

Efficient End-to-End Secure Key Management Protocol for Internet of Things

Yamina Ben Slimane¹, Khelifa Ben Ahmed²

¹Laboratory of Physics and Semi-conductor Device, University Tahri Mohamed, Bechar, Algeria

²Exact Sciences Department, University Tahri Mohamed, Bechar, Algeria

Article Info

Article history:

Received Jan 17, 2017

Revised Apr 12, 2017

Accepted May 2, 2017

Keyword:

6LoWPAN network

Internet of things

Key management protocol

6LoWPAN routers

AVISPA tool

ABSTRACT

Internet of things (IoT) has described a future vision of internet where users, computing system, and everyday objects possessing sensing and actuating capabilities are part of distributed applications and required to support standard internet communication with more powerful device or internet hosts. This vision necessitates the security mechanisms for end-to-end communication. A key management protocol is critical to ensuring the secure exchange of data between interconnecting entities, but due to the nature of this communication system where a high resource constrained node may be communicating with node with high energy makes the application of existing key management protocols impossible. In this paper, we propose a new lightweight key management protocol that allows the constrained node in 6LoWPAN network to transmit captured data to internet host in secure channel. This protocol is based on cooperation of selected 6LoWPAN routers to participate in computation of highly consuming cryptographic primitives. Our protocol is assessed with AVISPA tool, the results show that our scheme ensured security properties.

*Copyright © 2017 Institute of Advanced Engineering and Science.
All rights reserved.*

Corresponding Author:

Yamina Ben Slimane,

Laboratory of Physics and Semi-conductor Device,

Tahri Mohamed University-Bechar,

Street independence B.P. 417, Bechar, Algeria

Email: Yami.benslimane@gmail.com

1. INTRODUCTION

The internet of things has made a revolution in the world of communication by connected the physical objects to Internet. According to [1] (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services.

The internet of things (IoT) describes the next generation of Internet, where the physical things or objects are connected, accessed and identified through the Internet, many technologies are involved in IoT, such as WSN (Wireless Sensors network) [2], intelligent sensing, Radio Frequency Identification (RFID) [3], 6LoWPAN [4], Near Field communications (NFC) [5] [6], low energy wireless communication, cloud computing, and so on.

These technologies will interact with physical phenomena by employing more constrained sensing platforms and low-energy wireless communications, therefore, end-to-end communication between constrained sensing devices and other Internet host will be a fundamental requirement of many sensing application using these technologies, this aspects that seriously complicate the design and adoption of appropriate security mechanisms especially end-to-end security mechanisms.

In the literature, several research efforts have been introduced to overcome challenges and find appropriate solutions associated to security especially end-to-end security. Some research have focused their efforts to making the security protocol standards suitable to the context of IoT as Hummen et al in [7], have developed a complementary lightweight full extension to HIP DEX (Host Identity Protocol Diet Exchange) standard for working with the IoT architecture specification, this extension could be generalized to DTLS protocol and IKE. Other research as Granjal et al in [8], have proposed a procedure of delegation of large computation in DTLS protocol to a rich resource entity, Also Oleveau and Said in [9] have presented a distributed HIP (D-HIP) inspired from HIP-BEX, They are used proxies nodes to calculate the DH protocol of operations for session key establishment, each proxy node takes a calculation part.

Another vision of solution have been introduced, it is the proposal of compression schemes applied to different protocols. In [10, 11], the authors have proposed IPV6 header compression, extension headers, and UDP (User Datagram Protocol) header standardized through 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks). Authors in [12, 13] have presented 6LoWPAN compressions for IPsec payload headers: AH (Authentication Header) and ESP (Encapsulating Security Payload). Raza et al. [14] have proposed a modification of DTLS headers using the 6LoWPAN compression scheme. The modified protocol reduces the size of some headers (i.e. the DTLS record header, the handshake header, the handshake message).

So many works focus on the adaptation of existing security solutions to the specification related to IoT environment, our work provides a suitable key management protocol for IoT scenarios. In this paper, we propose a new lightweight key management protocol which is based on cooperation between selected routers in 6LoWPAN network to establish a secured communication channel between a highly resource constrained node in 6LoWPAN network and a remote entity (i.e. server). In our protocol, the third parties (routers) have a more active role through taking responsibility to computation of the highly consuming cryptographic primitives. We have assessed our protocol using AVISPA tool, the obtained results shows that our protocol is safe in terms of security properties. Our paper proceeds as follows: In section 2, we explain the research method. The result and discussion are presented in Section 3. Finally, Section 4 concludes the paper.

2. RESEARCH METHOD

In this section, we present our lightweight end-to-end key management protocol. Firstly, we give a brief overview on 6LoWPAN network. Then, we present the proposed network model and set of assumptions. Afterwards, we describe our proposed protocol. Finally we explain in detail the different phases of our model along with a summary of the notations used throughout the paper.

2.1. 6LoWPAN Network

6LoWPAN is connecting more things to the cloud. Low-power, IP-driven nodes and large mesh network support make this technology a great option for Internet of Things (IoT) applications. According to [15] a LoWPAN is Low-power Wireless Personal Area Networks (LoWPANs) composed of devices conforming to the IEEE 802.15.4-2003 standard defined by the IEEE [16]. IEEE 802.15.4 devices are characterized by short range, low bit rate (from 20 Kbits/s (868 MHz) to 250 Kbits/s (2.45 GHz)), Small packet size (the maximum transmission unit or MTU on IEEE 802.15.4 links is 127 bytes), low power, and low cost.

The IPv6 over Low-power WPAN (6LoWPAN) Working Group was formed in 2004 to work on protocol specifications to optimize the operation of IPv6 over networks made of IEEE 802.15.4 links in LoWPAN (Low-power Wireless Personal Area Networks), it was decided to exclusively work on the required IPv6 protocol extensions for LoWPAN (such as fragmentation and reassembly, header compression, neighbor discovery adaptation, etc.). The 6LoWPAN Working Group belongs to the Internet area (INT) of the IETF [17], Then the Routing Over Low-power and Lossy network (ROLL) Working Group was formed to deal with routing issues in networks with similar characteristics at the IP layer thus alleviating the restriction of using IEEE 802.15.4 links, since by definition routing operates at the network layer. IPv6 based Wireless sensor network can be considered as one enabling wireless technologies that offers greater advantage for the advancement of M2M communication.

The 6LoWPAN network is connected to the IPv6 network using an edge router. The edge router handles three actions:

- The data exchange between 6LoWPAN devices and the Internet (or other IPv6 network).
- Local data exchange between devices inside the 6LoWPAN.
- The generation and maintenance of the radio subnet (the 6LoWPAN network).

The 6LoWPAN networks are connected to other networks simply using IP routers. As shown in Figure 1, the edge router is considered like stub network. This means data going into the network is destined

for one of the devices inside the 6LoWPAN. 6LoWPAN device may be connected to the internet host in other IP networks through one or more edge routers that forward IP datagrams between different media.

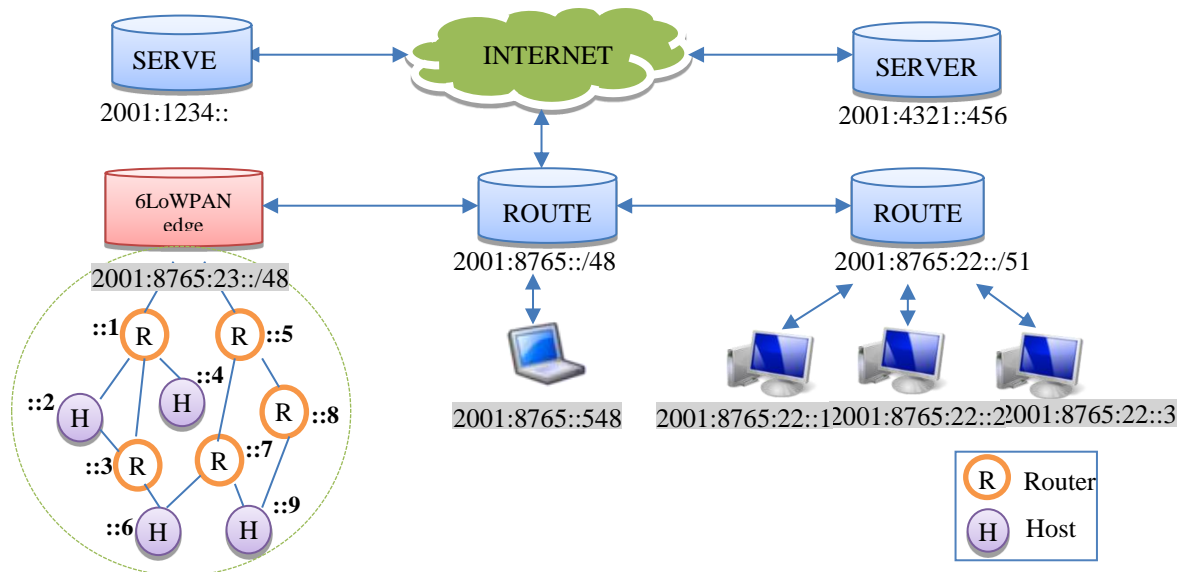


Figure 1. Connected 6LoWPAN network with IPV6 network

Connectivity to other IP networks may be provided through any arbitrary link, such as Ethernet, WI-Fi or 3G/4G. In the Typical 6LoWPAN network there are two other device types: routers and hosts. Routers can, as the name implies, route data destined to another node in the 6LoWPAN network. Hosts are not able to route data to other devices in the network. The host can also be a sleepy device, waking up periodically to check its parent (a router) for data, enabling very low power consumption.

The basic concept of 6LoWPAN stack is illustrated in Figure 2. 6LoWPAN is an adaptation layer is added between the network and IEEE 802.15.4 MAC layer. This layer is responsible to establish 6LoWPAN device’s direct communication with any server on the internet.

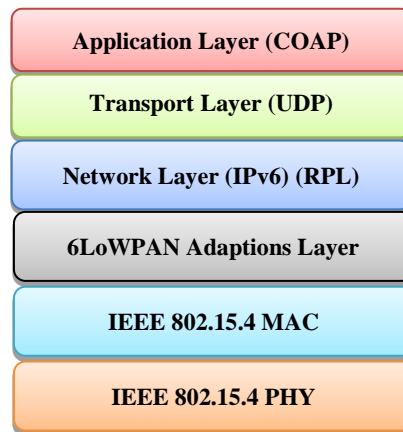


Figure 2. 6LoWPAN protocols stack

2.2. Network Model and Assumptions

In this work, the architecture shown in Figure 3 is considered. It consists of two parties, the first part consists of the 6LoWPAN host (H), 6LoWPAN Routers (R_i), Access Control server (AC) in 6LoWPAN

network, the second part consists of the remote server (RS) in IPV6 network, furthermore another component plays role in our architecture is the Certification authority server(CA) delivers authenticated certificates. The Access Control (AC) server supports authentication and trust operation in 6LoWPAN network and also possess a trust relationship with a remote server, 6LBR can serve as a gateway to the 6LoWPAN nodes while communicating with a remote server in the Internet.

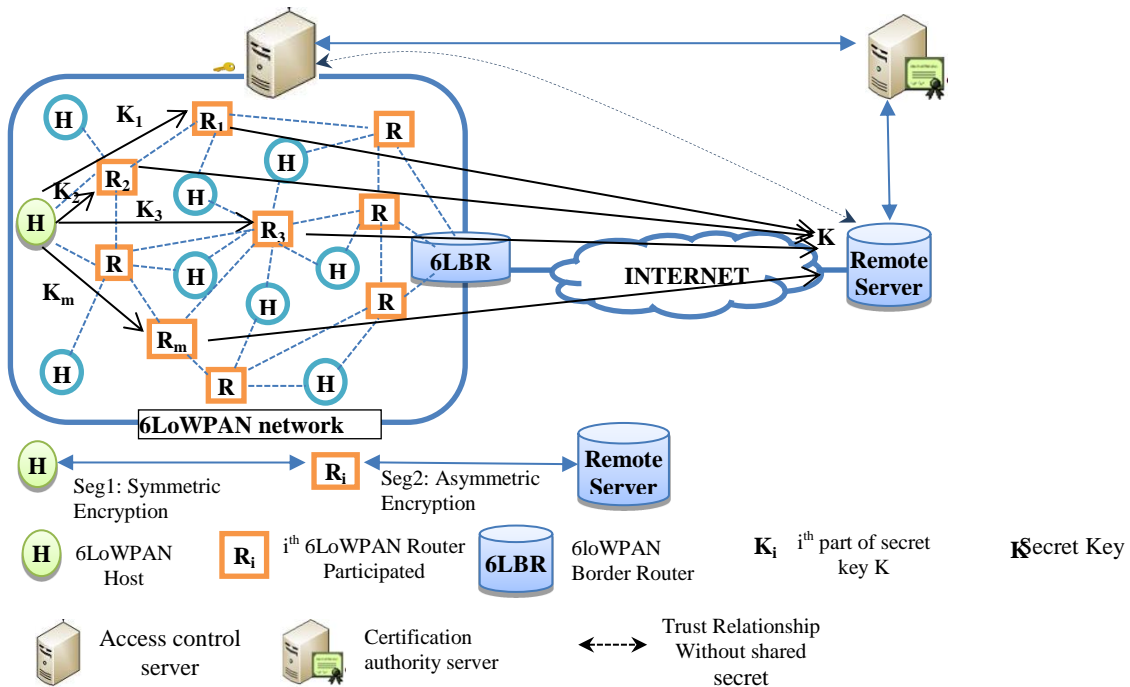


Figure 3. Network Model

In this architecture, it is assumed that all nodes that are registered to the 6LBR are motionless. The selected 6LoWPAN routers (R_i) are equipped with sufficient computation and storage capabilities than the 6LoWPAN host (H). During initial bootstrapping network, the security keys (which are refreshed periodically) are distributed to all nodes by The Access Control (AC) server. In this network we distinguish two types of nodes in term of storage capacities, computing power and energy resources:

The first, highly resource constrained node (6LoWPAN host (H)), which are unable to perform public key cryptographic operations. The second Node with high capabilities of storage, energy and computing power (the selected 6LoWPAN routers (R_i) and the remote server (RS)).

2.3. Description of Our Proposed Protocol

While guaranteeing E2E security between a 6LoWPAN host (H) and a remote server, we establish a shared key between the two ends of communication, for achieve this goal, a key exchange protocol is required between the two entities to secure these communications. In this section, we provide an overview over steps of our protocol. Firstly , the 6LoWPAN host(H) is willing establish a shared secret key with remote server ,it initiates our protocol, the 6LoWPAN host (H) generates a secret key (using one of the appropriate methods for resource constrained node) which is then randomly split to several secret parts, however this steps is performed after an authentication procedure between a 6LoWPAN host (H) and each 6LoWPAN routers (R_i). Each part of the secret key is encrypted and sent to corresponding 6LoWPAN router (R_i) by 6LoWPAN host(H), this latter use symmetric algorithm based shared key for encryption and MAC (message authentication code) to ensure authentication. Once the 6LoWPAN router (R_i) receives its corresponding part of the secret key, it decrypts the message then the 6LoWPAN router (R_i) encrypts the same message using public key encryption and send it to the remote server, the authentication between the 6LoWPAN routers and remote server ensures with digital signature. After receiving all the part of secret key by the remote server, it reassembles the shared secret, which will be used to derive further keying materials.

2.4. Notations and Formal Description

During an initialization phase, the resource-constrained 6LoWPAN host (H) carefully selects the R_1, \dots, R_m that will assist its key exchange, this operation is realized between the H and 6LBR where this latter delivers to H the selected 6LoWPAN routers (R_i)'s identifiers (IDs), the 6LBR relies on the model of trust management for selection of 6LoWPAN routers. Table 1. Summarizes the notations used to present the exchanged messages, and Figure 4 illustrate the succeeding steps of our protocol.

Table 1. The notations used in exchanged messages

<i>Notation</i>	<i>Description</i>
H	6LoWPAN Host
R_i	i^{th} 6LoWPAN Router
AC	Access Control Server
RS	Remote Server
CA	Certification Authority
N_X	Nonce generated by node X
$K_{X,Y}$	Shared pairwise key between X and Y
$K_{\text{public-X}}$	Public key of node X
$(\text{message})_K$	Message encrypted with the key K
Sign_X	X's digital signature
MAC	Message Authentication Code
K_i	Part of secret Key K
K	Secret Key K
Cert_X	X's Certificate delivered by CA
lifetime_X	X's Key lifetime
Ticket R_i	$(H, R_i, K_{H-R_i}, \text{lifetime}_{R_i}, \text{Cert}_{R_i}, N_H)$

Steps 1: 6LoWPAN host(H) initiates the protocol by sending a Hello_H message to remote server (RS). This message contains the security policies associated to the 6LoWPAN host (H) like encryption algorithms, lifetime, and compression methods. etc. the RS responds with Hello_RS message where it selects appropriate algorithms. The exchanged messages include the nonce to protect against replay message.

Steps 2: when the connection between the 6LoWPAN host (H) and the remote server is succeed, the 6LoWPAN host (H) requests AC server to obtain the security-related information's for 6LoWPAN routers (R_i) involved. The request message identifies the 6LoWPAN routers (R_i) and 6LoWPAN host (H), while also including a nonce. This message is encrypted with pre-shared key K_{H-AC} . The AC server responses with the encrypted message contain the secret shared key K_{H-R_i} between H and R_i plus 6LoWPAN host (H)'s ID and the nonce. Also the AC builds an authentication model contains the security information about R_i (Ticket R_i) and sends it together with a token containing the identification and a nonce of 6LoWPAN host (H) to each 6LoWPAN router R_i . When each 6LoWPAN router (R_i) receives this message, it compares the information contained in the two tokens received in order to authenticate the host (H). In the case of successful authentication, each 6LoWPAN router (R_i) is possess the shared secret key K_{H-R_i} . The reply message is encrypted with this key and carries to 6LoWPAN Host (H) with nonce.

Step 3: if step 2 is succeed, now the 6LoWPAN host(H) sends the message witch informs each 6LoWPAN router(R_i) about remote server identity, this message contains the RS's ID and encrypted with K_{H-R_i} , plus a Message Authentication Code. After R_i received the message, it provides the RS with their certificate containing its public key (delivered by CA). In addition, it requests the certificate of RS. In the response of this message, RS sends require information. The Nonce is also included in the exchanged messages to prevent replay attacks.

Step 4: in this step, the 6LoWPAN host (H) generates the secret Key K which will be used later to generate further keying materials at both H and RS sides. The secret is split into K_1, K_2, \dots, K_m parts. Each part K_i is encrypted with symmetric methods and securely sent with MAC to the appropriate 6LoWPAN router (R_i) in the message. At the level of each 6LoWPAN router R_i , each R_i uses RS's public key to encrypt message. This message contains the secret part K_i and R_i 's signature. RS verifies the authenticity of each message using R_i 's public key. If all the messages are received and authenticated successfully, then RS reconstructs the secret K. This secret along with the previous exchanged nonce are used to derive further key credentials. The nonces are included in the messages.

Step 5: this step terminates the exchanges message by proving to H the knowledge of the secret K. The derivation process is ensured by a hash function agreed upon during the first step. Both parties are then able to derive state connection keys for encryption and authentication of the exchanged data.

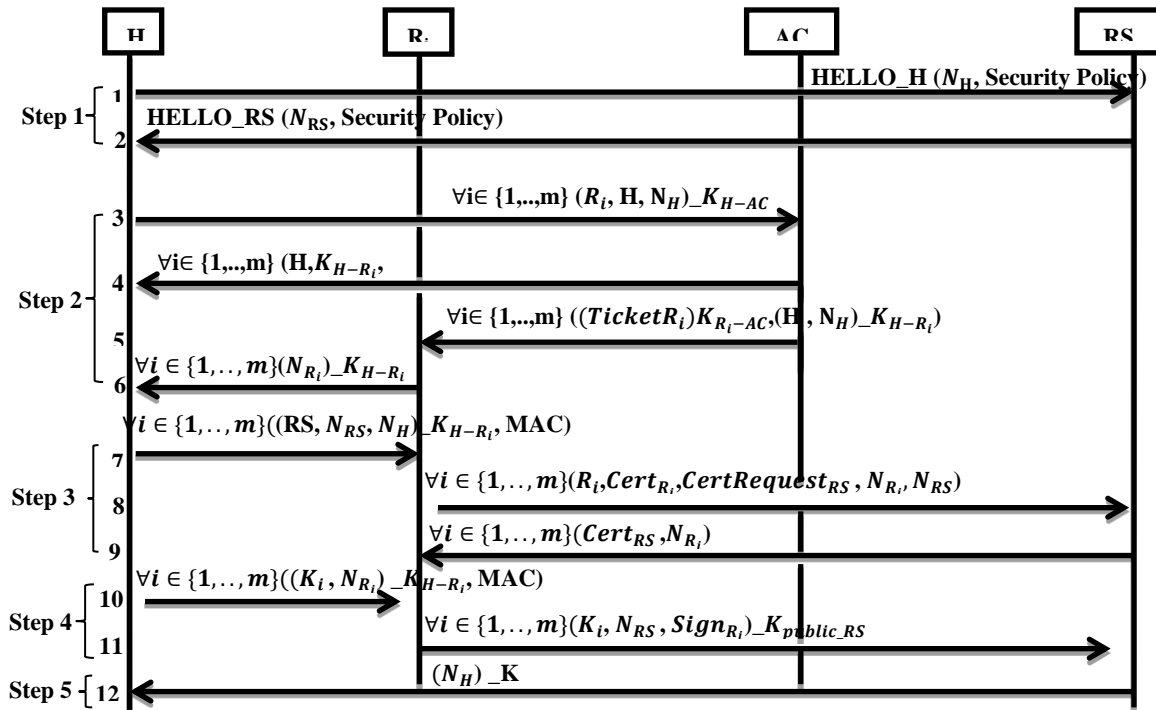


Figure 4. Illustration of the different steps and message exchanges of our protocol

3. RESULTS AND DISCUSSION

In this section, we provide a detailed analysis of our proposed key management protocol in terms of security properties then we present the validation of our protocol using *avispa* tool and compares the performance of our model with others research in literature.

3.1 Security Analysis

Our analysis is based on security properties of security protocols in IoT presented in [18] [19]. For the following discussion, we consider that our communication channel divides into two segments (explained in figure 3):

- **Confidentiality:** the confidentiality of exchange messages in our protocol is realized in two segments. For seg1, the symmetric encryption is effectuated with the set of pre-shared keys delivered from the trusted access server AC. we prefer the choose for encryption algorithms the AES-CCM mode that defines AES-CBC for MAC generation with AES-CTR for encryption [20]. For seg 2, the asymmetric encryption with public key is used for ensuring the security communication between entities. We recommend the use ECDH (Elliptic Curve Diffie–Hellman exchange). The CA delivers the required certificates to the involved entities. Our protocol can be run periodically to update the established keys in order to strengthen confidentiality, and prevent long term attacks
- **Integrity:** through the use of MAC (Message Authentication Code) [21] in exchanged messages in seg1, the data have not been altered. The same aim is ensured in seg2 by using the digital signatures,
- **Authentication and Authorization:** the AC server assures the authentication of the components in 6LoWPAN domain and possesses a trusted relationship with the remote server.
- **Freshness:** to avoid any replay attacks, we include nonce in the different exchanged messages.
- **Extensibility and scalability:** in our model, it is easy to integrate a new sensor. This later receives a pre-shared key with access control server during its bootstrapping phase in network. Then, it pass through an initialization phase and receive a selected 6lowpan routers' IDs that their participated in its key exchange protocol.

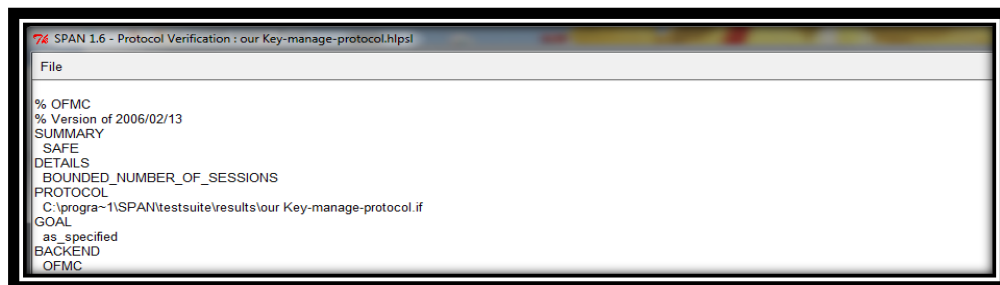
The 6LoWPAN network is vulnerable from many kinds of attack like replay attack, DDos attack, sinkhole attack, wormhole attack, rank attack, etc. Our protocol possess a mechanisms that protect the network from the effect of these attacks, for replay attack , we have implemented the mechanisms of the nonce in different exchange messages and the mechanisms of MAC that prevent modification, alteration,

insertion of messages by attacker. Through the authentication mechanisms in our protocol that inspired from Kerberos protocol [22], the access control server can check identity of each node in 6LoWPAN network. So, it is impossible to launch an attack like sinkhole, wormhole and DOS attacks.

3.2 Formal Validation With Avispa Tool

The AVISPA Tool [23] is a push-button tool for the Automated Validation of Internet Security Protocols and Applications. It provides a modular and expressive formal language for specifying protocols and their security properties, and integrates different back-ends that implement a variety of automatic protocol analysis techniques to illustrate whether the candidate protocol is safe or not. The tool provides a trace high lighting the steps that have led to the attack. In fact, AVISPA is considered as an effective tool for the analysis of different Internet security protocols and applications. In the literature, several security protocols have been validated through AVISPA [24], as IKE, TLS, AAA protocols of IETF. The tool implements the Dolev-Yao intruder model [25] able to eavesdrop, intercept messages, insert bogus data, or modify traffic passing through. AVISPA supports multiple backend model checkers. Some of the important back-end tools used by AVISPA are OFMC, CL-AtSe, SATMC and TA4SP.

The specification language HLPSL is used to describe the security protocol as sequences of exchanged messages between different entities. The action of each entity is organized in a module called basic role. However, the interactions of entities are described by composing multiple basic roles together into a composed role. In addition, the security goals of the analyzed protocol are specified in the goal section before launching the analysis. The formal validation of our protocol was achieved using AVISPA tool to prove the non-violation of the required security properties. In our model, we have first defined a basic role to describe the actions of the different entities involved. Then, we have described how the participating entities interact with each other in a composed role. The results of the simulation show that our protocol is “safe” against OFMC (see Figure 5), CL-AtSe (see Figure 6) and SATMC (see Figure 7). However, against TA4SP database, the result was “INCONCLUSIVE” (see Figure 8). These reports of each backend model produced by AVISPA tool explained that our protocol is safe regarding the specified security goal. It is impossible for an attacker to violate any of the specified security properties, and disrupt the functioning of the protocol.

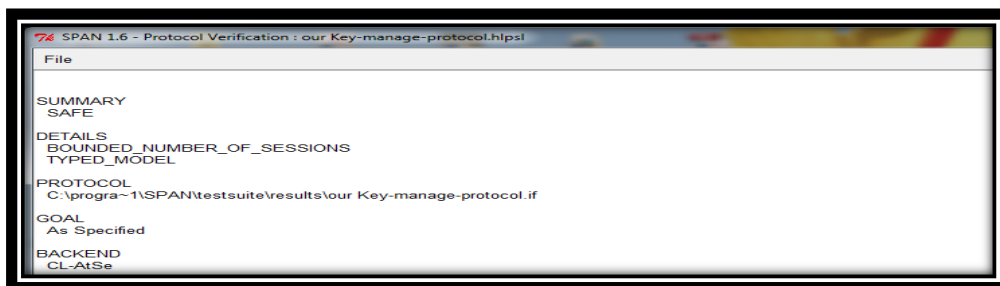


```

SPAN 1.6 - Protocol Verification : our Key-manage-protocol.hlpsl
File
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
C:\progra~1\SPAN\testsuite\results\our Key-manage-protocol.if
GOAL
as_specified
BACKEND
OFMC

```

Figure 5. Back-end AVISPA (OFMC)



```

SPAN 1.6 - Protocol Verification : our Key-manage-protocol.hlpsl
File
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
C:\progra~1\SPAN\testsuite\results\our Key-manage-protocol.if
GOAL
As Specified
BACKEND
CL-AtSe

```

Figure 6. Back-end AVISPA (CL-AtSe)

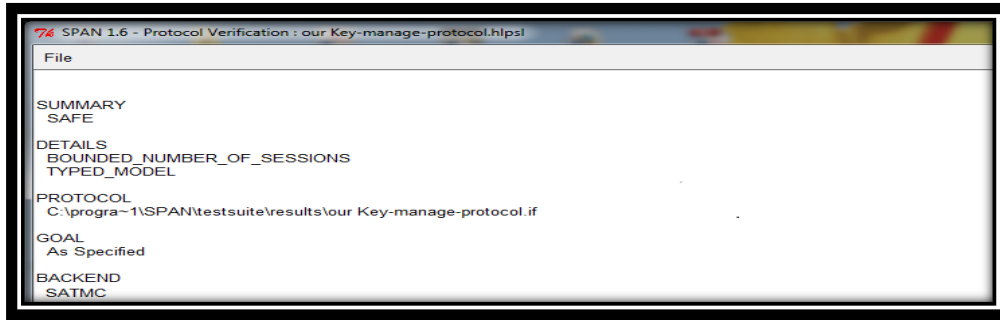


Figure 7. Back-end AVISPA (SATMC)



Figure 8. Back-end AVISPA (TA4SP)

In order to determine the performance of our proposed protocol, we compared our key exchange scheme against others schemes. As seen in table 2, one of the major differences between the proposed method and other mentioned methods is that we propose an authentication phase in our protocol without increasing computational and storage cost in 6LoWPAN network specially for 6LBR and router (R_i). for example in SAKES [26], there is one 6LoWPAN router only that participates in key establishment scheme using DH (Diffie–Hellman) algorithm. Thus, the storage and computational cost in 6LoWPAN router augmente. Unlike SAKES, the proposed model uses the selectioned set of routers based on trust model and employ the cryptographic algorithm ECDH (Elliptic Curve Diffie–Hellman) that it’s considerable as lightweight algorithm more than DH for constrained device .

Another advantage of the proposed method is the used of an access control server that ensure autorisation and authentication in 6LoWPAN network and decrease the storage cost in 6LBR, for example in [27]-[28] did not proposed the authentication system in 6LoWPAN network. However in SAKES, there is an module in border router that ensure authentication in 6LoWPAN network, but this mecanism increases the storage cost in 6LBR Which leads to the network cannot be easily extend.

Table 2. Summarizes the differents metrics of comparaison

Methods	Authentication in 6LoWPAN network	Storage cost in border router (6LBR)	Computational cost in 6LoWPAN router (R_i)	Encryption algorithms	Scalability & extensibility	Resilience
SAKES [26]	+	x	x	x	+	+
Secure communication in IP-based wireless sensor networks via a trusted gateway [27]	-	x	*	*	-	+
Secure and Cost-effective Application Layer Protocol with Authentication Interoperability for IOT [28]	-	*	*	*	-	+
Our protocol	+	*	*	*	+	+

Where+, -, x, *denote respectively: supported, not supported, Important, Low in Overhead.

4. CONCLUSION

Device and network constraints in IoT necessitate the employed protocols to be tailored towards the special requirements of IoT network environments, in this paper we presented a key management protocol suitable a constraint environments like 6LoWPAN network, this protocol has established a shared secret key between the 6LoWPAN Host and a remote server in IPV6 network. During the executing process of our protocol, the constrained node use only symmetric cryptography. Besides, the heavy asymmetric cryptography is affected to selected 6LoWPAN routers.

In addition, authentication system in 6LoWPAN is realized by AC server, this later stock all security-related information about components of 6LoWPAN network. This mechanism mitigate the overhead storage of security information in each node. The security properties are satisfied in our protocol. The future work focus on the adaptation of trust management protocol that allows the 6LoWPAN selects the trusted 6LoWPAN Routers.

REFERENCES

- [1] O. Vermesan, and P. Friess, *Internet of things-from research and innovation to market deployment*: River Publishers Aalborg, 2014.
- [2] F. Liang, L. Zhang, and P. Sun, "Study on the Rough-set-based Clustering Algorithm for Sensor Networks", *Bulletin of Electrical Engineering and Informatics*, vol. 3, no. 2, pp. 77-90, 2014.
- [3] K. Ashton, "That 'internet of things' thing", *RFID Journal*, vol. 22, no. 7, pp. 97-114, 2009.
- [4] C. Bormann, "6LoWPAN Roadmap and Implementation Guide", 2013.
- [5] B. Ozdenizci, V. Coskun, and K. Ok, "NFC internal: An indoor navigation system", *Sensors*, vol. 15, no. 4, pp. 7571-7595, 2015.
- [6] F. Ferdianti, and Y. Triyuswoyo, "Utilization of Near Field Communication Technology for Loyalty Management", *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 11, no. 3, pp. 617-624, 2013.
- [7] R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, "Tailoring end-to-end IP security protocols to the Internet of Things", in *2013 21st IEEE International Conference on Network Protocols (ICNP)*, 2013, pp. 1-10.
- [8] J. Granjal, E. Monteiro, and J. S. Silva, "End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication", in *IFIP Networking Conference, IEEE*, 2013, pp. 1-9.
- [9] Y. B. Saied and A. Olivereau, "D-HIP: A distributed key exchange scheme for HIP-based Internet of Things", in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, 2012, pp. 1-7.
- [10] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15. 4 networks", 2070-1721, 2007.
- [11] J. Hui and P. Thubert, "Compression format for IPv6 datagrams over IEEE 802.15. 4-based networks", Internet proposed standard, RFC 6282, 2011.
- [12] J. Granjal, E. Monteiro, and J.S. Silva, "Enabling network-layer security on IPv6 wireless sensor networks", in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, 2010, pp. 1-6.
- [13] S. Raza, S. Duquenooy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6LoWPAN with compressed IPsec", in *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, 2011, pp. 1-8.
- [14] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the internet of things", *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711-3720, 2013.
- [15] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals", 2070-1721, 2007.
- [16] L.M.S. Committee, *Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)*, 2003.
- [17] J.P. Vasseur, and A. Dunkels, *Interconnecting smart objects with ip: The next internet*: Morgan Kaufmann, 2010.
- [18] K.T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things", *Ad Hoc Networks*, vol. 32, pp. 17-31, 2015.
- [19] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the Internet of Things", *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147-159, 2011.
- [20] M.J. Dworkin, "Sp 800-38c. recommendation for block cipher modes of operation: the ccm mode for authentication and confidentiality", 2004.
- [21] Z. Gong, P. Hartel, S. Nikova, S.H. Tang, and B. Zhu, "TuLP: A family of lightweight message authentication codes for body sensor networks", *Journal of computer science and technology*, vol. 29, no. 1, pp. 53-68, 2014.
- [22] B.C. Neuman, and T. Ts'o, "Kerberos: An authentication service for computer networks", *IEEE Communications magazine*, vol. 32, no. 9, pp. 33-38, 1994.
- [23] Avispa – a tool for automated validation of internet security protocols. <<http://www.avispa-project.org>>.
- [24] S. Moedersheim and P. Drielsma, "AVISPA Project Deliverable D6. 2: Specification of the Problems in the High-Level Specification Language (2003)", ed, 1997.

- [25] D. Dolev and A. Yao, *On the Security of Public Key Products*: Department of Computer Science, Stanford University, 1981.
- [26] H.R. Hussen, G.A. Tizazu, M. Ting, T. Lee, Y. Choi, and K.H. Kim, "SAKES: Secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6LOWPAN)", in *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on*, 2013, pp. 246-251.
- [27] F. Van den Abeele, T. Vandewinckele, J. Hoebeke, I. Moerman, and P. Demeester, "Secure communication in IP-based wireless sensor networks via a trusted gateway," in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on*, 2015, pp. 1-6.
- [28] A.A. Chavan and M.K. Nighot, "Secure and Cost-effective Application Layer Protocol with Authentication Interoperability for IOT," *Procedia Computer Science*, vol. 78, pp. 646-651, 2016.