Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments

Pardeep Kumar, *Member, IEEE*, Andrei Gurtov, *Senior Member, IEEE*, Jari Iinatti, *Senior Member, IEEE*, Mika Ylianttila, *Senior Member, IEEE*, and Mangal Sain

***Abstract*— The proliferation of current wireless communications and information technologies have been altering humans lifestyle and social interactions—the next frontier is the smart home environments or spaces. A smart home consists of low capacity devices (e.g., sensors) and wireless networks, and therefore, all working together as a secure system that needs an adequate level of security. This paper introduces lightweight and secure session key establishment scheme for smart home environments. To establish trust among the network, every sensor and control unit uses a short authentication token and establishes a secure session key. The proposed scheme provides important security attributes including prevention of various popular attacks, such as denial-of-service and eavesdropping attacks. The preliminary evaluation and feasibility tests are demonstrated by the proof-of-concept implementation. In addition, the proposed scheme attains both computation efficiency and communication efficiency as compared with other schemes from the literature.**

***Index Terms*— Authentication, access control, security, smart homes, wireless sensor networks.**

I. Introduction

NOWADAYS, the advancement in electronics, communications and information technologies and the Internet have led to the rapid proliferation of smart home environments. The smart home environments are envisioned as being able to exhibit various forms of *advanced intelligence* by enhancing traditional home automation systems with new *smart functions and services* addressing diverse high-level goals of well-being like increasing comfort, reducing operational costs, and guaranteeing safety and security of the inhabitants.

Such smart homes have great possibilities to enable a variety of use cases, *e.g.,* light control system, appliance control system, climate control, multimedia system, smart energy system, and security and safety system [1]–[3]. Moreover, there is a tremendous business/research potential for the smart appliances in home environments that can give an independent life to the elderly and disabled people [4]. A smart home can also provide a remote care to a resident suffering from a cognitive deficit to complete his activities of daily living activities (ADL) [1], [5]. Recently, several research projects have been initiated to develop the smart homes, *e.g.,* HOPE (smart home for elderly people) [6], SM4ALL (smart home for all) [7] and GENIO (next generation home) [8], *etc*.

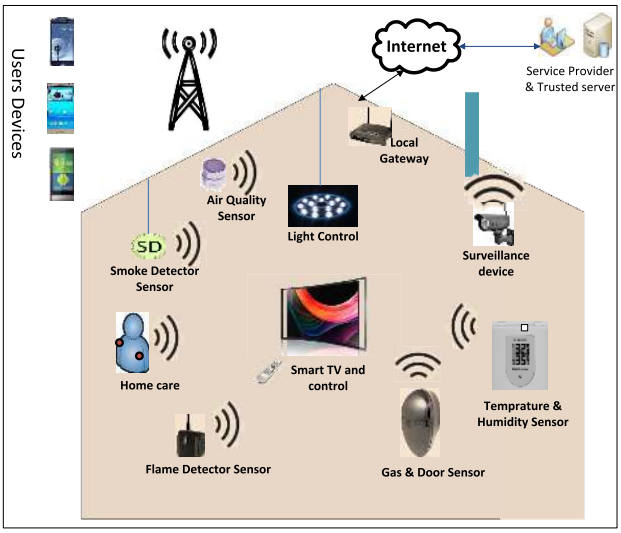

Fig. 1. Smart home environment.

Typically, a smart home network consists of a number of heterogeneous smart devices, such as, low-cost sensor, actuator, smart light, smart window shutter, smart thermostat and surveillance camera or other type of smart devices that are integrated with *intelligence*, as shown in Fig. 1. Note that home environments and networks are used interchangeably. Most of the devices are having resource-limitations (*e.g.,* computational power, bandwidth, and battery power) [9]. However, in such home networks, the SDs communicate over the wireless channels through the local home gateway. The home gateway acts as a bridge between the SDs and the users, and provides interoperability and control for the SDs, connect to the outer world via the Internet [10], [11]. Thus the novelties of SDs are enabling users to operate homes (or to monitor elderly and disabled people) remotely/directly using the smart phones, tablets, or through designated web apps, anywhere and anytime.

Nevertheless, smart homes open up an attack surface as the SDs data collected and communicated over insecure wireless networks, leaving them vulnerable to security attacks. The

Manuscript received July 31, 2015; accepted August 16, 2015. Date of publication September 1, 2015; date of current version December 10, 2015. This work was supported by TEKES under Project The Naked Approach, in part by RFBR research project (14-07-00252), and in part by the Dependable Wireless Healthcare Networks. The associate editor coordinating the review of this paper and approving it for publication was Prof. Subhas C. Mukhopadhyay.

P. Kumar, J. Iinatti, and M. Ylianttila are with the University of Oulu, P. O. Box 4500, FI-90014, Finland (e-mail: pkumar@ee.oulu.fi; ji@ee.oulu.fi; mika.ylianttila@cie.fi).

A. Gurtov is with the Helsinki Institute for Information Technology, Aalto University, P.O. Box 15600, 00076 Aalto, Finland and ITMO University, St Petersburg, Russia, 197101 (e-mail: gurtov@hiit.fi).

M. Sain is with Dongseo University, San 69-1, Jurye-2-Dong, Sasang-Gu, 617-716 Busan, Korea (e-mail: mangalsain1@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSEN.2015.2475298

ability for an unauthorized user to remotely monitor or control video and audio within a household would concern an owner. As such, an attacker may profit financially by selling the individual data obtained via eavesdropping on the smart home area networks. Maliciously heating or cooling a home at the extreme temperatures both increases utility costs and added additional strain on the heating, ventilating, and air conditioning (HVAC) systems [12]. However, there are several security challenges in an interconnected smart homes due to the lack of security standards of the SDs. Furthermore, most of the SDs are incompatible with standard networking protocols, which makes them susceptible to a number of security threats. In [13], Chen and Luo pointed out that the smart appliances (devices) are not yet equipped with enough security protection mechanisms. For instance, a smart meter follows the remote control commands without verifying the authenticity of such commands. Moreover, in such smart spaces, the threats arise due to inadequate designing of the security protocol in lossy smart devices. On the other hand, resource constrained nature of a SD makes it challenging to meet robust security because of the lower processor speed, a small amount of memory and a low link bandwidth.

Although, in recent years a significant amount of works guided towards the smart home security [2], [12]–[18], most of the approaches, *e.g.,* [2], [14]–[16] incurred the high amount of overhead to perform the device authentication and leaving out other security properties. Additionally, the studies so far only consider eavesdropping adversaries, SD compromise is not considered as a part of the threat model, which could be a more severe threat to the smart homes. Furthermore, how the poor security protocols can be abused to control the SDs are shown in [19] and [20], thus breaches the smart homes security. Apparently with regards to the technological advancements, it appears that the smart homes are vulnerable to unauthorized access (*i.e.,* because all the entities are not trusted) and security attacks. As a result, preventing the SDs sensitive data from being revealed to an adversary over insecure wireless channels, an adequate security is highly required from the very beginning of a home network deployment — that verify whether the entities involved in a smart home are the exact parties they appear to be.

To satisfy an adequate level of security, this paper presents a lightweight and secure session key establishment scheme. The scheme allows each entity should be performed a lightweight mutual authentication prior participation in the home network and establish a session key in a secure manner. To verify the device authentication and message integrity, we utilize the smart device's unique and immutable identifier, hereafter denoted as its *Silicon ID* (*i.e.,* a silicon serial chip number [21]). Unlike the other protocols, the proposed scheme uses the symmetric key cryptography [22] and a hash function to compliment other techniques in order to provide robust security in the smart homes. In addition, a new device can be easily entered arbitrarily and configured securely into the scheme to extend the smart home services. The security attributes (*i.e.,* authentication and confidentiality) are formally verified using the AVISPA tool [23]. Then, the security analysis shows that the proposed scheme is secure against the Dolev-Yao attack model [24]. The performance and efficiency of the proposed scheme are evaluated using the test bed.

The rest of this paper is organized as follows. Section II discusses the works that are relevant to this paper, and Section III shows system design and security properties. Section IV presents the proposed scheme, and Section V shows the proposed scheme analysis. Section VI concludes the paper.

II. Literature Survey

An enormous number of works incorporating security features in the smart home applications have been proposed, each scheme has its own merits and demerits. However, this paper describes those literatures that are recently proposed for the smart home area networks, and for the smart home appliances.

Gomez and Paradells [1] discussed a different types of wireless home automation network architectures and technologies, including security obstacles of the ZigBee, INSTEON, Wavenis and Z-wave, and for the IP-based technologies. Similar to [1], Ayday-Rajagopal has also noticed that the existing home area network (HAN) protocols (ZigBee, Z-wave, and INSTEON) support security only up to a certain level [25]. They introduced three different secure device authentication mechanisms for smart grid-enabled HAN. For example, (1) authentication mechanism between the gateway and the smart meter; (2) authentication between the smart appliances and the HAN; and (3) authentication between the transient devices and the HAN. However, to perform the authentication, the schemes presented in [25] are (heavily) depending on 3rd party (such as, the Internet service provider, or telecommunication companies), and then it providing security to the HAN.

The security scheme in [13] aimed a secure smart household appliances framework, named S2A. The authors conceptually focused on the usability, controlling electricity prices, and operational safety for the smart devices (*i.e.,* appliances). By employing a machine learning method, the S2A framework provides an effective and reliable security protection. However, it (S2A) does not consider the fundamental security properties (*i.e.,* device authentication, data confidentiality, and integrity), which means the framework may not withstand under a collaborative adversary model (*e.g.,* the Dolev-Yao model).

Vaidya et al. [15] proposed a device authentication mechanism for smart energy HANs. Based on the elliptic curve cryptography (ECC), each device has access to a certificate authority to obtain an implicit certificate. A session key is established between two involved entities. Authors claimed their scheme is efficient compared to other existing schemes. However, security analysis did not provide much details — how their device authentication is secure against attacks, and how the scheme is efficient than others.

Han et al. [16] presented a novel secure key pairing protocol for radio frequency for consumer electronics (RF4CE) ubiquitous smart home system. Different consumer electronics devices (*e.g.,* 802.15.4) are forming a smart home network. In the scheme, each device sends own authentication information to a mobile operator (MO) to be authenticated. After the

first-level of authentication, MO sends the device information further to the device manufacturers to be authenticated, again. The proposed scheme is based on the symmetric key cryptography, which is easy to implement in a home environment. However, the main requirement of Han et al.'s scheme is that the manufacturers have to be always online, it may not be always pragmatical. In addition, the communication costs of their proposed scheme would be expensive for the low-resource devices.

Guillet et al. [17] developed a correct by construction security approach to design a fault tolerant smart home for the disabled people. The proposed scheme exploits a formal technique named discrete controller synthesis (DCS) to automatically control the devices. To control a device, authors presented two types of security constraints expressed as boolean expressions: (i) *hypothesis* (supposed to remain true for all execution); and (ii) *guarantee* (enforced to remain true using DCS if and only if the *hypothesis* stays true), for a detailed information, reader may refer to [17]. Though, the scheme employing formal techniques and boolean expressions to control the devices states (*e.g.,* on/off), the authenticity of boolean expressions are not being verified. Therefore the scheme may not work under active attacks.

Kim et al. [2] presented a seamless integration of heterogeneous devices and access control in smart home. Authors observed that there is a lack of the de facto communication standard in the interoperability of device from different vendors in the smart homes. Therefore, based on the open services gateway initiative (OSGi) they proposed a smart home architecture that integrates heterogeneous protocols in the HAN. In their architecture, an access control model manages authentication and authorization for different users' requests. In addition, the remote access is available only through the Restful web services. However, this scheme did not consider a device authentication at the time of home network deployment.

Based on ECC, Li's [14] designed a key establishment protocol for smart home energy management system. The scheme consists of two entities, a node and a security manager. Each entity obtains public and private keys through an out-of-band channel from a trusted certificate authority. However, the security analysis of Li's scheme is very limited. In addition, the public key operations are still too expensive for a sensor, in terms of the time complexity.

In another research, Fabian and Feldhaus [18] proposed a peer-to-peer privacy-preserving data infrastructure for the smart home appliances. Their scheme uses a distributed hash table (DHT) and provides anonymity to the smart home appliances using RFID (radio frequency identification).

Different from the literature survey, in this paper we envision that there is still an immense need of lightweight security mechanism in the smart home networks (from the beginning of SDs deployment) that could be a trade-off between security and efficiency for the resource-constrained SDs.

III. System Design and Security Properties

A. System Design

Consider a smart home internal network that comprises of N number of heterogeneous SDs (temperature sensor, smart light, multimedia device, and the home gateway, *etc.*). As shown in Fig. 2, the resource-constrained SDs are communicating to the home gateway (HG) over the wireless channels using a HAN protocol (*e.g.,* ZigBee) [10], [25]–[28]. The communication pattern named as SD-To-HG [10]. With the hand-held devices (*e.g.,* smart phone and laptop), a user can monitor and operate the SDs either directly or remotely through the home gateway, which is connected to the Internet (IPv4/IPv6). In addition, the SDs would be controlled easily in an *ad-hoc* manner.

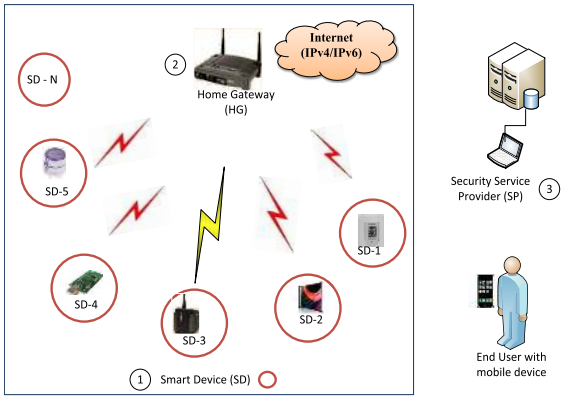

Fig. 2. SD-to-HG communication pattern in smart home.

As shown in Fig. 2, three entities are mainly involved in a smart home environment, as follows.

1) The SD forwards home data to the home gateway using a single-hop link. Similarly, the home gateway can perform queries to the SDs, whenever needed.
2) The home gateway is a special node that takes responsibility of controlling the network data, device and network interoperability, and security management [3]. In addition, the gateway works as a router between the SDs and the end users. It has two wireless interfaces: (i) a short-range wireless interface (*e.g.,* 802.15.4) maintains the connection within the internal (smart) devices, and (ii) a long-range communication interface (*e.g.,* Wi-Fi/GPRS) maintains a connection with the outer world [29].
3) Security service provider is a trusted server, and is responsible for generating and assigning the keying material to the smart home entities.

B. Security Properties

A number of recent works (*e.g.,* [3], [22]) have identified the detailed account of major security properties that should be considered from the beginning of a smart home internal networking, as follows.

1) *Mutual Authentication:* In a smart home, an adversary may pretend to be another legal entity in order to obtain the SDs sensitive data regarding the smart home services. Therefore, each SD should perform the mutual authentication and verify the legitimacy of involved entities. Thus it can prohibit unauthorized network access from the adversaries or compromised devices.
2) *Session Key Establishment:* After performing identification and verification processes, the legal

entities should be agreed on a session key that can ensure security for further communications between the legitimate entities.

3) *Message Confidentiality:* In a smart home network, since the SDs collect and forward sensitive data wirelessly to the home gateway, an adversary (eavesdropper) may enable indirect surveillance on the resident and appliances activities by monitoring the wireless channels [3]. Thus, the protocol messages are vulnerable to information leakage (and eavesdropping) attacks. The standard approach to protect the devices data is message confidentiality [14] that could avoid the eavesdropping attacks on the smart home networks.
4) *Message Integrity:* The inhabitants living in a smart home are relying on the SDs data, keeping confidentiality does not protect the data from external modifications (*e.g.,* data tampering). Message integrity would ensure to the receiver that received data is not altered by an attacker while in transit.
5) *Message Freshness:* Perrig et al. [30] suggested that it is not sufficient to guarantee only message confidentiality and authentication but an adequate security protocol must ensure freshness of each received message.
6) *Lightweightness:* The security protocols are an overhead to the applications, therefore authentication and session key establishment should be lightweight (and/or energy-efficient), particularly for the resource-hungry SDs [31].
7) *Safeguard to Popular Attacks:* Clearly, the security scheme should resist to different popular attacks, *e.g.,* masquerade, message forgery, message replay, known-key, node compromise and denial-of-service.

IV. Proposed Scheme

To provide an adequate security in the smart homes (refer Fig. 2), this section presents the proposed scheme that satisfies all the security properties outlined in Sub-section III-B. The smart devices are to be authenticated prior to their participation from the very beginning of the home network deployment. The proposed scheme can enable in many use-cases, *e.g.,* light system, appliance control system, climate control system, home-care, activities of daily living (ADL), smart energy system, and security and safety system. Table I defines the used symbols and our assumptions are followings.

1) The SP and the HG are trusted entities, and are connected securely with each other. The HG is a tamper-proof device that can protect the sensitive data.
2) The HG and the SDs are having identical symmetric cryptographic systems (*i.e.,* encryption, decryption and hash function).
3) All the heterogeneous devices (*i.e.,* SDs and HG) clocks are synchronized using the scheme of Li et al. [32], and are (mutually) agreed on a transmission delay (ΔT) to avoid replay attacks.

Our scheme including three phases: the system setup; authentication and key establishment; and ease of addition of a new smart device.

TABLE I
Symbols and Descriptions

Symbols	Descriptions
SP	Security service provider
id_A	Identity of smart device A
Sid_A	Silicon identity of device A [21]
G_{id}	Home gateway (HG) identity
$E_K[M]$	Message m is encrypted using secret key (K)
$D_K[M]$	Message m is decrypted using secret key (K)
$token_A$	a unique short authentication token for device A
MAC	Message authentication code
$HMAC$	Hashed message authentication code
$h()$	One way hash function, *e.g.,* SHA-1/SHA-2/MD-5
$\|\|$	Concatenation operation

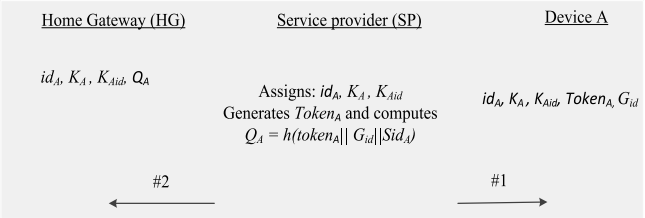

Fig. 3. System setup.

A. System Setup

First of all, each home device should be registered off-line to the security service provider (SP) and obtained security parameters. Prior to the network deployment, for every smart device A, firstly, SP assigns identity (id_A), and stores a unique secret key (K_A) along with key identifier (K_{Aid}) to the device memory [33]. SP generates a unique short authentication token ($token_A$) and computes $Q_A = h(token_A||G_{id}||Sid_A)$. Note that, Sid_A is a *Silicon-ID* (a silicon serial number) that presented on the devices [21]. Then, SP stores $Token_A$ and id_A to device A. In addition, SP also stores the HG identity (G_{id}) to device A. Secondly, SP stores each A's assigned identity (id_A), Q_A and key (K_A) along with its key identifier (K_{Aid}) to the home gateway (HG). Finally, SP maintains a database that keeps record of the deployed devices. For the smart home security purposes, it is practical to assume that all the stored keys have their life-time (*e.g.,* 6 to 12 months), which depends on the SP. Fig. 3 depicts the system setup.

B. Authentication and Key Establishment

To maintain an initial trust among the smart devices, this sub-section presents an authentication and key establishment mechanism. Assume the HG wants to start bootstrapping with the device A, as follows.

S1: HG generates a random nonce r and computes $C = MAC[Q_A, G_{id}||id_A||T1||r]$ and sends a *request* $\{G_{id}, C, T1, r\}$ message to the device A. Here $T1$ is the current timestamp of HG.

S2: Upon receiving *request* message from HG, device A checks $(T2 - T1) \leq \Delta T$, if yes then proceeds to the

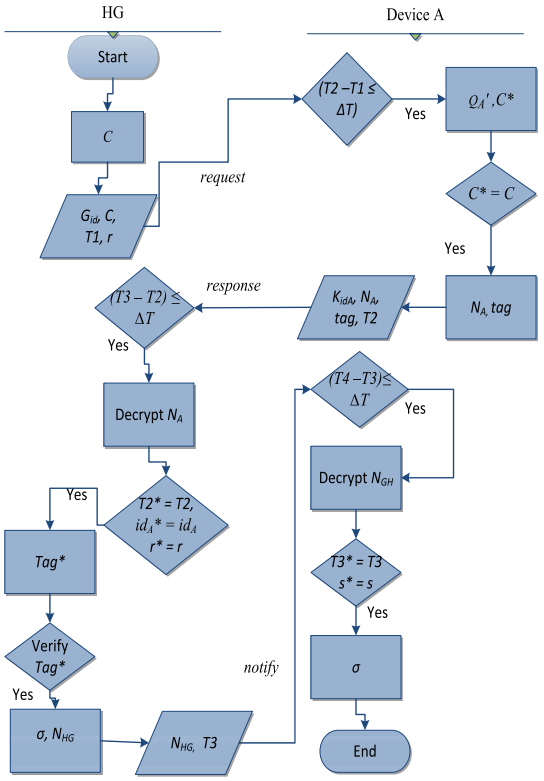

Fig. 4. Flowchart of proposed scheme.

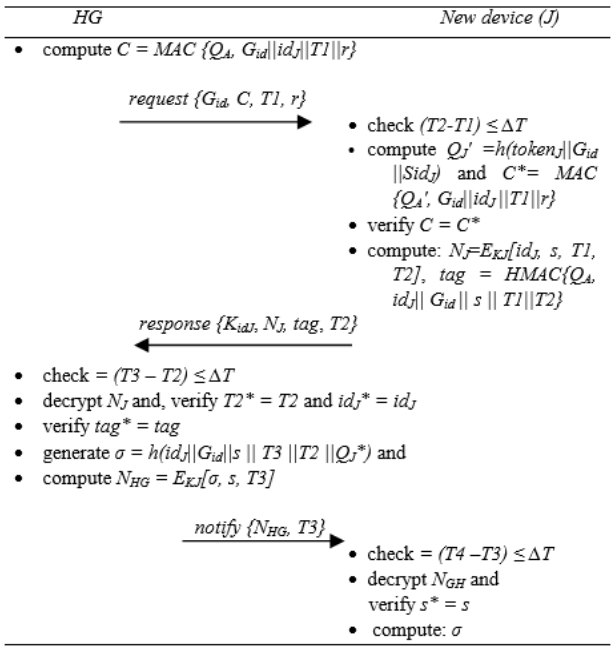

Fig. 5. Flow of addition a new smart device: Session key establishment.

next step. Computes $Q_{A'} = h(token_A||G_{id}||Sid_A)$ and $C^* = MAC\ [Q_{A'}, G_{id}||id_A||T1||r]$. Verifies $C = C^*$, if not, then it generates a *false* message and terminates the system. Otherwise, the device A generates a random secret s and computes $N_A = E_{KA}[id_A, s, r, T2]$ and $tag = HMAC\ [Q_{A'}, id_A||G_{id}||s||r||T2]$, and sends a *response* message (*i.e.,* $\{K_{idA}, N_A, tag, T2\}$) to the HG. Here $T2$ is the current timestamp of device A.

S3: HG checks $(T3 - T2) \leq \Delta T$, if hold then retrieves the corresponding key (K_A) of K_{idA} from own database and decrypts N_A to obtain $id_A^*, s, r^*, T2^*$. Now it verifies the following, $T2^* = T2$, $id_A^* = id_A$ and $r^* = r$, if not then aborts the system. Else it verifies $(HMAC[Q_A, id_A^*||G_{id}||s||r||T2]) = tag^*$. It generates the session key $\sigma = h(id_A||G_{id}||s||T3||T2||Q_A)$ and computes $N_{HG} = E_{KA}[\sigma, s, T3]$, and then it sends a *notify* message $\{N_{HG}, T3\}$ to the device A. Here, $T3$ is a current timestamp of the HG.

S4: Upon receiving *notify* from the HG, device A checks $(T4 - T3) \leq \Delta T$, if it holds then decrypts N_{HG} using K_A and obtains σ^*, s^* and $T3^*$. Verifies $T3^* = T3$, $s^* = s$, if yes then the session key $(i.e., \sigma = (h(id_A||G_{id}||s||T3^*||T2||Q_A^*)))$ will be securely established between the two legal entities. Here, $T4$ is the current timestamp of device A. Fig. 4 depicts the flowchart of session key establishment scheme.

C. Ease of Addition a New Smart Device

It is practical that a new wireless smart device can join the smart home arbitrarily. The proposed scheme provides an ease of addition a new device *(e.g., J)* in the smart homes. To do this, the SP will initiate the followings. First, the SP will assign identities (id_J, G_{id}) and embed required security-related $(K_J, K_{jid}, Token_J)$ credential to the new device (J). Then, the SP securely passes J's information to the home gateway $(i.e., id_J, K_J, K_{jid}$, and $Q_J (= h(token_J||G_{id}||Sid_J))$ and deploys the new device. Then, the HG and the new device will perform the same above mentioned procedure. The flow of new device addition is shown in Fig. 5.

V. Formal Verification, Security and Performance Analysis

This section is divided into three-fold: (a) formal analysis, (b) security properties and (c) performance analysis.

A. Formal Verification

In general, a formal verification ensures the whole security protocol behaves as expected or not, whereas using simulation or testing, a user can point out the errors only. Therefore, to find the design flaws, a formal verification is highly required before the real implementation or prototype. This sub-section presents a formal verification of the proposed scheme using automated validation of Internet security protocols and application (AVISPA) security analyzer tool [23]. The AVISPA tool has been used to analyze many of the security protocols, which are standardized by the Internet Engineering Task Force (IETF). In addition, this tool also have been used in academic research to verify the security protocols, *e.g.,* [34], [35]. AVISPA integrates automatic security protocol analysis and verification backends. The backends are names as on-the-fly model-checker (OFMC), Constraint-logic-based attack searcher (CL-AtSe), SAT-based model-checker (SATMC), and tree automata based on automatic approximations of the

```
goal

% Confidentiality (HG)
 secrecy_of Gid, C, T1, r

 % Confidentiality (Device)
 secrecy_of KidA, NA, tag, T2

% Confidentiality (HG)
 secrecy_of NHG, T3

 % Mutual authentication (Device)
 % Initial Device authenticates Gid
 authentication_on Gid

 % Mutual authentication (HG)
 % HG authenticates Device on NA, tag
 authentication_on NA, tag

end goal
```

Fig. 6. Goal: confidentiality and authentication.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE                    } Attacks
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/Project/PK_KeyEsta.if
GOAL
  as_specified            } Security Goals
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 2.02s
  visitedNodes: 0 nodes
  depth: 1000 plies
```

Fig. 7. Safe from Dolev-Yao attack model.

analysis of security protocols (TA4SP). AVISPA uses a high level protocol specification language (HLPSL) for security protocol specification. For more details, refer to [23].

The HLPSL is a role-based language, meaning that it specifies the actions of each participant in a module that is called a *basic role*. The *basic role* describes what information the participant can use initially (parameters), its initial state, and ways in which the transition can take place. The *composition role* describes a whole single session of the protocol by specifying how the legitimate participants are interacting with each other. In addition, a top-level role *(i.e., environment role)* contains global constants and a composition of one or more sessions, where the attacker may play some roles as a legitimate user. It also describes what knowledge the intruder has about the networks. In AVISPA [23], the attacker is modeled through the *channel(dy)* that is being used for the Dolev-Yao Intruder model [24].

However, in the HLPSL specification our proposed scheme has two *basic roles* (*i.e.,* HG and device A), a single *session role* and an *environment role* that have the knowledge of the Dolev-Yao attack model. For the validation and testing, we have transformed the HLPSL script into IF (*i.e.,* intermediate format) using the translator HLPSL2IF. This translated IF code is the input of four backends (OFMC, CL-AtSe, SATMC, and TA4SP) that are integrated with the AVISPA tool.

Fig. 6 and Fig. 7 are showing the formal verification results, confidentiality and authentication, and safe from the Dolev-Yao attack model, respectively. More precisely, as shown in Fig. 6, the message confidentiality is modeled by means of the goal predicate *secrecy* of *request* $(G_{id}, C, T1, r)$, *response* $(Kid_A, N_A, tag, T2)$ and *notify* $(N_{HG}, T3)$ messages that means the parameters are enough secret (and/or secured) between the HG and the device A. Similarly, authentication is modeled by means of the goal predicate *authenticate* G_{id}, N_A, Tag, which states that the device A verified the HG identity (G_{id}) and the HG verified the device A using (N_A). On the other hand, the proposed protocol has reported safe in the OFMC backend and the proposed scheme meets specified goals successfully, as depicted in Fig. 7. Likewise OFMC, the CL-AtSe and SATMC backends are being reported safe, whereas the TA4SP backend has reported *not_supported* and it produced *inconclusive* results. Hence, the Dolev-Yao attack model cannot harm on the proposed scheme. Note that a web-based interface for running the AVISPA tool available [36].

B. Security Analysis

This section discusses the resilience against possible attacks (*e.g.,* masquerade, message-forgery, message replay, known-key, device compromise and denial-of-service). Further, we will also analyze the security properties (mutual authentication, session-key establishment, message confidentiality, message integrity and freshness) to check whether the proposed scheme can be satisfied, as mentioned in Section III-B.

To analyze security of the proposed scheme, consider the Dolev-Yao threat model where an attacker can eavesdrop on wireless messages, intercept and inject(/or) modify packets in transit [24]. In addition, an attacker may physically capture a smart device, compromise the stored secret information for controlling the entire smart home functionalities.

Proposition: The proposed scheme resilient to masquerade attack and message-forgery attack between HG and device A.

Proof:

(1) Resist Masquerade Attack: The attacker cannot masquerade as the legal entity between the HG and the device A to join in the smart home network. Assume that an adversary (Tom) intercepts a *request* message $\{G_{id}, C, T1, r\}$, during one of HG's past requests. Then, Tom may initiate a masquerade attack to join the smart device A as a legal entity, he sends a fake *request* $\{G_{idTom}, C_{Tom}, T1_{Tom}, r_{Tom}\}$ to the device A, by following the procedure described in step: S1 (Section IV-B). However, in this fake attempt Tom will be faced difficulties in his *request* message verification, as follows:

(a) Device A cannot verify Tom's phony identity (G_{idTom}), because the real HG identity information (G_{id}) is hidden in $C(i.e., MAC[Q_A, G_{id}||id_A||T1||r])$. Here, we can notice that Tom's phony identity (G_{idTom}) cannot help him to pass this fake attempt. Moreover, to generate the same MAC $(i.e., MAC[Q_A, G_{id}||id_A||T1||r]))$, Tom must know how to compute Q_A, otherwise, he cannot pass authentication at the device A. For instance, Tom's sub-message (C_{Tom}) will not be verified during the MAC verification procedure at device A, since (C_{Tom}) is computed over a garbled key. Thus, Tom will be detected and then the device A will terminate the session.

(b) As long as Tom does not possess the real parameters $(token_A, G_{id}, Sid_A)$, he cannot deduce the original $Q_A(= h(token_A||G_{id}||Sid_A))$, which is a one-way hashed

value and its possessed by the legal entities only (service provider, HG, and device A). Therefore, Tom cannot masquerade as a legal HG to join the device A in a smart home network.

Similarly, Tom intercepts a *response* $\{K_{id}, N_A, tag, T2\}$ message between the device A and the HG to join the home gateway. From step: S2 (Section IV-B), it can be observed that as a matter of fact, Tom can capture the *response* message, nevertheless he cannot read the contents $(id_A, s, r, T2)$ of sub-message $(i.e., N_A)$ since it is encrypted by the unique key (K_A) that shared between the legal HG and the device A. Therefore, our scheme can resist the masquerade attack.

(2) Resist Message-Forgery Attack: Assuming that Tom may capture previous legal messages (*request* and *response*) passing between the HG and the device A. He would intentionally attempt to forge all the relevant parameters, *e.g.,* $C \ (= \ MAC[Q_A, G_{id}||id_A||T1||r])$ from the *request* message, and $tag \ (= HMAC[Q_A, id_A||G_{id}||s||r||T2])$ from the *response* message. To breach message integrity, then Tom sends a forged *request* message $\{G_{id}, C_{Tom}, T1, r_{Tom}\}$ to the device A by following S1 in Section IV-B. However, the forged $C_{Tom} \ (= \ MAC_{Tom}[Q_{ATom}, G_{id}||id_A||T1||r_{Tom}])$ will be easily detected at the device A because C_{Tom} is not computed using the original $Q_A \ (e.g., MAC[Q_A, G_{id}||id_A||T1||r])$. Therefore, the device A will generate a *"False"* message and terminate the system.

Similarly, Tom tries to send a forged *response* message $\{K_{id}, N_A, tag_{Tom}, T2\}$ to the home gateway as described in S2 (refer Section IV-B). Likewise C_{Tom}, the sub-message $tag_{Tom} (= HMAC[Q_{ATom}, id_A||G_{id}||s||r||T2])$ will not be verified at the HG, since tag_{Tom} is computed over Tom's fake value (Q_{ATom}). Hence, the HG will terminate the system.

More precisely, the HG and device A can mutually authenticate each other if and only if they could provide their correct messages, *i.e.,* $C = MAC[Q_A, G_{id}||id_A||T1||r])$ and $tag = HMAC[Q_{A'}, id_A||G_{id}||s||r||T2]$ that are computed over their shared secrets. In addition, with the effects of mutual authentication our scheme also resists the man-in-the-middle attack, and hence safe to message forgery attack. □

Proposition: The proposed scheme is secure against replay attack and known-key attack.

Proof:

(1) Resist Replay Attack: In the proposed scheme, Tom can intercept *request* $\{G_{id}, C, T1, r\}$, *response* $\{K_{idA}, N_A, tag, T2\}$ and *notify* $\{N_{HG}, T3\}$ messages and can initiate replay attack by sending them without modification. Following the Section IV-B, Tom tries to resend *request* message, *i.e.,* $\{G_{id}, C, T_{Tom}, r\}$ at the time T_{Tom} to the device A. The verification of replayed message cannot be passed due to the time interval $(T2 - T_{Tom}) \geqslant \Delta T$ at the device A, here ΔT is a mutually agreed transmission delay between the legal entities and the receiver (device A) will reject the message. Moreover, to generate a MAC including T_{Tom} $(i.e., MAC[Q_A, G_{id}||id_A||T_{Tom}||r]))$, Tom must know how to compute Q_A, otherwise, he cannot replay the message.

Similarly, assumed that Tom captures device A message, *i.e., response* $\{K_{idA}, N_A, tag, T2_{Tom}\}$ and then tries to replay captured message to the HG at the time $T2_{Tom}$. However, Tom's attempts will be detected when the HG checks the timestamp of device A, *i.e.,* $(T3 - T2_{Tom}) \geqslant \Delta T$, where ΔT is mutually agreed transmission delay. Moreover, when the HG decrypts N_A to obtain $id_A{}^*, s, r^*, T2^*$, Tom's attempt will be detected because $T2_{Tom}$ will not be verified $(T2^* \neq T2_{Tom})$. Likewise, the message *notify* $\{N_{HG}, T3\}$ resists to message replay attack.

(2) Known-Key Attack: In this attack, considered Tom has eavesdropped on wireless messages and studied some other session keys. However, our scheme uses the timestamp (of both entities) and ephemeral random secret s (of device A) in each session. We can note that the timestamp and random secret *(s)* are independent for each session, therefore, the secure session key $\sigma \ (= h(id_A||G_{id}||s||T3||T2||Q_A))$ is independent and different for every session. If Tom gets a past session key σ, he/she cannot get s, Q_A and id_A from the session key they are embedded in σ, which is protected by the one-way hash function as shown in S3 (Section IV-B). Therefore having the knowledge of previous session keys does not help to originate a new session. □

Proposition: Security against other threats: device compromised threat and denial-of-service threat.

Proof:

(1) Smart Device Compromised Threat: Assumed that Tom can capture the SD and may try to collect secret information from the device. It is well known that physical attacks are difficult to prevent if smart devices are not tamper-proof [37]. However, the proposed scheme relies on the *SD-To-HG* communication architecture [10], where each smart device stores a unique *key* that is shared with the HG. Therefore, no communication exists between two SDs [38] — means the proposed scheme can increase the network resilience against a node compromise threat. On the other hand, the identity of the SD being authenticated using its *Silicon-ID* (Sid), which is a unique and immutable identity [21], thus, any SD's (*e.g.,* Device A have an unique $Q_A = h(token_A||G_{id}||Sid_A)$) compromising cannot compromise the secure communication between other non-compromised SDs (*e.g.,* Device B). Moreover, in smart home settings, the SDs are physically secure since they are usually located inside the home where the HG can check at regular interval whether the SD is misbehaving using the scheme proposed in [39].

(2) Denial-of-Service (DoS) Threat: In this attack, Tom can launch a DoS attack by replaying old message. However, the scheme proposed in this paper can mitigate to DoS attack to some extent. As described in the Section IV-B, the proposed approach exploits the advantages of timestamps, *e.g.,* $T1$ and $T3$, $T2$ and $T4$ of the HG and device A, respectively. The proposed scheme can resist such DoS attacks. □

Proposition: Achieved mutual authentication and established a secure session key between the HG and device A.

Proof:

(1) Proper Mutual Authentication: To prohibit unauthorized access in smart home network, a proper mutual authentication is an important property that verifies authenticity for the involved parties. In the proposed scheme, mutual authentication between the HG and smart device A ensures trust of both communication entities. Upon receiving the first message,

i.e., request ($\{G_{id}, C, T1, r\}$), device A computes $Q_{A'}$ and verifies ($C^* = MAC[Q_{A'}, G_{id}||id_A||T1||r]$). If C^* does not verify then device A aborts the system. For instance, Tom fabricates a message (*e.g.*, $\{G_{id}, C_{Tom}, T1, r_{Tom}\}$) and sends it to the smart device A. We note that Tom's fabricated C_{Tom} cannot be passed the verification at the smart device A, because originally the sub-message C is computed over Q_A. Similarly, HG verifies ($id_A{}^* = id_A$) the authenticity of device A by decrypting sub-message $N_A (= D_{KA}[id_A, s, r, T2])$ using key K_A, which is only possessed by the HG. Therefore, to maintain a mutual trust, the proposed scheme achieved mutual authentication between the device A and the HG.

(2) Session Key Establishment: The proposed scheme provides a session-key agreement after performing the authentication. A session key established between the HG and device A *(i.e.,* $\sigma = h(id_A||G_{id}||s||T3||T2||Q_A)$). It is clear to see that σ is encrypted in N_{HG} using the secret key (K_A), which is known to only legal parties. In addition, to generate σ the HG exploits the timing values ($s||T3||T2$), therefore, in each session σ will be different. □

Proposition: The proposed scheme attained message confidentiality, integrity, and freshness.

Proof:

(1) Message Confidentiality: In order to prevent the eavesdropping attack, the scheme provides an adequate confidentiality to their messages, *e.g.,* ($C = MAC[Q_A, G_{id}||id_A||T1||r]$), ($N_A = E_{KA}[id_A, s, r, T2]$), ($tag = HMAC[Q_{A'}, id_A||G_{id}||s||r||T2]$), and ($N_{HG} = E_{KA}[\sigma, s, T3]$). In addition, for each device A, there is a unique key (K_A) along with its key-identity (K_{Aid}) stored at the HG side (refer Section IV-A, system setup). If the HG finds the corresponding key of (K_{Aid}) then decrypts sub-message $N_A (= D_{KA}[id_A, s, r, T2])$, as described in step: S3 (Section IV-B). Otherwise, HG cannot decrypt the garbled message.

(2) Message Integrity: With the proposed scheme, the HG computes a MAC for each *response* message originating from it. Notice that the MAC ($MAC[Q_A, G_{id}||id_A||T1||r]$) can only be computed by the legitimate HG that has Q_A, assigned by the SP, as described in the system setup (refer Section IV-A). If Tom tampers with a MAC, *i.e.,* C_{Tom} ($= MAC_{Tom}[Q_{ATom}, G_{id}||id_A||T1||r_{Tom}]$) in the *request* message, the device A cannot find a corresponding validation key that can compute a valid MAC for the message, and therefore Tom's message will be ignored. Likewise, the HG also verifies message integrity of the device A by computing ($HMAC[Q_A, id_A||G_{id}||s||r||T2]$).

(3) Message Freshness: This property ensures whether the protocol messages are fresh, *i.e.,* recent. It can be noticed, the proposed scheme exploits the clocks of involved entities that ensures each message is recent, not replayed. For instance, *request* $\{Gid, C, T1, r\}$, *response* $\{K_{idA}, N_A, tag, T2\}$ and *notify* $\{N_{HG}, T3\}$, hence, our scheme achieved freshness. □

C. Performance Analysis

This sub-section discusses the performance analysis of the proposed scheme, and then compares with [14]–[16] schemes. Note that this paper only focuses on the computation and communication costs of the authentication and key establishment phase.

In bytes	2	1	4	variable	variable	3	4
	Frame control	Seq. no.	Add. fields	Super frame	Beacon payload	Clock frequency	Synchronizing information

Fig. 8. Beacon frame format [32].

```
interface DS2411
        {

          command error_t read(DS2411_t* data);

          // retrieve moteFamily and SerialNumber
          command uint8_t getFamily(DS2411_t* data);
          command uint8_t* getSerialNumber(DS2411_t* data);
        }
```

Fig. 9. Silicon-ID interface using nesC [40].

1) Implementation Environment: As a part of a proof of concept implementation, nesC is used as the development environment. The nesC is an event-driven programming language for the TinyOS platform, which is a component based operating system and targets the platforms of wireless sensor networks [40]. The de-facto standard research platforms (*i.e.,* smart devices) in smart homes are ZigBee devices [41], [42]. We implemented the proposed scheme on a TelosB platform that equipped with a 16 bit processor runs at a clock frequency 8 MHz, 48 KB of ROM and 10 KB of RAM [43]. Due to the ease of implementation, this paper chose the AES (Advanced Encryption Standard) symmetric-key algorithm for the encryption. AES is the current encryption standard and one of the broadly integrated/used in *CC2420* radios [41]. To verify the message authentication (integrity), we have used cipher block chaining (CBC) to construct the message authentication code (*i.e.,* CBC-MAC). For a hashed message authentication code (HMAC) operation, we chose SHA-1 [44].

To synchronize the HG and SD local clocks, a time synchronization mechanism is used [32]. Consider the HG is a clock source of the smart home, the HG loads a beacon frame to the radio and sends to the SD. The beacon frame includes the local clock frequency and synchronization information, as shown in Fig. 8. Upon receiving the beacon frame, SD synchronizes its clock with the HG. However, the clock synchronization is currently outside the scope of this paper, for more details refer to [32]. In addition, assuming the extreme pessimistic conditions, and for the experiment purposes, authors have set one second transmission delay (*i.e.*, $\Delta T = 1$) for device A, and for the HG [45], to detect the replay attack.

Reading the *Silicon-ID* from a smart device during the computation is an issue. To do this, an *interface* (*i.e.,* DS2411) being used to read the (ZigBee-based) SD's *Silicon-ID* [40], as shown in Fig. 9.

2) Computation Cost: In this paper, we have implemented the authentication and key establishment phase considering the following message sizes, *i.e.*, IDs as 1 byte, MAC size as 4 bytes, random number as 4 bytes, time stamp as 4 bytes, key size as 16 bytes, and HMAC size as 16 bytes. Due to the sensor node's scarcity nature, this paper shows the price of security overhead (*i.e.,* memory consumption and execution time) for the SD.

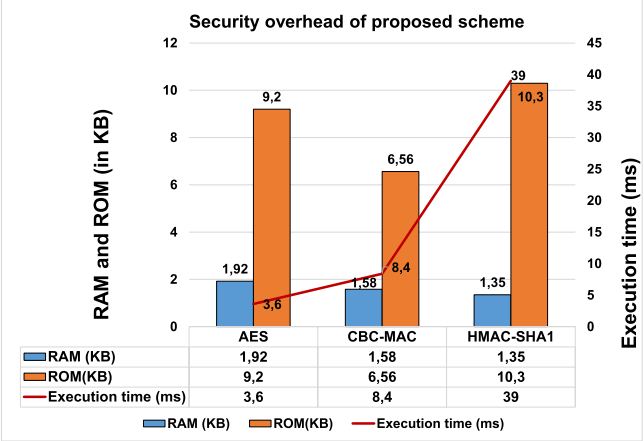

Fig. 10. Security overhead (memory consumptions and execution time (ms)) of proposed scheme.

TABLE II
ENERGY COSTS FOR CRYPTOGRAPHIC OPERATIONS

Operations at device A *(in bits)*	Energy costs *(in* µJ*)*
Encryption	19.44
CBC-MAC	45.36
HMAC-SHA1	210.6
Total computational energy costs	275.4

As shown in Fig. 10, security overhead for a SD is significantly low — AES, CBC-MAC, and HMAC needs reasonable RAM and ROM size. Hence, the proposed scheme leaves an ample storage space on a smart device to execute the other (smart home) services. In addition, AES, CBC-MAC, and HMAC operations take *3.6 ms (millisecond)*, *8.4 ms* and *39 ms*, respectively, computation time at the device A. The time complexity of our scheme is much more efficient than those of the public key based schemes (*e.g.,* [14] and [15]) which need high time complexity for point multiplication operations.

In order to measure the *lightweightness* of the proposed solution, here, we analyzed the energy consumption for the cryptographic operations, which are performed by the device A (TelosB). Similar to [41], [46], and [47], we have calculated the energy (E) consumed by the device A using the formula $E = V \times I$. Here, V is the voltage of the new batteries (2 AA) and I is the current of the circuit. For the sake of measurement purposes, the values V and I may be derived from the (TelosB) datasheet, 3 V(volt) and 1.8 µA (micro-amp), respectively, when the processor is in active mode [43]. By multiplying the values (*i.e.,*$V \times I$) with the execution time (t), we determined the energy consumption for cryptographic operations, such as encryption, CBC-MAC and HMAC-SHA1. As shown in Table II, the total computational energy incurred by the proposed scheme is 275.4 µJ (micro-joule). It can be observed that the impact on energy consumption from the encryption, CBC-MAC and HMAC-SHA1 computation is low, *i.e.,* 19.44 µJ, 45.36 µJ, and 210.6 µJ, respectively.

Additionally, Table III summarizes and compares the computational cost of proposed scheme, which is well-suited to a

TABLE III
COMPUTATION COST COMPARISONS

	[14]	[15]	[16]	**Proposed**
Point multiplication	2t	2t	–	–
Hash operation	1H	4H	5H	2H
MAC	1MAC	–	7MAC	1MAC
HMAC	–	–	–	1HMAC
Cryptosystem	1E+1D	–	4E+4D	1E+1D

t - the time for executing point-multiplication; H - the time for executing one-way hash function; E - the time for performing encryption; D - the time for performing decryption; MAC - the time for performing MAC operation; and HMAC - the time for performing HMAC operation.

TABLE IV
COMMUNICATION ENERGY COSTS

Messages at device A *(in bits)*	Energy costs *(in* µJ*)*
Receive *request* (108)	87.5
Sent *Response* (296)	213.12
Receive *notify* (160)	129.6
Total energy required	430.22

resource-constrained device, as it requires two hash operations, one MAC and one HMAC operations, and two cryptosystems (one encryption and one decryption) to execute the whole protocol. Whereas, in a similar environment to execute the whole protocol, Li's scheme [14] requires two point multiplication operations, one hash operation and one MAC operation, and two cryptosystems (one encryption and one decryption), and Vaidya et al.'s scheme [15] requires two point multiplication operations and four hash operations. In addition, the point multiplication operation incurs high time complexity at the resource-constrained devices. Similarly, Han et al.'s scheme requires five hash operations, seven MAC operations, and 8 cryptosystems (four encryption and four decryption) [16]. In this perspective the proposed scheme attains reasonable efficiency in comparison with other protocols.

3) Communication Cost: The communication cost means the energy spent by a SD (device A) having a packet of a given size to be transmitted/received. To evaluate the communication cost for the proposed scheme, we have adopted the energy model from de Meulenaer et al. [48]. On the TelosB platform, transmitting and receiving a single bit of data required 0.72 µJ and 0.81 µJ, respectively [48]. Table IV shows the communication energy costs for transmitting (*response* $\{K_{idA}, N_A, tag, T2\}$) and receiving (*request* $\{Gid, C, T1, r\}$, and *notify* $\{N_{HG}, T3\}$) messages at the SD. It can be seen from Table IV that the proposed scheme consumes only 430.22 µJ communication energy to execute the whole scheme, and therefore achieved communication cost efficiency. In addition, we have omitted the energy costs at the HG, since it has enough resources (*i.e.,* computational power and memory) to compute the complex cryptographic operations.

Furthermore, in Fig. 11, we are summarizing the communication costs comparisons (in terms of the number of message exchanges) of the proposed scheme and [14]–[16]. To execute the whole protocol, Li's scheme [14] takes four rounds of

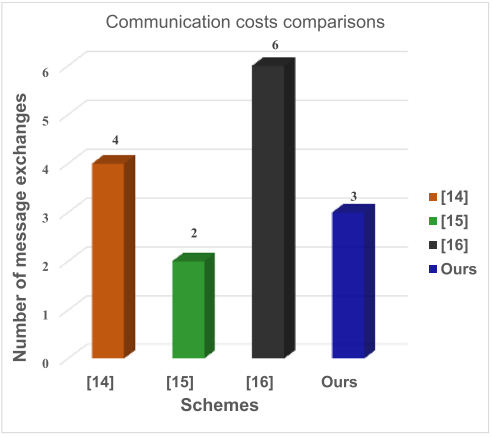

Fig. 11. Communication cost comparisons in terms of the number of message exchanges.

message exchanges, Vaidya et al.'s scheme needs two message exchanges [15], and Han et al.'s scheme [16] needs six rounds for a successful authentication and key establishment, as shown in Fig. 11. Whereas, our scheme requires three rounds of message exchanges (*request, response,* and *notify*, refer Fig. 4), which are quite practical in such smart home applications. Thus, considering the security overhead (*i.e.,* computational and communication costs), it is easy to say the proposed scheme can be a good alternative for securing the smart home environments.

VI. Conclusion

Indeed, the following recent technology trends for the next generation smart homes are already well under way — smart light systems, connected home appliances, home climate-control systems, demand/response systems for electricity (smart metering), security and safety systems. It is also worth noting that the big proportion of elderly population (for better life living at home) is also increasing. However, an absolute adoption of the smart homes is still a big concern in the society, especially, for the elderly inhabitants. One of the major challenge is the security in smart homes.

In this paper, we proposed a lightweight and secure session-key establishment scheme focusing on the smart homes. The formal analysis (using the AVISPA tool) revealed that the proposed scheme can achieve authentication and confidentiality, and security goals are as expected. In addition, the proof of concept demonstrated that a session key is established in a lightweight way, which is a paramount security requirement for the smart home environments.

References

[1] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Commun. Mag.*, vol. 48, no. 6, pp. 92–101, Jun. 2010.

[2] J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, and D. Mosse, "Seamless integration of heterogeneous devices and access control in smart homes," in *Proc. 8th Int. Conf. Intell. Environ. (IE)*, Jun. 2012, pp. 206–213.

[3] G. Mantas, D. Lymberopoulos, and N. Komninos, "Security in smart home environment," in *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*. Hershey, PA, USA: IGI Global, 2006.

[4] D. Pishva and K. Takeda, "A product based security model for smart home appliances," in *Proc. 40th Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, Oct. 2006, pp. 234–242.

[5] N. K. Suryadevara, S. C. Mukhopadhyay, R. Wang, and R. K. Rayudu, "Forecasting the behavior of an elderly using wireless sensors data in a smart home," *Eng. Appl. Artif. Intell.*, vol. 26, no. 10, pp. 2641–2652, Nov. 2013.

[6] *HOPE—Smart Home For Elderly People*. [Online]. Available: http://www.hope-project.eu/, accessed Jul. 15, 2015.

[7] *SM4ALL—Smart Homes for All*. [Online]. Available: http://www.sm4all-project.eu/, accessed Jul. 16, 2015.

[8] *GENIO—Next Generation Home*. [Online]. Available: http://projects.celtic-initiative.org/genio/, accessed Jul. 15, 2015.

[9] S. Bhardwaj, T. Ozcelebi, J. Lukkien, and C. Uysal, "Resource and service management architecture of a low capacity network for smart spaces," *IEEE Trans. Consum. Electron.*, vol. 58, no. 2, pp. 389–396, May 2012.

[10] H. Tschofenig, J. Arkko, and D. McPherson, "Architectural considerations in smart object networking," Internet Engineering Task Force, Fremont, CA, USA, Tech. Rep. RFC-7452, Jul. 2014.

[11] D. G. Korzun, S. I. Balandin, and A. V. Gurtov, *Deployment of Smart Spaces in Internet of Things: Overview of the Design Challenges* (Lecture Notes in Computer Science), vol. 8121. New York, NY, USA: Springer, 2013.

[12] M. Burrough and J. Gill. *Smart Thermostat Security: Turning up the Heat*. [Online]. Available: http://www.burrough.org/Documents/Thermostat-final-paper.pdf, accessed Apr. 10, 2015.

[13] Y. Chen and B. Luo, "S2A: Secure smart household appliances," in *Proc. 2nd ACM Conf. Data Appl. Secur. Privacy (CODASPY)*, 2012, pp. 217–228.

[14] Y. Li, "Design of a key establishment protocol for smart home energy management system," in *Proc. 5th Int. Conf. Comput. Intell., Commun. Syst. Netw. (CICSyN)*, Jun. 2013, pp. 88–93.

[15] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2011, pp. 787–788.

[16] K. Han, J. Kim, T. Shon, and D. Ko, "A novel secure key paring protocol for RF4CE ubiquitous smart home systems," *Pers. Ubiquitous Comput.*, vol. 17, no. 5, pp. 945–949, Jun. 2013.

[17] S. Guillet, B. Bouchard, and A. Bouzouane, "Correct by construction security approach to design fault tolerant smart homes for disabled people," *Proc. Comput. Sci.*, vol. 21, pp. 257–264, 2013.

[18] B. Fabian and T. Feldhaus, "Privacy-preserving data infrastructure for smart home appliances based on the octopus DHT," *Comput. Ind.*, vol. 65, no. 8, pp. 1147–1160, Oct. 2014.

[19] B. Fouladi and S. Ghanoun, *Hacking Z-Wave Home Automation Systems*. Las Vegas, NV, USA: BlackHat, 2013.

[20] D. Yadron, "Hackers expose how connected toilets, heaters and light bulbs are at risk," *Wall Street J.*, Jul. 2013.

[21] A. Seshadri, M. Luk, and A. Perrig, "SAKE: Software attestation for key establishment in sensor networks," *Ad Hoc Netw.*, vol. 9, no. 6, pp. 1059–1067, Aug. 2011.

[22] K. Islam, W. Shen, and X. Wang, "Security and privacy considerations for wireless sensor networks in smart home environments," in *Proc. IEEE 16th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2012, pp. 626–633.

[23] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theoretical Comput. Sci.*, vol. 155, pp. 61–86, May 2006.

[24] D. Dolev and A. C. Yao, "On the security of public key protocols," in *Proc. 22nd Annu. Symp. Found. Comput. Sci. (SFCS)*, 1981, pp. 350–357.

[25] E. Ayday and S. Rajagopal, "Secure device authentication mechanisms for the smart grid-enabled home area networks," Ecole Polytechnique Federale De Lausanne, Lausanne, Switzerland, Tech. Rep. EPLF-REPORT-188373, 2013, pp. 1–18.

[26] E. Callaway *et al.*, "Home networking with IEEE 802.15.4: A developing standard for low-rate wireless personal area networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 70–77, Aug. 2002.

[27] M. Xu, L. Ma, F. Xia, T. Yuan, J. Qian, and M. Shao, "Design and implementation of a wireless sensor network for smart homes," in *Proc. 7th Int. Conf. Ubiquitous Intell. Comput. 7th Int. Conf. Auto. Trusted Comput. (UIC/ATC)*, Oct. 2010, pp. 239–243.

[28] L. Liang, L. Huang, X. Jiang, and Y. Yao, "Design and implementation of wireless smart-home sensor network based on ZigBee protocol," in *Proc. Int. Conf. Commun., Circuits Syst. (ICCCAS)*, May 2008, pp. 434–438.

[29] H. Tschofenig and J. Arkko, "Report from the smart object workshop," Internet Engineering Task Force, Fremont, CA, USA, Tech. Rep., Apr. 2012.
[30] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Proc. Wireless Netw.*, 2001, pp. 189–199.
[31] N. E. Petroulakis, E. Z. Tragos, A. G. Fragkiadakis, and G. Spanoudakis, "A lightweight framework for secure life-logging in smart environments," *Inf. Secur. Tech. Rep.*, vol. 17, no. 3, pp. 58–70, Feb. 2013.
[32] Y. Li, Y. Huang, and H. Sun, "A time synchronization mechanism for heterogeneous wireless sensor networks," in *Proc. Int. Conf. Autom. Control Artif. Intell. (ACAI)*, Mar. 2012, pp. 317–320.
[33] P. Kumar, M. Ylianttila, A. Gurtov, and M. Sain, "An efficient and simple key distribution scheme for smart environments," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2014, pp. 468–469.
[34] C. Chen, D. He, S. Chan, J. Bu, Y. Gao, and R. Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network," *Int. J. Commun. Syst.*, vol. 24, no. 3, pp. 347–362, Mar. 2011.
[35] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, Jun. 2014.
[36] *AVISPA: Automated Validation of Internet Security Protocols and Applications*. [Online]. Available: http://www.avispa-project.org/web-interface/basic.php, accessed Jan. 15, 2015.
[37] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.
[38] Y. Cheng and D. P. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 35–48, Jan. 2007.
[39] M. Drozda, S. Schaust, and H. Szczerbicka, "AIS for misbehavior detection in wireless sensor networks: Performance and design principles," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Sep. 2007, pp. 3719–3726.
[40] P. Levis, *TinyOS Programming*. Cambridge, U.K.: Cambridge Univ. Press, Mar. 2009.
[41] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Comput. Netw.*, vol. 54, no. 17, pp. 2967–2978, Dec. 2010.
[42] P. Nie, J. Vähä-Herttua, T. Aura, and A. Gurtov, "Performance analysis of HIP diet exchange for WSN security establishment," in *Proc. 7th ACM Symp. QoS Secur. Wireless Mobile Netw. (Q2SWinet)*, 2011, pp. 51–56.
[43] *Telos Ultra Low Power IEEE 802.15.4 Compliant Wireless Sensor Modules*. [Online]. Available: http://www2.ece.ohio-state.edu/~bibyk/ee582/telosMote.pdf, accessed Dec. 20, 2014.
[44] D. Eastlake and P. Jones, "US secure hash alrorithm," Internet Engineering Task Force, Fremont, CA, USA, Tech. Rep. RFC 3174, Sep. 2001.
[45] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A secure sensor network communication architecture," in *Proc. 6th Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2007, pp. 479–488.
[46] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4638–4646, Sep. 2013.
[47] G. Ateniese, G. Bianchi, A. Capossele, and C. Petrioli, "Low-cost standard signatures in wireless sensor networks: A case for reviving pre-computation techniques?" in *Proc. NDSS*, San Diego, CA, USA, Feb. 2013.
[48] G. de Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *Proc. IEEE Int. Conf. Wireless Mobile Comput. Netw. Commun. (WIMOB)*, Oct. 2008, pp. 580–585.

Pardeep Kumar received the M.Tech. degree in computer science and technology from Chaudhary Devi Lal University, Sirsa, India, in 2006, and the Ph.D. degree in computer science from Dongseo University, Korea, in 2012. Since 2012, he has been with the Centre for Wireless Communications, University of Oulu, Finland. His current research interests include security in sensor networks, smart environments, body area networks, Internet of Things, and cloud computing.

Andrei Gurtov (SM'10) received the M.Sc. and Ph.D. degrees in computer science from the University of Helsinki, Finland, in 2000 and 2004, respectively. He was a Professor of Wireless Internet with the University of Oulu from 2010 to 2012. He worked with TeliaSonera, the Ericsson Nomadic Laboratory, and the University of Helsinki. He was a Visiting Scholar with the International Computer Science Institute, Berkeley, in 2003, 2005, and 2013. He is currently a Principal Scientist with the Helsinki Institute for Information Technology. He is also an Adjunct Professor with Aalto University, the University of Helsinki, and the University of Oulu. He has co-authored over 150 publications, including three books, research papers, patents, and five IETF RFCs. He is a Senior Member of ACM.

Jari Iinatti (SM'05) is currently a Professor of Telecommunication Theory with the Department of Communications Engineering, University of Oulu. His research interests include future wireless communication systems, transceiver algorithms, and medical ICT. He has authored over 200 international papers, holds four patents, co-edited two books, and authored five book chapters. He was the TPC Chair of ISMICT2007, the TPC Co-Chair of PIMRC'2006, BodyNets'2012, and PIMRC'2014, and the General Co-Chair of ISMICT-2011, 2014, and 2015. He has been the TPC Member of about 25 conferences, and was also an Organizer of FEELIT in 2008 and 2011 and UWBAN from 2012 to 2015.

Mika Ylianttila (SM'08) received the Ph.D. degree in communications engineering from the University of Oulu, in 2005. He was a Visiting Researcher with the Center for Wireless Information Network Studies, Worcester Polytechnic Institute, MA, and the Internet Real Time Laboratory, Columbia University, New York, USA. He is currently a Professor with the Centre for Wireless Communications, and the Director of the Center for Internet Excellence, a research and innovation unit. He is also an Adjunct Professor of Computer Science and Engineering with the Faculty of Information Technology and Electrical Engineering. He has co-authored over 100 international peer-reviewed articles in broadband communications networks and systems, including aspects on wireless security, mobility management, distributed systems, and novel applications. He is an Editor of the *Wireless Networks* journal.

Mangal Sain received the Master of Application degree in India in 2003, and the Ph.D. degree in computer science from Dongseo University, Busan, Korea, in 2011. Since 2011, he has been an Assistant Professor with the Department of Information and Communication Engineering, Dongseo University, Korea. He has authored over 20 international publications. His research interests include wireless sensor network, middleware, cloud computing, embedded system, and Internet of Things. He is a member of TIIS.