electronics

MDPI

Article

A Situation-Aware Scheme for Efficient Device Authentication in Smart Grid-Enabled Home Area Networks

Anhao Xiang and Jun Zheng *

Department of Computer Science and Engineering, New Mexico Institute of Mining and Technology, Socorro, NM 87801, USA; anhao.xiang@student.nmt.edu

* Correspondence: jun.zheng@nmt.edu

Received: 27 May 2020; Accepted: 10 June 2020; Published: 13 June 2020

Abstract: Home area networks (HANs) are the most vulnerable part of smart grids since they are not directly controlled by utilities. Device authentication is one of most important mechanisms to protect the security of smart grid-enabled HANs (SG-HANs). In this paper, we propose a situation-aware scheme for efficient device authentication in SG-HANs. The proposed scheme utilizes the security risk information assessed by the smart home system with a situational awareness feature. A suitable authentication protocol with adequate security protection and computational and communication complexity is then selected based on the assessed security risk level. A protocol design of the proposed scheme considering two security risk levels is presented in the paper. The security of the design is verified by using both formal verification and informal security analysis. Our performance analysis demonstrates that the proposed scheme is efficient in terms of computational and communication costs.

Keywords: smart grids; device authentication; situational awareness; home area networks

1. Introduction

Smart grids offer many valuable benefits compared with traditional power grids. By enabling distributed power generation, distributed power storage, and microgrids in smart grids, more efficient and reliable power supply can be achieved [1]. The power generation of smart grids uses a mix of traditional fuel based power sources and renewable power sources such as wind farm and solar plant, which can significantly reduce the carbon footprint. The study in [2] shows that by 2030, CO_2 emissions can be reduced by 5% when adopting conservative approach to smart grids. The reduction can be nearly 16% if aggressive approach is adopted. The connection of home area networks (HANs) to smart grids enables the automation of home energy use. Smart grids also provide important infrastructure support for increased using of electric vehicles (EVs) through vehicle-to-grid (V2G) networks [3].

On the other hand, the implementation of smart grids faces major challenges in both physical and cyber domains. Since smart grids contain millions of nodes along with a complex control system, how to achieve the collaboration between components and the large-scale deployment of new devices and technologies becomes a crucial challenge [1]. Connecting power grids to cyber networks for advanced monitoring and control exposes the grids to cyber-attacks which can result in catastrophic damages as demonstrated by the 2015 Ukrine Blackout [4].

In this work, we concentrate on the security of smart grid-enabled HANs (SG-HANs), which connects many smart devices (SDs) of a smart home such as smart appliances, renewable energy sources and storage, EVs, etc. to smart grids. HANs are the most vulnerable part of smart grids since utilities have no direct control of this part [5]. Device authentication is one of the most important

mechanisms to protect the security of SG-HANs against various attacks. In addition to the security consideration, the device authentication protocol must be lightweight since many of the SDs have limited computation power and memory storage. To this end, we propose a situation-aware scheme for efficient device authentication in SG-HANs. Unlike existing work, the proposed scheme selects a suitable authentication protocol based on the security risk information assessed by the smart home system. The aim of the scheme is to provide adequate security protection with reduced computational complexity, communication cost and power consumption. To the best of our knowledge, the proposed scheme is the first work that utilizes the situational awareness feature of smart home system for efficient device authentication in HANs.

The rest of this paper is organized as follows. Related work on device authentication in SG-HANs, situational awareness of smart home and situation-aware security schemes is described in Section 2. The system architecture of SG-HANs and the adopted attack model are introduced in Section 3. Section 4 presents the proposed situation-aware device authentication scheme for SG-HANs. The security analysis and performance analysis of the proposed scheme are provided in Sections 5 and 6, respectively. Finally, conclusions are drawn in Section 7.

2. Related Work

2.1. Device Authentication in SG-HANs

There are a number of works in the literature on device authentication in SG-HANs. Li proposed a ECC (Elliptic Curve Cryptography) based authenticated key establishment (EAKE) protocol for smart home energy management system in [6]. The EAKE protocol has two phases: a device or a security manager receives private/public key pair from the Certificate Agent (CA) through an out-of-band channel in the first phase; the initial session key is then established between the device and the security manager using the EAKE protocol in the second phase. In Ref. [7], Vaidya et al. also proposed a device authentication protocol for smart energy home area networks based on ECC. Both protocols of [6,7] are expensive for resource-limited devices due to the use of public key cryptography.

In Ref. [8], a secure key agreement protocol was proposed for radio frequency for consumer electronics (RF4CE) ubiquitous smart home systems based on symmetric key cryptography. In the proposed protocol, the initial unique secure information is pre-shared between the devices and manufacturers. The RF4CE-based controller receives the secret information from the manufacturer to authenticate a new device.

Ayday and Rajagopal [5] proposed three different device authentication mechanisms for the SG-HANs that provide (1) authentication 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. The design of the three authentication mechanisms is based on symmetric key cryptography with the help of the trust center through the Internet.

Kumar et al. [9] proposed a lightweight and secure scheme for establishing session-key in smart home environments based on symmetric key cryptography. The smart home devices register with the security service provider offline to obtain security parameters including identity, a secret key with key identifier and a short authentication token. They also proposed a secure authentication and key agreement framework for smart home environments in [10] which realizes anonymity and unlinkability. The protocol is lightweight in comparison to other schemes because the design uses less encryption and decryption operations, and the number of exchanged messages is small.

Gaba et al. [11] proposed a robust and lightweight mutual authentication scheme called RLMA for distributed smart environments such as smart homes and smart buildings. The scheme utilizes implicit certificates to achieve simple and efficient mutual authentication and key agreement between smart devices in a smart environment.

2.2. Situational Awareness of Smart Home

Situational awareness is one of the essential features for smart homes [12]. The majority of the existing works for the situational awareness of smart homes are on activity recognition. For example, Wan et al. [13] proposed a dynamic sensor stream segmentation technology which helps the smart home system to categorize multiple sensor streams that belong to the same activity. Sensor correlation calculation and time correlation calculation are applied for the task. In Ref. [14], a data-driven approach based on neural network ensembles was developed for human activity recognition in smart home environments. Various approaches were explored to resolve conflicts between base models used in ensembles. Cicirelli et al. [15] proposed a framework for activity recognition under the cloud-assisted agent-based smart home environment (CASE). By using cloud computing technology, a smart home system can have greater analytic power. The work introduces an innovate approach, which embed activity recognition tasks including data acquisition, feature extraction, activity discovery, and activity recognition into different layers of CASE.

There are only a few works on the situational awareness of the smart home in cyberspace. A framework to measure the security risk of information leakage in IoT-based smart homes was proposed by Park et al. in [16]. The risk assessment is performed using the factor analysis of information risk (FAIR) method. The risk level for cyber situational awareness is obtained through risk grade clustering based on security scenarios.

2.3. Situation-Aware Security Schemes

There are a few recent works on developing situation-aware security schemes. Kim et al. [17] proposed DAoT, a dynamic and energy-aware authentication scheme for IoT devices. The scheme selects different key establishment (KE), message authentication code (MAC) and handshake operations to achieve energy efficient device authentication. The work evaluated the energy costs of different KE, MAC and handshake operations.

In Ref. [18], Hjelm and Truedsson investigated situation-aware adaptive cryptography for an IP camera. Situation parameters from WiFi and Bluetooth connections of the IP camera are used to determine the protection level. The cryptographic algorithms for encryption, hash and message authentication are then selected that are most suitable for the protection level. The power consumption, computational time and communication throughput were examined for different cryptographic algorithms.

Gebrie and Abie [19] proposed a risk-based authentication scheme for health care-related IoT authentication in smart homes. The channel characteristics in wireless body area network (WBAN) including Received signal strength indicator (RSSI), channel gain, temporal link signature, and Doppler measurement are used to determine risk level by using a naive Bayes algorithm. The authentication decision is then performed based on the risk level. For example, timeout and re-authentication will be performed if the risk level is determined as abnormal. It should be noted that there are no actual protocols designed in [17–19].

3. System Architecture and Attack Model

In this section, we introduce the system architecture of SG-HANs and the adopted attack model.

3.1. System Architecture of SG-HANs

The system architecture of SG-HANs considered in our work is shown in Figure 1, which consists of the infrastructure part and the HAN part. The infrastructure part controlled by utilities consists of smart meters (SMs), neighborhood area network (NAN) gateways, and control center. The HAN part in each house is controlled by the home owner, which consists of a number of SDs and one HAN gateway (HGW). A SD communicates with the HGW using a wireless protocol such as ZigBee or MQTT. In this work, we are interested in the authentication between SDs and HGW in the HAN part,

which is helped by the control center. We assume that the smart home system is installed in the HAN with a situational awareness feature. Although the design of situational awareness feature is out of the scope of this work, we envision that the security risk assessment of the smart home system should combine activity recognition in physical domain [13–15] and risk analysis in cyber domain [16].

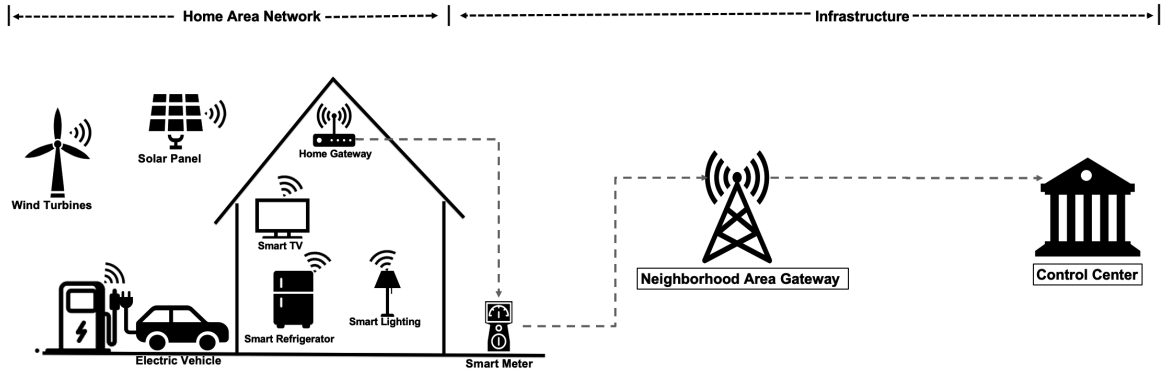

Figure 1. System architecture of SG-HANs.

3.2. Attack Model

The attack model considered in this work is the Dolev–Yao model [20]. In the model, the attacker can eavesdrop, intercept, inject, replay and modify messages exchanged on the open channel. Accordingly the attacker can launch various types of attacks including man-in-the-middle (MITM) attacks, replay attacks and impersonation attacks. Under this attack model, the proposed scheme will achieve security goals of message integrity, mutual authentication and session key establishment, and resistance against various attacks.

4. Proposed Scheme

In this section, we present a protocol design of the proposed situation-aware device authentication scheme for SG-HANs. Without loss of generality, we assume that the security risk assessed by the smart home system has two levels, low and high. The design can be easily extended to more than two security risk levels. The proposed scheme consists of two phases: device registration phase and device authentication and key agreement phase. Table 1 lists the notations and their descriptions that are used in the paper.

Table 1. Notations and their descriptions used in this paper.

Notation	Description
ID_A	Identity of SD A
ID_G	Identity of HGW
RC_A	Random number
R_A	Random number
R_G	Random number
S_i	Secret
A_i	Secret
SK_A	Session key
$H()$	one-way hash function
$E_K(M)$	Encrypt message M using key K
$D_K(M)$	Decrypt message M using key K
$\oplus$	XOR operation
$\|\|$	Message concatenation
T	Timestamp
ΔT	Maximum transmission delay

We have made the following assumptions for the proposed scheme: (1) SD has a clock which runs on its own battery and its assumed to be syAyday2013nchronized with the HGW's clock. (2) HGW is assumed to be authenticated before SD-HGW authentication takes place.

4.1. Device Registration Phase

Before installed in a SG-HAN, each SD needs to be registered offline at the control center. During the registration, the control center assigns an identification number ID_A to the registered SD A along with a random number RC_A. Furthermore, the control center computes secret $S_i = H(ID_A||RC_A)$. Finally, the control center sends ID_A and S_i to the SD A, and ID_A and RC_A to the HGW. The device registration phase is illustrated in Figure 2.

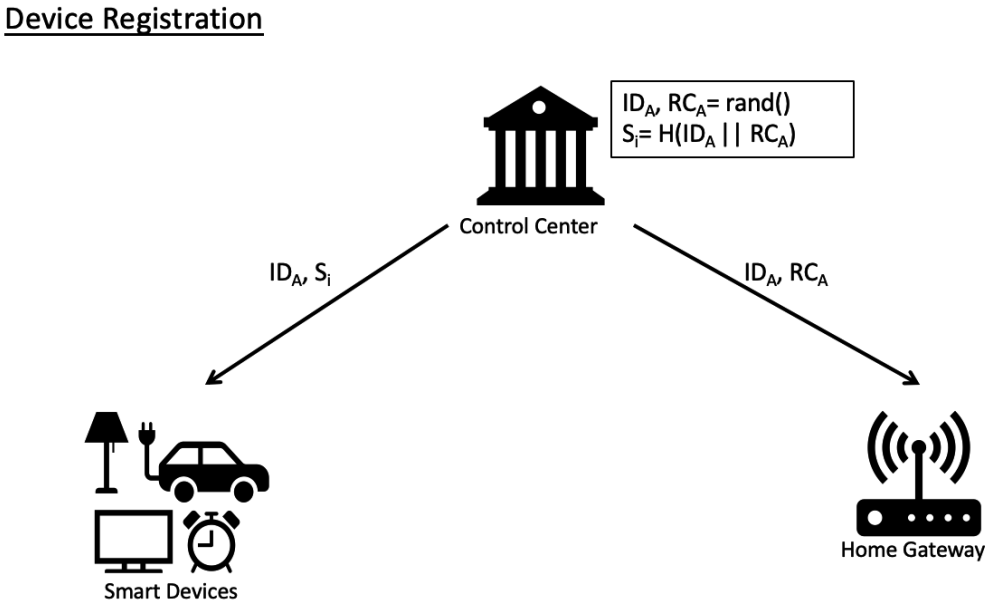

Figure 2. Illustration of device registration phase.

4.2. Device Authentication and Key Agreement Phase

After the registration, the SD A starts the authentication and key agreement process by sending the message MSG_1 to the HGW. MSG_1 includes an message header $HE_1 = 'SD - AUTH'$ and ID_A as shown below:

$$MSG_1 = [HE_1||ID_A]$$

Upon receiving MSG_1, the HGW obtains the current security risk level from the smart home system. The following messages between the SD A and the HGW are generated based on the security risk level.

(a) ***Low security risk***

When the security risk is low, the HGW computes $S_i^* = H(ID_A^*||RC_A)$ and extracts current time stamp T_1. Then the HGW computes $C_{1,L} = (ID_G||T_1) \oplus S_i^*$ and $C_{2,L} = H(HE_{2,L}||ID_G||T_1||S_i^*)$. $HE_{2,L} = 'HGW - LOW'$ is the header of the message $MSG_{2,L}$ that the HGW sends to the SD A.

$$MSG_{2,L} = [HE_{2,L}||C_{1,L}||C_{2,L}]$$

Upon receiving the message $MSG_{2,L}$ at time stamp $T_1{}'$, the device A knows from the message header that the current security risk level is low. The ID of the HGW $ID_G{}^*$ and $T_1{}^*$ can be obtained by computing $ID_G{}^*||T_1{}^* = C_{1,L} \oplus S_i$. The device A also computes $C_{2,L}{}^* = H(HE_{2,L}{}^*||ID_G{}^*||T_1{}^*||S_i)$.

Then the SD A will check if ${T_1}' - {T_1}^* \leq \Delta T$ and ${C_{2,L}}^* == C_{2,L}$, where ΔT is the transmission delay. If not, the authentication process will be aborted. Otherwise, the SD A generates the secret $A_i = H({ID_G}^*||H(ID_A||S_i))$ and extracts the current time stamp T_2. Then the SD A computes $C_{3,L} = (ID_A||T_2) \oplus A_i$ and $C_{4,L} = H(HE_{3,L}||ID_A||T_2||A_i)$, where $HE_{3,L} = 'SD - LOW'$ is the header of the message $MSG_{3,L}$. Finally, the SD A sends $MSG_{3,L}$ to the HGW:

$$MSG_{3,L} = [HE_{3,L}||C_{3,L}||C_{4,L}]$$

The SD A computes the key $SK_A = H({T_1}^*||T_2||S_i||A_i)$ which will be used as the shared session key between the device and the HGW.

When the HGW receives $MSG_{3,L}$ at time stamp ${T_2}'$, it first computes ${A_i}^* = H(ID_G||H(ID_A||{S_i}^*))$ and then extracts ${ID_A}^*$ and ${T_2}^*$ by computing $C_{3,L} \oplus {A_i}^*$. The HGW checks if ${T_2}' - {T_2}^* \leq \Delta T$ and ${C_{4,L}}^* == C_{4,L}$, where ${C_{4,L}}^* = H({HE_{3,L}}^*||{ID_A}^*||{T_2}^*||{A_i}^*)$. Assume all checks pass, the HGW adds ID_A to the trusted list of devices and computes the key $SK_A = H(T_1||{T_2}^*||{S_i}^*||{A_i}^*)$. After this step, both the SD A and the HGW have generated the symmetric session key which will be used for future data communication.

(b) ***High security risk***

When the security risk level obtained by the HGW is high, the message exchange between the SD A and the HGW needs higher security strength.

Upon receiving MSG_1 under high security risk, the HGW computes ${S_i}^* = H(ID_A^*||RC_A)$ and generates a random number R_G. Then the HGW extracts current time stamp T_1 and forms $MSG_{2,H}$ as following:

$$MSG_{2,H} = [HE_{2,H}||C_{1,H}||C_{2,H}]$$

where $HE_{2,H} = 'HGW - HIGH'$ is the message header of $MSG_{2,H}$, $C_{1,H} = E_{S_i^*}(ID_G||T_1||R_G)$ and $C_{2,H} = H(HE_{2,H}||ID_G||T_1||R_G)$. Finally, the HGW sends $MSG_{2,H}$ to the SD A.

Upon receiving the message $MSG_{2,H}$ at time stamp ${T_1}'$, the SD A learns from the message header that the security risk level is high. The SD A then uses S_i to decrypt ${C_{1,H}}^*$ to obtain ${ID_G}^*$, ${T_1}^*$ and ${R_G}^*$. Then it checks if ${T_1}' - {T_1}^* \leq \Delta T$ and ${C_{2,H}}^* == C_{2,H}$, where ${C_{2,H}}^* = H({HE_{2,H}}^*||{ID_G}^*||{T_1}^*||{R_G}^*)$. The authentication process will be terminated if the check is failed. Otherwise, the SD A generates the secret $A_i = H({ID_G}^*||H(ID_A||S_i))$ and a random number R_A. Then the device extracts the current time stamp T_2 and computes $C_{3,H} = E_{A_i}(ID_A||T_2||R_A)$ and $C_{4,H} = H(HE_{3,H}||ID_A||T_2||R_A)$, where $HE_{3,H}$ = 'SD-HIGH' is the message header of $MSG_{3,H}$. The message $MSG_{3,H}$ is then formed and sent to the HGW:

$$MSG_{3,H} = [HE_{3,H}||C_{3,H}||C_{4,H}]$$

Finally, the SD A computes the shared key SK_A as $H({T_1}^*||T_2||S_i||A_i||R_A||R_G^*)$.

After receiving $MSG_{3,H}$ at time stamp ${T_2}'$, the HGW computes the secret ${A_i}^* = H(ID_G||H(ID_A||{S_i}^*))$ and extract ${ID_A}^*$, ${T_2}^*$ and ${R_A}^*$ by performing $D_{A_i^*}(C_{3,H})$. The HGW then computes ${C_{4,H}}^* = H({HE_{3,H}}^*||{ID_A}^*||{T_2}^*||{R_A}^*)$ and checks if ${T_2}' - {T_2}^* \leq \Delta T$ and ${C_{4,H}}^* == C_{4,H}$. If all checks pass, the HGW adds ID_A to the trusted list of devices and computes the session key $SK_A = H(T_1||{T_2}^*||{S_i}^*||{A_i}^*||{R_A}^*||R_G)$.

Figures 3 and 4 show the message flows of the proposed scheme under low security risk and high security risk, which are denoted as two protocols P_L and P_H, respectively.

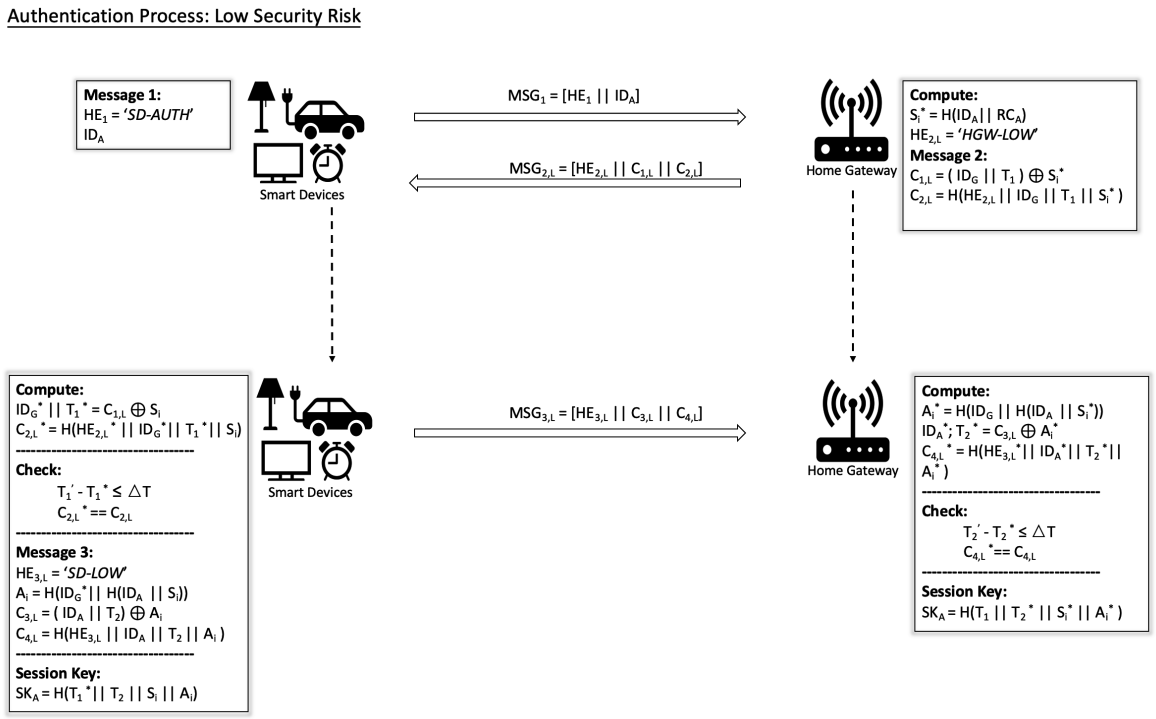

Figure 3. The message flow of the proposed scheme at low security risk (P_L).

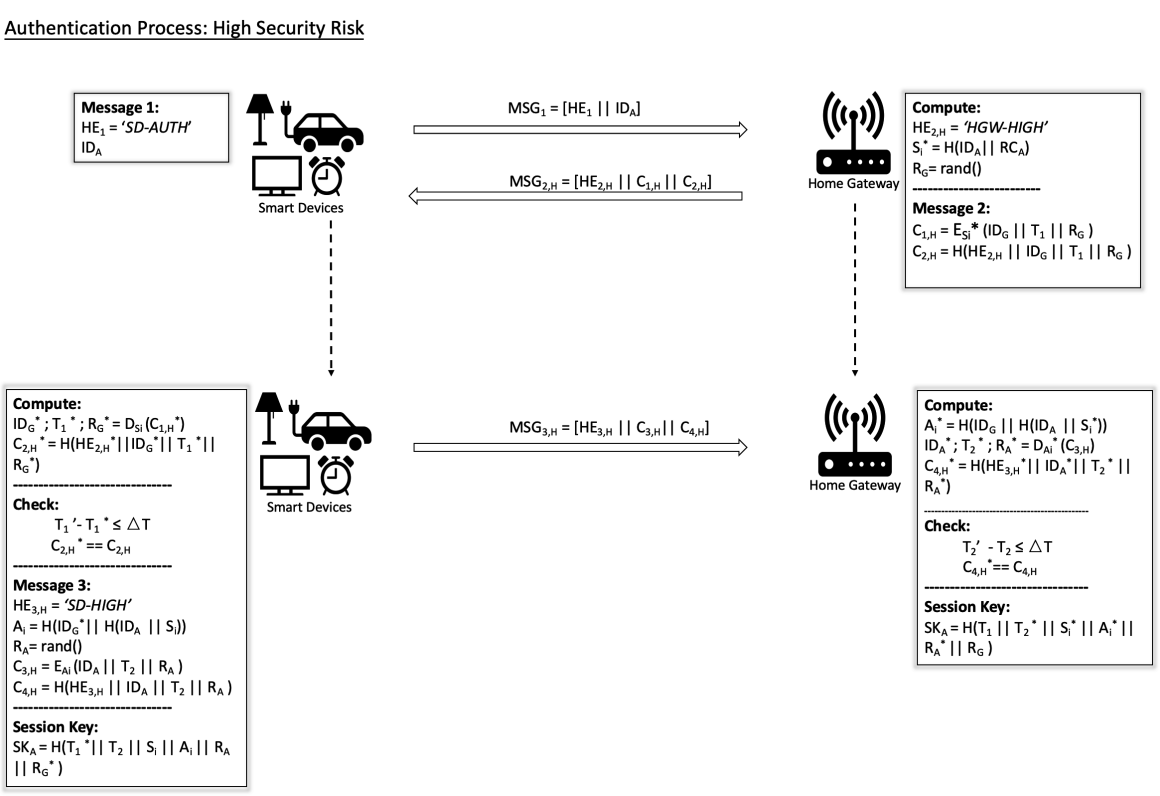

Figure 4. The message flow of the proposed scheme at high security risk (P_H).

5. Security Analysis

In this section, we verify the security of the proposed scheme using formal verification and informal security analysis.

5.1. Formal Security Verification

The formal security verification of the proposed scheme was done by using the automated validation feature of the Internet Security Protocols and Applications (AVISPA) tool [21], which is a push-button security analyzer tool designed for large scale internet security-sensitive protocols. AVISPA tool has been widely applied for formal security analysis of authentication protocols [9,10,22–24].

The architecture of AVISPA tool is illustrated in Figure 5. High Level Protocol Specification Language (HLPSL) is used to describe protocol design and specify security goals. AVISPA tool takes a HLPSL file as input and translates the file into intermediate format (IF) by using HLPSL2IF translator. The IF code becomes the input to the backend, where protocol security goals will be verified. Finally, the backend outputs the security report. As shown in Figure 5, the backend of AVISPA tool consists of four components: on-the-fly Model-Checker (OFMC), CL-based Attack Sercher (CL-AtSe), SAT-based Model-Check (SATMC), and Tree Automata-based Protocol Analyzer (TA4SP). Users can choose the backend components according to security requirements of their design. Notice that HLPSL is a role based language. The basic role states initial variables, constants, and transition steps. The composed role instantiate one or more basic roles. Finally, a top level role called environment role, states global constants and a composition of multiple sessions.

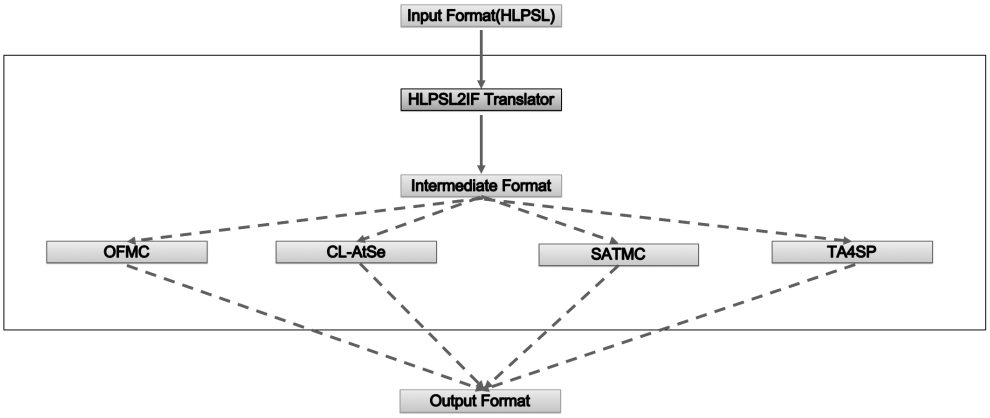

Figure 5. Architecture of the AVISPA tool [21].

The security goals of the proposed scheme are specified in Figure 6 as: (1) *secrecy_of sessionkey* means that the session key generated in the proposed scheme is kept secret between the SD and the HGW; (2) *authentication_on gateway_Si* means that secret S_i will be verified at the SD; (3) *authentication_on_device_Ai* means that secret A_i will be verified at the HGW; (4) *authentication_on_device_t2* means that the timestamp T_2 generated by the SD will be agreed between the SD and the HGW; (5) Similarly, *authentication_on_gateway_t1* verifies the agreement on timestamp T_1 between the HGW and the SD. The first security goal tests the strength and secrecy of the session key against various attacks such as MITM attack. The second and third security goals together confirm the establishment of mutual authentication, and the last two security goals test the protocol design against replay attacks. By running the HLPSL file through the backend, we test not only the protocol design against various attacks, but also whether the protocol satisfies specific requirements.

Figures 7 and 8 specify the roles of the SD and the HGW for low security risk, respectively. In the SD role, State 0 indicates the beginning of the authentication process. At State 0, the SD starts the authentication process by sending identity ID_A to the HGW through the $SND()$ function. On the other side, the HGW receives the device identity ID_A at State 0 by using the $RCV()$ function. Upon receiving ID_A, the HGW will move to State 1, where secret S_i is generated by using the built-in hash function $H()$, T_1 will be generated as random number by calling $new()$ function. Then the HGW uses built-in *xor* function to generate the response message. Similarly, after sending ID_A to the HGW, the SD will

move to State 1 and wait for the response message from the HGW. Both SD and HGW generates the session key at State 2. Similar to low security risk, Figures 9 and 10 specify the SD and HGW roles for high security risk, respectively.

```
goal

 secrecy_of sessionkey
 authentication_on gateway_t1
 authentication_on device_t2
 authentication_on gateway_si
 authentication_on device_ai

end goal
```

Figure 6. Specification of security goals of the proposed scheme.

```
role device (A, B:     agent,
             H:        hash_func,
             SND,RCV:  channel(dy))
played_by A def=

  local State: nat,
     Device_id, Gateway_id, Rc, Si   :text,
     C0,C1,C2,C3,C4,C5               :message,
     T1, T2, Ai, Ks                  :text,

  init State := 0

  transition
    1.  State = 0   /\ SND(Device_id') =|>
        State' := 1

    2.  State = 1   /\ RCV(C0'.C1'.C2') =|>
        State' := 2 /\ Gateway_id' := xor(C0', Si)
             /\ T1' := xor(C1', Si)
             /\ T2' := new()
             /\ Verify' := H(Gateway_id'.T1'.Si)
             /\ Ai' := H(Gateway_id'.H(Device_id.Si))
             /\ C3' := xor(Ai',Device_id)
             /\ C4' := xor(Ai',T2)
             /\ C5' := H(Device_id.T2',Ai')
             /\ SND(C3'.C4'.C5')
             /\ Ks' := H(T1'.T2'.Si.Ai')
             /\ secret(Ks', sessionkey, {A,B})
             /\ witness(A,B,device_t2,T2')
             /\ witness(A,B,device_ai,Ai')

end role
```

Figure 7. Specification of the SD role for low security risk.

```
role gateway (A,B:      agent,
              H:        hash_func,
              SND,RCV:  channel(dy))
played_by B def=

  local State: nat,
     Device_id, Gateway_id, Rc, Si  :text,
     C0,C1,C2,C3,C4,C5              :message,
     T1, T2, Ai, Ks                 :text,

  init State := 0

  transition
    1.   State = 0 /\ RCV(Device_id') =|>
         State' := 1  /\ Si' := H(Device_id'.Rc)
              /\ T1' := new()
              /\ C0' := xor(Si',Gateway_id)
              /\ C1' := xor(Si',T1')
              /\ C2' := H(Gateway_id.T1'.Si')
              /\ SND(C0'.C1'.C2')
              /\ witness(B,A,gateway_t1,T1')
               /\ witness(B,A,gateway_si,Si')

    2.  State = 1 /\ RCV(C3', C4',C5') =|>
         State' := 2/\ Ai' := H(Gateway_id.H(Device_id.Si))
              /\ T2' := xor(Ai',C4)
              /\ Ks' := H(T1.T2'.Si.Ai')
              /\ secret(Ks', sessionkey, {A,B})

end role
```

Figure 8. Specification of the HGW role for low security risk.

```
role device (A,B      :   agent,
             H        :   hash_func,
             SND,RCV  :   channel(dy))
played_by A def=

  local State: nat,
     Device_id,Gateway_id,Rc,Si     : text,
    C0,C1,C2,C3,C4,C5               : message,
    T1,T2,Ai,Ks,RG,RA               : text,

  init State := 0

  transition
    1.   State = 0  /\ SND(Device_id') =|>
         State' := 1

    2.   State = 1   /\
    RCV({Gateway_id'.T1'.RG'}_Si.C2') =|>
         State' := 2 /\ T2' := new()
            /\ Verify' := H(Gateway_id'.T1'.Si)
            /\ Ai' := H(Gateway_id'.H(Device_id.Si))
            /\ RA' := new()
            /\ C4' := ({Device_id.T2'.RA'}_Ai')
            /\ C5' := H(Device_id.T2',Ai')
            /\ SND({Device_id.T2'.RA'}_Ai'.C5')
            /\ Ks' := H(T1'.T2'.Si.Ai'.RA'.RG')
            /\ secret(Ks', sessionkey, {A,B})
            /\ witness(A,B,device_t2,T2')
            /\ witness(A,B,device_ai,Ai')
end role
```

Figure 9. Specification of the SD role for high security risk.

```
role gateway (A,B      :  agent,
              H        :  hash_func,
              SND,RCV  :  channel(dy))
played_by B def=

  local State: nat,
         Device_id,Gateway_id,Rc,Si : text,
         C0,C1,C2,C3,C4,C5          : message,
         T1,T2,Ai,Ks,RG,RA          : text,

  init State := 0

  transition
    1.   State = 0 /\ RCV(Device_id') =|>
         State' := 1 /\ RG' := new()
              /\ Si' := H(Device_id'.Rc)
              /\ T1' := new()
              /\ C1' := ({Gateway_id.T1'.RG'}_Si')
              /\ C2' := H(Gateway_id.T1'.Si')
              /\ SND({Gateway_id.T1'.RG'}_Si.C2')
              /\ witness(B,A,gateway_t1,T1')
              /\ witness(B,A,gateway_si,Si')

    2.   State = 1 /\ RCV({Device_id.T2'.RA'}_Ai'.C5') =|>
         State' := 2 /\ Ai' := H(Gateway_id.H(Device_id.Si))
              /\ Ks' := H(T1.T2'.Si.Ai'.RA'.RG)
              /\ secret(Ks', sessionkey, {A,B})
end role
```

Figure 10. Specification of the HGW role for high security risk.

Figure 11 specifies the protocol session role. In this role, we instantiate one instance of each basic role and compose them together to construct the whole protocol session. *Channel(dy)* declaration means that the intruder has full control over the channel, where *dy* stands for the Dolev–Yao attack model. Finally, the top-level environment role is defined in Figure 12. This role defines device ID, gateway ID, *rc* and *si* as global constants, and a composition of three sessions. Note that the intruder represented as constant *i*, will have names of all agents as initial knowledge.

```
role session(A,B  : agent,
             H    : hash_func)
def=
  local SC, CR, SD, DR, SG, GR: channel (dy)

  composition
        device(A,B,H,SD, DR)
     /\ gateway(B, A, H, SG, GR)
end role
```

Figure 11. Specification of the session role.

```
role environment()

def=

  const  a,b                              : agent,
         h                                : hash_func,
         device_id, gateway_id,rc, si     : text,

     sessionkey    : protocol_id,
     gateway_t1    : protocol_id,
     device_t2     : protocol_id,
     gateway_si    : protocol_id,
     device_ai     : protocol_id

  intruder_knowledge = {a,b}

  composition
     session(a,b,h)
     /\ session(i,b,h)
     /\ session(a,i,h)

end role
```

Figure 12. Specification of the environment role.

The outputs of the OFMC and CL-AtSe backends for P_L and P_H of the proposed scheme are shown in Figures 13–16. The results show that the proposed scheme is safe in the OFMC and CL-AtSe backends. This means that the proposed scheme successfully meets specified security goals.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/protocol1.if
GOAL
  as_specified
BACKEND
  OFMC
```

Figure 13. Output of OFMC backend for low security risk.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/protocol2.if
GOAL
  as_specified
BACKEND
  OFMC
```

Figure 14. Output of OFMC backend forhigh security risk.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/protocol1.if
GOAL
  As Specified
BACKEND
  CL-AtSe
```

Figure 15. Output of CL-AtSe backend for low security risk.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/protocol2.if
GOAL
  As Specified
BACKEND
  CL-AtSe
```

Figure 16. Output of CL-AtSe backend for high security risk.

5.2. Informal Security Analysis

In this section, we perform an informal security analysis to show how the proposed scheme achieves different security objectives.

5.2.1. Message Integrity

Both P_L and P_H of the proposed scheme use one-way hash functions to achieve the message integrity. To tamper the transmitted messages, the attacker needs to learn the secrets S_i and A_i which can not be obtained through the eavesdropped messages. Thus, the attacker cannot compute a valid hash value for a message, which means that the proposed scheme achieves the message integrity properly.

5.2.2. Mutual Authentication

Mutual authentication is an important property to verify the legitimacy of the SD and HGW to each other. In the proposed scheme, the SD authenticates the HGW by verifying the validity of the value $C_{2,*}$ using the secret S_i. The HGW then authenticates the SD by verifying the validity of the value $C_{4,*}$ using the secret A_i. As the secrets S_i and A_i cannot be obtained from the eavesdropped messages, the proposed scheme support the mutual authentication between the SD and HGW.

5.2.3. Resistance against MITM Attack

An attacker can launch the MITM attack by relaying and manipulating the messages exchanged between the SD and HGW. In the proposed scheme, the attacker needs to learn the secret S_i to manipulate the messages successfully. Since the secret S_i cannot be obtained from the previously eavesdropped messages, the propose scheme can resist the MITM attack.

5.2.4. Resistance against Replay Attack

In the replay attack, the attacker can replay previously eavesdropped messages to establish an authenticated session with the targeted entity. The proposed scheme uses the timestamp to verify if a

received message is valid or not. Since the replayed message has the old timestamp, it cannot pass the verification. Thus, the proposed scheme can resist the replay attack.

5.2.5. Resistance against Impersonation Attack

An attacker may impersonate a SD by forging the request message MSG_1 with a fake/stolen ID as MSG_1 is in plain text. However, the response message $MSG_{2,*}$ from the HGW cannot be interpreted by the attacker since the secret S_i is unknown to the attacker. Therefore, the attacker cannot continue the authentication process. There is also no way for the attacker to impersonate the HGW by forging the response message since the HGW identity ID_G is protected with the secret S_i during the transmission. Thus, the proposed scheme can resist the impersonation attack.

6. Performance Analysis

Since a SD is usually resource limited, the design of authentication scheme should not overwhelm the SD's computational and communication resources. In this section, we perform an analysis of the computational and communication costs of the proposed scheme.

6.1. Communication Cost

The communication cost of the proposed scheme is evaluated using the total number of bits sent and received by the SD and the communication energy cost. In the analysis, we assume that message header is 3 bits in length, device ID and HGW ID are 8 bits, timestamp and random number are 32 bits, and outputs of hash and encryption operations are 128 bits.

Table 2 compare the proposed scheme with [6,8,9] in terms of total number of exchanged messages. Both P_L and P_H of the proposed scheme require three messages exchanged between the SD and the HGW, which is comparable to that of [9] and less than those of [6,8].

Table 2. Comparison of total number of exchanged messages.

Scheme	Total Number of Messages
Li [6]	4
Han et al. [8]	6
Kumar et al. [9]	3
P_L	3
P_H	3

The communication overheads of P_L and P_H of the proposed scheme in terms of total number of bits are shown in Table 3, which are calculated using aforementioned parameters. Figure 17 shows the communication overhead of the proposed scheme with different percentages of P_L and P_H being used. Generally, the higher chance that P_L is used, the lower the communication overhead of the proposed scheme. The communication overheads of three existing works [6,8,9] are also plotted in Figure 17. It is obvious that the proposed scheme achieves the lowest communication overhead even only P_H is used.

Besides communication overhead, communication energy cost is another important factor when evaluating communication cost. In order to simulate a resource limited SD, we used the TelosB platform which embeds a 16-bit processor running at 8 MHz clock frequency. TelosB also has limited amount of memory: 48 KB of ROM and 10 KB of RAM [25]. To measure the communication energy cost, we obtained the energy costs of sending and receiving one bit of data on TelosB platform as 0.72 μJ and 0.81 μJ from [26]. Then the communication energy costs of P_L and P_H are obtained as 269.55 μJ and 403.47 μJ (Table 4). Table 5 compares the communication energy cost of the proposed scheme with those of [6,8,9]. We assume that P_L and P_H have equal chance to be used for the proposed scheme. The results indicate that the proposed scheme is more efficient than other schemes in terms of communication energy cost.

Table 3. Communication overhead (in bits).

Message	P_L	P_H
MSG_1	11	11
MSG_2	171	259
MSG_3	171	259
Total	353	529

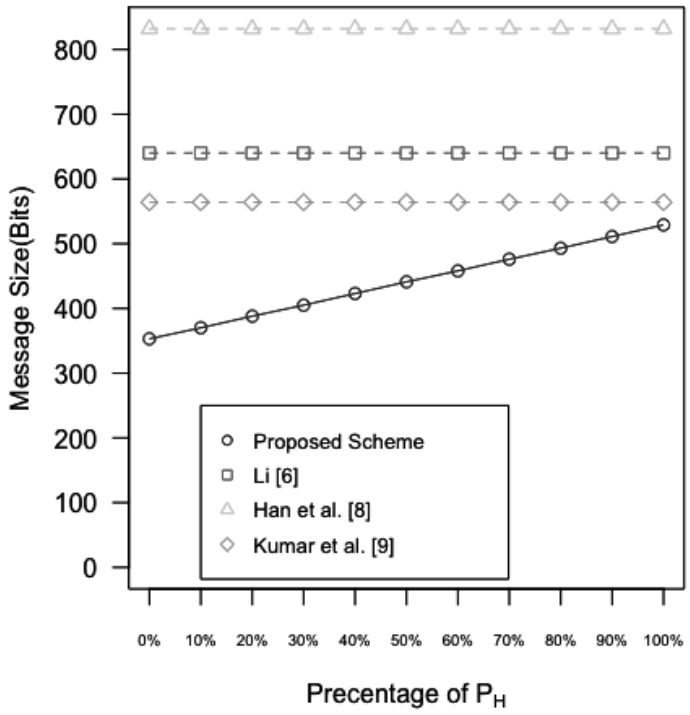

Figure 17. Communication overhead of the proposed scheme compared with those of three existing works [6,8,9].

Table 4. Communication energy cost.

P_L	Energy Cost (μJ)	P_H	Energy Cost (μJ)
MSG_1	7.92	MSG_1	7.92
$MSG_{2,L}$	138.51	$MSG_{2,H}$	209.79
$MSG_{3,L}$	123.12	$MSG_{3,H}$	185.76
Total:	269.55	Total:	403.47

Table 5. Comparison of communication energy cost.

Scheme	Communication Energy Cost (μJ)
Li [6]	483.84
Han et al. [8]	656.64
Kumar et al. [9]	430.22
Proposed Scheme (50% P_L + 50% P_H)	336.51

6.2. Computational Cost

Table 6 compares the computational cost of the proposed scheme with those of [6,8,9]. In the table, 'H' represents the time to execute one hash function. 'XOR' represents the time to perform an exclusive-or operation. 'E' and 'D' represent the times to perform encryption and decryption, respectively. 'MAC' and 'HMAC' represent the times used to compute the message authentication

code and the hashed message authentication code, respectively. 't' is the time to perform a point multiplication operation. As shown in Table 6, P_L of the proposed scheme requires five hash operations and two XOR operations while P_H requires five hash operations, one encryption operation and one decryption operation. Since both P_L and P_H use five hash operations, a time and memory efficient hash algorithm such as BLAKE2 [27] is recommended for the proposed scheme. In comparison, the scheme proposed in [6] requires two point multiplication operations, one MAC operation, one encryption operation, one decryption operation, and one hash operation. Note that the point multiplication operation has high computational complexity compared with other operations. The scheme proposed in [8] requires seven MAC operations, four encryption operations, four decryption operations, and five hash operations. Finally, two hash operations, one MAC operation, one HMAC operation, one encryption operation and one decryption operation are required for the scheme of [9]. Overall, the proposed scheme is computational efficient and easy to implement compared with other schemes.

Table 6. Comparison of computational costs.

Operation	Li [6]	Han et al. [8]	Kumar et al. [9]	P_L	P_H
Hash	1H	5H	2H	5H	5H
XOR	–	–	–	2XOR	–
Cryptosystem	1E + 1D	4E + 4D	1E + 1D	–	1E + 1D
MAC	1MAC	7MAC	1MAC	–	–
HMAC	–	–	1HMAC	–	–
Point Multiplication	2t	–	–	–	–

We also analyzed the computational energy cost of the proposed scheme using a similar method of [9]. The energy consumption of a SD (E) is calculated by using the formula $E = V \times I$, where V is the voltage of the new batteries and I is the current of the circuit. Both V and I were retrieved from the TelosB datasheet [25]. The energy costs of executing hash function and encryption algorithm on TelosB platform can be computed based on the work of [28]. To compare with other schemes, we also obtained the energy costs of MAC and HMAC operations and point multiplication operation from [9,26], respectively. Since the time of executing XOR operation is negligible compared with other operations, it was excluded from the evaluation. The computational energy costs of different operations are shown in Table 7. Table 8 compares the total computational energy cost of the proposed scheme (50% P_L and 50% P_H) with those of [6,8,9]. The results indicate that the proposed scheme is more efficient than other schemes in terms of computational energy cost.

Table 7. Computational energy costs of different operations.

Operation	Energy Cost (μJ)
Hash	8.1
Encryption	14.9
MAC	45.36
HMAC	210.6
Point Multiplication	17,000

Table 8. Comparison of computational energy costs.

Scheme	Computational Energy Cost (μJ)
Li [6]	34,068.36
Han et al. [8]	417.62
Kumar et al. [9]	287.06
Proposed Scheme (50% P_L + 50% P_H)	55.4

7. Conclusions

Situation awareness is the essential feature of a smart home system which can be used to develop various smart applications. In this paper, we propose an efficient device authentication scheme for SG-HANs that can adapt to the security risk information assessed by the smart home system. The scheme selects a suitable authentication protocol based on the assessed security risk level that provides adequate security protection with reduced computational and communication costs. We presents a protocol design of the proposed scheme by considering two security risk levels. A formal security verification using AVISPA tool and an informal security analysis are performed to prove the security of the design. The performance analysis demonstrates that the proposed scheme is efficient for device authentication in SG-HANs in terms of both computational and communication costs. In future, we will research how to use the information collected by the smart home system in both physical and cyber domains to assess the security risk level, which is the key to enable the proposed scheme.

Author Contributions: Conceptualization, J.Z.; methodology, A.X. and J.Z.; formal analysis, A.X. and J.Z.; software, A.X.; writing–original draft preparation, A.X. and J.Z.; writing–review and editing, A.X. and J.Z.; supervision, J.Z.; funding acquisition, J.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This material is based upon work funded by the National Science Foundation EPSCoR Cooperative Agreement OIA-1757207.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fang, X.; Misra, J.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. [CrossRef]
2. Hledik, R. How green is the smart grid? *Electr. J.* **2009**, *22*, 29–41. [CrossRef]
3. Shaukat, N.; Khan, B.; Ali, S.M.; Mehmood, C.A.; Khan, J.; Farid, U.; Majid, M.; Anwar, S.M.; Jawad, M.; Ullah, Z. A survey on electric vehicle transportation within smart grid system. *Renew. Sustain. Energy Rev.* **2018**, *81*, 1329–1349. [CrossRef]
4. Liang, G.; Weller, S.; Zhao, J.; Luo, F.; Dong, Z. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. [CrossRef]
5. Ayday, E.; Rajagopal, S. *Secure Device Authentication Mechanisms for the Smart Grid-Enabled Home Area Networks*; Technical Report; 2013; pp. 1–18. Available online: https://infoscience.epfl.ch/record/188373/files/smart_grid_tech_report.pdf (accessed on 20 May 2020)
6. Li, Y. Design of a key establishment protocol for smart home energy management system. In Proceedings of the 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, Spain, 5–7 June 2013; pp. 88–93.
7. Vaidya, B.; Makrakis, D.; Mouftah, H.T. Device authentication mechanism for smart energy home area networks. In Proceedings of the 2011 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 9–12 January 2011; pp. 787–788.
8. Han, K.; Kim, J.; Shon, T.; Ko, D. A novel secure key pairing protocol for RF4CE ubiquitous smart home systems. *Pers. Ubiquit. Comput.* **2013**, textit17, 945–949. [CrossRef]
9. Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. Lightweight and secure session-key establishment scheme in smart home environments. *IEEE Sens. J.* **2016**, *16*, 254–264. [CrossRef]
10. Kumar, P.; Braeken, A.; Gurtov, A.; Iinatti, J.; Ha, P.H. Anonymous secure framework in connected smart home environments. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 968–979. [CrossRef]
11. Gaba, G.S.; Kumar, G.; Monga, H.; Kim, T.-H.; Kumar, P. Robust and lightweight mutual authentication scheme in distributed smart environments. *IEEE Access* **2020**, *8*, 69722–69733. [CrossRef]
12. Lee, S.-Y.; Lin, F.J. Situation awareness in a smart home environment. In Proceedings of the 2016 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 678–683.
13. Wan, J.; O'grady, M.J.; O'hare, G.M. Dynamic sensor event segmentation for real-time activity recognition in a smart home context. *Pers. Ubiquit. Comput.* **2015**, *19*, 287–301. [CrossRef]

14. Irvine, N.; Nugent, C.; Zhang, S.; Wang, H.; Ng, W.W.Y. Neural network ensembles for sensor-based human activity recognition within smart environments. *Sensors* **2020**, *20*, 216. [CrossRef] [PubMed]
15. Cicirelli, F.; Fortino, G.; Giordano, A.; Guerrieri, A.; Spezzano, G.; Vinci, A. On the design of smart homes: A framework for activity recognition in home environment. *J. Med. Syst.* **2016**, *40*, 200. [CrossRef] [PubMed]
16. Park, M.; Oh, H.; Lee, K. Security risk measurement for information leakage in IoT-Based smart homes from a situational awareness perspective. *Sensors* **2019**, *19*, 2148. [CrossRef] [PubMed]
17. Kim, Y.; Yoo, S.; Yoo, C. DAoT: Dynamic and energy-aware authentication for smart home appliances in internet of things. In Proceedings of the 2015 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 9–12 January 2015; pp. 196–197.
18. Hjelm, V.; Truedsson, M. Situation-Aware Adaptive Cryptography. Master's Thesis, Lund University, Lund, Sweden, 2018.
19. Gebrie, M.T.; Abie, H. Risk-based adaptive authentication for internet of things in smart home ehealth. In Proceedings of the 11th European Conference on Software Architecture (ECSA), Canterbury, UK, 11–15 September 2017; pp. 102–108.
20. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
21. Viganò, L. Automated security protocol analysis with the AVISPA tool. *Electron. Notes Theor. Comput. Sci.* **2006**, *155*, 61–86. [CrossRef]
22. Chen, C.; He, D.; Chan, S.; Bu, J.; Gao, Y.; Fan, R. Lightweight and provably secure user authentication with anonymity for the global mobility network. *Int. J. Commun. Syst.* **2011**, *24*, 347–362. [CrossRef]
23. Nicanfar, H.; Jokar, P.; Beznosov, K.; Leung, V. Efficient authentication and key management mechanisms for smart grid communications. *IEEE Syst. J.* **2014**, *8*, 629–640. [CrossRef]
24. Mohammadali, A.; Haghighi, M.S.; Tadayon, M.H.; Nodooshan, A.M. A novel identity-based key establishment method for advanced metering infrastructure in smart grid. *IEEE Trans. Smart Grid* **2018**, *9*, 2834–2842. [CrossRef]
25. *TelosB Datasheet*. Available online: http://www.memsic.com/userfiles/files/Datasheets/WSN/telosb_datasheet.pdf (accessed on 20 May 2020).
26. de Meulenaer, G.; Gosset, F.; Standaert, F.-X.; Pereira, O. On the energy cost of communication and cryptography in wireless sensor networks. In Proceedings of the 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Avignon, France, 12–14 October 2008; pp. 580–585.
27. Fast Secure Hasing. Available online: https://blake2.net (accessed on 20 May 2020).
28. Pereira, G.; Alves, R.; de Silva, F.; Azevedo, R.; Albertini, B.; Margi, C. Performance evaluation of cryptographic algorithms over IoT platforms and operating systems. *Secur. Commun. Netw.* **2017**, *2017*. [CrossRef]