A secure authentication protocol for IP-based wireless sensor communications using the Location/ID Split Protocol (LISP)

A Secure Authentication Protocol for IP-Based Wireless Sensor Communications using the Location/ID Split Protocol (LISP)

Ali Raheem, AboubakerLasebae, Jonathan Loo
Dept. of Computer & Communication EngineeringSchool of Science and Technology, Middlesex University, London, UK
{A.Raheem; A.Lasebae; J.Loo}@mdx.ac.uk

***Abstract*—the future of the Internet of Things (IoT) involves a huge number of node devices such as wireless sensors that can communicate in a machine-to-machine pattern, where devices will be globally addressed and identified. As the number of connected devices increased, the burden on the network infrastructure and the size of the routing tables and the efficiency of the current routing protocols in the Internet backbone increased as well. Recently, an IETF working group, along with the research group at Cisco, are working on a Locator/ID Separation Protocol as a routing architecture that provides new semantics for IP addressing, in order to simplify routing operations and improve scalability in the future of the Internet such as the IoT. In the light of the previous issue; this paperproposesan efficient security authentication anda key exchange scheme thatis suited for Internet of things based on Locator/ID Separation protocol. The proposed protocol method meets practicability, simplicity, and strong notions of security. The protocol is verified using Automated Validation Internet Security Protocols and Applications (AVISPA) which is a push button tool for the automated validation of security protocols and the achieved results showed that they do not have any security flaws.**

Keywords- Internet of Things;Sensors; LISP; Validation of Internet Protocols; Security communication; Authentication Protocol; AVISPA.

I. INTRODUCTION

There has been a tremendous increase in the use of Internet, from the 365 million users in 2000 to 1.7 billion users and 4 billion of mobile users with over 570 million Internet-enabled handheld devices[1] [2]. That is only the beginning, since it is estimated that the extension of the Internet to smart things will reach 50 to 100 billion devices connected to Internet by the year 2020[3].

This growth leads to a serious scalability problem as well as manageability, addressing/ identity and robustness. In addition, the openness and ubiquity features of the current Internet present problems in providing suitable solutionsfor confidentiality, privacy and security of communications. Therefore, new redesign of the Internet architecture and adefinition of new protocols are required to solve such problems for the Future IoT [4] [5]. For this purpose, several projects from industrial and international collaboration are being carried out to define the Future of the Internet architecture that can solve the limitations of the current architecture [6].The Internet Engineering Task Force (IETF) is working along with the research group at Cisco on the Locator/ID Separation Protocol (LISP) [7]. Since LISP separates hosts' locations and identities; it specifies an architecture and mechanism for replacing the addresses that are currently being used by IP with two separate name spaces: Endpoint IDs (EIDs) used within the EID sites and Routing Locators (RLOCs) used on the transit networks such as the Internet infrastructure. To achieve this separation, LISP defines protocol mechanisms for EID to RLOC mapping [8]. Moreover, LISP assumes the existence of a mapping system in the form of distributed database to store and propagate those mappings globally. The functionality of the mapping system can be summarised by the following: firstly, the registration stage, where the Map Server learns the EIDs-to-RLOC mapping from an authoritative LISP-Capable Router and publishes them in the database. Secondly, it addresses the resolving stage, where the Map Server (MS) accepts Map-Requests from routers, looks up the database and returns the requested mapping previous researches that have concentrated mainly on defining the LISP overall architecture as well as the structure of the LISP packets such as the Map-Register, Map-Notify and Map-Reply [9].

This paper aims to provide secure communication for sensor nodes with a robust authentication key exchange establishment technique resilient to some well-known attacks such as Man in the middle attack, Secret key guessing attack, and replay attack, etc.A formal verification method is used to verify the proposed security protocol. The analysis and the verification of the designed protocol have been implemented via using Automated Validation of Internet Security Protocols and Applications (AVISPA) and SPAN.

The rest of this paper will be sectioned as following: Section II presents a background and related work. Section III demonstrates the proposed protocol for IP-based wireless sensor network using Lisp architecture. Section IV analyses the proposed security protocol while section V discusses the formal verification and validation of the proposed protocol via using AVISPA tool and finally section VI concludes the paper.

II. RELATED WORKS

A number of cryptographic mechanisms have been introduced in the literature for secure authentication and encryption in WSNs such as block ciphers as part of standards based protocols. Thus, these mechanisms need to be modified to suite the resulting IoT scenario.

Figuer et al. [10] proposed a security protocol to access web services in 6LoWPAN. The protocol's objective is to provide a reliable end to end security communication for6LoWPAN by using a compression/decompression of Internet protocol. Furthermore, the protocol provides confidentiality to WSN (6LoWPAN) networks via the use of SNOW Stream cipher. However, this protocol does not address a number of attacks. For example, if the adversary captures one of the sensor nodes of 6LoWPAN,he can find out about the cryptographic data which is stored in the sensor node and disclose the network confidentiality. Added to this, the attacker can launch DoS and wormhole/ sinkhole attacks that make the sensor nodes believe that they are neighbor nodes and forward the packets between them. This may cause confusion to the getaway in locating the node by receiving false data. Another attack may affect the network security called the rushing attack which occurs through the deployment nodes; this could breakdown the communication between the source and the destination by transmitting a huge number of packets at the same time.

Zhou et al. [11] proposed an amended security gateway protocol based on 6LoWPAN, which connects WSN (6LoWPAN) with the IPv6 network. The proposed protocol has used an SNEP mechanism to achieve authentication and confidentiality through providing a secure guarantee to communicate between networks. The main objective of this protocol is to provide security between the getaway and the node against the malicious nodes or any suspected attacks that can compromise the network. However, this protocol does not address the resource consumption attacks i.e. replayed attacks, DoS and physical node capture attacks. E.g. the adversary captures a sensor node (6LoWPAN) via using selective forward attacks or even stealing cryptographic material which is stored on the node by injecting fake packets in the networks. The attacker can launch a man in middle attack between the getaway and the sensor node and steal/or modify the information between them. Also, the Sybil attacks may have a negative impact on the network, where malicious nodes can deliver false information messages to the getaway.

Kothmayr et al**.** [12] hasproposed a security authentication protocol for 6LoWPAN based on RSA mechanism which uses public key cryptography algorithm. The objective of this protocol is to perform authentication in Datagram Transport Layer Security (DTLS) between nodes and the source publisher via the use of handshake based on an exchange of x.509 certificates containing RSA keys. Furthermore, the security protocol provides message integrity, confidentiality and authenticity. However, this study does not consider the encryption of data between the nodes (6LoWPAN). Therefore, a malicious node can spoof the original node information that can cause confusion to the system by transmitting false data, even though it can claim to be an original node to the getaway/or other neighboringnodes by using the act technique.Ikram et al. [13] proposed a simple authentic bootstrapping protocol for IPv6 based on6LoWPAN by using AES encryption which is an encryption standard in IEEE 802.15.4. The purpose of this protocol is to provide resource efficiency and security features assured by secure communications. Furthermore, this protocol dependson the key management infrastructure and it addresses different types of attacks such as, replay attack, location privacy attack, passive eavesdropping, DoS attack and data loss attack. This study assumed that every node (RFDs and FFD) in 6LoWPAN is equipped with AES-CMAC-128, AES-CTR and AES- CCM-128. However, the adversary can launch an overwhelming attack, which can destroy the routing by generating a lot of traffic to affect the performance of the getaway. Moreover, if the adversary compromises nodes; he can launch a combination of wormhole and sinkhole attacks in order to manipulate the use of the routing lists that are included in the route request query. Adding to this, an adversary can manipulate the end-to-end integrity control by modifying a number of messages which will have to travel to their destination to discover that they have been altered. This means that the energy is wasted due to the fact that integrity violations are not detected as soon as possible and the maliciously modified packet is still forwarded to its destination.

Raza et al. [14] proposed a security protocol based on CoAP for IoT. This study has provided a solution to reduce the overhead of DTLS in 6LoWPAN header compression by integrating DTLS and CoAP for IoT. However, the provided protocol offers a secure communication (End-to-End Security) to the 6LoWPAN devices in compression with the DTLS. As ,it does not address the authentication or encryption scheme, a malicious node can claim that it is an original node and can communicate with the getaway or even act as a fake getaway and steal all the information nodes. Furthermore, spoofing on the data can occur, since there is no encryption that provides confidentiality between nodes. Nevertheless, the attacker can track the legitimate encrypted packet of the node. It can copy the encrypted data from the node and givea false information to the getaway which could cause an overloaded network and break down the communication link.

Kim.H [15] provided an analysis of security threats to the 6LoWPAN adaptation layer from the point of view of IP packet fragmentation attacks. The proposed work showed that IP fragmentation is the attack that can mostly affect the 6LoWPAN. As a result, a security mechanism against the packet fragmentation attacks and replay attacks has been proposed. This security mechanism uses Timestamp and None Options that are added to the fragmented packets at the 6LoWPAN adaptation layer. Nevertheless, the mechanism does not address a number of attacks e.g. Packet drop attack/or blackhole which can occur when the router is compromised due to different causes; one of these causes is through the DoS attack because packets are routinely dropped from a network. The adversary can effectively launch a combined rushing and wormhole attack during the neighbour discovery phase and convince the remote sensor nodes that he is one of the neighbouring nodes and adding him to their list.

Bonetto et al. [16] investigated the ability to secure the communication of smart IoT objects. The objective of thiswork is to design a security protocol procedure to set up

secure end to end channels between unconstrained and remote peers and IoT devices. This study addressed the security in terms of resilience against node capture via using IPsec security association. However, this is not enough to provide a high level of protection to the network. The adversary can launch a DoS attack which can affect the performance of the network. Also, the attacker can capture legitimate nodes by launching the selective forwarding attack or by combining the wormhole/ sinkhole/ rushing attacks that affect the communication between the nodes and the getaway. Shaid et al. [17] suggestedanother security protocol based on IPsec to secure the communication between sensor nodes in 6LoWPAN and the hosts in the IPv6-enabled Internet. The goal of this protocol is to provide end to end security via using existing methods and infrastructures. Also, it provides confidentiality and data integrity between the sensor node and the 6LoWPAN router which is connected to the Internet source. However, the attacker can sniff the legitimate encrypted packet of the node. It can copy the encrypted data from the node and give false information to the getaway.

Jung et al. [18] proposed a security protocol for IP-WSN (6LoWPAN) via using ECC based on SSL. The objective of this protocol is to secure both the sensor and the client which is connected to the Internet and that has been achieved by using ECC and SSL which is based on the handshake protocol. The handshake protocol allows the sensor and getaway that are connected to the Internet to be authenticated by negotiating cryptographic algorithms and keys. The protocol provided authentication and confidentiality. Also, there is end to end security between the WSN and getaway that are connected to the source (internet). However, the adversary can launch Man in middle attacks which can be set between the WSN (6LoWPAN) and the getaway as a third party and spoof the data or even modify and send it to other nodes or getaways. Therefore, the need to propose a new authentication protocol that can overcome such deficiencies.

III. THE PROPOSED PROTOCOL FOR IP-BASED WIRELESS SENSOR NETWORK USING LISP ARCHITECTURE

This section discusses an authentication and key exchange protocol to secure sensor nodes communication based on LISP protocol architecture. The protocol uses bit-wise exclusive or operation technique.In this protocol, the used notations are described as the following:

Table 1: Protocol Notations

The Notation	Definition
Sensor-A and Sensor-B	Two communication parties, Wireless Sensor Node; its sensor device has IP address and prefixes identifying the end-points call EID.
XTR	XTR refers to a device which functions both as an Ingress Tunnel RouterITR and an Egress Tunnel RouterETR (which is usually typical),
$(\mathcal{G}, g, p)$	A finite cyclic group $\mathcal{G}$ generated by an element g of prime order p;
N, Z	Is an element in $\mathcal{G}$
PSK_A, PSK_B	Public keys of Sensor–A and Sensor-B which is shared with XTR
K_A, K_B	Private Keys of Sensors-A and B
$\oplus$	Bit-wise exclusive or operation;
H, H'	Two secure on-way hash functions.
SK	Session key of (Sensor-A and Sensor-B)

In this system it has been assumed that two communication parties Sensor-A and Sensor-Bwant to communicate together in secure way. Let PSK_Abe the secret key shared between the Sensor-A and XTR which is arbitrary bit string. Here Sensor-A stores(K_A, PSK_A), while the XTR stores $(PSK_A, U_{Sensor-A})$ where $U_{Sensor-A} = g^{kA}$ and $(PSK_A, K_A)H(PSK_A, K_A, id_{Sensor-A},)$. Similarly, PSK_B can be the secret key shared between Sensor-B and XTR. Again, Sensor-B stores(PSK_B, K_B)while the XTR stores $U_{Sensor-B} = g^{KB}$ and$(PSK_B, K_B)H(PSK_B, K_B, id_{Sensor-B})$.

3.1 The Security Protocol

The following messages show the protocol procedures:

Step1a. Sensor-A chooses a random number $x \in_R \mathbb{z}_q$ and computes $(id_{Sensor-B}, id_{Sensor-A}, PSK_A)H \oplus g^x \rightarrow \mathrm{N}_{\mathrm{Sensor-A}}$and sends $(N_{Sensor-A}, id_{Sensor-A})$ to Sensor-B.

Step1b. Sensor-B chooses a random number $y \in_R \mathbb{z}_q$ and computes $(id_{Sensor-B}, id_{Sensor-A}, PSK_B)H \oplus g^y \rightarrow \mathrm{N}_{\mathrm{Sensor-B}}$ and sends $(N_{Sensor-A}, id_{Sensor-A}), (N_{Sensor-B}, id_{Sensor-B})$ to XTR router.

Step2a. Upon receiving $(N_{Sensor-A}, id_{Sensor-A})$and $(N_{Sensor-B}, id_{Sensor-B})$, XTR uses PSK_A and PSK_B to compute $(id_{Sensor-B}, id_{Sensor-A}, PSK_A)H \oplus \mathrm{N}_{\mathrm{Sensor-A}} \rightarrow g^x$ and $(id_{Sensor-B}, id_{Sensor-A}, PSK_B)H \oplus \mathrm{N}_{\mathrm{Sensor-B}} \rightarrow g^y$ respectively.

Step2b. Then XTR chooses a random number $z \in_R \mathbb{z}_q$ to compute $(U_{Sensor-B})^z, (U_{Sensor-A})^z, g^z \rightarrow L$,$(g^x)^z \rightarrow g^{xz} \rightarrow a$, $(g^y)^z \rightarrow g^{yz} \rightarrow b$. Then XTR computes $((U_{Sensor-A})^z, g^x, id_{Sensor-B,} id_{Sensor-A,} PSK_A)H \oplus b \rightarrow Z_{Sensor-A}$ and $((U_{Sensor-B})^z, g^y, id_{Sensor-B,} id_{Sensor-A,} PSK_B)H \oplus a \rightarrow Z_{Sensor-B}$ and sends $(Z_{Sensor-A}, L), (Z_{Sensor-B}, L)$ to Sensor-B.

Step3a. OnceSensor-B receives the sent message it uses KB to compute $L^{KB} \rightarrow (U_{Sensor-B})^z$ and $((U_B)^z, g^y, id_{Sensor-B}, id_{Sensor-A}, S_{Sensor-B})H \oplus Z_{Sensor-B} \rightarrow a$ and authenticates XTR. Now, Sensor-B uses y to compute$a^y \rightarrow g^{xyz} \rightarrow K$, $(K, id_{Sensor-B}, id_{Sensor-A})H \rightarrow \alpha$and forwards $(Z_{Sensor-A}, L), \alpha$to Sensor-A.

Step3b. Sensor-A receives $(Z_{Sensor-A}, L, \alpha)$ and it uses K_A to compute $(U_{Sensor-A})^z \rightarrow L^{KA}$ and $((U_{Sensor-A})^z, g^x, id_{Sensor-B}, id_{Sensor-A}, PSK_A)H \oplus Z_{Sensor-A} \rightarrow b$ and authenticates the XTR router. Then Sensor-A uses x to compute $b^x \rightarrow g^{xyz} \rightarrow K$ and checks whether $(K, id_{Sensor-B}, id_{Sensor-A})H \rightarrow \alpha$ holds or not. If it does hold, Sensor-A terminates the protocol, otherwise Sensor-A is convinced that K is valid session key. After that Sensor-A computes $(K, id_{Sensor-B}, id_{Sensor-A})H \rightarrow \beta$ and forwards it to Sensor-B. Sensor-A computes the Session Key $(K, id_{Sensor-B}, id_{Sensor-A})H' \rightarrow Sk_{Sensor-A}$.

Step3c. Upon receiving β, Sensor-B computes $(K, id_{Sensor-B}, id_{Sensor-A})H \rightarrow \beta$ and verifies whether computed β is equal to the received β. If both are equal then B authenticates Sensor-A and computes the session key $(K, id_{Sensor-B}, id_{Sensor-A}) \rightarrow Sk_{Sensor-B}$

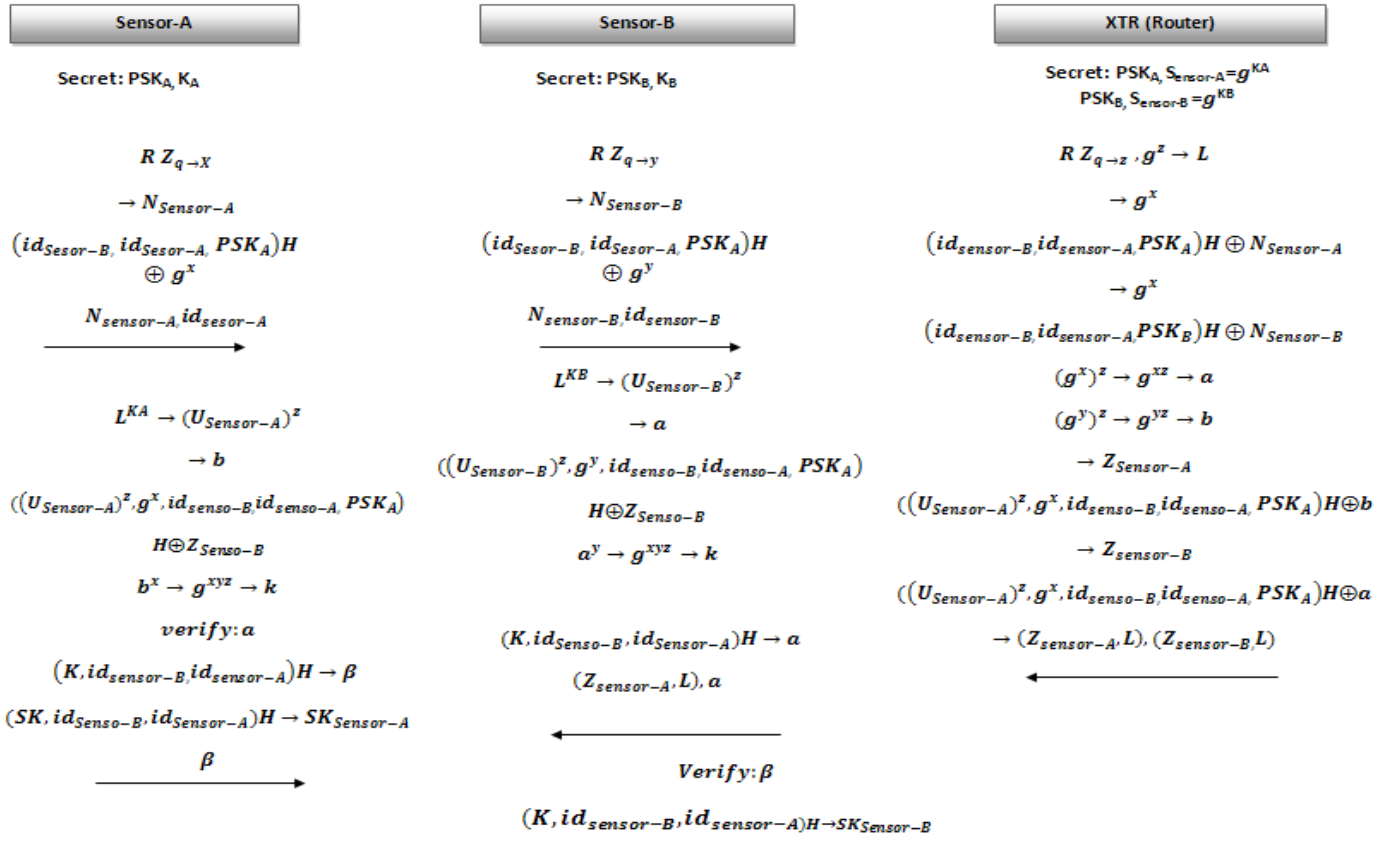

Figure 1: The Proposed Security Protocol for Sensor node communication using LISP network

IV. SECURITY PROTOCOL ANALYSIS

The main goal of the proposed protocol is to achieve mutual authentication between the sensor nodes and router XTR when the nodes are communicating with each other. Therefore, this paper presents a simple example for authenticating the communicationbetween two nods (Sensor-A and Sensor-B) and between the XTR.

-Trivial attacks:

Computing the session key from the transmitted messages $\alpha$and$\beta$is impossible due to the one-way of hash function and, also, for computing it from other transmitted messages. The latter can be$Z_{Sensor-A}$ or $Z_{Sensor-B}$ where an attacker has to face the difficulty of a discrete logarithm problem. Therefore, this protocol is resistant to trivial attack.

-Secret keys guessing attacks:

Suppose an attacker or a malicious node Sensor-B tries to guess Sensor-A secret key as PSK_A generates $(id_{Sensor-B}, id_{Sensor-A}, PSK_A)H \oplus N_{Sensor-A} \rightarrow g^{x'}$ and sends it to the XTR router in online Message 1 of the protocol. To verify the correctness of his guessed secret key; it needs to compute $((U_{Sensor-A})^z, g^x, id_{Sensor-B}, id_{Sensor-A}, PSK_A)$ $H \oplus Z_{Sensor-A} \rightarrow$ band$((U_{Sensor-B})^z, g^y, id_{Sensor-B}, id_{Sensor-A}, PSK_B)$ $H \oplus Z_{Sensor-B} \rightarrow a$as it needs the values of K_A and K_B for computing $(U_{Sensor-A})^z$ and $(U_{Sensor-B})^z$. Similarly remaining off-line also, using the transferred messages $N_{Sensor-A}, N_{Sensor-B}, Z_{Sensor-A}, L$, an attacker cannot verify the correctness of its guessed secret key.

-Man in the middle attack:

In message 2 of the protocol, XTR authenticates the two communicating parties Sensor-A and Sensor-B from the message $(id_{Sensor-B}, id_{Sensor-A}, PSK_A)H \oplus g^x \rightarrow N_{Sensor-A}$ and $(id_{Sensor-B}, id_{Sensor-A}, PSK_B)H \oplus g^y \rightarrow N_{Sensor-B}$ sent by Sensor-B. Sensor-A and Sensor-B authenticate XTR, from $((U_{Sensor-A})^z, g^x, id_{Sensor-B}, id_{Sensor-A}, PSK_A)H \oplus b \rightarrow Z_{Sensor-A}$ and $((U_{Sensor-B})^z, g^y, id_{Sensor-B}, id_{Sensor-A}, PSK_B)H \oplus a \rightarrow$

$Z_{Sensor\ -B}$ as PSK_A, PSK_B are known only to XTR. Finally, Sensor-A authenticates Sensor-B from$(K, id_{Sensor\ -B}, id_{Sensor\ -A})H \rightarrow \alpha$. Thus, in each message of the protocol, each party authenticates the other communicating party and hence there is no scope for man in the middle attack.

-Forgery attacks:

In this case the XTR is compromised, the attacker is required to compute $(id_{Sensor\ -B}, id_{Sensor\ -A}, PSK_A)H \oplus N_{Sensor\ -A} \rightarrow g^x$ and $(id_{Sensor\ -B}, id_{Sensor\ -A}, PSK_B)H \oplus N_{Sensor\ -A} \rightarrow g^y$ where PSK_A and PSK_B are secret keys of Sensor-A and Sensor-B respectively. However it is not possible to compute these values without the knowledge of the secret keys and hence Sensor-A and Sensor-B cannot construct the common session key.

-Replay attack:

Since one wayhash function is used, this protocol is invulnerable to this attack.

-Perfect forward secrecy:

When the secret keys of PSK_A and PSK_B of Sensor-A and Sensor-Bdeceives are compromised, the attacker cannot calculate the session key as K_A and K_B are known. These values remain unknown even to the XTR router so there is no chance of any compromise. Also, the session key is independent on any session and x, y, z are randomly chosen.

The security-related goals could be achieved using different protocols, examples of that; there are the Internet key Exchange (IEK) and the virtual Private Network (VPN) protocols such as the Internet Protocol Security (IPSec). However, these protocols will increase the number of exchanged messages significantly, at least five extra messages in the case of IKE and more than this, in the case of IPSec (based on the IPSec mode). Furthermore, packets encapsulation due the tunneling process in VPN protocols will lead to adding extra load to the header of Sensor communication packets which make them incompatible with the current implementation Sensor communication capable devices.

V. FORMAL VERIFICATION AND VALIDATION OF THE PROPOSED PROTOCOL

5.1. AVISPA

AVISPA is a push tool for the automated validation of security protocols. A modular and expressive formal language called High level protocols specification language (HLPSL) is used by AVISPA to specify the security protocol and their properties. HLPSL is a role-based language, meaning that we first specify the sequence of actions of each kind of protocol participant in a module, which is called a basic role. This specification can later be instantiated by one or more agents playing the given role. Later on, this paper will specify how the resulting participants interact with one another by combining multiple basic roles together into a composed role. HLPSL specification is translated into the Intermediate Format (IF), using hlpsl2if. The IF specification is then processed by model-checkers to analyze if the security goals are violated. There are four different verification back end tools use to analyze the IF specification namely; OFMC (on-the-Fly Model-Checker), CL-AtSe (Constraint-Logic-based Attack Searcher), SATMC (SAT-based Model-Checker), TA4SP (Tree Automata-based Protocol Analyzer). Possible flaws in a protocol can be identified using these back end tools. As, exponential and XOR operations are supported by CL-AtSe and OFMC back ends, OFMC back end tool will be used with AVISPA and SPAN (Animation tool for AVISPA) to analyze the proposed protocols.

5.2. Specification and Verification of protocol

As mentioned earlier, the proposed protocol has been implemented and evaluated using AVISPA protocol analysis tool. The achieved result has shown that no attack is being found. For this protocol, three basic roles played by Sensor (A), Sensor (B) and XTR (R) router have been defined. PSK_A and PSK_B are shared with XTR and hence represent the symmetric keys . K_A andK_B remain secret with Sensor-A and Sensor-B as their private keys. XTR router gets $U_{Sensor\ -A} = \exp(G, K_1)$ from Sensor-A and $UB = \exp(G, K_2)$ from Sensor-B. Hence $U_{Sensor\ -A}$ and $U_{Sensor\ -B}$ are the public keys whose inverse is known only to Sensor-A and Sensor-B respectively. After defining the #basic roles, it is essentially needed to define the composed roles which describe the sessions of the protocol. The #composed roles have no transition section, but rather a composition section in which the basic roles are instantiated.

The /\ operator indicates that these roles should execute in parallel. In the *session role*,it usually declares all the channels used by the basic roles. These variables are not instantiated with concrete constants. The *channel* type takes an additional attribute, in parentheses, which specifies the intruder model that assumed for that channel. Here, the type of the declaration *channel (dy)* stands for the Dolev-Yao intruder model. Under this model, the intruder has full control over the network, i.e. all messages, sent by agents, will go to the intruder. He may intercept, analyze and /or modify message (as far as he knows the required keys), and send any message he composes to whoever he pleases, posing as any other agents. Finally, a top-level role is always defined. This role contains global constants and a composition of one or more sessions, where the #intruder may play some roles as a legitimate user. There is also a statement which describes what knowledge the intruder initially has. Typically, this includes the names of all agents, all the symmetric keys and any shares with others.Note that the constant 'I'is used to refer to the intruder as the source code shows in the appendix.

#Specifying Security Goals are specified in HLPSL by augmenting the transitions of the basic roles with the so-called goal facts and by then assigning them a meaning by describing, in the HLPSL *goal* section, what conditions – i.e. what combination of such facts indicate an attack and a violation of *secrecy*. The goal declaration section describes that it should be considered as an attack when the intruder learns a secret value internally, the attack conditions are

specified in terms of temporal logic but useful and concise macros are provided for two most frequently used security goals, authentication and secrecy.

Table 1 shows the results of security protocol authentication for sensor nodes communication based on LISP network.

Table 1: AVISPA Tools (OFMC, ATSE, SATMC, and TA4SP) Results

Version	Tool	Description	Result
Basic session	OFMC	VisitedNodes:23453 nodes Depth: 6 plies Search Time: 0.8s	SAFE
Basic session	ATSE	Analysed: 3874 States Reachable: 2635 States Translation: 0.00 seconds Computation: 0.06 seconds	SAFE & goal as specified
Basic session	SATMC	STATISTICS Attack Found : false Boolean Upper Bound Reached: true Boolean Graph Leveled off: 5 steps Sat Solver: zchaff Solver Max Steps Number: 11 Steps Steps Number : 5 Steps Atoms Number: 543 Atoms Clauses Number 1613 Clauses Encoding Time: 0.2 Seconds If2Sate Compilation Time 0.06 Seconds ATTACK TRACE %%no attacks have been found…	SAFE
Basic session	TA4SP	STALISTICS SECURITY-As specified ATTACK TRACE No attack found	SAFE

VI. CONCLUSION

With the increasing need for authentication and secure communication, this paper has proposed a security protocol for ip-based sensor network using LISP architecture. The achieved results showed that the proposed scheme is more secure and efficient than the existing protocols .Moreover; it can resist all the well-known attacks. The formal verification of the proposed protocol via using AVISPA tool showed that there are no attacks against any of the checked assertions that the protocol successfully achieved through a number of crucial security requirements. Examples of such requirements arethe mutual authenticating, the participating parties and maintaining the security of the session key between Sensor A and Sensor B.

ACKNOWLEDGMENT

The authors would like to thank all those who contribute to the completion and success of this work. Thanks are extended to the science and technology department at Middlesex University that has played indeed a significant role in supporting and backing this work.

REFERENCES

[1] H.Sundmaeker, P.Guillemin,P.Friess,andS.Woelffle. ‘Vision and Challenges for Realising the Internet of Things’. European cluster CERP-IoT, European Union, ISBN: 978-92-97-15088-3,2010.

[2] G. Shen, and B. Liu, ‘The visions, technologies, applications and security issues of Internet of Things’. E-Business and and E-Government (ICEE), 2011 International Conference, Shanghai, China, pp. 1–4.

[3] L. Atzori, A. Iera, G. Morabito, “The Internet of Things: A survey. Computer Network”, Computer Networks 54, 2010, Elsevier, 54(15):2787–2805.

[4] D.Papadimitriou, H,Tschofenig,H,Rosas, and S.Zahariadis, ‘Fundamental Limitations of Current Internet and path to Future Internet and the path to Future Internet, European Commission’’ FIArch Group, Ver.1.9,2010.

[5] ITU Internet Reports. ‘The Internet of Things’. Available at: http://www.itu.int/osg/spu/publications/internetofthings/, Access on12.jan.2013

[6] N. Kushalnagar, G.Montenegro, J.Hui, D. Culler, ‘Transmission of IPv6 Packets over IEEE 802.15.4 Network’’ ,RFC 4944, 2007.

[7] V. Kafle, P. Otsuki, and H .Inoue. ‘An ID/locator split architecture for future networks’, Communications Magazine, 2010 IEEE, pp.138-144.

[8] Cisco. ‘Locator/ID Separation Protocol Security’. Available at: http://www.cisco.com/web/strategy/docs/gov/45325_encrypEnviron_wp.pdf Accessed on 2.Mar.2013.

[9] F. Maino, V. Ermagan, A.Cabellos, A. Saucez, and O. Bonaventure, ‘LISP-Security (LISP-SEC)’.Network Working Group Internet-Draft. Available at: http://tools.ietf.org/wg/lisp/draft-ietf-lisp-sec/draft-ietf-lisp-sec-03-from-02.diff.htmlAccessed on 4.Feb.2013

[10] P.Figueroa, J.Perez, I.Amezcua, V.Hernandez, ‘’A Lightweight and secure protocol to Access web services in 6LoWPAN’’ IEEE the Electrical Communications and Computers (CONIELECOMP), 2012 22nd International Conference, 978-1-4577-1326-2, 27-29 Feb. 2012

[11] Y.Zhou, Z.jia, X.Sun, L,ju, ‘’Design of Embedded Secure Gateway Based on 6LoWPAN’’ communication technology (ICT), 2011 IEEE 13th International Conference, 978-1-61284-306-3, 25-28 sept. 2011.

[12] T.Kothmayr, C.Schmitt,CW.Hu, M.BruningG.Carle, ‘’DTLS based security and two-way authentication for the Inernet of Things’’ Ad Hoc Network journal (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.003

[13] S.Khan, C.Pastrone, L.Lavagno, M.Sporito. ‘’An Authentication and Key Establishment Scheme for the IP-Based Wireless Sensor Network’’ The 7th International symposium on Intelligent Systems Techniques for Ad hoc and Wireless sensor Network (IST-AWSN), SciVersescienceDirect, 2012.

[14] S.Raza, H.Shafagh, K.Hewage, R.hummen,T.Voigt, ‘’Lithe: Lightweight Secure CoAP for the Internet of Things’’ Sensors Journal,IEEE, vol., no., pp.3711-3720, oct.2013

[15] H.Kim, ‘’Protection against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer’’ Convergence and Hybrid Information Technology,2008. ICHIT 08.Interational Conference, vol., no., pp.796-801, June 28-30 Aug 2008.

[16] R.Bonetto, N.Bui, V.Lakkundi, A.olivereau, A.Serbanati, M.Rossi, ‘’Secure Communication for Smart IoT Objects Protocol Stacks, Use Cases and Practical Examples’’ World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International symposium , no., pp.1-7, June 25-28 Aug 2012.

[17] S.Raza, S.Duquennoy, T.Chung, D.YazarT.Voigt, U.Roedig ‘’Securing Communication in 6LoWPAN with Compressed IPsec’’ Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference, no., pp.1-8, June 27-29 2011.

[18] Jung,W; Hong,S;Ha,M;kim,Y;Kim,D; ‘’ SSL-based Lightweight Security of IP-based Wireless Sensor Networks’’ Advanced Information Networking and Applications Workshops, 2009.WAINA 0, International conference , no., pp.112-1117, June 26-29 2009.