Secure and efficient routing protocol for low-power and lossy networks for IoT networks

Soukayna Riffi Boualam[1], Mariya Ouaissa[2], Mariyam Ouaissa[2], Abdellatif Ezzouhairi[1]
[1]Engineering, Systems and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco
[2] Departement of Computer Science, Moulay Ismail University, Meknes, Morocco

ABSTRACT

Routing protocol for low power and lossy (RPL) is destined to support the specific requirements of low power and lossy networks (LLN). This type of network suffers from the problem of determining and securing a routing protocol to best suit an environment. This article aims to present a new version of the efficient and secure RPL protocol. The proposed scheme consists of two parts: i) Proposing a new objective function (OF) based RPL which combines three nodes and links metrics are: expected retransmission number (ETX), hope count (HC), and the residual energy in order to have a precise decision to choose the optimal way to the destination. ii) To securing the new efficient RPL protocol by combining an improved Diffie-Hellman (DH) algorithm for a robust key exchange model with keyed-hash message authentication code (HMAC) to ensure the authentication and integrity of RPL data exchanged. To verify the level of security, we apply a formal verification using AVISPA tool which indicate that the secure and efficient RPL (SE-RPL) achieve all security requirements. Simulation results on the Contiki platform illustrate that our proposed is more efficient in terms of packet delivery ratio (PDR) and energy compared to others standard OF.

Corresponding Author:

Mariya Ouaissa
Moulay Ismail University
Marjane 2, BP: 298, Meknes 50050, Morocco
Email: mariya.ouaissa@edu.umi.ac.ma

1. INTRODUCTION

Many technological advancements in various industries have emerged with the rapid evolution of networks. They have resulted in new internet applications. These include, but are not limited to, miniaturization of hardware designs, embedded computing, and wireless communication technologies. The internet of things (IoT) [1] is a new paradigm in which real-world items incorporate measurements and actuators that are connected to the Internet. This emergence allows many elements implemented to make their data disposable on the online, as well as receive orders via the Internet. The usage of the Web's services and data enables for the development of new applications, thereby improving people's quality of life. This appears in the fields of e-health, smart cities, industrial applications [2].

Indeed, the internet of things ubiquitously integrates multiple computing devices used in different fields. These have different shapes and sizes. For this omnipresence to be a criterion present in the IoT network, interoperability, the ability of different technologies such as communication protocols, operating systems, hardware platforms, mobile and fixed nodes, to communicate, understand and react are key aspects that must be taken into account when innovating connected objects. This interoperability uses standard technologies as the main factor. IPv6 is a communication technology used for the internet [3]. IPv6 low

power wireless personal area networks (6LoWPAN) was thus able to pave the way for integrating the Internet into low-consumption and low-cost wireless devices [4].

Nowadays, IoT is regarded as the main component in our life. It is constructed with several intelligent objects that are cheap and very small gadgets. The appearance of low power and lossy network (LLN) [5] has many resources that are largely restricted in terms of cost, power, battery, memory, data processing capability and the transmission rate. Usually, the nodes, which are using in communication between the transmitter and the sink are characterized generally by low power, limited batteries and low transmission rate. To ensure communication between nodes, routing over low power and lossy (ROLL) working group has presented a new IPv6 routing protocol for LLN named routing protocol for low-power and lossy (RPL) that permits a good communication of these types of devices through the internet [6]. This latter opens the gates to many opportunities in different domains and applications, like smart cities, healthcare, industry, and automation. In addition, RPL is the source of interest of the industrials and scientific people; also, it is still under development and open to be developed even if it has good maturity [7], [8].

Due to their deployment in open environments, their limited resources; objects networks have to face many attacks. Without security measures, a malicious agent can launch several types of attacks that can harm the work of IoT networks and prevent their proper deployment purpose. Security is therefore an important dimension for these networks.

The main of this work, is firstly propose an efficient RPL protocol which focuses mainly on a new objective function (OF). It combines between three nodes and link metrics are expected retransmission number (ETX), hope count (HC), and remaining energy using fuzzy logic. The major aim of this new OF is to calculate the best way to transmit data to the sink taking into consideration energy conserving and the lifetime of the network. This combination permit to find solutions and overcome some limitation of application. The second phase is to secure this new efficient RPL protocol to ensure the authentication and integrity of data, where each node want to communicate with another must have a shared secret key. This key calculated by a new enhanced Diffie-Hellman (DH) algorithm will be exploited by the Keyed-Hash message authentication code (HMAC).

The remainder of this paper is organized as shown in: the next section presents the background includes an overview of RPL protocol. Section 3 discuss the security requirements and aspects of RPL. Section 4 studies the main methods cryptographic utilized in our scheme. In section 5, we present a secure and efficient RPL protocol. In section 6, the security of the protocol and the simulation results are checked and evaluated. Ultimately, we draw our conclusion in section 7.

2.   BACKGROUND
2.1. RPL routing protocol
The internet of things (IoT) results in the deployment of lossy and low-power networks called LLN networks. These networks allow many on-board devices such as sensors to be able to communicate with each other. A routing protocol called RPL has been specially designed by the internet engineering task force (IETF) to meet the specific constraints imposed by this type of network. However, this protocol remains exposed to numerous security attacks. The RPL protocol is a distance vector routing protocol using IPv6, specially designed by the IETF to meet the needs of LLN networks [9].

RPL is a proactive protocol based on a distance vector algorithm, it is designed to detect and react to routing loops. Distance vector protocols make it possible to operate with a minimum of resources. Indeed, the routing information to be stored corresponds only to the neighbourhood, unlike link-state protocols which require knowing the characteristics of the links of all the nodes of the network.

2.2. DAG and DODAG structure
RPL is a routing protocol including a network structuring algorithm. The topology created by RPL is a directed acyclic graph (DAG). The DAG describes a tree structure specifying the default pathway between the nodes of the LLN. Nevertheless, a DAG structure is more than a typical tree in the sense that a node can be associated with multiple parents in the DAG.

The goal of this topology is to provide efficient and reliable routing of any network point to the root of the DAG [10]. The RPL protocol organizes the nodes in the form of direction-oriented directed acyclic graph (DODAG). That is to say a directed graph towards a destination which is the root of the network (only one parent is authorized) as illustrated in Figure 1 each DODAG has a version number.
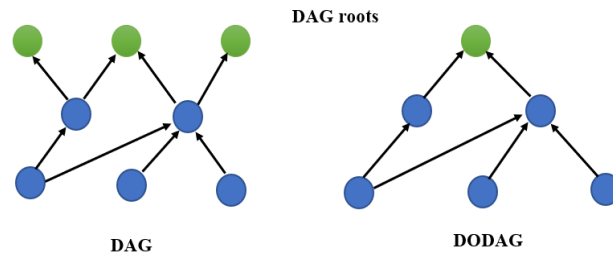
Figure 1. DAG and DODAG Structure

2.3. Objective function

RPL protocol permit to create a route to the root based on the goal function. Due to this, the objective function is examined as the principal factor to establish, in the network, the preferred parent of the neighbor candidate node. A node can have more than one particular parent in a network with huge density. For this, the Goal function tries to select which parent is suitable for a node than others. Furthermore, the parent choice by the objective function is based on one or more specific criteria which are metrics. These metrics can be specified by the designer according to his needs. So far, the ROLL working group has specified two OFs [11]:

- OF0: objective function zero (OF0), here the routing metric adopted is the number of hops. OF0 is designed to authorize interoperability between differing implementations of RPL [12].
- Minimum rank hysteresis objective function (MRHOF): the metric used by MRHOF is determined in the DIO's metric container. Most often it is the expected retransmission number (ETX) [13] that is used with hysteresis to avoid small rank differences. This metric permits RPL to find stable paths from nodes to a root. In the absence of a metric in the DODAG information object (DIO) metric container, MRHOF defaults to ETX [14].

2.3.1. Inference system used by fuzzy logic

The reasoning system using fuzzy logic transforms multiple input metrics into a single output value. To apply fuzzy logic, we perform in three steps: a first step is fuzzification. It is followed by a step which contains two phases: inference and aggregation. And finally, we end with the defuzzification step [15], [16]. For the sake of simplicity and efficiency, we use the fuzzy inference model called Mamdani. It uses basic arithmetic operations like maximum and minimum such as combination and aggregate operators [17].

2.4.2. Fuzzification

The first phase of the control system that uses fuzzy logic is fuzzification. The idea is to determine the level of belonging (on a scale from 0 to 1) of the scalar input to the different fuzzy sets of the linguistic variable considered. It involves the following functions:

- Retrieve the measured scalar values of the linguistic variable as input.
- Define the correspondence functions or membership functions transforming the input scalar data into elements of the universe of speech (also called fuzzy sets).
- Carry out the fuzzification function which calculates, for each value of the linguistic variable, its degree of belonging to fuzzy sets.

3.   SECURITY ASPECTS OF RPL
3.1. Existing protection mechanisms in RPL

RPL integrates different mechanisms to avoid loops, detect inconsistencies and repair the graph. The rank plays an important role in constructing a loop-free topology. Indeed, a node can only choose a parent whose rank is lower than its own, in other words all the nodes found in the sub-DODAG of a node have a rank higher than this node. If a node does not respect this rank property, the graph is no longer acyclic. Moreover, to avoid loops, if a node has to change its rank, it must use a mechanism of poisoning or disconnection

In cases where loops appear in the graph, the RPL protocol provides a feature called data path validation. Control information is carried in data packets via flags placed in the IPv6 Hop-By-Hop extension header. Two main repair mechanisms are used in RPL networks in case of inconsistencies or failures: local and global repair. Local repair consists of finding an alternative path to route the packets. For example, when

the communication with the preferred parent is broken, a node can choose another parent to forward its packets. If no other parent is available, it can also send packets to a sibling, i.e., a node of the same rank. If the local repairs are not sufficient, the root can initiate a global repair, i.e. the complete reconstruction of the graph by incrementing the version number of the DODAG.

Regarding security, RPL offers two security modes. The first is called "pre-installed" mode and consists of encrypting messages using keys pre-installed on the nodes. The second, the authenticated mode, works like the previous mode. However, if a node wants to participate as a router it should acquire another key from an authenticated authority. With the pre-installed key, a node can only participate as a leaf in the graph. However, the standard does not define how to concretely implement these two security modes, in what context to select them, or how key management takes place [18].

3.2. Taxonomy of attacks against the RPL protocol

The different attacks targeting the RPL protocol were classified according to whether they primarily threatened node resources, network topology and traffic as shown in Figure 2. The attacks of the first category aim to consume the energy, the memory or the calculation time of the nodes. Attacks in the second category target the network topology. While the last category concerns attacks targeting traffic [19].
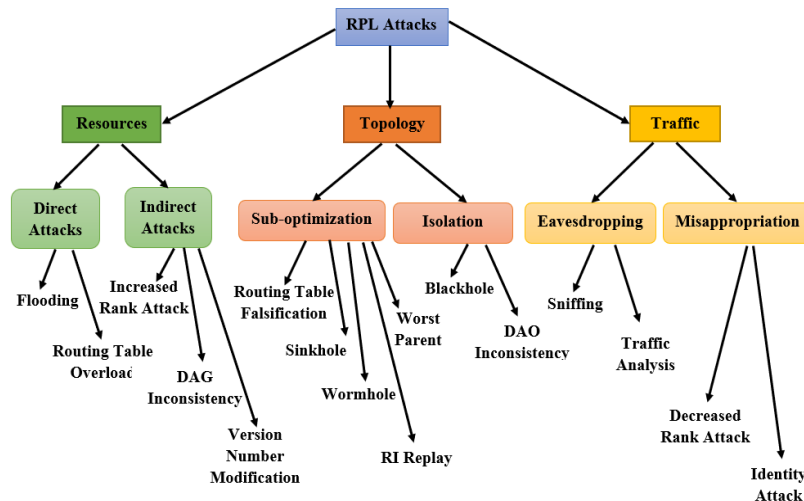

Figure 2. Taxonomy of attacks against the RPL protocol

4. PRELIMINARIES
4.1. Diffie-hellman key exchange protocol

The Diffie-Hillman algorithm is a new encryption method based on the use of a secret key between two entities. This method is called the public key approach. The latter makes it possible to remedy the problems of key exchange encountered by symmetric key methods. The Diffie-Hillman method permits two participants A and B to get and share a single confidential key, by proceeding as shown in: The two participants publicly agree on the Diffie Hillman parameters, g (the generator > 2) and p ($<< g$), p and g are prime numbers [20]. Here is how the exchange takes place (schematically). The calculations shown are made in the group G, so in our example modulo p. Diffie Hellman key exchange procedure shown in Figure 3.
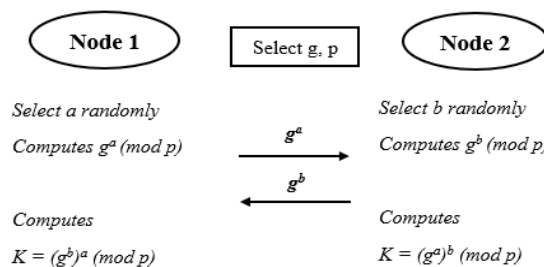

Figure 3. Diffie-Hellman key exchange protocol

4.2. Message authentication code (MAC)

A message authentication code (MAC) is a mechanism which mainly ensures and reinforces the authentication of the messages exchanged. Its role is to accompany the messages during their transmission phase in order to ensure their integrity, by making it possible to check whether they have undergone any modification. The implementation of this mechanism is based on the use of the secret key and on functions similar to those of hash [21].

To calculate the message authentication code, there are some existing algorithms in literature. These algorithms can be classified in three categories:
- Hash-based MAC (HMAC): based on hashing algorithms
- Cipher-based MAC (CMAC).: based on symmetric ciphers
- High-performance block cipher-based MAC (VMAC).

To choose the most suitable MAC algorithm in term of execution time, we implemented and ran some ones on Intel Core 2 1.83 GHz Processor under Windows environment based on Crypto++ Library (Table 1).

Table 1. Execution time of MAC algorithms

Symmetric Algorithms	HMAC	CMAC	VMAC
Execution Time (µs)	0.509	0.600	3.738

4.3. Advanced encryption standard (AES)

AES is a standard and symmetric algorithm based block cipher used to protect sensitive data. Unlike the majority of asymmetric encryption algorithms whose security relies on difficult mathematical problems such as the discrete alogarithm in the case of Elliptic-curve cryptography (ECC), or the integer factorization in the case of RSA, AES derives its strength from the combination between permutation and substitution, more commonly known as substitution permutation networks (SPN), we can say that the AES itself is a difficult problem, because many qualified people tried to break the AES encryption and failed. The key length in AES can be 128, 192, or 256 bits [22]. To justify the use of AES algorithm like a cryptographic method in our solution, we compare and implement it with other symmetric algorithms namely data encryption standard (DES) and Blowfish in term of execution time. Table 2 illustrates the measurements of test running on a Pentium 4 2.1 GHz processor under Windows using Crypto++ Library [23] with 128 bits is a size of keys.

Table 2. Execution time of symmetric algorithms

Symmetric algorithms	AES	DES	Blowfish
Execution time (µs)	2.196	5.998	3.976

5.   PROPOSED SCHEME

The scheme we propose in this work is named the secure and efficient RPL (SE-RPL) protocol. The scheme is a combination, between the two models. The first model is an efficient version of the RPL routing protocol based on fuzzy logic. The second model is the security of our enhanced protocol based on enhanced cryptographic methods.

5.1. Enhanced and efficient version of RPL

In this paper, we define a new OF based on three metrics combined using fuzzy logic which allows to work on imprecise notions (intermediaries between TRUE and FALSE), approximate or uncertain knowledge. In comparison with classical logic, it adds the possibility of calculating a parameter, by simply saying to what extent it must be in such or such zone of value.

The metrics used are links and nodes, they are presented as shown in Figure 4:
- The number of hops between a node and the sink (HC).
- The number of expected retransmission (ETX).
- Residual energy.

We demonstrate the membership function related to each parameter that will be considered in our objective function as it is shown in Figure 5. In our study, firstly, we combine HC and ETX to have a view on QoS, then we add residual energy to QoS aiming to maximize the lifetime of the network and choose the route with the best quality using fuzzification.
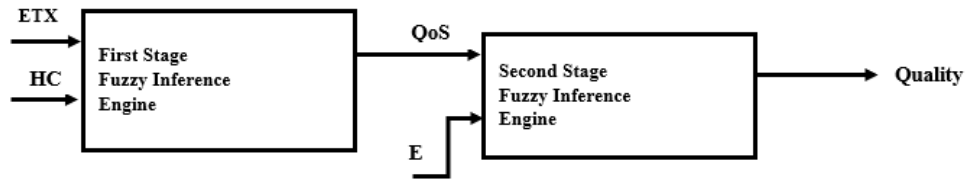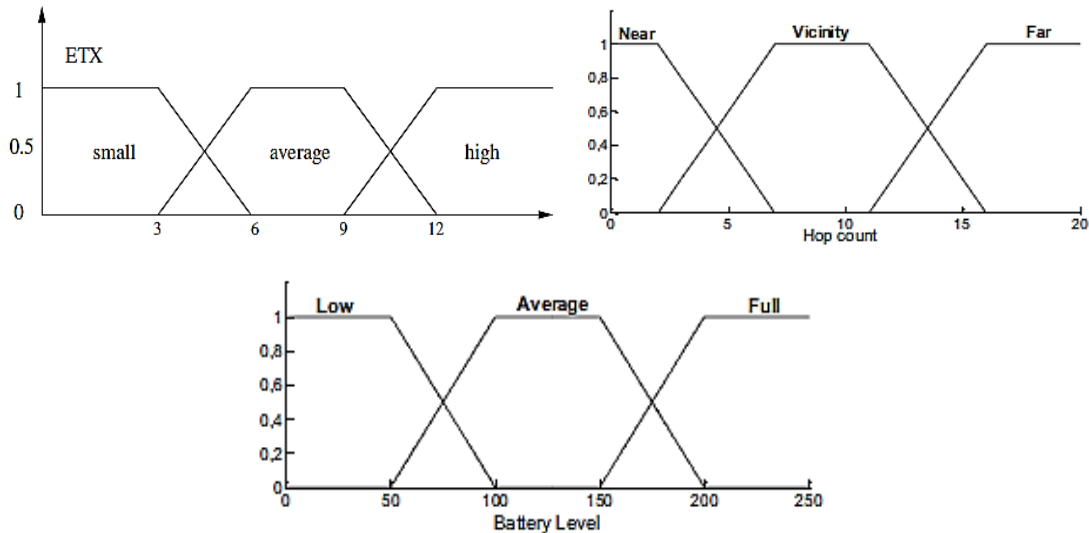
Figure 4. Fuzzy inference engine

Figure 5. Membership functions of ETX, battery level and HC

5.2. Secure efficient RPL

To secure the keys exchanged between nodes and RPL packet during our new efficient RPL protocol, we will ensure the verification of all nodes identities and also the optimal route of all transfer of data. In following points, we will explain the main steps of our model:

- Establishment of secret keys: the idea behind this step is to generate a secret key that will be used during the exchange of data in the next steps. The standard DH algorithm faced several challenges during the communication specially man in the middle (MITM) attack. In this context we propose an enhanced DH algorithm of our solution to guarantee the level of security, that is based on commitment scheme to afront the existing attacks presented in DH algorithm (Figure 6). In an effort to resist attacks in the DH algorithm, the enhanced Diffie-Hellman algorithm is based on a commitment scheme. A commitment scheme is an important cryptographic primitive that allows for the formation of blocks. This scheme enables an individual user to commit an allocated value or message with the capability of eventually revealing the committed message or value while remaining invisible to other users. A commitment scheme is described by the two functions commit and open. We supposed that Node1 and Node2 choose the following parameters: G, g, p. Where G is a finite cyclic group, g is a generator in G, and p is a large prime number. The two nodes select randomly their secret exponents X_a and X_b, compute DH public parameters g^{Xa} and g^{Xb} respectively and generate random values N_a and N_b. The Node1 and Node2 calculate the messages m_a and m_b, in order to prepare the commitment/opening pair (C_a, D_a). Then both the nodes generate verification strings S_a and S_b, if they are match, Node1 and Node2 accept each other's DH-parameters g^{Xa} and g^{Xb} as being authentic and unchanged. Then, they both generate shared key K.
- Application of hash function based MAC: the objective of this step is to ensure the authentication and integrity of data transferred by using the HMAC-SHA256 function base secret key generated by DH improved. In general, the HMAC value is determined using MD5 and SHA-1 cryptographic hash functions.
- Encryption using AES algorithm: In addition to authentication and integrity, our scheme can ensure also the confidentiality by encrypted the data sent combined with the message authentication code (MAC) generated in second step using the secret key generated in first step (Figure 7).
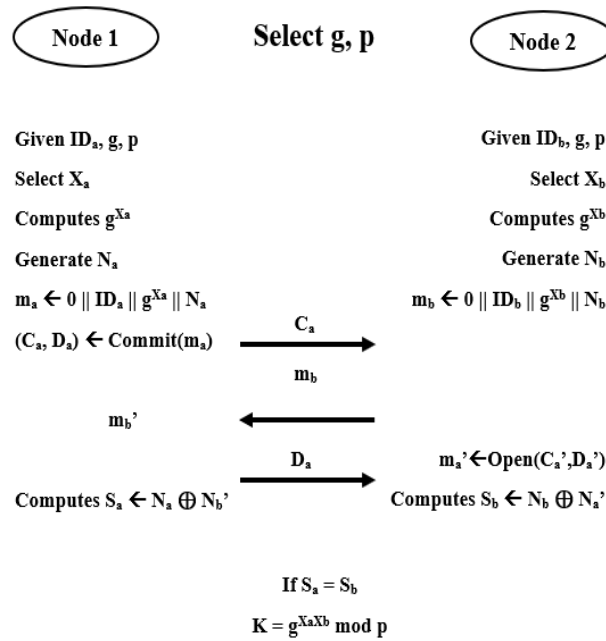
Node 1   **Select g, p**   Node 2

Given ID_a, g, p   Given ID_b, g, p

Select X_a Select X_b

Computes g^{Xa} Computes g^{Xb}

Generate N_a Generate N_b

$m_a \leftarrow 0 \parallel ID_a \parallel g^{Xa} \parallel N_a$ $m_b \leftarrow 0 \parallel ID_b \parallel g^{Xb} \parallel N_b$

$(C_a, D_a) \leftarrow Commit(m_a)$ $\xrightarrow{\quad C_a \quad}$

$\xrightarrow{\quad m_b \quad}$

$m_b' \quad \xleftarrow{\qquad\qquad}$

$\xrightarrow{\quad D_a \quad}$ $m_a' \leftarrow Open(C_a', D_a')$

Computes $S_a \leftarrow N_a \oplus N_b'$ Computes $S_b \leftarrow N_b \oplus N_a'$

If $S_a = S_b$

$K = g^{XaXb} \bmod p$

Figure 6. Enhanced Diffie-Hellman protocol
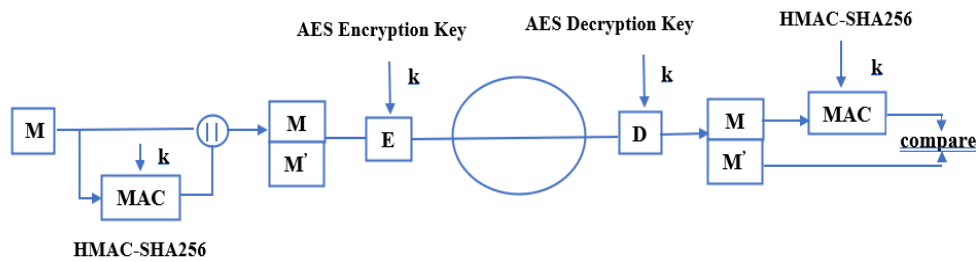
Figure 7. Hash based-MAC and encryption

6. RESULTS AND DISCUSSION

6.1. Security analysis

We used the automatic validation of internet security protocols and applications (AVISPA) tool [24] to provide a formal modular and expressive language to specify the security properties of protocols. The tool contains a set of back-end used which uses a variety of automatic machine analysis techniques. The AVISPA tool uses the Dolev-Yao intrusion model where the attacker can spy on all transmitted messages, usurp the identity of a legitimate entity (attack by identity theft) and modify or inject messages, but he considers that the cryptography is perfect, i.e. the attacker cannot break the cryptography.

Our proposed protocol aims the ensure a high security level of the secret key exchanged between IoT nodes. Using AVISPA tool, we test the proposed solution under the two backends on-the-fly model checker (OFMC) and constraint-logic-based attack searcher (CLATSE) in order to demonstrate that integrity and authentication objectives will be ensured with success against different attacks, namely DoS, replay and secrecy attacks. Figures 8 and 9. show the results checking in AVSIPA.

6.2. Simulation results

In this paper, we will study some OFs used in the RPL protocol. We will use Cooja Simulator [25], [26] running on the Contiki operating system (version 2.7). We will evaluate the performances of our new OF by comparing it with other OF, the interference range is 100 m, the number of nodes varies between 0 and 60 which are called Tmote Sky with random positions (Table 3). We implement our scheme under two attacks: i) Sinkhole attack, in this type of attack, the intruder tries to attract as many paths as possible to him, allowing him to control most of the data circulating in the network. ii) Blackhole attack, in which a dishonest

node tries to present itself in the network. The objective of the attack is the tampering of the neighbourhood to affect the operation of the routing, or exploitation or getting more resources.

- Packet delivered ratio: We have varied the number of nodes from 0 to 60, in order to measure the packet delivery ratio (PDR) that mean the packets delivered with success according to the number of packets sent in a malicious environment. The simulation results in In Figure 10 show that our proposed SE-RPL offers the better PDR compared to other RPL based OF0 and MRHOF, this is due that our protocol uses an OF combined three metrics namely ETX, HC and energy in order to select the best secure link to transfer reliability data

- The lifetime of the network: We monitor the energy consumption of the nodes to demonstrate the lifetime of our network. In this context, we choose to simulate 20 nodes in a malicious environment for RPL based different type of OF and our solution SE-RPL. The Figure 11 illustrates that the two RPL based OF0 and MRHOF respectively give a less consumed energy compared to our proposal this is due that these standard protocols use only one metric. In other hand, we notice that our secure RPL consumes more energy due to the calculations carried out which takes more time to find the optimal route. We can say that the consumption of more energy will affect the survival of the network but not the failure of the nodes.

Figure 8. Results reported by the OFMC back-end

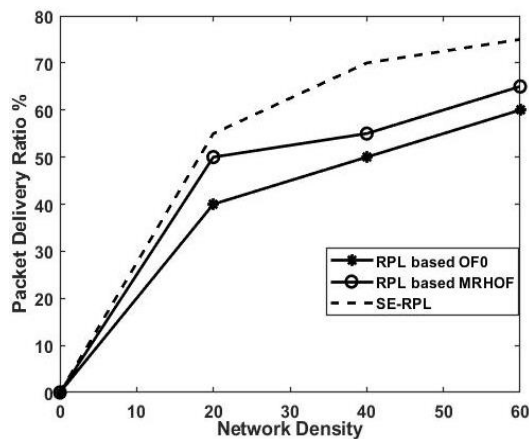Figure 9. Results reported by the CL-AtSe back-end

Figure 10. Packet delivery ratio vs. network density
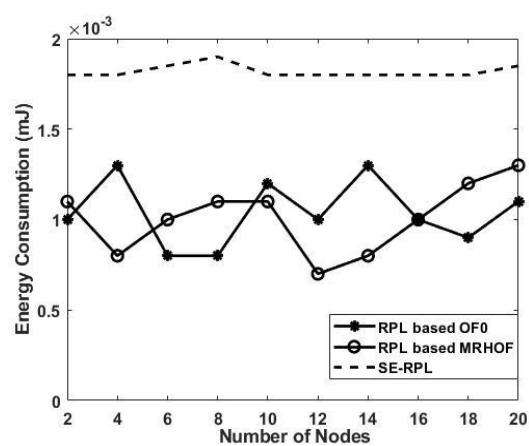
Figure 11. Energy consumption vs. number of nodes

Table 3. Simulation parameters

Parameters	Value
Number OF nodes	From 0 to 60
Emulated nodes	Tmote Sky
Deployment type	Random position
Interference range	100 m
Total simulation time	2J

7. CONCLUSION

Nowadays, IoT technology is becoming very grounded and in the next coming years, most of the objects in daily life will be connected to each other and to the Internet. The RPL routing protocol is driven by the need to support infrastructure such as agricultural field and home network applications. However, there are still many problems to solve in this protocol in order to be able to use them in real conditions, among the problems that can be encountered in this kind of protocols we cite the problem of choosing the optimal route for the transfer of packets as well as security. In this paper, we propose a secured and efficient version pf RPL protocol. In this paper, we have proposed a secure and efficient version of RPL protocol that consist to propose new OF based RPL in order to have a precise decision to select the optimal paths to the destination, and to secure this new proposition to ensure the authentication and integrity of RPL data exchanged. According to the security analysis based formal verification, it can be seen that SE-RPL achieved the design goals of the system and ensure reliable security. Simulation results on the Contiki platform illustrated that our secured proposed is more efficient in terms of PDR and energy compared to others standard OF.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
[2] M. Ouaissa, A. Rhattoy, and I. Chana, "New security level of authentication and key agreement protocol for the IoT on LTE mobile networks," in *Proceedings - 2018 International Conference on Wireless Networks and Mobile Communications, WINCOM 2018*, Oct. 2019, pp. 1–6, doi: 10.1109/WINCOM.2018.8629767.
[3] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC 4944," *Network Working Group*, Sep. 2007. doi: 10.17487/rfc4944.
[4] M. Ouaissa, M. Ouaissa, and A. Rhattoy, "An efficient and secure authentication and key agreement protocol of LTE mobile network for an IoT system," *International Journal of Intelligent Engineering and Systems*, vol. 12, no. 4, pp. 212–222, Aug. 2019, doi: 10.22266/ijies2019.0831.20.
[5] O. Gaddour, A. Koubaa, R. Rangarajan, O. Cheikhrouhou, E. Tovar, and M. Abid, "Co-RPL: RPL routing for mobile low power wireless sensor networks using Corona mechanism," in *Proceedings of the 9th IEEE International Symposium on Industrial Embedded Systems, SIES 2014*, Jun. 2014, pp. 200–209, doi: 10.1109/SIES.2014.6871205.
[6] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: A Review," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 5952–5967, Aug. 2019, doi: 10.1109/JSEN.2019.2910881.
[7] T. Watteyne, K. Pister, D. Barthel, M. Dohler, and I. Auge-Blum, "Implementation of gradient routing in wireless sensor networks," in *GLOBECOM - IEEE Global Telecommunications Conference*, Nov. 2009, pp. 1–6, doi: 10.1109/GLOCOM.2009.5425543.
[8] N. Accettura, L. A. Grieco, G. Boggia, and P. Camarda, "Performance analysis of the RPL Routing Protocol," in *2011 IEEE International Conference on Mechatronics, ICM 2011 - Proceedings*, Apr. 2011, pp. 767–772, doi: 10.1109/ICMECH.2011.5971218.
[9] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, "Proposing a secure RPL based internet of things routing protocol: A review," *Ad Hoc Networks*, vol. 101, p. 102096, Apr. 2020, doi: 10.1016/j.adhoc.2020.102096.
[10] A. J. H. Witwit and A. K. Idrees, "A comprehensive review for rpl routing protocol in low power and lossy networks," in *Communications in Computer and Information Science*, vol. 938, 2018, pp. 50–66.
[11] A. Paul and A. S. Pillai, "A review on RPL objective function improvements for IoT applications," in *ACCESS 2021 - Proceedings of 2021 2nd International Conference on Advances in Computing, Communication, Embedded and Secure Systems*, Sep. 2021, pp. 80–85, doi: 10.1109/ACCESS51619.2021.9563294.
[12] P. Thubert, "RFC 6552 - Objective Function zero for the routing protocol for low-power and lossy networks (RPL)," *Internet Requests for Comments*, 2012. [Online]. Available: http://www.rfc-editor.org/info/rfc6552.
[13] P. Levis and O. Gnawali, "The ETX objective function for RPL," *Internet-Draft, Networking Working*, 2010. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-gnawali-roll-etxof-01.
[14] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th annual international conference on Mobile computing and networking - MobiCom '03*, 2003, p. 134, doi: 10.1145/938985.939000.
[15] O. Gaddour, A. Koubâa, and M. Abid, "Quality-of-service aware routing for static and mobile IPv6-based low-power and lossy sensor networks using RPL," *Ad Hoc Networks*, vol. 33, pp. 233–256, Oct. 2015, doi: 10.1016/j.adhoc.2015.05.009.
[16] P. O. Kamgueu *et al.*, "Energy-based routing metric for RPL," *[Research Report] RR-8208, INRIA*, 2013. [Online]. Available: https://hal.inria.fr/hal-00779519.
[17] P. O. Kamgueu, E. Nataf, and T. N. Djotio, "On design and deployment of fuzzy-based metric for routing in low-power and lossy networks," in *Proceedings - Conference on Local Computer Networks, LCN*, Oct. 2015, vol. 2015-December, pp. 789–795, doi: 10.1109/LCNW.2015.7365929.
[18] K. Avila, D. Jabba, and J. Gomez, "A nonlinear robust sliding mode controller with auxiliary dynamic system for the hovering flight of a tilt tri-rotor UAV," *Applied Sciences (Switzerland)*, vol. 10, no. 18, p. 6472, Sep. 2020, doi: 10.3390/APP10186472.
[19] S. Mangelkar, S. N. Dhage, and A. V. Nimkar, "A comparative study on RPL attacks and security solutions," in *Proceedings of 2017 International Conference on Intelligent Computing and Control, I2C2 2017*, Jun. 2018, vol. 2018-January, pp. 1–6, doi: 10.1109/I2C2.2017.8321851.
[20] W. Diffie, W. Diffie, and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.
[21] B. Preneel and P. C. Van Oorschot, "On the security of iterated message authentication codes," *IEEE Transactions on Information Theory*, vol. 45, no. 1, pp. 188–199, 1999, doi: 10.1109/18.746787.
[22] S. Heron, "Advanced encryption standard (AES)," *Network Security*, vol. 2009, no. 12, pp. 8–12, Dec. 2009, doi: 10.1016/S1353-4858(10)70006-4.

[23]   Q. Guo, Z. Ke, S. Wang, and S. Zheng, "Persistent Fault Analysis against SM4 Implementations in Libraries Crypto++ and GMSSL," *IEEE Access*, vol. 9, pp. 63636–63645, 2021, doi: 10.1109/ACCESS.2021.3074708.
[24]   L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, no. 1 SPEC. ISS., pp. 61–86, May 2006, doi: 10.1016/j.entcs.2005.11.052.
[25]   M. Kovatsch, S. Duquennoy, and A. Dunkels, "A low-power CoAP for Contiki," in *Proceedings - 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS 2011*, Oct. 2011, pp. 855–860, doi: 10.1109/MASS.2011.100.
[26]   F. Osterlind and A. Dunkels, "Contiki COOJA Hands-on Crash Course: Session Notes," *Swedish Institute of Computer Science*, pp.1-14, 2009.

BIOGRAPHIES OF AUTHORS

Soukayna Riffi Boualam 🆔 🔍 SC P is currently a Professor at Specialized Institute of Applied Technology. She received her engineer's degree in Network and Telecommunications in 2016. She is currently a PhD student at ENSA, Sidi Mphammed Ben Abdallah University Fez, Morocco. Her research interests include Network, Telecommunications, Internet of Things and Routing Protocols. She can be contacted at email: riffisoukayna2@gmail.com.

Dr. Mariya Ouaissa 🆔 🔍 SC P is currently a Professor at Institute Specializing in New Information and Communication Technologies, Researcher Associate and practitioner with industry and academic experience. She is a Ph.D. graduated in 2019 in Computer Science and Networks, at the Laboratory of Modelisation of Mathematics and Computer Science from ENSAM-Moulay Ismail University, Meknes, Morocco. She is a Networks and Telecoms Engineer, graduated in 2013 from National School of Applied Sciences Khouribga, Morocco. Dr. Ouaissa has made contributions in the fields of information security and privacy, Internet of Things security, and wireless and constrained networks security. Her main research topics are IoT, M2M, D2D, WSN, Cellular Networks, and Vehicular Networks. She has published over 20 papers (book chapters, international journals, and conferences/workshops), 8 edited books, and 5 special issue as guest editor. She can be contacted at email: mariya.ouaissa@edu.umi.ac.ma.

Dr. Mariyam Ouaissa 🆔 🔍 SC P Mariyam Ouaissa is a Professor/Trainer and Researcher Associate. She is a Ph.D. in Computer Science and Networks graduated in 2019, at the Laboratory of Modelisation of Mathematics and Computer Science, from Moulay Ismail University, ENSAM, Meknes, Morocco. She is a Networks and Telecoms Engineer, graduated in 2013 from National School of Applied Sciences Khouribga. Her main research topics are IoT, M2M, WSN, Vehicular Networks, Cellular Networks. She is mainly working on M2M congestion overload problem, security and the resource allocation management. She has published more than 20 research papers. She is a Editor in several books (Springer, De Gruyter, RGN Publications) and Guest Editor in several special issues of journals (IGI Global, River Publishers, EAI Publisher, RGN Publications). She can be contacted at email: mariyam.ouaissa@edu.umi.ac.ma.

Prof. Dr. Abdellatif Ezzouhairi 🆔 🔍 SC P received the M.Sc and the PhD degrees in Mobile computing from Ecole Polytechnique Montreal Canada. He worked as an adjunct researcher at the Mobile Computing and Networking Research Laboratory (LARIM) Chair Ericsson Canada. He is now a Professor at ENSA Fez Morocco. His interests: NGN integration, mobility and sensor/MANET. He can be contacted at email: abdellatif.ezzouhairi@polymtl.ca.