International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:6, 2018

Lightweight and Seamless Distributed Scheme for the Smart Home

Muhammad Mehran Arshad Khan, Chengliang Wang, Zou Minhui, Danyal Badar Soomro

***Abstract*—**Security of the smart home in terms of behavior activity pattern recognition is a totally dissimilar and unique issue as compared to the security issues of other scenarios. Sensor devices (low capacity and high capacity) interact and negotiate each other by detecting the *daily behavior activity* of individuals to execute common tasks. Once a device (e.g., surveillance camera, smart phone and light detection sensor etc.) is compromised, an adversary can then get access to a specific device and can damage daily behavior activity by altering the data and commands. In this scenario, a group of common instruction processes may get involved to generate deadlock. Therefore, an effective suitable security solution is required for smart home architecture. This paper proposes *seamless distributed Scheme* which fortifies low computational wireless devices for secure communication. Proposed scheme is based on lightweight key-session process to upheld cryptic-link for trajectory by recognizing of individual's behavior activities pattern. Every device and service provider unit (low capacity sensors (LCS) and high capacity sensors (HCS)) uses an authentication token and originates a secure trajectory connection in network. Analysis of experiments is revealed that proposed scheme strengthens the devices against device seizure attack by recognizing daily behavior activities, minimum utilization memory space of LCS and avoids network from deadlock. Additionally, the results of a comparison with other schemes indicate that scheme manages efficiency in term of computation and communication.

***Keywords*—**Authentication, key-session, security, wireless sensors.

I. Introduction

SMART home environments use the advanced innovative technology of the Internet of Things (IOT). The total number of devices that are connected to each other through the internet has increased in number than the number of living people in the world, as mentioned in [1], [4]. Our earlier work in the lab [2] on activity pattern-based knowledge extracted from routes in smart homes defined that automation becomes vital and conceivable when all devices are connected with each other virtually. It is observed that smart home architecture does not have a secure scheme to meet the security issues regarding daily behavior activities. Smart homes comprise of light detection wireless sensors, flame control system, security and surveillance system, appliance control system, and home care systems [9]. Individuals can also utilize the functionality of home care system during daily living activities (DLA) [3], [4]. Some companies have started to build smart homes last few years e.g., GENIO (next generation home) [5], SM4ALL (smart home for all) [6], and HOPE (a smart home for the elderly) [7], etc. Smart home environments consist of various devices, including wireless remote devices, surveillance camera, smart window shutters, flame detection devices and numerous types of devices as shown in Fig. 1. Mostly, smart homes devices have low computation capacity and are resource restrained [8]. The smart home is basically divided into three man parts, (i) smart home device/ nodes, (ii) smart home gateway (SHG), and (iii) secure service provider server (SSPS) [9]. The smart home gateway works as a router between smart home devices and the main server. The smart home environment is comprised of LCS and HCS. LCS devices are resource hungry, have low process capability, less bandwidth and resource limited memory. HCS devices have good memory capacity, bandwidth and are rich in resources. Data is forwarded from HCS to LCS devices in smart homes. The not tamper-proof behavior of Low computational capacity sensors (LCS) has made them a security issue for smart environment architecture [11].

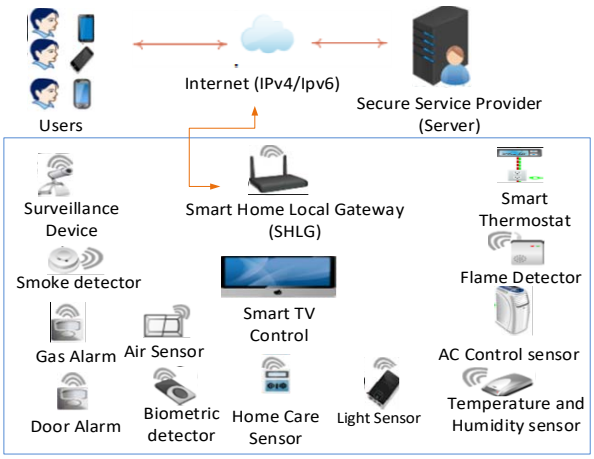


Fig. 1 Smart home environment

From our recent research [10], we realized that security is a very serious challenge for smart homes due to the possibility of attacks (e.g. denial-of-service, masquerade attack and device compromised attack) by adversaries. Smart home

Muhammad Mehran Arshad Khan, College of Computer Sciences and Technology, Chongqing University, China (corresponding author, phone: +86-15736123601; e-mail: to_rabimehranrana@yahoo.com).
Professor, Dr. Chengliang Wang, College of Computer Sciences and Technology, Chongqing University, China (phone: +86-18983055830; e-mail: wangcl@cqu.edu.cn).
Minhui Zou, College of Computer Sciences and Technology, Chongqing University, China (phone: +8615922867551, e-mail: zouminhui@outlook.com).
Danyal Badar Soomro, School of Software Engineering, Chongqing University, China (phone: +8613896135349, e-mail: daniyalsoomro@yahoo.com).

devices (SHD) do not have an adequate level of security [11]. While the current research clearly outlined and discussed security issues related to the wireless sensor network [4]-[9], very few studies have focused on the security requirements of smart environments. The security of the smart home in terms of behavior activity patterns is completely unique and a different idea and concept. Therefore, we propose a simple and seamless scheme which is suitable for the smart home environment. This new scheme based on a mutual authentication process can verify if SHDs (which appear for the communication in smart home) are real or fake. The mutual authentication process is comprised of key distributed sessions, which is discussed in detail in Section III. The proposed scheme provides the following advantages: (i) secure trajectories for communication between LCSs and HCSs, (ii) fortify the SHDs against a device compromised attack, (iii) low utilization of memory space of the SHDs during the process.

II. Literature Review

The smart home is a new technology, so that very limited research is available about the security of smart home environments. However, recent research works are discussed in this section and each research have its advantages and disadvantages. Hoang Pishva presented a new pattern of transmission between various devices to secure the system of smart home. This scheme is based on TOR and utilizes the public-key approach for cryptography. This approach is not feasible and suitable for LCSs in the smart home due their low memory capacity [13]. TOR's application is mostly work as an anonymous internet browser which is operated where surfing actions are performed. Moreover, this scheme did not discuss the authentication process of the devices. The work of [14] discussed the current working technologies (e.g. ZigBee, INSTEON and Z-Wave) of the home area network (HAN) and claimed that these are suitable for providing security in the smart home only up to a certain level. In this paper, the author described the mechanism in three steps: (i) authentication, which is necessary between the home gateway and smart meter; (ii) authentication, which is also required between the smart appliances and HAN; and (iii) HAN and the transient devices should also have performed authentication. However, the internet is required to perform authentication process and complete the three steps. The basic drawbacks of this scheme are that the scheme totally depends on a third part. The authors of [11] proposed an anonymous secure framework (ASF), and they also covered the anonymity, unlinkbility, and authentication and integrity of devices in the smart home. Key agreement based on the key sharing process and authentication token are utilized to deploy secure connections in the smart home. However, this scheme does not provide a solution to save daily behavior activities, and it also lacks the distributed security concept of sensors. LCS do not stay faceless and can be identified easily by adversaries to gain access. This scheme did not discuss the method to secure the identity of devices from attacks at initial configuration and after stay offline over the network. Another drawback of this approach is that it the stores key attributes of the scheme on static devices.

III. Proposed Seamless Distributed Scheme

This research is an extension of our previous work [2], [10]. In this section, a secure seamless distributed scheme is proposed to protect the transmission in smart home architecture (SHA). The seamless distributed scheme is based on a key distributed session and mutual authentication process. This section is described in the following four phases:

A. Distributed Scheme

Definition: The distributed approach is used to facilitate sensors. These sensors perform encrypted process during communication while utilizing key-session attributes of proposed scheme. The attributes of proposed scheme are shared between devices of the smart home architecture by the service provider server.

Actually, sensors of smart home architectures coordinate and detect the daily behavior activities of living persons in order to perform various tasks. For example, when a person goes to the kitchen to cook breakfast, the kitchen sensors' become active to determine the activity and then send the behavior activity to the main server. Each sensor device has its own capacity for the computation process of appliances, which is basically support to the distributed scheme and interaction with each other to recognize a common task. In such kinds of architecture, a specific suspicious command/ activity may get involved in communication blockage. To detect this kind of blockage due to abnormal activity while keeping the rest of the network functional, it is necessary to launch a secure seamless distributed scheme which is based on the user's daily living behavior activity pattern.

B. User's Behavior Activity Layout

Sensors stimulate and detect instruction directly from the personal daily behavior activity for execution of appliances. For example, heat detection sensors, flame detection, and temperature control nodes, all these devices are directly interacted user's behavior actions and these actions are utilized in the proposed encrypted key-session scheme to protect and secure the smart home architecture. In Fig. 2, m stands for module of sensor inside the room and s represents the sensors trajectory outside of the boundary.

Consider a connected smart home architecture where wireless sensor nodes (LCS and HCS) and SMDs are connected to coordinate with each other. A secure service provider server (SSPS) meets the adequate security level of the smart home. In smart homes, each device can communicate to another device directly and indirectly, and thus, the proposed scheme is very simple and strengthens the network. A secure service provider server (SSPS) can meet the adequate security level needs of smart home architecture. Table I defines the notations used in this scheme.

C. Person's Activity Recognition Model

- Activity recognition in the smart home is routinely detecting a person's activities from the data captured by

sensors. A person's activity recognition model is relevant and very close to most common applications like a human body for instance motion detecting sensors, surveillances, DLA, health care and temperature control. The time stamp frame of a person's activities is incorporated in the smart architecture, as shown in Fig. 3.

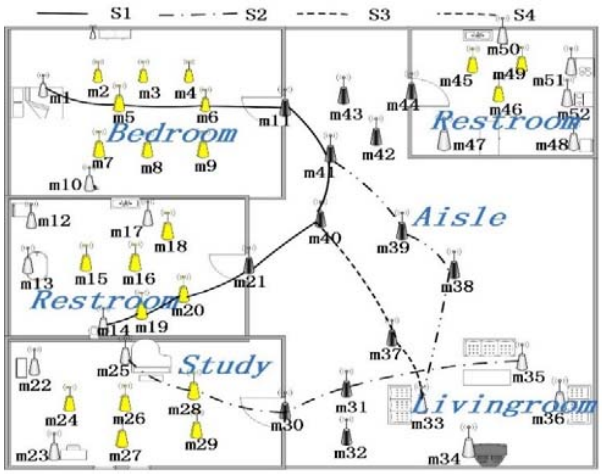


Fig. 2 A person's behavior pattern layout of the new environment interaction with sensors, devices and trajectories layout for encryption

TABLE I
NOTATIONS AND DESCRIPTIONS

Sr.	Notations	Descriptions
1	*SSPS*	Secure Service Provider Server
2	id_{HG}	Value of home gateway (HG)
3	Id_X	Value of smart home device
4	α_{XId}	Authentication token value
5	$\|\|$	XOR and concatenation
6	Q_{Xid}	Value of compute function
7	ΔT	Value of Time stamp
8	S_x	Value of behavior activity
9	M_t	Value of trajectory

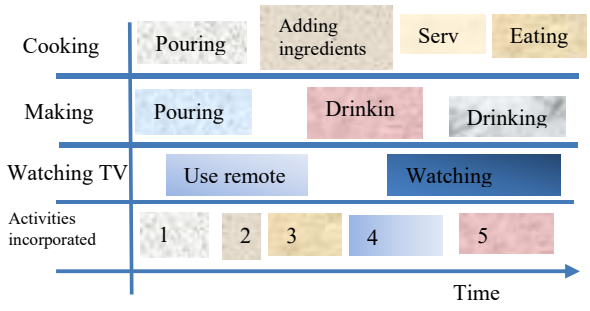


Fig. 3 Time stamp of incorporated activities

Here, we distinguish some activities:

- Person's simple activity: This is commonly the most basic atomic activity, e.g. pour water, and drink water.
- Person's composite activity: This is defined as comprising of many sub activities, for example, the activity "cooking rice in the kitchen" is a model of sub-activities that include measuring quantity of water, measuring quantity of rice, pouring contents into the pot, adding other ingredients and cooking.
- Activity of daily life (ADL): It is distinguished into two parts, (i) basic daily life activities, relating to self-caring (eating, dressing, watching, toilet hygiene, bathing, showering etc.). (ii) General activities (pouring water, drinking water, etc.) of daily life (ADL) [7], [8]. General activities are basically not necessary for smart home architecture and users can do general activities at any time, for instance, shopping, taking medicine, meeting with colleagues etc. The time frame of activities incorporated in smart architecture is shown in Fig. 3.

D. Distributed Activity Key-Session Process Model

Definition: Two or more than two sensors devices start transaction for communication to complete the specific task after taking instructions from the user's behavior activity. Configuration of the new key-sessions attributes for whole networks is required prior in order to meet the adequate level of security. Here, an activity is assigned by S_x value and trajectories are assigned by M_t value. A set of activities and a set of trajectories are represented as below:

Set of activities S_x= (S1, S2, …Sn)

Set of trajectoriesm_t= (m1, m2, ...mn).

Definition: Sensors are assigned unique encrypted keys and an authentication token value is shared among the devices. Each key has a complete value set of the necessary attributes of all connected nodes/ devices of the entire network for smooth transformation of the communication. The steps of the encrypted key-session distribution are as below:

- All sensor nodes have a specific capacity to store value and to perform the computational process for appliances. A person's behavior daily activity is noted and assigned with a specific key-value.
- While offline, all devices acquired secret credentials ($id_{HG,}$ $Id_{X,}$ Q_{Xid}, ΔT, $S_{x,}$, M_t) of proposed scheme from SSPS and it generates and computes key edifice as in Fig. 4. Lastly, it generates a set of unique keys for identification.
- Firstly, an authentication token α_{XId} is generated by the SSPS to uphold the secure trajectory. This authentication token checks the identity of the device as well as the trajectories of the smart home. If any device does not have the same authentication token, then the behavior of that specific device (sensor) will be under observation to secure the remaining communication and individual behavior activity in smart home architecture.
- After the authentication process, the SSPS records the identity of all devices and ensures that each one has a unique key value and also a time stamp, ΔT. If the unique identification of each device does not match then the communication is aborted. If ΔT (ΔT_a time stamp of device A and ΔT_b time stamp of device B) of device A and device B $\Delta T_a \neq \Delta T_b$, then transmission will be terminated. Such non-recognized devices are required to

request the main server again for their authentication token.

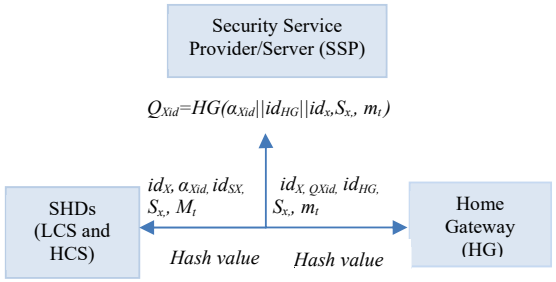


Fig. 4 Key distribution process of the proposed seamless scheme

- When the SSPS establishes a secure connection, then a secure transmission upheld between the devices (LCS and HCS). If a unique edifice of any sensor device is mismatched, then rest of the devices will perform their process as per their edifice by avoiding such suspicious device.

IV. Analysis of the Proposed Scheme

To check the performance of the proposed scheme against a device compromised attack, we performed experiments in the recognized security analyzer tool named as automatic verification of internet security protocol and application tool (AVISPA) [16]. AVISPA is comprised of four backend process steps, which are:

- OFMC (i.e., on-the-fly model-checker),
- CL-AtSe (i.e., constraint-logic-based attack searcher),
- SATMC (i.e., sat-based model checker), and
- TA4SP (i.e., tree automata-based security protocol).

Basically, AVISPA executes the above mentioned functions to evaluate the authenticity of the scheme against attacks.

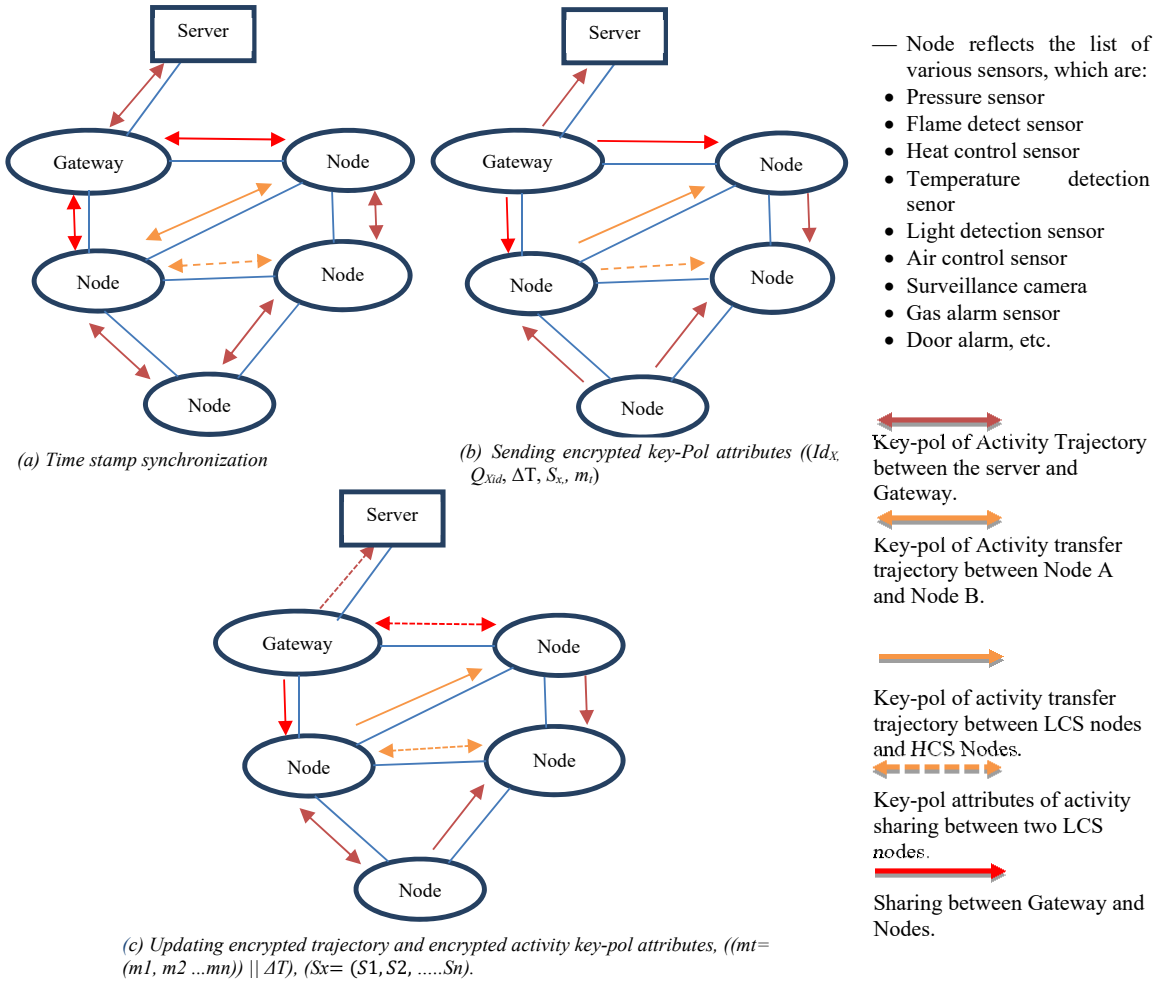


Fig. 5 Encrypted activity of the key-session updating and sharing mode

A. Analysis of Encrypted Activity Transfer against Attack

Definition: Encrypted activity transfer is helpful in terms of the transformation of activities from one to another. To recognize the encrypted activity transfer process, the activity

attributes of trajectory considers verifying the token authentication (α_{Xid}), as shown in Table I. The activity transfer process needs the activity trajectory set and the time duration ΔT.

Trajectory set : $(m_t = (m1, m2 ...mn)) \| \Delta T$

Key-pol's Attributes set of device: (Id_X, Q_{Xid}, ΔT, S_x, m_t)

Encrypted keys hold the attributes of the activity transfer process and trajectory process, as shown in Fig. 3. Old and new encrypted activity key-sessions have some similarities due to their functionality and condition. In order to explain the specific activity transfer, we consider the daily activity routine of an individual through the sensors for record keeping.

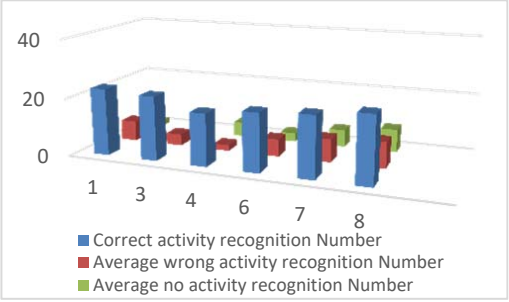
Therefore, this process is used to uphold communication and cryptic-link among the devices of the smart home architecture. An activity's key updating and sharing process is shown in Fig 5.

B. Comparison Analysis of Activity Recognition Based on Trajectory Transfer and on Mining

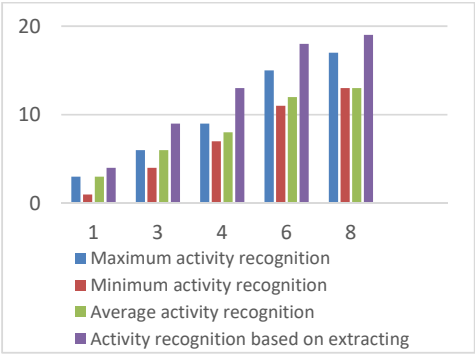
To calculate results more accurately, we evaluate the activity recognition result based on trajectory transfer and on activity recognition mining using various encrypted key-pol attributes sharing process. To evaluate the activity recognition under an uncertain attack, the experiment was executed four times. The results show that the encrypted activity recognition remained secured, as shown in Fig. 6 (a). We also calculated the output of encrypted activities recognition during 1 to 6 attacks which is based on mining. The results revealed that the security of encrypted activities recognition remain high. This is also categorized into maximum, average and minimum activity recognition, as shown in Fig. 6 (b).

C. Case: Device Compromised Attack and Activity Recognition

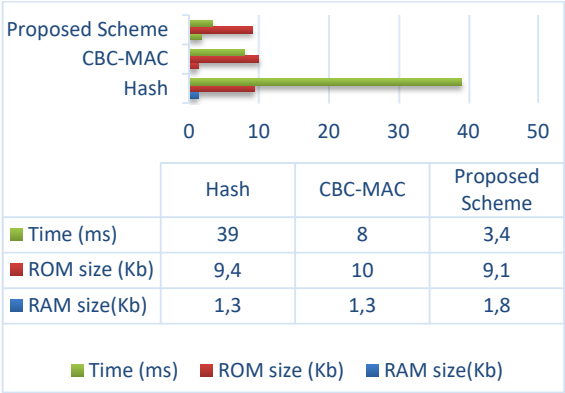
Proof: *Output of the proposed scheme against a device compromised attack*; this type of attack mostly takes place during communication between devices in the smart home, when an unauthorized person (e.g. adversary (Tom)) attempts to access control of a device (e.g. surveillance camera and door lock sensor). The proposed scheme secured these devices from an adversary's attacks due to its unique value α_{XId} of the authentication token. Authentication token value α_{XId} is comprised of α_{Xid} ($id_{HG} \| id_{SX}$). If Tom manages to seize one legal message and intentionally forge a few parameters of the message to disrupt its integrity, this activity will be easily detected by device X because the time stamp value ΔT of the captured message will not match the actual value of time stamp. In another case, when an adversary successfully manages the time mechanism, the unique encrypted identity of the sensor (device) will then be checked out and if found to be mismatched by the actual identity assigned, then the proposed distributed approach will pause the specific device, while the remaining devices will continue to be functional. Results also revealed that such suspicious devices are treated specially after recognizing their abnormal behavior.



(a) Activity recognition under uncertain attacks

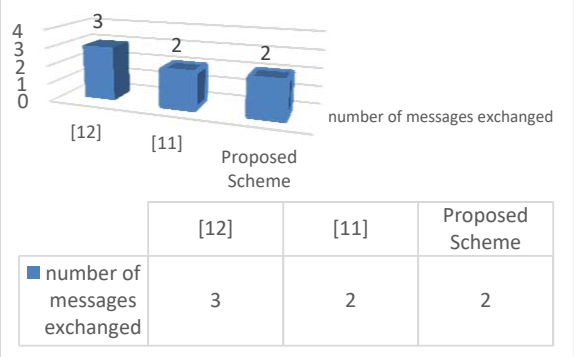


(b) Activity recognition average based on mining



	Hash	CBC-MAC	Proposed Scheme
Time (ms)	39	8	3,4
ROM size (Kb)	9,4	10	9,1
RAM size(Kb)	1,3	1,3	1,8

(c) Computational cost comparison of proposed scheme



	[12]	[11]	Proposed Scheme
number of messages exchanged	3	2	2

(d) Number of messages cost comparison of proposed scheme

Fig. 6 Result analysis of the proposed scheme

D. Computational and Communicational Cost Comparison

Clock synchronization is beyond the scope of this paper, the required size of memory (ROM and RAM) and time execution is shown in Fig. 6 (c). Hash, CBC-MAC and AES required *39 ms (milliseconds)*, *8 ms* and *3.4 ms,* respectively, for computation operation at node X. The proposed scheme is more efficient in terms of time consumption in comparison to other schemes which require longer time to complete their operations. The scheme proposed in [12] takes 2t + 1H + 1Sig, which is not suitable for low cost nodes. The schemes of [4], [11], [12], require almost the same computational costs. In [12], for investigation of communicational cost, the authors proposed the size of a message in the smart home as follows; node X_ID as 1 byte, time stamp as 4 bytes, random number as 4 bytes, 16 bytes for hash functions and 16 bytes as the key size. The proposed scheme requires 1H + 1E + 1D for operations, which means that it requires low computational cost compared to other schemes in terms of time execution for resource constraint devices. Where, t represents the time execution point multiplication; H – the time for execution 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 [15]. The computational cost comparison result shows that the proposed scheme is efficient when compared to other schemes. To evaluate the communication cost comparison of the proposed scheme with other schemes [11] and [12], we use the number of messages process. The communication cost can be calculated by packet size consumed energy during transmission/ receiving of devices. In [12], the author takes three rounds of message exchange during execution, and in [11], the author takes two rounds of message exchange, which are calculated as shown in Fig. 6 (d). The proposed scheme sends 196-bit and receives 104-bit messages, while the scheme proposed by [11] sends 232-bit and receives 72-bit messages. The scheme proposed in this paper revealed that it can secure trajectories and fortify devices against attacks. It also minimizes the use of memory space of LCS in the smart home.

V. Conclusion and Future Work

This paper covers the integrity and device authentication by keeping identity of devices faceless. The proposed scheme establishes a trustworthy session via establishing a connection based on an encrypted lightweight key-session process. This new scheme comprehends the freshness of a message actively via timestamp and uses a person's behavior activity pattern to recognize any abnormal activity of the devices in smart home. Distributed approach enforces the devices to communicate by avoiding dead lock. Furthermore, the proposed scheme secures and fortifies devices, especially LCS, against a device compromised attack and minimizes the use of memory space in the smart home architecture.

In our future work, we will consider other features related to the security applications of smart home environments. We will focus on providing different suitable levels of security for smart home architecture, especially in terms of the behavior activity pattern. Our research deeply focused to make secure smart home architecture. This research also avoids damage to the privacy of smart home architecture. The methodology of the study is innovative and the experiments met the current challenges.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under grant No. 61672115 and Chongqing Social Undertakings and Livelihood Security Science and Technology Innovation Project Special Program (No. cstc2015jcyjBX0124 and No. cstc2017shmsA30003).

References

[1] D. Desai, and H. Upadhyay, "Security and Privacy consideration for internet of things in smart home environments," *International Journal of Engineering Research and Development,* vol. 10, no. 11, pp. 73-83, November 2014.

[2] Chengliang Wang, Y. Peng, D. De, W. Song, "DPHK Real-Time Distributed Predicted Data Collecting based on activity pattern Knowledge mined from trajectories in Smart Environment", *Frontiers of Computer Science*, Vol. 10, Issue 6, pp. 1000–1011, 2016.

[3] 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).* pp. 206-213 June 2012.

[4] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttilla, and M. Sain, "Lightweight and secure session-key establishment scheme in smart home environments," *IEEE Sensors Journal,* vol. 16, no. 1, pp.254-264, 2016.

[5] A. Kailas, V. Cecchi, and A. Mukherjee, "A survey of communication and networking technologies for energy management in building and home automation," *Journal of Computer Networks and communication*, vol. 2012, 2012.

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

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

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

[9] R. Roshan, and A. Kr. Ray, "Challenges and risk to implement IOT in smart homes: An Indian perspective," *International Journal of Computer Applications*, vol. 153, no. 3, pp. 16-19, November 2016.

[10] Chengliang Wang, Yu Zhang, "Time-Window and Voronoi-Partition Based Aggregation Scheduling in Multi-Sink Wireless Sensor Networks", *Ad Hoc & Sensor Wireless Networks*. Vol. 32, issue, 3-4, pp. 221-238, in 2016.

[11] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," *Journal of Latex Class Files, IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, 2017.

[12] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area network", in *Proc. IEEE Int. Conference Consum. Electron. (ICCE),* June, 2013, pp. 88-93.

[13] N. P. Hoang and D. Pishva, "A TOR-based anonymous communication approach to secure smart home appliances," in *2015 17th International Conferences on Advanced Communication Technology (ICACT).* IEEE, 2015, pp. 517-525.

[14] E. Ayday and S. Rajagopal, "Secure Device Authentication Mechanisms for the Smart Grid-Enabled Home Area networks," *Tech. Rep*., 2013.

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

[16] "AVISPA: Automated Validation of Internet Security Protocols and Applications," http://www.avispa-project.org/web-interface/basic.php.