of smart gateways that manage devices mobility, and the cloud layer consists of data analysis servers. This solution enables an end-to-end security solution between the MN and the end-user by providing authentication and data encryption, and at the same time provides session resumption after the handoff phase.

Another work done by Kang *et al.* [6] addresses the problem of lack of authentication in PMIPv6 protocol. This work focuses mainly on the PMIPv6 protocol without taking into consideration the IoT requirements. Thus, the proposed solution is a general solution and could not be adapted directly to IoT or LPWANs.

In Sharma *et al.* [7] work, the authors proposed a mobility management solution based on Fast Proxy Mobile IPv6 (FPMIPv6) to provide a proactive handoff approach, and based on Media Independent Handover (MIH) framework [10] which is a framework providing heterogeneous handoff using three

 ISBN: 978-1-61208-940-9

MIH services. Moreover, the authors propose an authentication scheme based on pre-shared keys to provide secure MIH communication between the MN and the network entities. This solution was intended for IoT and not for LPWAN having more constraints, thus it cannot be directly adapted into LPWANs.

In the work of Ayoub *et al.* [11], the authors proposed to use a modified version of Static Context Header Compression protocol (SCHC) [12] protocol named Dynamic Context Header Compression (DCHC) protocol along with the use of Mobile IPv6 (MIPv6) and a light version of MIH framework. This work was designed to operate in an LPWAN environment especially with LoRaWAN and Narrow Band-Internet of Things (NB-IoT).

Thus, as shown, several works try to deal with the mobility aspect of devices. However, these works either cannot be directly integrated into LPWAN, or do not provide a security mechanism for network access. In the next section, we present a new PMIPv6-based mobility solution boosted with an authentication mechanism taking into consideration LPWAN constraints.

III. PROPOSED SOLUTION

In this section, we present our mobility solution that provides both intra-domain and inter-domain mobility types for LoRaWAN, where the MN may move inside or outside its home operator network coverage.

A. Protocol Stack

The protocol stack used for the communication between the MN and the network is represented in Figure 1.

The upper layers consist of application and transport layers which are dependent on the deployment purpose of the network. These layers are used to send/receive the application data.

The network layer consists of IPv6 as a routing protocol and PMIPv6 as a network layer mobility management protocol. As we are dealing with LoRaWAN technology which is considered as a layer 2 or link-layer technology, we propose to modify the LoRaWAN protocol stack to be operable with the added IPv6 and PMIPv6 network layer functions. The integration of PMIPv6 requires the adoption of PMIPv6 network architecture, as discussed in the following subsection. However, the addition of this layer leads to additional overhead which should be examined carefully in LoRaWAN since the maximum payload length is 256 bytes. The advantage of using IPv6 is to achieve global mobility independently of the lower layer technology, since each technology can deploy its lower layer mobility protocol.

For that, we propose to use an adaptation layer to overcome the previous problem. In this layer, Static Context Header Compression protocol (SCHC) [12] is used to compress the IPv6 packet headers in order to fit suitable payload lengths for LPWANs. Upon a connection establishment, the sender and the receiver agree on a SCHC context. This context

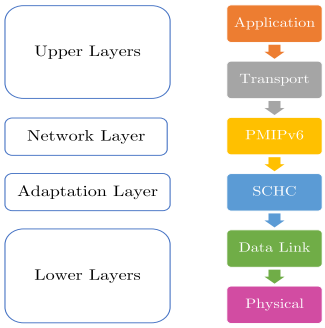

Figure 1. Mobile Node Protocol Stack.

contains several rules identified by RuleID. Each rule contains a list of entries. An entry contains a field identifier, a Compression/Decompression (C/D) action, a target value and a matching operator. An uplink packet header field is compared with the target value according to the matching operator, and if the comparison test succeeds, the C/D action is executed. In this way, the RuleID and the compression residues are sent instead of sending the entire header. At the receiver side, the reverse process is executed.

The lower layers consist of the data link and physical layers of the used LPWAN technology. In the case of LoRaWAN, the data link layer is LoRaWAN Media Access Control Layer and the physical layer is LoRa physical layer.

B. Network Architecture

The main entities in LoRaWAN are the Network Server (NS), the Join Server (JS) and the Gateways (GWs). The improved LoRaWAN architecture is called evolved LoRaWAN and is shown in Figure 2. We endeavored to integrate the two necessary PMIPv6 entities, which are the Media Access Gateway (MAG) and the Local Mobility Anchor (LMA), in the LoRaWAN architecture.

We propose to place the LMA functionalities within the NS since the latter is the anchor point of LoRaWAN architecture. Furthermore, a new entity called LoRa Mobile Access Gateway (LoRaMAG), is inserted between GWs and NS. Therefore, several GWs will be connected to one LoRaMAG and an MN should authenticate itself with the new LoRaMAG when it moves from a GW to another connected to a different LoRaMAG. LoRaMAG will play the role of the MAG of PMIPv6 architecture. It is responsible for the detection of MN movement, initiating the mobility signaling with the LMA, and data forwarding between MN and LMA through the dedicated tunnel.

The use of PMIPv6 adds more scalability where the NS functions are divided over several LoRaMAGs like the downlink GW selection. In addition, PMIPv6 is known to be to suitable for constrained devices since MIPv6 binding update messages are executed by MAG on the MN behalf.

Another entity used for the authentication between the MN and the LoRaMAG called the Authentication Server (AuS) is added also in each PMIPv6 domain (which is in this case the LoRaWA network). The detailed operation of the AuS function is shown in the next subsection.

 ISBN: 978-1-61208-940-9

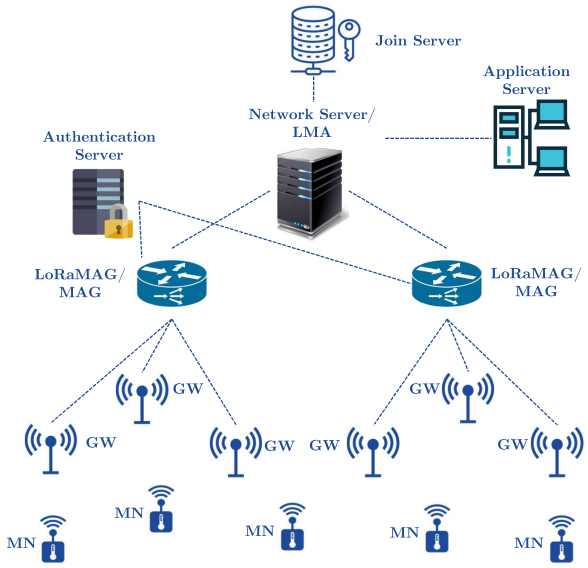

Figure 2. Evolved LoRaWAN Network Architecture.

C. Authentication Scheme

The proposed authentication scheme is used to authenticate the MN with the LMA in the PMIPv6 domain using AuS entity. In the following, we distinguish between two scenarios: intra-domain mobility and inter-domain mobility (or roaming).

In case of intra-domain mobility, the MN moves inside the coverage of a GW connected to a LoRaMAG belonging to its home domain, thus MN credentials are saved in the domain AuS where the MN is initially registered.

In case of inter-domain mobility, the MN moves towards the coverage of GWs of a visited domain having its visited LMA (vLMA), visited AuS (vAuS), and will be connected through visited LoRaMAG (vLoRaMAG). The MN is initially registered in its home domain in home AuS (hAuS) having MN credentials.

The proposed scheme consists of two phases: the registration phase and the authentication phase. We will present the authentication phase in case of roaming (device moving in the visited operator coverage).

In this scheme, we tried to integrate the PMIPv6 signaling with the authentication scheme signaling. This solution is compatible with class A LoRaWAN devices based on one transmission frame followed by two reception frames.

1) Registration Phase: The hAuS holds two secret keys X and Y which are only known by itself. Then, a MN_i having an identity ID_i and the hAuS holds two pre-shared keys:

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

We presume that we have secure links between {GWs and vLoRaMAG}, {vLoRaMAG and vAuS}, {vAuS and hAuS}. so that data confidentiality and integrity are ensured on these links. These links can be secured using Public Key Infrastructure (PKI) [13] or any authentication and key agreement scheme. We focus on the {MN and vLoRaMAG} link where LoRaWAN limitations are present.

2) Authentication Phase: In this phase, the MN tries to authenticate itself in the visited PMIPv6 domain with the vLoRaMAG through vAuS and hAuS, using the exchanges shown in Figure 3. Since the GWs only forward the messages, we do not represent them for more clarity. Moreover, this phase is divided into two sub-phases: home authentication sub-phase, and visited authentication sub-phase.

In home authentication sub-phase (red part in Figure 3), the MN sends its authentication request which passes to hAuS through vAuS. The hAuS checks the authentication request validity and derives two keys and shares them with vAuS. This sub-phase is executed **in case of roaming only and once per visited domain**.

In visited authentication sub-phase (green part in Figure 3), after the vAuS gets the visited keys from the hAuS, it uses them to authenticate the MN as long as it is in the visited domain without the need to send requests to hAuS. So after the first sub-phase, the second sub-phase can be repeated several times to authenticate the mobile when it moves between different vLoRaMAGs.

The message exchanges are detailed below. T_1 through T_4 are timestamp variables used to prevent replay attack.

1) MN_i computes $K_i = H(X_i) \oplus H(Y_i)$ and $MIC_1 = H(ID_i \| T_1 \| K_i)$ then sends a message with *AuthReq* tag consisting of $\{ID_i \| ID_{hAuS} \| T_1 \| MIC_1\}$.
2) vAuS checks the requested AuS by inspecting the second field of the request. In this case, the requested AuS is hAuS thus vAuS forwards this request to hAuS.
3) hAuS receives the request and gets the identity ID_i, then hAuS queries its database for the corresponding keys X_i and Y_i. Thereafter, hAuS computes $K_i = H(X_i) \oplus H(Y_i)$ and checks if $MIC_1 = H(ID_i \| T_1 \| K_i)$.
4) hAuS generates a random nonce N and computes two derived keys $vX_i = H(X_i \oplus N)$ and $vY_i = H(Y_i \oplus N)$. These two derived keys are intended to be sent to vAuS. Moreover, hAuS computes $MIC_2 = H(ID_i \| N \| T_2 \| K_i)$. hAuS sends a message with *RoamingAuthResp* tag consisting of $\{ID_i \| vX_i \| vY_i \| N \| T_2 \| MIC_2\}$. Note that this message is sent over a secure link.
5) vAuS receives the response and gets vX_i and vY_i, then saves them along with ID_i in its database. Thereafter, vAuS forwards the rest of the response to MN_i with its identity ID_{vAuS}. A mapping between ID_i and $DevAdd_i$ is saved in the vLMA/NS.
6) MN_i receives the response and checks if $MIC_2 = H(ID_i \| N \| T_2 \| K_i)$. MN_i gets N from the message then computes $vX_i = H(X_i \oplus N)$ and $vY_i = H(Y_i \oplus N)$ to be used for the authentication in the visited domain. At this step, home authentication sub-phase is finished and should not be executed again as long as MN_i is inside this domain.
7) After the reception of the $RoamingAuthResp$ by the vLoRaMAG in case of first authentication request (home authentication sub-phase), or in case of attach event detection by vLoRaMAG in second or upper MN_i at-

 ISBN: 978-1-61208-940-9

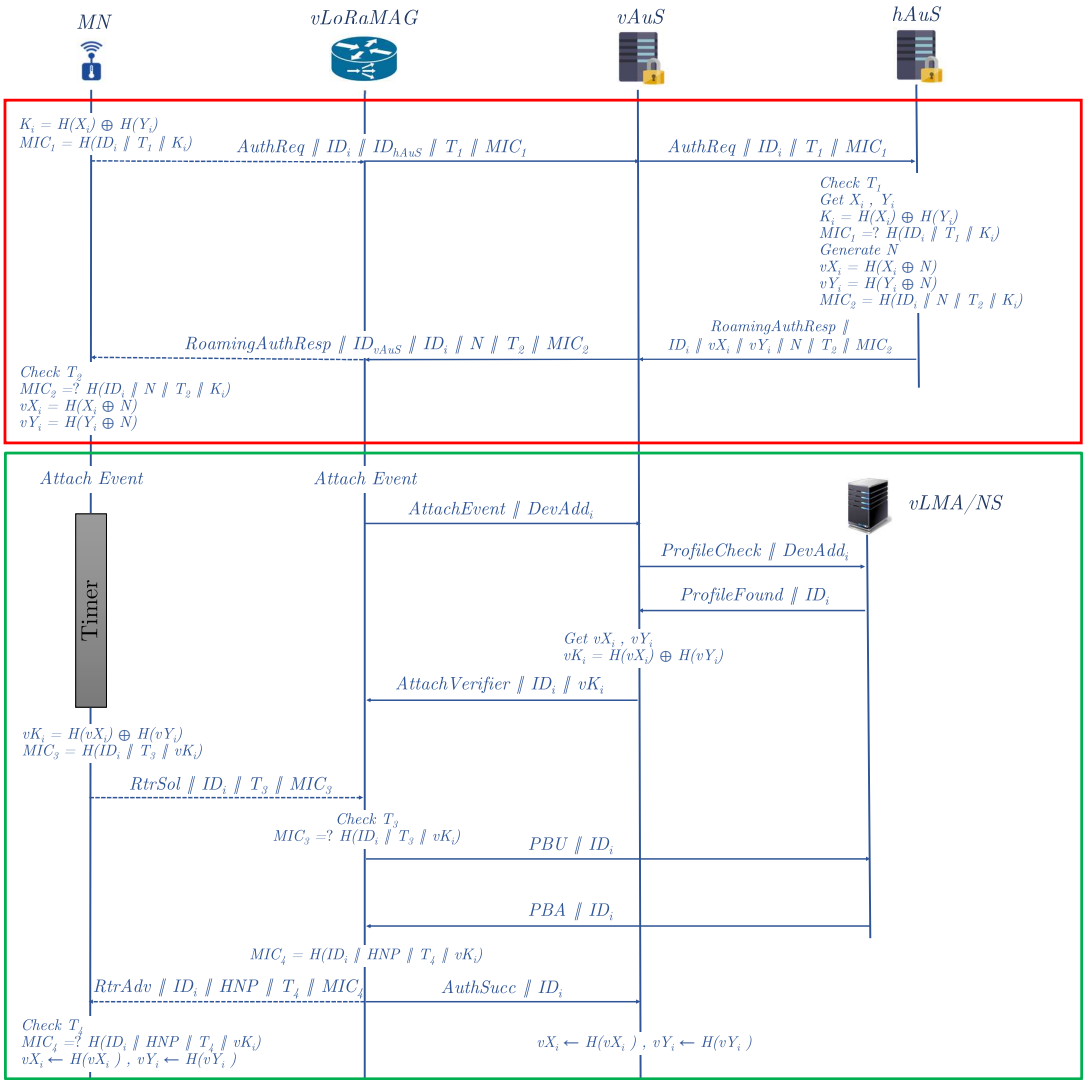

Figure 3. Message Exchange During Authentication Phase.

tachment (after a successful LoRaWAN Join Procedure); vLoRaMAG sends a message with *AttachEvent* tag consisting of $\{DevAdd_i\}$ to vAuS. This step is the first step of visited domain authentication sub-phase.

8) vAuS receives the attach event notification from vLoRaMAG then sends a message with *ProfileCheck* tag consisting of $\{DevAdd_i\}$ to vAuS/NS. vAuS/NS in its turn replies with a message with *ProfileFound* tag consisting of the corresponding $\{ID_i\}$.
9) vAuS queries its database based on ID_i to get vX_i and vY_i, then it computes $vK_i = H(vX_i) \oplus H(vY_i)$ and sends a message with *AttachVerifier* tag consisting of $\{ID_i \| vK_i\}$ to vAuS/NS. Note that this message is sent over a secure link.
10) After elapsing the timer launched by MN_i after the link layer attach, which is configured to be equivalent to the duration of the four previous exchanges, MN_i computes $vK_i = H(vX_i) \oplus H(vY_i)$ and $MIC_3 = H(ID_i \| T_3 \| vK_i)$. Then sends a message with *RtrSol* tag consisting of $\{ID_i \| T_3 \| MIC_3\}$ to vLoRaMAG in order to get a *RtrAdv* message to configure its network layer interface.
11) vLoRaMAG receives the *RtrSol* message and checks if $MIC_3 = H(ID_i \| T_3 \| vK_i)$. If so, vLoRaMAG sends a Proxy Binding Update (PBU) message along with ID_i to vLMA which is also the NS. Therefore vLMA performs the needed operations according to PMIPv6 protocol to register/update the Binding Cache Entry (BCE) of MN_i. Then it replies with Proxy Binding Acknowledgment (PBA) message along with ID_i to vLoRaMAG.
12) vLoRaMAG accepts the PBA message and computes $MIC_4 = H(ID_i \| HNP \| T_4 \| vK_i)$ and sends a message with *RtrAdv* tag consisting of $\{ID_i \| HNP \| T_4 \| MIC_4\}$ to MN_i. Home Network Prefix (HNP) is the network prefix corresponding to MN_i. vLoRaMAG sends another message with *AuthSucc* tag along with ID_i to vAuS to confirm the authentication success.

13) MN_i receives the *RtrAdv* message and checks if $MIC_4 = H(ID_i \| HNP \| T_4 \| vK_i)$ where it can now configure its network layer interface using HNP.
14) MN_i and vAuS update the two derived keys by performing the following operations $vX_i \leftarrow H(vX_i)$ and $vY_i \leftarrow H(vY_i)$ which will be used in the next authentication trial.

IV. RESULTS AND ANALYSIS

In this section, we present the performance evaluation and the security analysis of our solution. In addition, we compare the performance evaluation and the security features of our solution with related work.

A. Performance Evaluation

We evaluated the performance of the proposed authentication scheme by simulation using Network Simulator 3 (NS-3). The simulation scenario consists of the entities used in the authentication scheme. The link between MN and GW is a LoRaWAN radio link and is considered an unsecured link. The MN is trying to authenticate itself to the visited domain using the proposed scheme. The source code of implementation can be found in [14].

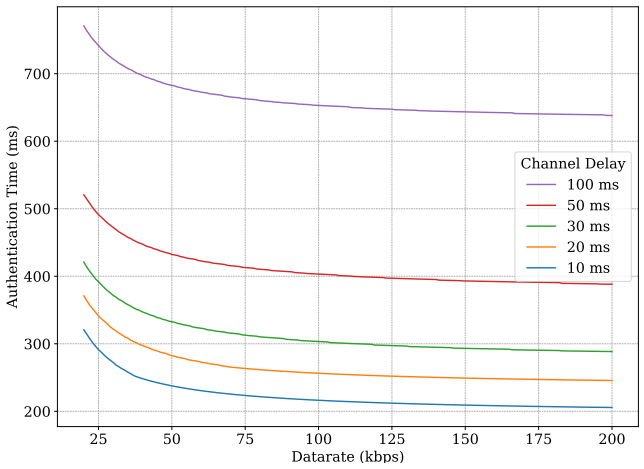

Figure 4. Authentication Time for Variable Data Rates and Channel Delays.

The evaluation metric is the time needed to perform the authentication scheme and the simulation parameters are the data rate (R_b) and the channel delay (τ) for the link between MN and GW. For that, we run simulations at LoRaWAN data rate range, i.e., R_b from 20 to 200 kbps and at $\tau \in \{10, 20, 30, 50, 100\}$ ms. The results are shown in Figure 4.

In Figure 5, we show the overall handoff latency for related work presented in Section II. The results show that our solution provides competitive results with other solutions where we work on low data rates and we provide inter-domain authentication. Moosavi *et al.* [9] and Sharma *et al.* [7] use high data rates reaching 8 Mbps whereas in Ayoub *et al.* [11], and in this work, the data rates used are that used in LoRaWAN (between 20 to 200 kbps) forming a low latency mobility solution.

Moreover, the longest message payload on the LoRaWAN link is that tagged with $RoamingAuthResp$. The hash used in this scheme is SHA-256 thus hash length ($L_{Hash} = 32\ Bytes$). The lengths of identities, nonce and timestamp are respectively $L_{ID} = 4\ Bytes$, $L_{Nonce} = 8\ Bytes$ and $L_{Timestamp} = 10\ Bytes$. Thus $L_{Payload} = 2 \times L_{ID_i} + L_{Nonce} + L_{Timestamp} + L_{Hash} = 58\ Bytes < 256\ Bytes$ (Maximum LoRaWAN payload length). Thus, the authentication mechanism is suitable for LoRaWAN technology and more particularly for class A devices since it is based on reception after transmission.

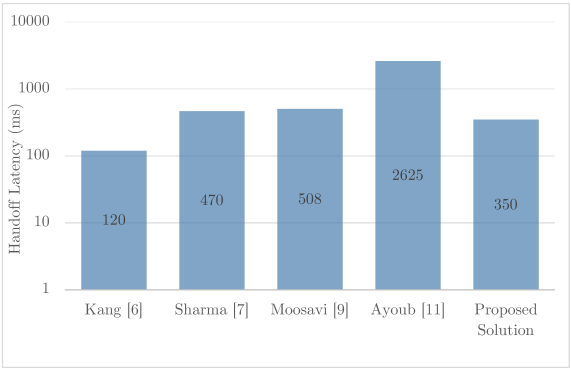

Figure 5. Performance Comparison of the Proposed Mobility Solutions.

B. Security Analysis

We assess the security of the proposed authentication scheme based on attacks related to device mobility as mentioned in our previous work [2].

- ◇ Device re-authentication: the proposed authentication scheme aims to provide secure access when the mobile node moves between different domains, thus it can be identified and authenticated in case of intra-domain and inter-domain mobility.
- ◇ Spoofing signaling message: the exchanged signaling messages between MN and network entities are integrity protected using MIC field through K_i or vK_i keys only known by the concerned entities. Thus, an attacker cannot modify the content of these messages without being detected.
- ◇ Address squatting and spoofing: an attacker cannot squat or spoof the device address since HNP is provided to MN during the authentication phase based on PMIPv6 specifications. And the network layer interface is configured after the authentication phase based on the provided HNP.
- ◇ Old address control: the MN IPv6 address is re-configured after the handoff phase based on the received IPv6 HNP. Thus, an attacker uses a device address without the completion of the authentication phase.
- ◇ Mutual authentication: the authentication between the mobile node and the hAuS is ensured using the hash key K_i, and between the MN and the vLoRaMAG using the hash key vK_i. These keys are confidential and cannot be derived by an attacker since it does have and cannot predict the key materials X_i, Y_i, vX_i and vY_i.

 ISBN: 978-1-61208-940-9

◇ Key freshness: the hash key vK_i is calculated during each authentication trial by a way it cannot be predicted in the next authentication trial based on the use of vX_i, vY_i. Even if vLoRaMAG having vK_i cannot predict it at next trial.
◇ Replay attack: this kind of attack is prevented by the use of timestamps $T1$ through $T4$.

In Table I, we compare the security features provided by related work presented in Section II.

TABLE I
COMPARISON OF SOLUTIONS ACCORDING TO SECURITY ISSUES

	Kang *et al.*[6]	Sharma *et al.*[7]	Moosavi *et al.*[9]	Ayoub *et al.*[11]	Proposed Solution
Device re-authentication	✓	✓	✓	✗	✓
Spoofing signaling message	✓	✓	✓	✗	✓
Address squatting and spoofing	✓	✓	✓	✗	✓
Old address control	✗	✓	✓	✗	✓
Mutual authentication	✓	✓	✓	✗	✓
Key freshness	✗	✓	✗	✗	✓
Replay attack	✗	✓	✓	✗	✓
Suitable for LPWAN	✗	✗	✗	✓	✓

✓ : Resistant ✗ : Vulnerable

C. Security Validation using AVISPA

We used Automated Validation of Internet Security Protocols and Applications (AVISPA) [15] as a validation tool for the security of the proposed authentication scheme. The implementation codes using HLPSL language can be found in [14]. Testing the implemented scheme using AVISPA shows that our solution is secure, as shown in Figure 6.

V. CONCLUSION

In this paper, we proposed an inter-domain mobility solution for LoRaWAN. We tried to solve the problem of domain access in PMIPv6 protocol by the use of the proposed authentication mechanism. Our solution is simulated using NS-3 and presents competitive results compared to other works in the literature. We conducted our scheme also through AVIPSA validation tool to prove its security.

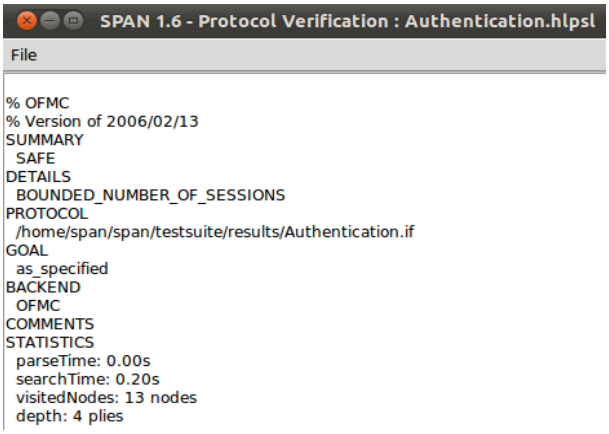

Figure 6. AVISPA Validation of the Proposed Authentication Scheme.

REFERENCES

[1] J. Lin *et al.*, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, pp. 1125–1142, 2017.
[2] H. Jradi, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Overview of the mobility related security challenges in lpwans," *Computer Networks*, p. 107 761, 2020.
[3] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of lpwan technologies for large-scale iot deployment," *ICT express*, vol. 5, no. 1, pp. 1–7, 2019.
[4] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2018.
[5] S. Gundavelli *et al.*, "Proxy mobile ipv6," *IETF RFC 5213*, Aug. 2008.
[6] D. Kang, J. Jung, D. Lee, H. Kim, and D. Won, "Security analysis and enhanced user authentication in proxy mobile ipv6 networks," *Plos one*, vol. 12, no. 7, pp. 1–20, 2017.
[7] V. Sharma *et al.*, "Mih-spfp: Mih-based secure cross-layer handover protocol for fast proxy mobile ipv6-iot networks," *Journal of Network and Computer Applications*, vol. 125, pp. 67–81, 2019.
[8] C. Perkins *et al.*, "Ip mobility support," *IETF RFC 2002*, Oct. 1996.
[9] S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare internet of things," *Future Generation Computer Systems*, vol. 64, pp. 108–124, 2016.
[10] V. Gupta *et al.*, "Ieee802. 21 standard and metropolitan area networks: Media independent handover services," *Draft P802*, vol. 21, p. D00, 2009.
[11] W. Ayoub *et al.*, "Media independent solution for mobility management in heterogeneous lpwan technologies," *Computer Networks*, vol. 182, p. 107 423, 2020.
[12] A. Minaburo, L. Toutain, C. Gomez, D. Barthel, and J.-C. Zúñiga, "Schc: Generic framework for static context header compression and fragmentation," Technical Report RFC8724, Tech. Rep., 2020.
[13] C. Adams and S. Lloyd, *Understanding public-key infrastructure: concepts, standards, and deployment considerations*. Sams Publishing, 1999.
[14] H. Jradi, ns-3 and AVISPA Implementation source codes, retrieved: Mar, 2022. [Online]. Available: github . com / HassanJradi/secure-mobility-secure.git.
[15] L. Vigano, "Automated security protocol analysis with the avispa tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, 2006.

 ISBN: 978-1-61208-940-9