Journal of Theoretical and Applied Information Technology
31st March 2015. Vol.73 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# SYMMETRIC CRYPTOGRAPHY KEYS MANAGEMENT FOR 6LOWPAN NETWORKS

[1]ANASS RGHIOUI, [2]RIAD ABDMEZIEM, [3]SAID BOUCHKAREN, [1]MOHAMED BOUHORMA
[1]LIST, Faculty of Science and Technology of Tangier, Abdelmalek Essaadi University, Morocco
[2] LSI, University of Science and Technology, Algiers, Algeria
[3] LabTIC, Laboratory of Technology of Information and Communication, Morocco
E-mail: [1] rghioui.anass-etu@uae.ac.ma

**ABSTRACT**

Thanks to the 6LoWPAN (IPv6 over Low power Wireless Personal Area Network) technology, each object will get the opportunity to obtain an IPv6 address and integrate the world of the Internet of Things. This provides the ability to collect and monitor data remotely.

Objects are heterogeneous; they vary depending on their operation, their material resources, and their role: data server, data requester or both. They are deployed everywhere and the information communicated via the internet between two separate objects is not secure and is vulnerable to an eavesdropping or modification attacks. We must implement an end-to-end security system to protect exchanged data confidentiality and integrity. Efficient used systems are based on asymmetric cryptography, but since these objects are resource-constrained and low power energy, it is not practical to adopt such solutions.

Thus, 6LoWPAN combines between two different networks: LoWPANs and IPv6, we need a solution that addresses the security of internal communications and those across the internet. Existing solutions address the security of each type of communication separately from each other, where we must implement multiple solutions to secure a single network, the thing that is not practical for networks with resource constraints.

In this paper, we propose a hybrid solution suitable for 6LoWPAN networks, based on the use of a remote server for authentication and security keys management, which aim to secure inter-LoWPAN and end-to-end communications. Our simulations and performance analysis shows that our solution provides security, and it is efficient in computation, communication, and storage.

**Keywords:** *6LoWPAN, IoT, KMS, Network security, AVISPA.*

## 1. INTRODUCTION

With the immense and rapid development of the Internet of Things (IoT) [1], integrating different devices to the internet becomes an indispensable need. Communication interaction transforms from human-to-human (H2H) to machine-to-machine (M2M) [2].

In practice, this technology progress facilitates the leading of smart cities [3], where different cohabited object can communicate and interact to decide instead of human, or to help managers to make decisions that are more effective. It supports the improvement on many life applications like logistic, healthcare, industry ... etc. Mainly for monitoring requirement where we must use sensors devices to capture data in physical or environmental conditions.

Enabling resource-constrained devices to connect to the internet by implementing them by IPv6 protocol, gives the possibility to transfer data to any location in the entire world. The IETF 6LoWPAN work group introduced the specifications to use IPv6 through the IEEE 802.15.4 in the two RFCs 4919 [4] and 4944 [5]. The idea of 6LoWPAN is to combine between the IPv6 networks and IEEE 802.15.4 networks by adding an adaptation layer that optimizes IPv6 packets (1280 bytes) through fragmentation and assemblies to be supported by the 802.15.4 link layer (128 bytes).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The choice of the IPv6 technology has many benefits, this solution allows the use of existing network infrastructure, also, 6LoWPAN devices can be connected easily to other IP networks without the need for translation gateways or proxies.

IPv6 is a strategic choice too; it provides the addressing of a huge number of devices since an IPv6 address is 128 bits long, this provides 3.4 $10^{38}$ addresses, more than 667 million billion addresses per square millimeter of land surface.

A 6LoWPAN is composed of one or a set of local LoWPAN formed by a set of nodes that are characterized by short radio range, low data rate, low power and low cost. These resource-constrained nodes have the ability to connect to the internet by the IPv6 through a local edge router, which communicates through a common backbone such as a transit link to translate packets through the LoWPAN to hosts from the Internet.

Because of routing issues in 6LoWPAN, another team was created, IETF-ROLL (Routing over Low-power and Lossy Network) working group, to seek a proper routing solution to this kind of networks.

The IETF-ROLL work group proposes the routing protocol RPL (Routing Protocol for Low power and lossy networks) [7], it is based on the distance vector routing algorithm, which operates according that each router has a routing table indicating, for each destination network, the local interface to reach it via the best available distance.

RPL based on the concept of the DAG (Direct Acyclic Graph) to avoid the loops formation in the tree constructed by the distance vector algorithm. With the ability to have multiple paths back to the same destination and possess alternative routes whenever default routes are inaccessible.

Inasmuch as the Internet of Things is based on an open architecture [6], and the weaker characteristics of resource-constrained devices, security issues becomes more sensitive. Another issue is that different and heterogeneous objects will be connected together, objects with powerful resources and other with very limited resources, so the security solution must be suitable for all connected devices.

Symmetric cryptography is the most suitable security solution as it does not require many resources and does not consume a lot of energy, but its problem persists in choosing the right method of security keys management. Especially in this kind of network that lacks infrastructure and gathers a set of heterogeneous devices. Unfortunately, most of existing solution deal only with local resource-constrained nodes networks and does not provide an end-to-end security.

6LoWPAN combines two different networks: LoWPAN and IPv6. There are security solutions suitable for each of the two types, but the solutions that deal with LoWPAN networks treated as an isolated network and manages only the communications between nodes inside the LoWPAN, and does not handle communication between a node and a remote IP-host. Regarding communications through the internet in the end-to-end mode, there is adapted solutions from existing protocols for devices with resource constraints, but they only treat the end-to-end communications between two separated devices and does not deal with inter-LoWPAN communications.

Since 6LoWPAN network has the low-power as main characteristic. The use of multiple protocols at once consumes more energy and occupies more storage and memory space.

In this paper, we propose a security key management scheme that depends on the control of a Remote Server and it is based on the internal device key generation to avoid sharing keys in the network. Simulation results show that our solution is energy efficient.

The structure of the paper is as follows: Section 2 gives a brief security review of the 6LoWPAN; Section 3 presents the proposed security solution. Section 4 and 5 analyses and discusses the simulation results. Finally, Section 6 concludes the paper and gives some perspectives.

## 2. 6LOWPAN SECURITY REVIEW

The cryptography solution ensures confidentiality, authentication and integrity of exchanged messages. By encrypting the data, no one can understand the message contents without mechanisms to decrypt it.

Applying cryptography in 6LoWPAN networks must take into consideration characteristics and constraints of devices implementing this technology, such as low power battery, low storage ability and low computing capacity, to optimize resources and provide to nodes longer life lasting.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Even if efficient key management systems exist in today's internet, but their underlying cryptographic algorithms are either too heavy to run on resource-constrained nodes, or do not provide a satisfactory security level.

Several recommendations [1], [4], [7]–[9] propose the use of key management protocols based on symmetric shared keys instead of the asymmetric for such limited resources networks since its operation does not consume a lot of energy. However, a leading issue that must be addressed is the mechanisms used for establishing these shared keys in the first place.

Existing solutions are based either on pre-shared information between nodes of the same network or depends on a trusted third party that manages the security keys between these nodes.

In the pre-shared based solutions, we find the use of a secret master key pre-shared between all nodes in the same network to use it as a basis for generation of session keys between them. Other solution based on multiple pre-shared keys that if a network gather N nodes, each node will hold N - 1 pairwise key shared with network nodes. In addition, there are solutions that use a random sharing key and depends on probability functions or nodes location to find at least one shared key between two nodes on the same network. Yet there are solutions that use a trusted third party to manage security keys, usually it is the base station or a local powerful nodes.

These solutions deal only with local networks. However, 6LoWPAN networks are open to outside communications, with external IP-hosts, also the immediate neighbors of a node or its corresponding nodes from other IP networks cannot be predicted in advance; consequently, these keys will need to be established after the network is deployed.

As already mentioned in the previous paragraph, in the case of 6LoWPAN networks, we need solutions that guarantee the end-to-end communication security such as IPsec [10] and its key management protocol IKE [11], which are used to secure IP-based communications, yet they are very greedy for resource-constrained networks as they are based on asymmetric cryptography. Many contributions have proposed lightweight implementations of asymmetric solutions in networks with constrained-resources as for example whose based on ECC (Elliptic Curve Cryptography) that demonstrations have shown that a key ECC 160-bit provides the same level of security than RSA 1024-bit key, while having a lower energy consumption and faster time calculation than RSA. However, the use of ECC in highly constrained-nodes, like 6LoWPAN nodes, still greedy especially for the nodes that provide services as a server.

As the 6LoWPAN is a recent under developing technology, there is no many security solution are proposed yet. Our contribution aim to propose a key management scheme with hybrid security solution that benefit from symmetric and asymmetric advantages, as the first is energy efficient and the second guarantee the end-to-end security establishment. The challenge we address is to maximize 6LoWPAN networks security performance while minimizing nodes resource consumption.

## 3. PROPOSED SOLUTION

In this section, we present our proposed solution in bipartite. In the first part, we present the key establishment in a local LoWPAN. In the second part, we present the end-to-end security establishment between two nodes in two different LoWPANs or a LoWPAN's node and an IP-host.

### 3.1 Assumptions

We consider a LoWPAN network consisting of a set of nodes and an edge router the bridge between the nodes and the internet. According to RPL protocol, LoWPAN nodes form the topology parent-son tree according to the scheme designed by the RPL, the information flow destination is either upward or downward, from or to the edge router, we assume that the immediate neighboring nodes of any device will not be known in advance. Some nodes serves as a router between the other nodes and the edge router. Each node has a unique and secret ID. A remote server installed remotely plays the role of the network monitoring. This remote server is equipped with a database implemented by the LoWPAN's nodes information. The necessary information we will need in this database are the nodes physical addresses and their secret IDs. We consider the probability that the edge router or the remote server be compromised is negligible as they are powerful devices.

Journal of Theoretical and Applied Information Technology
31st March 2015. Vol.73 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We designed our scheme to provide a solution for key management in 6LoWPAN networks to ensure its security, taking into account the performance requirements as energy optimization, scalability, flexibility and connectivity.

### 3.2 LoWPAN nodes key establishment

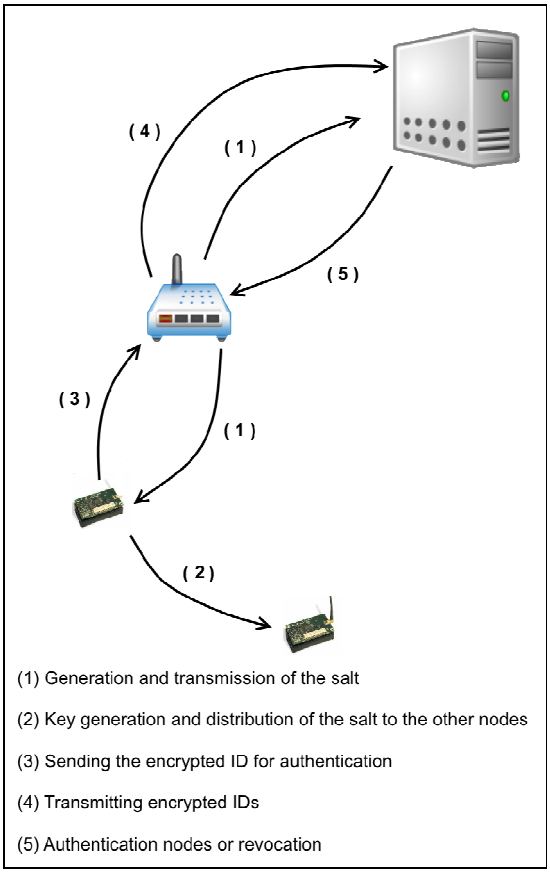


*Figure 1: LoWPAN nodes key establishment schema*

In the bootstrapping phase, each node begins to discover the way to the edge router by linking relations with its neighboring nodes, but at this stage, it is possible that a malicious node was introduced into the network. To avoid any contact with a suspicious intruder node, we chose in our method that the nodes start in listening mode waiting for the first message sent by the edge router (Figure 1).

The first key is a unique and individual symmetric key; each node in the network will share this key with the remote server *RS*.

Firstly, the edge router *ER* establishes a secure connection with the *RS* to identify it the network. *ER* generates a salt *S*; at the same time, it sends it to the *RS* and broadcasts it in its network. S will be accompanied by a timestamp *Ts* and its time expiration *Te*. In addition, *S* will be accompanied by a level *L* that will be initialized by 1 and incremented from a level to another.

We use *Ts* to avoid replay attacks, and to differentiate between an obsolete *S* of an old session and a new *S* for the current session.

*RS* will use the *S* and the nodes IDs stored in the database to generate its shared pairwise key for each node. *RS* will record the keys in its database. It will recognize nodes using their physical addresses.

There are two cases; either the *RS* already know the network nodes, so the *RS* will generate the keys directly for each node. Otherwise, each node generates a key, when it will send its first message encrypted in *RS*, *RS* will identify it using its physical address; it will generate the key and will try to decrypt the received message.

In the LoWPAN side, each node that receives the message containing *S*, will check the *Ts* if it has expired or not, and the level *L* if it is lesser or not, for two reasons: the first is that since each node that receives the *S* passed to its neighbors, so each node may receive the same *S* several times. If it has already received a one, it suffices to check the level *L*: if it is equal to or greater than its level, it rejected. The second reason for using the *L* is the construction of the first routes of the network where each node receives the S from another node in a lower level; it considers it as a gateway to the edge router *ER*.

Nodes shares the *S* so on until all nodes in the network will receive it; each one determines its level and its gateway to the *ER*.

Each node *i* that receives the *S* will use it with its secret ID to generate its pairwise key $K_i^{RS}$ with the *RS*. After that, each node encrypts its ID with $K_i^{RS}$, and sent it to the *RS*. If *RS* succeeded to decrypt the message, and find the received ID in its database, it claims that the node is legitimate and return a confirmation of legitimacy to the *ER*. Otherwise, it sends it a command to revoke the involved node.

Journal of Theoretical and Applied Information Technology
31st March 2015. Vol.73 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

### 3.3 Inter-LoWPAN nodes key establishment

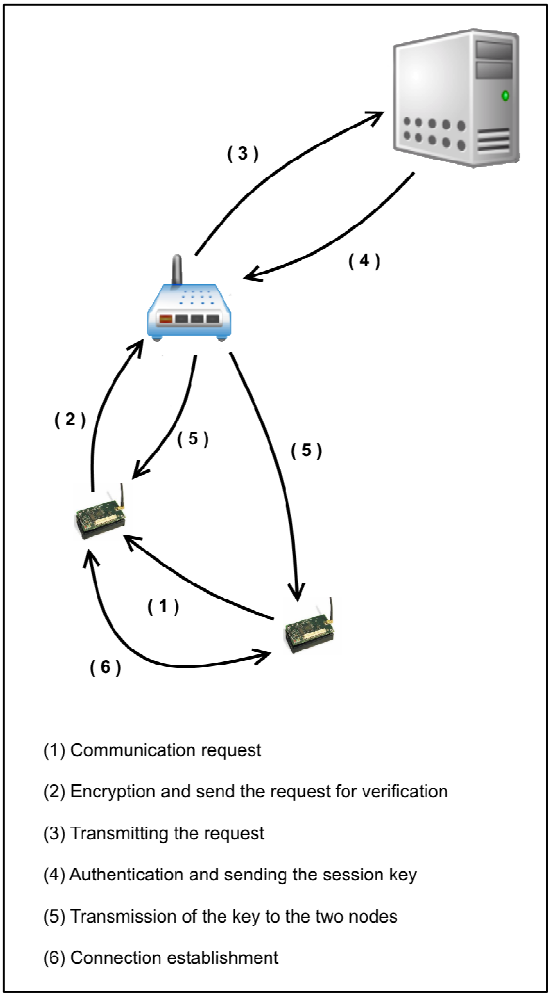


*Figure 2: Inter-LoWPAN key establishment schema*

Authentication is required for all types of packets, whereas confidentiality may only be required for some types of packets. For example, routing control information usually does not require confidentiality, whereas readings reported by a sensor node and the queries sent by the base station may require confidentiality.

After establishing primary parent-son relations by establishing routes that connect each node to the ER, nodes will need to communicate to each other. Since 6LoWPAN nodes have limited storage capacity, we will restrict the sharing of keys between nodes that have a parent-son relationship. The goal is that each parent node shares its key $K_i$ with its son nodes (Figure 2).

We take the example of two neighboring nodes A in the level $L_i$ and B in the level $L_{i+1}$. B sends a "Hello" message to A. In order to avoid an attack of "Hello flooding": A records the B address and waits for its authentication, as it warned, each next request from B will be rejected. Here, because A level is the closest to the *ER*, it is who will take over the key exchange process. A generates a key $K_A$, encrypts it with the B address of its key $K_A^{RS}$ and sends all to the *RS*. When the *RS* decrypts the message, it will find the key of A and B address, it will understand that A wants to share its key with B. After checking the two nodes A and B in its database, the ER encrypts A's $K_A$ by B's $K_B^{RS}$ and sends it to the latter.

The same method used between two non-neighboring nodes that belong to the same network, i.e. two nodes that shares the same IPv6 prefix (see paragraph). However, since in this case the communication will be temporary and for a specific session, the node receiving the request, supposedly A, will encrypt the request and the applicant's address, supposedly B, by its key $K_A^{RS}$ and sends it to *RS*. After checking the nodes, *RS* will generate a session key and sends to A encrypted by $K_A^{RS}$ and to B encrypted by $K_B^{RS}$, joining a timestamp *Ts* and its time expiration *Te*, depending on the type of communication requested by B.

### 3.4 End-to-end key establishment

To establish an end-to-end connection between two nodes $N_1$ and $N_2$ whose are in the $LoWPAN_1$ and $LoWPAN_2$ networks, we will use the *RS* of two networks as a proxy (Figure 3).

$RS_1$ and $RS_2$ will exchange a secret *n* by Diffie-Hellman algorithm, the best known and most widely used key agreement protocol. After that, every *RS* will pass *n* to its node encrypted by its $K_{Ni}^{RSi}$, both nodes must use the same hash function to generate $K_n$ their pairwise symmetric key.

The Diffie-Hellman (DH) protocol [12] requires that two peers A and B first agree on appropriate prime *p* and generator *g*. Then, A and B choose secret values, respectively *a* and *b*, compute the corresponding public values, respectively $g^a \bmod p$, and exchange these public values with each other. The same Diffie-Hellman shared secret *n* is then obtained at A by computing $(g^b \bmod p)^a$ and B by computing $(g^a \bmod p)^b$.

Journal of Theoretical and Applied Information Technology
31st March 2015. Vol.73 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

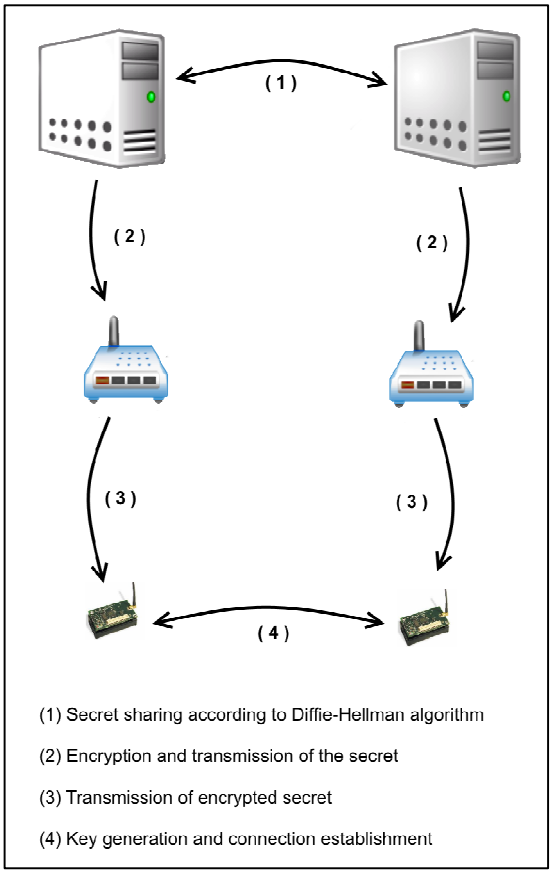


*Figure 3: End-to-end key establishment schema*

Considering two LoWPANs 1 and 2 belonging to $RS_1$ and $RS_2$, and two nodes $N_1$ and $N_2$. $N_1$ wants to share a symmetric key with $N_2$, for this $N_1$ sends its request to $RS_1$, $RS_1$ shares a secret $n$ with $RS_2$ using Diffie-Hellman method. Also, they agree on the key generation method that the nodes belonging to their networks will use. Then $RS_1$ passes $n$ to $N_1$ encrypted by its $K_{N1}$ $^{RS1}$ and indicate it the method that will use to generate the key $K_n$. The same will be done by $RS_2$ with $N_2$. After establishing $K_n$ key, $N_1$ will generate a nonce $no_1$ and send it encrypted by $K_n$ $N_2$ that will increment it and return the result to $N_1$. The same process will be done by $N_2$ generating a nonce $no_2$.

### 3.5 Re-keying

Rekeying contributes in improving the system protection by changing the security keys in a specific time interval.

In the case of nodes pairwise keys with the server, the rekeying follows the same method explained in broadcasting a new Salt. For shared keys between nodes, in the case of the parent-son relationship: The parent node generates a new key and broadcasts it encrypted by its current key to its children nodes. In the case of two nodes that need to communicate frequently, after the end of the current session key, or after an order from the server in case of intrusion detection, since both nodes already share a key. The first node will generate a nonce $no_1$ and sending encrypting the second node follows the same process by generating a nonce $no_2$. At the end of the exchange, both nodes combines $no_1$ and $no_2$ to generate their new symmetric key.

All the old session keys must be deleted after generating the new key, but only after checking that it worked.

The constraint in the rekeying is the good choice of changing key frequency. A change in a very short time interval will consume nodes resources, and the choice of a longer period will offer to attackers more time to compromise the keys.

## 4. PROPOSED SOLUTION ANALYSIS

### 4.1 Network model

In our solution, we will use the node physical address as its primary identifier, but the node authentication will be using its symmetric key and its secret ID.

As the ID will remain secret only in the RS, an urgent solution in the case of a temporary malfunction of a *RS* (it is estimated as a rare case since we must use other secondary servers), the network will continue to operate normally and the data collected will be stored at the *ER* before restoring connection with the *RS*. In the case of the introduction of a new node, as the *ER* does not have its ID to generate its pairwise symmetric key, it will put it on hold and will preclude its neighboring nodes to communicate to it until its authentication.

### 4.2 Post deployment operations:

In each designed security key management protocol proposed for resource-constrained networks, it must respect and take into

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

consideration a set of requirements and constraints to be an applicable and effective protocol.

#### 4.2.1 Resiliency

Inside a LoWPAN, our scheme supports two types of key: an individual key for each node, shared with the Remote Server, and another shared between a parent node and its children nodes. Therefore, in case of a compromised node, it will not affect other nodes in the network because everyone has a unique key and a unique ID which is the basis for the generation of the key. Or only the entire node that belongs to the same group, which is in general and especially in our case a very limited group.

Thus, most existing solutions are hypothesized no node is compromised or malicious node is introduced during the bootstrapping phase. However, this phase is dangerous because the establishment of routes and recognition of nodes is done in this phase. Our scheme takes into account the security of this phase by the designated sharing key mechanism, no node communicates with another before its authentication by the *RS*. Thus, no node that its secret ID is not recorded in the Remote Server database will have the opportunity to establish a key.

#### 4.2.2 Scalability

Our scheme is flexible regarding changes in network topology and supports scalability, it suffices that the node ID been stored in the database of the *RS* to make it able to join the network and establish a connection with other nodes.

If a new node wants to join a LoWPAN network, it broadcasts a request to all neighboring nodes that are close to it. The node that receives this request establishes the same mechanism of key exchange between parent and son nodes. Except in this case since the node is new in the network, firstly *RS* sends it the salt to generate its unique pairwise key before it passed it the keys of these neighboring nodes claiming to be its parent nodes.

In case the *ER* loses all connection with the main and secondary Remote Servers, it will not accept any new node since it does not hold its ID to generate the security key $K_i^{RS}$. It puts it in standby state and prohibits its neighboring nodes to communicate to it until its authentication.

#### 4.2.3 Key connectivity

It is determined by the number of keys that every node must have to ensure the stability of communications within the network.

Each node two different types of keys: the first is a single and unique $K_i^{RS}$, the key shared between each node and the Remote Server. The second type concerns the key shared between a parent node and its children nodes, it is generated by a single node and is shared it with others. Except upper level nodes whose play only the role of parent nodes, and nodes in the last row that play only the role of children nodes, all other nodes play a dual role at the same time, so any node holds its own key that it shares with its children, and the keys of its parents. Since in 6LoWPAN networks, the RPL protocol establishes communication upward / downward where the node communicates only with the nodes of different level of its own, except for an updated topology, a node will not have much of key to store.

#### 4.2.4 Storage requirements

Storing keys also depends on the relationships each node has established. In our scheme, a node needs to keep five types of keys. It needs to store one individual key with the *RS*, p pairwise keys with its parents, c pairwise keys with its children, and one with its end-to-end correspondent. However, it depends on the type of relationship is that for a long session or for a short session. For a long session, relationships can be identified as follows: the relationship with the *RS*, the relationship with a parent node, the relationship with a child node, and relationships with corresponding of neighbors who share with them many communications. What remains for the short session are only relations with corresponding, out neighbors, in need of treatment of an instant request, especially the end-to-end relationship.

So for the long session, a node can hold: number of keys = 1 + p + c + i, where, p = number of parent, c = number of children and i = number of internal corresponding. For the short session: number of keys = i + e, where e = end-to-end node.

We can say that our scheme does not take much space especially with the use of small keys and key sessions that the system remove them after the end of the period of validity.

Journal of Theoretical and Applied Information Technology
31st March 2015. Vol.73 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

## 5. PROPOSED SOLUTION EVALUATION

### 5.1 Performance evaluation:

The evaluation of our scheme is based on simulations made on the TOSSIM simulator of TinyOS. The simulations were compiled for the TelosB platform. TelosB is based on the low-power microcontroller MSP430 16-bit with a clock frequency of 4 MHz. It implements the IEEE 802.15.4 transceiver CC2420 with a claimed data rate of 250 Kbps. We used AES 128-bit as the symmetric cryptography protocol. We used PowerTOSSIM plugin for energy analysis.

The Figure 1 gives the result values of key generation in a LoWPAN (we do not count the cost of communications between the *RS* and *ER* or between two *RS*s as they are powerful machines).

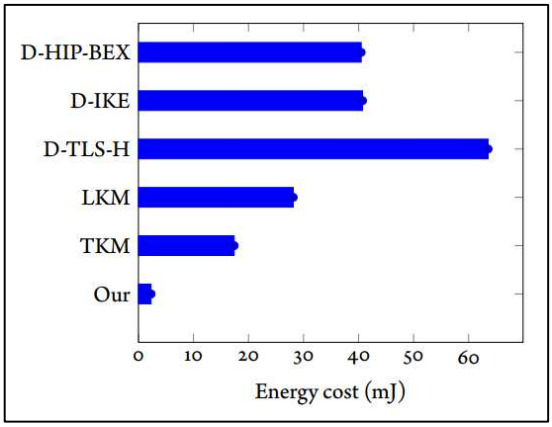


*Figure 1: Energy consumption of keys establishement*

The result is very interesting and energy efficient compared to other schemes. We only compare our results with the only solutions that have been proposed in the context of the Internet of Things like the hybrid solutions that propose symmetric and asymmetric key establishment; Trust Key Management Scheme for Wireless Body Area Networks (TKM) 28.13 mJ [13] and Lightweight Key Management Scheme (LKM) 17.40 mJ [14]. On the other hand, lightweight public key establishment like distrusted TLS handshake (D-TLS-H) 63.54 mJ, distributed IKE (D-IKE) 40.73 mJ and distributed HIP BEX (D-HIP-BEX) 40.48 mJ [15]. There is a huge difference since our solution is totally based on symmetric cryptography, although other solutions are either hybrid, i.e. it uses both cryptography protocols, asymmetric and symmetric. Asymmetric is just used as a basis for sharing symmetric keys that are subsequently used for cryptography. Other solutions are adapted versions of standard patterns of sharing Internet asymmetric keys. Knowing that all these schemes are based on the Elliptic Curve Cryptography (ECC).

From energy point of view, which is an essential metric for LR WPAN networks, and a critical criterion of choice to adopt or not a solution, our model does not require a lot of calculation or exchange between devices to establish security keys, it can be considered as an energy-economizer.

The time of generation of a symmetric key is negligible. However, the key distribution takes a significant time, with the increase in the number of nodes, the time spent in key distribution increases linearly.

Several factors can influence the time of the distribution key as devices gathering, network topology, routing protocol, a device response time, total number of devices on a net-work, average number of neighboring devices, etc..

### 5.2 Formal evaluation:

To prove the fulfillment of the objectives desired security of the proposed systems, we used AVISPA tool to conduct a formal safety analysis. AVISPA is a push-button that analyzes the security protocols based on formal methods to check whether the candidate protocol is secure or not. In the case of detection of a vulnerability, it offers the attack track and the step where that was made possible. The tool implements the Dolev-Yao intruder model able to modify traffic passing through, intercept messages, eavesdrop, or insert bogus data.

AVISPA implements four different automatic protocol analysis techniques for protocol falsification: OFMC (on-the-fly model-checker), (CL-AtSe) (constraint-logic based attack searcher), SATMC (SAT-based model checker), and TA4SP (tree automata based on automatic approximations for the analysis of security protocols).

AVISPA uses High Level Protocol Specification Language (HLPSL) to illustrate the protocols to be analyzed. It is a special input language used to model the security protocols.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We modeled our proposed solution using the HLPSL to analyze our protocol; we analyzed the LoWPAN and the Inter-LoWPAN keys. For the end-to-end key, we claim that is secure as it is based on a Diffie-Hellman known protocol.

### 5.2.1 LoWPAN key evaluation:

The HLPSL code is:

```
role
role_R(R:agent,IdN:text,SND,RCV:channel(dy))
played_by R
def=
        local
        State:nat,Ts:text,S:text,Te:text,Ker:symmet
ric_key,Krn:symmetric_key
        init
                State := 0
        transition
                1. State=0 /\
RCV({S'.Ts'.Te'}_Ker') =|> State':=1
                4. State=1 /\
RCV({{IdN}_Krn'}_Ker) =|> State':=2
end role

role role_E(E:agent,S:text,SND,RCV:channel(dy))
played_by E
def=
        local
        State:nat,Te:text,Ts:text,Ker:symmetric_ke
y,IdN:text,Krn:symmetric_key
        init
                State := 0
        transition
                1. State=0 /\ RCV(start) =|>
State':=1 /\ Ker':=new() /\ Te':=new() /\ Ts':=new()
/\ SND({S.Ts'.Te'}_Ker') /\ SND(S.Ts'.Te')
                3. State=1 /\ RCV({IdN'}_Krn')
=|> State':=2 /\ SND({{IdN'}_Krn'}_Ker)
end role
role
role_N(N:agent,IdN:text,SND,RCV:channel(dy))
played_by N
def=
        local
        State:nat,Te:text,S:text,Ts:text,Krn:symmet
ric_key
        init
                State := 0
        transition
                2. State=0 /\ RCV(S'.Ts'.Te') =|>
State':=1 /\ Krn':=new() /\ SND({IdN}_Krn')
end role
role
session1(S:text,E:agent,R:agent,N:agent,IdN:text)
def=
        local

        SND3,RCV3,SND2,RCV2,SND1,RCV1:ch
annel(dy)
        composition
                role_N(N,IdN,SND3,RCV3) /\
role_E(E,S,SND2,RCV2) /\
role_R(R,IdN,SND1,RCV1)
end role
role environment()
def=
        const
        r:agent,s:text,e:agent,n:agent,const_1:text
,auth_1:protocol_id
        intruder_knowledge = {}
        composition
                session1(s,e,r,n,const_1)
end role
goal
        authentication_on auth_1
end goal
environment()
```

### 5.2.2 AVISPA evaluation result:

We used AVISPA web tool to evaluate our solution, both gives the same result in the output:

AVISPA Tool Summary

OFMC : SAFE
CL-AtSe : SAFE
SATMC : SAFE
TA4SP : INCONCLUSIVE

As we see, OFMC, CL-AtSe and SATMC tools have reported that our solution is safe. However, the TA4SP has reported that our solution is INCONCLUSIVE; that is because the case of the existing of compromised nodes in the network, that is clear, cryptography alone cannot provide a complete solution to any system, we have to choose other systems in parallel to solve the shortcomings of cryptography, such as intrusion detection systems.

## 6. CONCLUSION

We can claim that our scheme provides a complete solution for securing the 6LoWPAN network while minimizing the use of resources. Knowing that we can optimize more resources by

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

adding other parameters such as by limiting the number of correspondence of each node.

Until the writing of this paper, we do not find in the literature a complete cryptography solution that secures 6LoWPAN networks. Solutions found are adaptation techniques created for sensor networks to ensure security inside the LoWPAN and other coping techniques of end-to-end security solutions to ensure network security outside the LoWPAN.

In addition, our solution is based on the protocols used by the 6LoWPAN networks such as RPL and Neighbor Discovery protocol for two reasons: the protocol will be well suited to this kind of network does not need change adaptation and to take advantage of existing protocols to optimize the cost of using resources. Also, It is based on symmetric key cryptography for all the communications and hence occupies the smallest portion of memory.

Overall, we conclude our scheme is scalable and efficient in computation, communication and storage.

As assumptions, we try to optimize more our solution, and try it with other routing protocols.

**REFRENCES:**

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] K. Chang, A. Soong, M. Tseng, and Z. Xiang, "Global Wireless Machine- to-Machine Standardization," *IEEE Internet Comput.*, vol. 15, no. 2, pp. 64–69, 2011.

[3] E. Negre and C. Rosenthal-Sabroux, "Recommendations to Improve the Smartness of a City," in *Smart City*, R. P. Dameri and C. Rosenthal-Sabroux, Eds. Springer International Publishing, 2014, pp. 101–115.

[4] C. P. P. Schumacher, N. Kushalnagar, and G. Montenegro, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals." [Online]. Available: https://tools.ietf.org/html/rfc4919. [Accessed: 10-Mar-2014].

[5] N. Kushalnagar, G. Montenegro, D. E. Culler, and J. W. Hui, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks." [Online]. Available: http://tools.ietf.org/html/rfc4944. [Accessed: 10-Mar-2014].

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[7] S. Ullah, M. Mohaisen, and M. A. Alnuem, "A Review of IEEE 802.15.6 MAC, PHY, and Security Specifications," *Int. J. Distrib. Sens. Netw.*, vol. 2013, Apr. 2013.

[8] A. Rghioui, M. Bouhorma, and A. Benslimane, "Analytical study of security aspects in 6LoWPAN networks," in *2013 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)*, 2013, pp. 1–5.

[9] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks," *CSE J. Artic.*, Jan. 2006.

[10] K. Seo and S. Kent, "Security Architecture for the Internet Protocol." [Online]. Available: http://tools.ietf.org/html/rfc4301. [Accessed: 27-Aug-2014].

[11] P. Eronen, C. Kaufman, Y. Nir, and P. Hoffman, "Internet Key Exchange Protocol Version 2 (IKEv2)." [Online]. Available: http://tools.ietf.org/html/rfc5996. [Accessed: 27-Aug-2014].

[12] E. Rescorla, "Diffie-Hellman Key Agreement Method," May 1999.

[13] M. Mana, M. Feham, and B. A. Bensaber, "Trust key management scheme for wireless body area networks," *Int. J. Netw. Secur.*

[14] R. Abdmeziem and D. Tandjaoui, "A Lightweight Key Management Scheme for E-health applications in the context of Internet of Things," CERIST, Technical Report CERIST-DTISI/RR--14-0000000010--dz, Mar. 2014.

[15] Y. B. Saied, "Collaborative security for the internet of things," phdthesis, Institut National des Télécommunications, 2013.