2016 IEEE 27th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC): MAC & Cross-Layer Design

Ephemeral: Lightweight Pseudonyms for 6LoWPAN MAC addresses

Jessye Dos Santos*, Christine Hennebert*, J.C. Fonbonne* and Cédric Lauradoux†
*CEA, DRT, 38054 Grenoble, FRANCE.
†INRIA Rhône-Alpes, 38330 Montbonnot Saint-Martin, FRANCE.
Email: [jessye.dossantos, christine.hennebert, jeanchristophe.fonbonne]@cea.fr ; cedric.lauradoux@inria.fr

***Abstract*—Privacy is a major issue for 6LoWPAN networks and the use of persistent identifiers (MAC addresses) in the core mechanism is particularly challenging. Indeed, nodes use the SLAAC protocol to auto generate their IPv6 addresses based on their MAC addresses. Persistent addresses simplify the routing in the network but allow an adversary to analyze the traffic and recover sensitive information. We propose Ephemeral, a MAC pseudonym scheme compliant with SLAAC. It provides dynamic pseudonyms cryptographically generated without the need to reconstruct the routing tables when the pseudonyms change. Our simulation based on `CONTIKI 3.0` and `WSNET` shows that Ephemeral improves MT6D, a previous MAC pseudonyms scheme, by 16% in term of application packet delivery.**

I. Introduction

Persistent identifiers such as MAC or IPv4/IPv6 addresses have been used for years in Internet and in Wireless Network to route packets. The emergence of the Internet-Of-Things has exacerbated the need to uniquely identify devices. The convenient persistent identifiers have suddenly become a privacy issue because they can be used to track people or to infer sensitive information. Pseudonyms also known as address randomization have been rapidly adopted to answer this problem. For instance, it is now enforced in iOS 8 and in Tail Linux. Address randomization adds complexity to routing. This is particularly true for network in which the nodes have limited resources like Wireless Sensor Networks (WSNs). Our paper is dedicated to the deployment of a pseudonym scheme in a IPv6 LoW Power Wireless Area Networks (6LoWPAN) [12] WSN.

We propose Ephemeral to create dynamic pseudonyms compatible with the Routing Protocol for Low Power and Lossy Networks (RPL) and the StateLess Address AutoConfiguration (SLAAC) to hide source and destination MAC addresses in the packet. Our scheme is backboned by the use of the security at the link layer. We design Ephemeral with several goals in mind. The pseudonym modification do not provoke the reconstruction of the neighbor nor routing tables. It does not require synchronization and it can be either event-driven or time-driven.

This paper is organized as follows. Section II presents the context of our work: 6LoWPAN and RPL. In Section III, we present the threats against privacy and the mitigation proposed in the past. Ephemeral is described in Section IV. We discuss the implementation of Ephemeral in Section V. Our simulation results are given in Section VI. We compare the routing performance of Ephemeral with MT6D [17]. Finally, we conclude in Section VII.

II. Addressing and Routing in 6LoWPAN

IPv6 standard [10] was introduced in 1998 as solution to the lack of IPv4 addresses face to the increase of connected objects. With 128-bits of addressing, IPv6 offers sufficiently addresses. Suitable for 6LoWPAN networks [24], SLAAC [14] enables a device to auto-configure its IP address thanks to simple metrics. 6LoWPAN standard recommends RPL [21] as routing protocol. RPL is able to route packets in a constrained network [7] using the MAC addresses for the hop-by-hop routing and the IPv6 addresses generated from the MAC addresses following SLAAC process for the source to finale destination routing strategy.

RPL organizes the 6LoWPAN nodes on a Destination Oriented Directed Acyclic Graph (DODAG). It provides new ICMPv6 control messages. DODAG Information Object (DIO) broadcast frames include information on the network topology. It is used to establish and maintain the DODAG. Destination Advertisement Object (DAO) frames are sent by a node to its parents to propagate downward route information along the DODAG. A periodical polling protocol is defined using DIO messages to request DAO frames in order to maintain the routing DODAG. The last ICMPv6 frame provided by RPL is the DODAG Information Solicitation (DIS) frame. It allows nodes to request DODAG information and represents the first exchange of the association protocol. The reception of a DIS drives the broadcast of DIO frames by the neighboring nodes.

III. Privacy issues in 6LoWPAN and mitigation

The metadata included in the header of the control messages provides information about privacy accessible to an attacker by eavesdropping [5]. In [9], the automation control in an underground metro station is ensured by a Contiki based WSN. The wireless communications are accessible to anyone.

A. Threat model

The attacks against privacy can be either passive or active. In a passive attack, the intruder is an outsider who observes the traffic exchanged by the nodes. He observes the control traffic and data. It is important to notice that the payload of the traffic might be encrypted or not. Still the intruder can recover

978-1-5090-3254-9/16/$31.00 ©2016 IEEE

valuable information [8]. In-depth packet analysis brings information on the device, their role, and their capabilities as well as the overall functioning of the network. In active attacks, the intruder is an insider. For instance, a sinkhole attack [22] can be used to attract all the traffic and observe everything in the network. Many attacks can compromise privacy, see [16] for more details. A way to counter the majority of these attacks is to mask the addresses used by the routing protocol in the header of the packet sent over the air. By this way, the data collected are more difficult to analyze.

Combination of passive and active attacks enable to launch powerful targeted attacks. For example in [9], Denial of Service (DoS) attacks could be launch on identified gateways in order to disrupt the real time monitoring. Due to the constrained resources of the nodes, the deployment of an embedded IDS allows the monitoring of only one type of intrusion by node.

B. Mitigation

Two classes of solutions have been proposed to mitigate privacy issues in sensor networks: encrypted tunnels and pseudonyms.

1) Encrypted tunnels: onion routing approach has been proposed in [4]. To send a message, the path is first identified and the encryption key of the intermediate routers recovered. The message is then formed by successive encryption of the frame with the key collected, beginning with the key of the farthest router and finishing with the nearest router key. At each stage, the IPv6 address of the next router is included before encryption to disclose only the information necessary for the local hop. Once the message sent, each router on the path peels the frame by decrypting the content to know the next destination router. To do this, a fixed header of 500 bytes is added to the message, making this technique unsuitable to 6LoWPAN WSN where 127 bytes frames are exchanged with a header field that must be reduced as much as possible.

The IPsec in tunnel mode is another possible option to provide anonymity for peer-to-peer communications. The whole frame including both header and payload is enciphered and encapsulated into a new frame with an anonymous IP header. But, this protocol introduces a serious overhead and masks only the IP addresses and not the MAC addresses used for hop-by-hop routing.

2) Pseudonyms: the basic idea consists in replacing long term identifier by short term pseudonyms which are refreshed. This approach has received more attention recently and is the one supported in this paper.

Simple Anonymity Scheme (SAS) [23] provides to the nodes a static list of n pseudonyms distributed by a trusted authority. An intruder can recover the list of each node after $n\log(n)$ refreshes (Coupon's collector argument) which limits the guarantee provided by SAS. SAS has been improved by the Cryptographic Anonymity Scheme (CAS) [15]. The pseudonym values are not stored by the routers but checked with a Bloom filter for each incoming packet. As for SAS, [15] uses static lists of pseudonyms allowing an eavesdropper to deduce the routing information by the observation of the traffic on a long period of time.

The IETF published two RFCs [3], [13] both aimed at generating pseudonyms to hide IPv6 addresses by the use of hash functions. Both methods lead to huge computational resources and present the disadvantage to encrypt only the source address, leaving the destination address in clear. Extending [13], the authors of [18] present an addressing scheme based on the use of elliptic curves (ECC) and named SSAS (Simple Secure Addressing Scheme). It relies on an authority capable of binding a MAC address to an ECC public key. However, checking an ECC signature at each hop of the routing for the verification of the pseudonyms is too intensive in a constrained WSN.

Groat *et al.* described in [6] explains a solution named Moving Target IPv6 Defense (MT6D). This protocol allows a node to protect IPv6 and MAC source and destination addresses using symmetric cryptography. The pseudonym of the MAC address is directly deduced from the pseudonym of the IID part of the IPv6 address. The key distribution is not specified. The change of pseudonyms is defined by the use of a temporal window. It requires that the nodes of the network are synchronized.

MT6D was created for classic IP network but Preiss *et al.* [17] provides a proof-of-concept on Contiki OS, an open source OS for the Internet-of-Things. The pseudonyms of the MAC addresses are implemented by counters. It needs to reconstruct the routing tables and the DODAG at each pseudonym change by the use of additional RPL traffic. Later, Sherburne in his PhD Thesis [19] adapts it to a WSN made up of a border router and one node. It appears as a well suited solution provided in the literature to manage pseudonyms in a WSN.

In the following, Ephemeral is designed as a privacy solution enabling multi-hops routing that doesn't introduce traffic overhead nor impact the routing tables.

IV. Ephemeral

A. Hypothesis

In Ephemeral, we assume that security is enforced at the MAC layer. The nodes of WSN use the security mechanism provided by the standard [1]. It ensures confidentiality, integrity and authenticity of the MAC payload thanks to encryption and the use of a message authentication code. All the nodes store two secrets: a secret LK that ensures the encryption of the MAC payload and a secret K_t, which can be updated, that is used to hide the MAC addresses included in the MAC header. A node is able to join the 6LoWPAN network secured with LK thanks to a secure bootstrap protocol during which K_t is encrypted using LK.

Ephemeral still uses IPv6 addresses to identify resources at the top layers. However, they are never communicated in the clear. A simplified view of the packets exchanged in the network is given in Fig. 1. The purpose of Ephemeral is to replace the addresses used in the clear to route the packets in the WSN by pseudonyms.

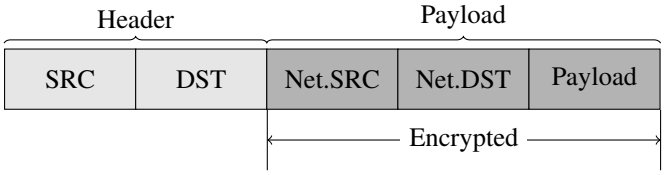


Fig. 1. Classical packet structure (simplified).

B. Pseudonym generation

In the following, the network nodes are indexed by $i = 1, .., n$ and the EUI-64 MAC address of node i formed as described on [11] is denoted a_i (m bits). The function which transforms a_i into a pseudonym is denoted F:

$$\begin{aligned} F(a_i, \mathrm{IV}_t, K_t) &= a_i \oplus E_{K_t}(\mathrm{IV}_t) \bmod 2^m \\ \mathrm{IV}_t &= g(\mathrm{IV}_{t-1}), \end{aligned}$$

where E is a block cipher of block length greater than ℓ. We assume that it is the AES but it can be replaced by any ℓ-bit lightweight block ciphers. For any $t > 0$, IV_t is composed of two blocks: $\mathrm{IV}_t = R||\mathrm{cpt}_t$. The first block R is composed of ℓ_1 bits. It is randomly generated and it is updated only periodically. The second block cpt_t of length $\ell_2 = \ell - \ell_1$ bits is a counter updated at given time intervals. The transition function g is defined by:

$$g(\mathrm{IV}_{t-1}) = R||(\mathrm{cpt}_{t-1} + 1),$$

where $||$ is the concatenation and $\mathrm{cpt}_0 = 0$.

C. Privacy analysis

The choice of g and the structure of IV_t are fundamental to understand when collisions occurs and when IV_t are reused. The occurrence of collisions is critical to ensure the uniqueness of pseudonym and prevent ambiguity when routing. The probability that two nodes share the same pseudonym is given by the birthday paradox. As long as $n \ll 2^{\frac{m}{2}}$, the probability of this event is negligible. In our case, we have $m = 64$ and n is about 30.

The values IV_t cannot be reused since they produce collision of pseudonyms or they can be exploited by an adversary to re-identify the original MAC addresses. The problem was discussed by Zenner in [25] when he discussed several designs for numbers used once. Our design is called *m*ixed solution 2 by Zenner [25] and it is the concatenation of an ℓ_1-bit random value with a ℓ_2-bit counter. Zenner gives the following formula to characterize when collisions occur:

$$\ell \geq \log_2 \left(n \cdot \frac{\alpha^2 - \alpha}{2 \cdot p_{max}} \right),$$

the probability for a collision, in case of IV_t is reset, is less than p_{max} and α is the number of time IV_t is reset. Let us assume that the cpt_t is increased every 60s and $\ell_2 = 8$ bits. Then, R must be reset every 256 min since we have reached the limit for cpt_t. If our network is supposed to operate 10 years, it implies that our network performs 20532 resets. If we consider for instance $n = 30$, we obtain $p_{max} \approx 2^{-95}$.

The counters cpt_t are transmitted in the clear in Ephemeral along with the corresponding pseudonym. An adversary can attempt to use the value of cpt_t to re-identify a node. Indeed, if each node has a different value for cpt_t then cpt_t becomes a unique identifier. A similar situation occurs when a node join the network. The counter of the new node is not synchronized (or closed) to the counter of the nodes already in the network. Such de-synchronization allows an adversary to identify the packets associated to the new node. To prevent such a case, each node checks that the counter they receive are all closed. Let consider two nodes i (cpt_t) and i' (cpt'_t) without loss of generality. If we have $\mathrm{cpt}_t \geq \mathrm{cpt}'_t + \delta$ for $\delta \geq 0$, then the value cpt'_t is updated to the value cpt_t. The extreme case (most paranoid and privacy preserving) corresponds to ensure that $\delta = 0$.

V. Implementation

A. Initialization and routing

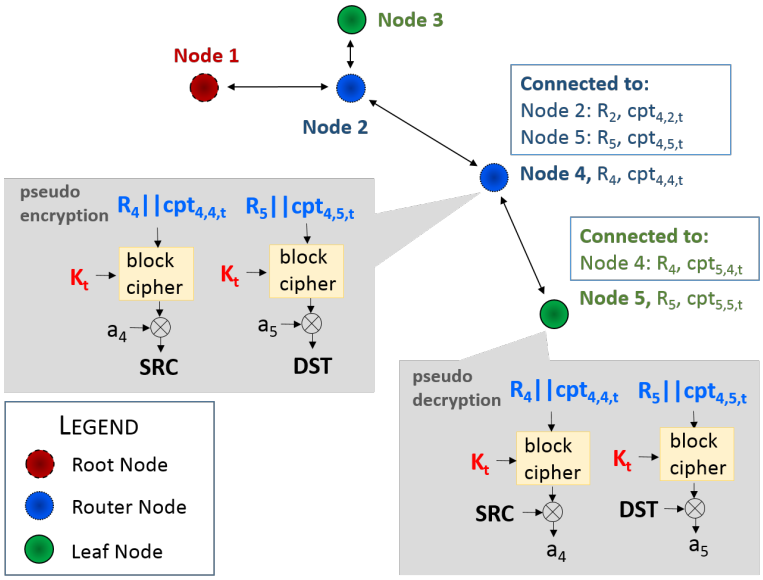


Fig. 2. Ephemeral Network

The topology of the simulated WSN is depicted on Fig. 2. At initialization, each node receives the secret key K_t used for the pseudonyms encrypted with LK and its dedicated value R as part of the initialization vector. Then, each node i recovers from its q neighbors their MAC addresses a_j, $(j \neq i)$ and the corresponding value R_j. Their pseudonym table of q entries includes the current counter $\mathrm{cpt}_{i,j,t}$ for each hop-by-hop communication.

When Node 4 sends an ephemeral frame to Node 5 as depicted in Fig. 3, it should compute both the pseudonym source address SRC and the pseudonym destination address DST as illustrated on Fig. 2. The MAC payload is encrypted thanks to LK. At receiving, Node 5 decrypts DST using the stored value R_5 and the received counter $\mathrm{cpt}_{4,5,t}$. It checks

that the resulting address corresponds to its real MAC address, and whether the counter value received does not exceed the previous over δ. If so, it uses LK to decipher the MAC payload and gets access to the content.

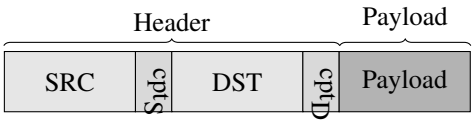


Fig. 3. Packet structure for Ephemeral.

B. Distribution and regeneration of pseudonym materials

To run correctly, Ephemeral needs to add some fields into the IEEE 802.15.4 MAC header. This can be achieved in compliance with the standard. The amendment IEEE 802.15.4e of 2012 [2] provides Information Element (IE) fields that enable to extend the MAC header with new fields. This possibility is used in Ephemeral to add two bytes, the first one for cpt_S, and the second one for cpt_D.

The next implementation aim is to consider IV_t. Ephemeral leans on RPL mechanism to share the $\text{IV}_t = \text{R}||\text{cpt}_t$. Indeed, RPL defines periodical sent of ICMP frames to maintain the routing tables. RPL also provides optional unused fields on both DIO and DAO frames [20]. By defining a new RPL control message option, we enable the inclusion of R into these fields. By waiting the periodical DIO RPL frames, each node i is enabled to share its current R. Because leaf does not sent DIO, these nodes use DAO frames. Thus, Ephemeral does not introduce extra control frames to propagate IV_t material. However, the length of both DIO/DAO frames is increased: an 8-bit header is needed to indicate that the RPL control message option followed by a 8-bits header for the length of the option. According to the size of the counter (8/16 bits), the including R introduces 15 bytes of overhead, for a total of 17 bytes added to the original frame (14 bytes for R and 16 bytes in total if 16-bits counters).

The same mechanism is also used for the update of the IV_t. Because we lean on the periodicity of RPL, we have to pay attention on the maximum interval between two DIO frames. Indeed, if a counter reaches it maximum value, we must change R value after the sent of the next DIO including the new R value. But if DIO sent doesn't occur before new incrementation of the counter, we have to use the current R with an already used value of counter. To prevent this security leak, we take margin of safety in compliance with the maximum DIO Interval value defined in Contiki. Let us consider $\ell_2 = 8$ bits as the length of cpt_t which enables 256 increments, one per minute. Because the maximum value defined by Contiki to send periodic DIO is around 18 minutes, we have to start the regeneration of the R at least when cpt_t reaches 255 - 18 = 237. We are in lossy packet network, neighbors can miss DIO with new update. In this case, application can be disrupt until new sent of DIO including R. Contiki defines maximum and minimum values to send DIO. These value can be adapted to the use case to lose the least of application frames. The Table I shows the probability for a collision, computed with the formula provided by Zenner, in case of R is reset at each DIO emission for the minimal and maximal values defined by Contiki.

Supposing a network which operates 10 years with 30 nodes.

DIO interval	nb of reset	p_{max}
4s	78750000	$\approx 2^{-71}$
17 min	308 823	$\approx 2^{-87}$

TABLE I
PROBABILITY OF COLLISION.

Even with the minimum value defined by Contiki the probability for a collision of IV_t is reasonable to not force the regeneration of the key during 10 years. This probability is of course reduce if the countermeasure against desynchronization is performed driving raise of reset.

VI. SIMULATIONS

We compare Ephemeral both with a reference scheme that uses RPL without pseudonyms and MT6D thanks to a simulated multi-hops 6LoWPAN WSN according to the network topology illustrated on Fig. 2.

A. Simulation environment

The simulated platform enables the communications between a host located on the Ethernet network and nodes located on the WSN. A border router (6BR) ensures the interoperability between the two communication stacks. It plays also the role of root node located on the top of the RPL DODAG.

The nodes can be either routers or leafs. They can communicate with each other within the 6LoWPAN network by using a virtualized RF link based on a posix radio and WSNET2.0 simulator. They implement Contiki 3.0 communication stack in native mode.

The typical WSN scenario deployed consists in sending for each node UDP frames including their identities, every 10s, either to the host via the root node to study Inter-network communications (IR), or to a node located on another branch of the DODAG in response to a demand of identity for Intra-network communications (IA).

Concerning the routing, RPL storing mode is used in our experiments and requires each node to store two tables: the neighbor and the routing tables. The root node registers and stores all the routing paths of the DODAG, whereas the routers register only the route through their children. Finally, leafs have no routing table. The maximum number of entries for each table is set to 30. Our simulation records twenty minutes of communications. In MT6D and Ephemeral, we choose to change the pseudonyms every 60s.

During the experiments, each node of the DODAG is monitored to register the dynamic evolution of the neighbor and routing tables. When the DODAG is established, while

the network remains static - no node joins, leaves nor moves - the two tables do not need to be updated.

B. Network performances

The impact of Ephemeral is compared to a scenario without pseudonym (no privacy) and to a network running MT6D. Two metrics are considered: the relative proportion of control frames sent to maintain the DODAG at each RPL instance and the amount of RPL control frames versus UDP frames.

To achieve this goal, both DIS, DIO and DAO RPL control frames are monitored in the whole network as well as the UDP frames sent by the nodes to perform the typical application scenario both for IR and IA communications.

Table II details the total number of control frames necessary for the network management (ICMPv6 frames) and the application frames used to send data (UDP frames).

In the worst case (Table II), MT6D increases by 49% the number of frames exchanged whereas it remains roughly stable using Ephemeral. This difference is due to the need for MT6D to reconstruct the neighbor and routing tables when the pseudonyms change, leading to extra control messages and energy. Ephemeral consumes less energy to compute the pseudonyms for each incoming/outcoming packet.

Experiment		UDP	ICMPv6	DIS	DIO	DAO
Reference	IR	951	376	5	135	236
	IA	1849	375	5	133	237
MT6D	IR	816	1163	85	355	723
	IA	1446	1120	81	351	688
Ephemeral	IR	952	358	5	133	220
	IA	1800	285	5	114	166

TABLE II
NB OF FRAMES IN 20 MIN

Indeed, the Fig. 4 shows the tradeoff between UDP application frames and RPL control frames used to maintain the routing tree within the network.

Regardless the type of communications, for the reference network, the UDP frames are more numerous than the ICMPv6 frames. The number of ICMPv6 frames is just about equal whatever the routing strategy. DIO and DAO frames represent the major number of ICMPv6 frames. The difference of the ratio observed between the two type of communication (roughly 72/28 IR against 83/17 IA) is provided by the increase of UDP frames for IA communications as shown in Table II. This factor is due to the application that consists, in IA communication, to request first identity to the node and results of an answer frame including the identity doubling the UDP traffic.

For Ephemeral, the network performances are closed to those of the reference experiment. The slight difference is due to the lack of queuing mechanism for the incoming packets in Contiki. In fact, the check of the pseudonyms by the receiver node leads to a computational timing during which incoming packets may be ignored introducing most packet lost. Nevertheless, the consumed energy ratio between UDP and ICMP frames is approximately the same for Ephemeral and the reference.

For MT6D, the Fig. 4 shows a significant loss of performance on the network efficiency compared to the reference whatever the routing strategy IR or IA. The number of RPL control frames is near the number of application frames, so 50% of the frames exchanged over the network is dedicated to the routing process. It has triple in comparison with the reference. This is due to the complete reconstruction of the DODAG at each pseudonym change. The ratio of DIO and DAO frames remains the same as for the reference experiment because the topology of the network remains the same. The network performances are disturbed and more power consumption is used to send control frames compared to the reference or Ephemeral even if the network is static.

Ephemeral does not add emitting nor receiving control frames compared to the reference. However, the frames include 2 additional bytes for the *cpt* and some DIO and DAO frames contain an R field of 14 or 15 bytes, which requires more energy to send over the air. This can be reduced by implementation optimization and also by the recording of several pseudonyms (previous, current and following). Due to the authorized drift δ, it will be necessary to record $2 * \delta + 1$ pseudonyms, each of 64-bits length. However, this latter solution pulls an overhead of data memory challenging in constrained devices. This feature is analyzed in the following and more especially the occupancy of the routing and neighbor tables.

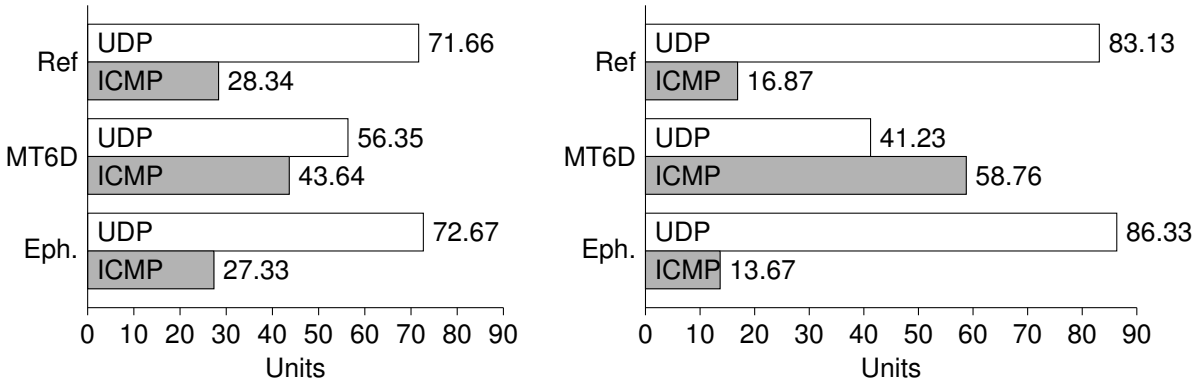
For a pseudonym update in MT6D, the addresses registered in the routing and neighbor tables are no more valid disabling the routing paths. At each pseudonym change, the neighbor table will grow with the addition of the new addresses. When the maximum of entries is reached, the oldest neighbor addresses are removed to leave the place to the new ones. The update of the routing table operates in the same way. So, the neighbor and routing tables are enlarged at each change of pseudonyms that occurs every 60s for our experiments, even when the network does not evolve which impact the memory size. Moreover, they contain numerous entries that are no longer in effect in the network.

For Ephemeral, the registration of the two tables has no impact and it works in the same way as in the reference.

Finally, an observation of MT6D scheme on a long period of time makes appear problems of de-synchronization between the nodes of the network. In fact, all the nodes of the network change their pseudonyms at the same time. But over time, there is a glitch of their relative internal clocks, increasing as consequence the amount of RPL control frames sent to update the routing paths. This participates to deteriorate the performances of the network efficiency because the time interval needed to update the pseudonyms of the addresses grows with time. Re-synchronization techniques should be used to circumvent this problem. Ephemeral does not need to be synchronized to allow the check of the pseudonyms.

VII. CONCLUSIONS

The novel scheme Ephemeral introduced in this paper to generate and manage pseudonyms of the MAC addresses in a



(a) IR communications

(b) IA communications

Fig. 4. ICMPv6 vs UDP frames

6LOWPAN WSN appears to be very efficient. While its impact on the network performance are negligible, it complicates notably the collection and the use of private information by an attacker.

It represents a real advance to ensure the anonymity of the messages in constrained networks as it improves by 16% the efficiency of MT6D, known to be the best scheme up to now, for the application message delivery. Moreover, Ephemeral consumes less energy.

Future work will focus on implementing Ephemeral in the technology OpenMote and to achieve a large scale deployment.

VIII. Acknowledgments

This research work was supported by the FP7 European projects SocIoTal under contract no. 609112.

References

[1] I. S. Association. Part 15.4: Low-rate wireless personal area networks (lr-wpans), 2006.

[2] I. S. Association. Part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 1: Mac sublayer, 2012.

[3] T. Aura. Cryptographically generated addresses (cga). 2005.

[4] E. D. Cristofaro, X. Ding, and G. Tsudik. Privacy-Preserving Querying in Sensor Networks. In *International Conference on Computer Communications and Networks, IEEE ICCCN 2009*, pages 1–6, San Francisco, CA, August 2009. IEEE.

[5] J. Granjal, E. Monteiro, and J. Sa Silva. Security for the internet of things: a survey of existing protocols and open research issues. *Communications Surveys & Tutorials, IEEE*, 17(3):1294–1312, 2015.

[6] S. Groat, M. Dunlop, W. Urbanksi, R. Marchany, and J. Tront. Using an ipv6 moving target defense to protect the smart grid. In *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, pages 1–7. IEEE, 2012.

[7] S. A. A. Hakeem, T. M. Barakat, and R. A. A. Seoud. New real evaluation study of rpl routing protocol based on cortex m3 nodes of iot-lab test bed. *Middle-East Journal of Scientific Research*, 23(8):1639–1651, 2015.

[8] C. Hennebert and J. Dos santos. Security protocols and privacy issues into 6lowpan stack: A synthesis. *IEEE Internet of Things Journal Issue OCTOBER 2014*, 1(16):1–15, 2014.

[9] J. Hiltunen and M. Valta. Design, implementation and experimental results of a wireless sensor network for underground metro station author (s) hiltu. 2014.

[10] R. Hinden. Ip version 6 addressing architecture. Technical report, RFC 2373, 1998.

[11] M. Hossen, A. Kabir, R. H. Khan, A. Azfar, et al. Interconnection between 802.15. 4 devices and ipv6: implications and existing approaches. *arXiv preprint arXiv:1002.1146*, 2010.

[12] J. Hui, D. Culler, and S. Chakrabarti. 6lowpan: Incorporating ieee 802.15. 4 into the ip architecture. *IPSO Alliance White Paper*, 3, 2009.

[13] T. Narten, R. Draves, and S. Krishnan. Privacy extensions for stateless address autoconfiguration in ipv6. 2007.

[14] T. Narten, S. Thomson, and T. Jinmei. Ipv6 stateless address autoconfiguration. 2007.

[15] N. Oualha, A. Olivereau, and A. Boudguiga. Pseudonymous communications in secure industrial wireless sensor networks. In *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on*, pages 98–102. IEEE, 2013.

[16] P. Pongle and G. Chavan. A survey: Attacks on rpl and 6lowpan in iot. In *Pervasive Computing (ICPC), 2015 International Conference on*, pages 1–6. IEEE, 2015.

[17] T. Preiss, M. Sherburne, R. Marchany, and J. Tront. Implementing dynamic address changes in contikios. In *International Conference on Information Society (i-Society), 2014*, pages 222–227. IEEE, 2014.

[18] H. Rafiee and C. Meinel. Ssas: A simple secure addressing scheme for ipv6 autoconfiguration. In *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on*, pages 275–282. IEEE, 2013.

[19] M. G. Sherburne. *Micro-Moving Target IPv6 Defense for 6LoWPAN and the Internet of Things*. PhD thesis, Virginia Tech, 2015.

[20] T. Tsvetkov. Rpl: Ipv6 routing protocol for low power and lossy networks. *Sensor Nodes–Operation, Network and Application (SN)*, 59:2, 2011.

[21] J. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, and C. Chauvenet. Rpl: The ip routing protocol designed for low power and lossy networks. *Internet Protocol for Smart Objects (IPSO) Alliance*, 36, 2011.

[22] L. Wallgren, S. Raza, and T. Voigt. Routing attacks and countermeasures in the rpl-based internet of things. *International Journal of Distributed Sensor Networks*, 2013, 2013.

[23] X. Wang and Y. Mu. Addressing and privacy support for 6lowpan. 2015.

[24] J. Westö and D. Björklund. The internet of things: An overview of enabling technologies for. 2014.

[25] E. Zenner. Nonce Generators and the Nonce Reset Problem. In *Information Security, 12th International Conference, ISC 2009*, volume 5735 of *Lecture Notes in Computer Science*, pages 411–426, Pisa, Italy, September 2009. Springer.