H-infinity adaptive observer enhancements for vehicle chassis dynamics-based navigation sensor fault construction

Linlin Xia
Jingyu Cong
Xun Xu
University of Wollongong, xun@uow.edu.au
Yiping Gao
Shufeng Zhang

Follow this and additional works at: https://ro.uow.edu.au/aiimpapers

Part of the Engineering Commons, and the Physical Sciences and Mathematics Commons

Recommended Citation
Xia, Linlin; Cong, Jingyu; Xu, Xun; Gao, Yiping; and Zhang, Shufeng, "H-infinity adaptive observer enhancements for vehicle chassis dynamics-based navigation sensor fault construction" (2020).


Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au
H-infinity adaptive observer enhancements for vehicle chassis dynamics-based navigation sensor fault construction

Abstract
© The Author(s) 2020. The issues of chassis dynamics-based navigation sensor fault and state estimation in land vehicles are specialized in this study. Owing to the essential attributes of robust theory-based observers, an H-infinity adaptive observer is proposed to implement the fault reconstructions of faulty sensors, offering a reference to vehicles for further favorable control decision-making. This observer fuses a linear matrix inequality convex optimization strategy, with the dynamics of land vehicles established mathematically, the consequent problems associated with augmented descriptor system state-space model, Lyapunov stability and linear matrix inequality convex optimization are discussed in detail. The numerical simulations on vehicular systems that suffered with single-existing deadlocking, gain scheduling, and constant deflection sensor fault are conducted. The results indicate, the fault channel outputs fairly reflect the variations of real faults under severe step-type fault input circumstances, so that the applicability of the fault observer against sensor failures is guaranteed. The proposed sensor fault construction idea is further extended to a loosely coupled inertial measurement units/global positioning system (GPS) illustration with GPS unavailable in its north velocity channel. After reconstructing the priori system state for “State one-step prediction” of Kalman filter, the compensated navigation parameters by state estimator exhibit consistent with the references as expected, the vehicle chassis dynamics-based sensor fault construction method, therefore, may be recognized as an effective measure to a class of integrated navigation systems experiencing some unknown sensor failures.

Disciplines
Engineering | Physical Sciences and Mathematics

Publication Details

This journal article is available at Research Online: https://ro.uow.edu.au/aiimpapers/4094
Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment

Mohammad Wazid, Student Member, IEEE, Ashok Kumar Das, Member, IEEE, Vanga Odelu, Neeraj Kumar, Member, IEEE, and Willy Susilo, Senior Member, IEEE

Abstract—The Information and Communication Technology (ICT) has been used in wide range of applications, such as smart living, smart health and smart transportation. Among all these applications, smart home is most popular, in which the users/residents can control the various smart sensor devices of home by using the ICT. However, the smart devices and users communicate over an insecure communication channel, i.e., the Internet. There might be the possibility of various types of attacks, such as smart device capture attack, user, gateway node and smart device impersonation attacks and privileged-insider attack on a smart home network. An illegal user, in this case, can gain access over data sent by the smart devices. Most of the existing schemes reported in the literature for the remote user authentication in smart home environment are not secure with respect to the above specified attacks. Thus, there is need to design a secure remote user authentication scheme for a smart home network so that only authorized users can have access to the smart devices. To mitigate the aforementioned issues, in this paper, we propose a new secure remote user authentication scheme for a smart home environment. The proposed scheme is efficient for resource-constrained smart devices with limited resources as it uses only one-way hash functions, bitwise XOR operations and symmetric encryptions/decryptions. The security of the scheme is proved using the rigorous formal security analysis under the widely-accepted Real-Or-Random (ROR) model. Moreover, the rigorous informal security analysis and formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool is also done. Finally, the practical demonstration of the proposed scheme is also performed using the widely-accepted NS-2 simulation.

Index Terms—Smart home, user authentication, key agreement, provable security, AVISPA, NS2 simulation.

1 INTRODUCTION

The advancement of ICT and the Internet have provided the support for rapid growth in smart home environments. A smart home contains the advanced automation systems for monitoring and controlling of various smart devices. In a smart home, the residents can control various smart sensing devices such as temperature monitoring sensors, lighting equipments sensors, or occupancy sensors, etc. [1], [2], [3], [4]. The smart home environment provides a high level of comfort with reduced operational costs to provide safety and security to its residents [5]. One of the major advantages of this type of environment is for the elderly and disabled people in which these people get assistance in estimating their body parameters using smart gadgets [6]. A smart home is equipped with a number of smart devices (SD)j, such as low-cost sensors, smart light controllers, smart window shutters, smart AC controllers various and surveillance cameras. Most of the SDj are resource-constrained having limited computational and communication power, and limited battery backup [3]. A smart home network can be implemented with the help of these SDj in which all SDj communicate over wireless channels using the home gateway node (GWj). The GWj acts as a bridge between SDj and smart home user (Ui). The GWj provides interoperability and control for the SDj and connects them to the external world using the Internet. This facilitates the Ui to operate the smart home appliances remotely using the Internet-enabled smartphones, tablets, etc. anytime from anywhere in the world [5], [7].

1.1 Network Model

The network model depicted in Fig. 1 consists of the smart home users Uij who want to access smart devices SDij as per their requirements. Suppose there is a user Ui, who wants to access certain SDj (e.g. temperature & humidity sensor). To access that SDj, Ui first needs to register himself/herself at the trusted registration authority RA. Similarly, all SDij and the gateway node GWj (which acts as the bridge between the SDj and Uij, and connects SDj to the external world using the Internet) are also registered at the RA. The GWj is thus a special node
that takes responsibility of controlling the network data, device and network interoperability and secure management [5]. The registration authority (RA) is a trusted server and it is responsible for registering all the smart devices, users $U_i$’s and the GWN securely. After the successful registration of $U_i$, SD$_j$ and GWN securely, the RA stores this useful information in the memory of smart phone $SP_i$ of $U_i$, and also in the memory of $SD_j$ and GWN, which are further used at the time of authentication and key establishment process. $U_i$, who wants to access a $SD_j$, sends an authentication request directly to the GWN as both of them have already performed the registration phase at the RA. Three categories of mutual authentications happen: 1) between $U_i$ and GWN, 2) between GWN and $SD_j$ and 3) between $U_i$ and $SD_j$. Moreover, $U_i$ and $SD_j$ establish a secret session key $SK_{ij}$ between them to protect the exchanged messages.

![Smart Home Environment](image)

**Fig. 1.** Smart home environment (Adapted from [5])

### 1.2 Motivation

Consider the following scenario in smart home environment [8]. Recently, it is noticed that the major trend throughout Europe is the aging society, which is affected by an increasing life expectancy and decreasing birth rates. A large proportion of the European society will be not only from the group of people over 65, but also from a significant increase in the number of people over 80. The proportion of population aged over 65 and over is rising in all countries, however differences can be observed. It is also reported that “the ratio for Iceland, Ireland, Slovak Republic and Turkey lie well below the average for Europe, whereas the ratio for Finland, Germany, Greece, Italy and Sweden lie far above the average for Europe” [8].

The $SD_j$s in smart homes communicate over the insecure communication channels. There might be the possibility of various attacks in a smart home network. An illegal user (attacker), who can monitor the activities in a smart home, can break the security, and also can gain access over the $SD_j$s and other smart home appliances. For example, the attacker can watch the activities in the home by accessing the surveillance camera illegally where disabled people live in the smart home. Most of the existing authentication schemes reported in the literature in a smart home environment are not secure against various known attacks, such as smart device capture attack, user, gateway node and smart device impersonation attacks, and privileged-insider attack. Most of those schemes also fail to preserve traceability and anonymity properties of the users, the GWN as well as of the smart devices $SD_j$s. Moreover, using the smart phone stolen attack, it is possible that an adversary $A$ can capture a user’s secret credentials, such as identity, password and biometrics key with the help of the extracted information stored in the smart phone. In addition, with the help of the user, gateway node and smart device impersonation attacks, $A$ can create valid messages on the behalf of a user $U_i$, GWN and smart device $SD_j$, respectively, and can send the corresponding messages to $U_i$, GWN and $SD_j$ so that these messages are treated as valid by $U_i$, GWN and $SD_j$, respectively. In a privileged-insider attack, an insider user of the RA can act as an adversary. The privileged-insider of the RA being an adversary can use the registration information of the users sent to the RA by a legal $U_i$ during the registration phase and derive user’s secret credentials, such as identity, password and biometrics key. However, the GWN registration is usually performed in offline mode securely by the RA, and hence, an adversary can not compromise the sensitive information stored in the tamper-resistant GWN device. Considering various possible attacks in a smart home environment, there is a great need to design a secure remote user authentication scheme suitable for a smart home network so that only authorized users can access the information collected by the deployed $SD_j$s.

### 1.3 Threat Model

- We have used the Dolev-Yao threat model [9] in our scheme. According to this model, any two communicating parties communicate over an insecure channel and the end-point entities such as $U_i$ and $SD_j$ are not considered as trusted entities. An adversary, say $A$, can eavesdrop the exchanged messages, and also can modify or delete the message contents during transmission.

- It is assumed that an adversary can physically capture some smart devices equipped at the smart home which are not tamper-resistant, and can extract all the sensitive data stored in those devices.

- As in [5], we also assume that the GWN is fully trusted and can not be compromised by an adversary. Otherwise, the whole network is compromised if the GWN is compromised. For this purpose, as in Bertino et al.’s scheme [10], we also assume that the GWN is equipped with the tamper-resistant device so that all the sensitive information including the cryptographic keying materials stored in it is protected from $A$. Hence, the use of a tamper-resistant GWN makes the security of the proposed scheme is strong enough. Though the attacks on tamper-resistant devices are possible, the attacker $A$ needs a special equipment to perform attacks to extract the information. Since it is cheaper to install the GWN than the special equipment, so $A$ does not have economic incentives to mount such an attack [10]. Moreover, the GWN can be physically secured by putting it under a locking system inside the smart home of a user so that the physical capture of the GWN can be much difficult as compared to that for the smart devices.

- The RA is also fully trusted and can not be compromised by an adversary.
1.4 Contributions

Based upon the above discussion, the following contributions are presented in this paper:

- We propose a new remote user authentication scheme for securing a smart home network. The proposed scheme allows three types of mutual authentications: 1) between a user \( U_i \) and the GW \( N \), 2) between the GW \( N \) and a smart device \( SD_j \), and 3) a user \( U_i \) and a smart device \( SD_j \). At the end, a symmetric session key is established between \( U_i \) and \( SD_j \), and they can use the established symmetric key for their future secure communications using a symmetric cipher (for example, the stateless CBC (Cipher Block Chaining) mode of the Advanced Encryption Standard (AES-128), known as AES-CBC [11], [12], [13]).

- The proposed scheme is suitable and efficient for resource-constrained \( SD_j \)s with limited resources as it uses only hash invocations, simple bitwise XOR operations and symmetric encryption/decryption operations.

- The security of the proposed scheme is proved using the formal security analysis under the widely-accepted ROR model [14], and also using the rigorous informal security analysis. The formal security discussed in Section 5.1 proves the semantic security of the proposed scheme against an adversary to get the session key between a user and a smart device in the smart home environment. On the other hand, using the informal security analysis, we have shown that the proposed scheme is secure against other possible known attacks, which are discussed in detail in Section 5.3.

- The formal security verification of the proposed scheme in Section 5.2 is done using the broadly-used AVISPA tool [15] and the simulation results show that it is also secure against replay and man-in-the-middle attacks.

- Finally, the practical demonstration of the proposed scheme is provided through the widely-accepted NS-2 simulation [16].

1.5 Roadmap of the Paper

The rest of the paper is structured as follows. We briefly discuss the relevant mathematical preliminaries in Section 2. A brief survey of various existing schemes proposed in the literature is given in Section 3. A new user authentication and session key agreement scheme for smart home environment is presented in Section 4. The rigorous formal and informal security analysis are given in Section 5. In addition, the formal security verification using the popular AVISPA tool is also given in this section. The practical demonstration of the proposed scheme using widely-accepted NS-2 simulation is given in Section 6. The performance comparison with the existing relevant schemes is given in Section 7. Finally, Section 8 concludes the article.

2 Mathematical Preliminaries

In this section, we briefly discuss the one-way cryptographic hash function and its properties, and also the indistinguishability of encryption under chosen plaintext attack (IND-CPA), which are necessary to analyze the security of the proposed scheme.

2.1 One-way Cryptographic Hash Function

A one-way cryptographic hash function \( h : \{0, 1\}^* \rightarrow \{0, 1\}^l \) takes an arbitrary-length input, say \( x \in \{0, 1\}^* \), and outputs a fixed-length (say, \( l \)-bits) message digest \( h(x) \in \{0, 1\}^l \).

Definition 1. As defined in [17], the formalization of an adversary \( \mathcal{A} \)’s advantage in finding hash collision is given by \( \text{Adv}^\text{SHA}_\mathcal{A}(t) = \Pr[(a, b) \leftarrow \mathcal{A} : a \neq b \text{ and } h(a) = h(b)] \), where \( \Pr[X] \) denotes the probability of an event \( X \), and \( (a, b) \leftarrow \mathcal{A} \) denotes the pair \((a, b)\) is randomly selected by \( \mathcal{A} \). In this case, \( \mathcal{A} \) is allowed to be probabilistic and the probability in the advantage is computed over the random choices made by \( \mathcal{A} \) with the execution time \( t \). By an \((\epsilon, t)\)-adversary \( \mathcal{A} \) attacking the collision resistance of \( h(\cdot) \), it is meant that the runtime of \( \mathcal{A} \) is at most \( t \) and that \( \text{Adv}^\text{SHA}_\mathcal{A}(t) \leq \epsilon \).

2.2 Indistinguishability of Encryption Under Chosen Plaintext Attack

The indistinguishability of encryption under chosen plaintext attack (IND-CPA) is formally defined as follows [18], [19]:

Definition 2. Let \( SE/ME \) be the single/multiple eavesdropper respectively, and \( OR_{e_{k_1}}, OR_{e_{k_2}}, \ldots, OR_{e_{k_N}} \) be \( N \) different independent encryption oracles associated with encryption keys \( e_{k_1}, e_{k_2}, \ldots, e_{k_N} \), respectively. The advantage functions of \( SE \) and \( ME \) are defined, respectively, as \( \text{Adv}^\text{IND-CPA}_{SE}(k) = |2\Pr[SE \leftarrow OR_{e_{k_1}} : (p_0, p_1) \leftarrow R \text{ SE}] - \delta| \), \( \text{Adv}^\text{IND-CPA}_{ME}(k) = |2\Pr[ME \leftarrow OR_{e_{k_1}}, \ldots, OR_{e_{k_N}} : (p_0, p_1) \leftarrow R \text{ ME}] - \delta| \), where \( \delta \) is the probability of the encryption scheme. We call \( \Omega \) is IND-CPA secure in the single (multiple) eavesdropper setting if \( \text{Adv}^\text{IND-CPA}_{SE}(k) \) (respectively, \( \text{Adv}^\text{IND-CPA}_{ME}(k) \)) is negligible (in the security parameter \( k \)) for any probabilistic, polynomial time adversary \( SE/ME \).

A deterministic encryption scheme means the same message, when it is encrypted twice, yields the same ciphertext. Thus, any deterministic encryption scheme is not IND-CPA secure [13]. There are five modes of symmetric encryption: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR). Out of these modes, ECB is not IND-CPA secure [13]. Since the adversary knows the Initialization Vector (IV), CBC is essentially reduced to ECB, and hence, the stateful CBC is IND-CPA insecure [13]. On the other hand, in the stateless CBC, the IV value is chosen at random for each message, and due to this property, the stateless CBC is IND-CPA secure [13]. If the stateless CBC of AES-128 symmetric encryption scheme is used for encryption/decryption purpose, it then becomes IND-CPA secure.

3 Related Work

Jeong et al. [20] presented a one-time password based user authentication scheme using smart card for smart home networks. Their scheme is lightweight as it uses one-way hash function operations. Their scheme does not provide mutual authentication between \( GW/N \) and smart device as well as between user and smart device. Their scheme does not provide traceability, and user anonymity properties as the user identity is sent in plaintext and also the messages can be easily traced by an adversary. Furthermore, their
scheme is insecure against stolen smart card attack and privileged-insider attack as the adversary can derive secret credentials of a user from the extracted information stored in the smart card. In addition, their scheme is not resilient against smart device physical capture attack.

Vaidya et al. [21] proposed a password based remote user authentication scheme for digital home network. Their scheme is also based upon lightweight computation modules such as hashed one-time password and hash-chaining methods. Similar to Jeong et al. [20], their scheme does not provide mutual authentication between GW/N and smart device as well as between user and smart device. Kim and Kim [22] analyzed Vaidya et al.’s scheme [21] and identified that it is vulnerable to password guessing attack and does not provide forward secrecy with lost smart card. They also proposed a new scheme which withstands the security weaknesses observed in Vaidya et al.’s scheme [21]. Vaidya et al.’s scheme [21] scheme is insecure against stolen smart card attack and privileged-insider attack as the adversary can derive secret credentials of a user from the extracted information stored in the smart card. In addition, their scheme is not resilient against smart device physical capture attack. Later, Vaidya et al. [23] also proposed an elliptic curve cryptography (ECC) based authentication technique for smart energy home area network which requires more overheads as compared to the scheme in [21]. Kim-Kim’s scheme [22] is however not resilient against privileged-insider attack, user impersonation attack and password guessing attack. In addition, Kim-Kim’s scheme [22] also fails to preserve traceability and anonymity of user and smart device.

Hanumanthappa et al. [24] proposed a secure three-way authentication mechanism for user authentication and privacy preservation. In their mechanism, the users or service providers can check whether the device is compromised or not by the help of their proposed encrypted pass-phrases mechanism.

Santoso and Vun [25] proposed ECC based user authentication scheme for a smart home system. In their scheme, the mobile user can authenticate with the devices deployed in the smart home using a central node, called the home gateway. Similar to the schemes of Jeong et al. [20], Vaidya et al. [21], and Kim and Kim [22], their scheme does not provide traceability, and user anonymity properties. Furthermore, their scheme is insecure against stolen smart card attack and privileged-insider attack. In addition, their scheme is not resilient against smart device physical capture attack.

Chang and Le [26] recently proposed a two-factor user authentication scheme in wireless sensor networks (WSNs), which uses a user’s password and smart card. Their scheme has two protocols: P1 and P2. While P1 is based on bitwise XOR and hash functions, P2 uses ECC along with bitwise XOR and hash functions. However, Das et al. [27] proved that both P1 and P2 are insecure against session specific temporary information attack and offline password guessing attack, while P1 is also insecure against session key breach attack. Moreover, they pointed out that both P1 and P2 are inefficient in authentication and password change phases. To erase the security limitations in P1 and P2, a new authentication and key agreement scheme using ECC in WSNs is presented [27].

Kumar et al. [28] presented a lightweight and secure session key establishment scheme for smart home network. To establish the mutual trust, each smart device control unit establishes a session key with the GW/N by using a short authentication token. However, their scheme does not preserve the GW/N anonymity and also the traceability properties. In addition, their scheme does not provide mutual authentication between user and smart device as well as between user and the GW/N.

Li et al. [29] proposed an ECC based key establishment scheme for smart home energy management systems. Through the implementation, it is shown that their scheme is efficient with respect to execution time and memory usage. Han et al. [29] presented a secure key agreement scheme for ubiquitous smart home systems, which is particularly applicable to the consumer electronics devices in a smart home. The security and functionality features of the existing schemes summarized in Table 4 are also discussed in detail in Section 7.

### TABLE 1 Notations used

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA</td>
<td>Registration authority</td>
</tr>
<tr>
<td>GW/N</td>
<td>Gateway node</td>
</tr>
<tr>
<td>SD/j</td>
<td>jth smart device in the home</td>
</tr>
<tr>
<td>U/i</td>
<td>ith user</td>
</tr>
<tr>
<td>SP/i</td>
<td>ith user’s smart phone</td>
</tr>
<tr>
<td>1D/i</td>
<td>ith user’s identity</td>
</tr>
<tr>
<td>1D_SD/j</td>
<td>SD/j’s identity</td>
</tr>
<tr>
<td>PW/UI, BIO/i</td>
<td>U/i’s password &amp; personal biometrics, respectively</td>
</tr>
<tr>
<td>Tt</td>
<td>Current timestamp</td>
</tr>
<tr>
<td>ΔT</td>
<td>Maximum transmission delay</td>
</tr>
<tr>
<td>KGW/N−U/i</td>
<td>Secret key of GW/N for U/i</td>
</tr>
<tr>
<td>KGW/N−SD/j</td>
<td>Secret key of GW/N for SD/j</td>
</tr>
<tr>
<td>EK(·)/D_K(·)</td>
<td>Symmetric encryption/decryption (for example, AES-CBC (128 bits) [12] using key K</td>
</tr>
<tr>
<td>ρi</td>
<td>Biometric secret key of Ui</td>
</tr>
<tr>
<td>τi</td>
<td>Public reproduction parameter of Ui</td>
</tr>
<tr>
<td>t</td>
<td>Error tolerance threshold used in fuzzy extractor</td>
</tr>
<tr>
<td>Gen</td>
<td>Fuzzy extractor probabilistic generation procedure</td>
</tr>
<tr>
<td>Rep</td>
<td>Fuzzy extractor deterministic reproduction procedure</td>
</tr>
<tr>
<td>h(·)</td>
<td>One-way collision-resistant cryptographic hash function</td>
</tr>
<tr>
<td>[l, r]</td>
<td>Concatenation and bitwise XOR operations, respectively</td>
</tr>
</tbody>
</table>

## 4 The Proposed Scheme

We propose a new user authenticated key establishment scheme for the smart home environment. In the proposed scheme, we have a registration authority, several smart sensing devices, a gateway node (GW/N) and several users, who want to access the smart devices. First of all, the secure offline registration of each smart device and GW/N is done at the registration authority (RA). Then a user, who wants to access the smart devices, needs to register at the registration authority providing his/her necessary information. Each user has a smart phone, which is capable to read the credential information such as the user’s identity, password and biometric (fingerprint scanning etc.) provided by that user. The GW/N acts as an intermediary node. The legal user’s authentication request goes to the GW/N and then the GW/N forwards the request to the requested smart device. The smart device sends response to the GW/N accordingly and then the GW/N forwards the response to the user. As discussed in the threat model provided in Section 4.3, the GW/N is fully trusted and all the sensitive informations stored in the GW/N are protected from an adversary [5]. Moreover, we assume that all the heterogeneous devices (i.e., GW/N, users (smart phones) and smart devices) are synchronized with their clocks, and agree (mutually) on a maximum transmission delay (ΔT) to protect replay attacks in the proposed scheme [5].
Our scheme has six phases: 1) offline smart device and gateway registration, 2) user registration, 3) login, 4) authentication and agreement, 5) biometric and password update, and 6) dynamic smart device addition. The notations presented in Table 1 are used in the proposed scheme. We assume that there are m users and n smart devices in the smart home environment. In addition, we assume that n’ additional smart devices can be added into the network through the dynamic smart device addition phase, where n’ << n. We also use the fuzzy extractor to verify the biometrics. The fuzzy extractor is a tuple \( \langle M, l, t \rangle \), which is composed of the following two algorithms [30], [31].

**Gen:** It is a probabilistic algorithm, which takes a biometric template \( B_i \) from a given metric space \( M \) as input, and then outputs a biometric metric \( \sigma_i \in \{0,1\}^l \) and a public reproduction parameter \( \tau_i \), that is, \( Gen(B_i) = (\sigma_i, \tau_i) \), where \( l \) denotes the number of bits present in \( \sigma_i \).

**Rep:** This is a deterministic algorithm, which takes a noisy biometric template \( B_i' \in M \) and a public parameter \( \tau_i \) and \( t \) related to \( B_i \), and then it produces (recovered) the biometric key \( \sigma_i \). In other words, \( Rep(B_i', \tau_i) = \sigma_i \) provided that the Hamming distance between \( B_i \) and \( B_i' \) is less than or equal to a predefined error tolerance threshold value \( t \).

### 4.1 Offline Smart Device and Gateway Registration Phase

The offline smart device (\( SD_j \)) and GWN registration is done by the registration authority (\( RA \)) in offline secure (for example, in person). For each \( SD_j \) (\( j = 1, 2, \ldots, n \)), the RA selects a unique identity \( ID_{SD_j} \) and also generates a unique random 1024-bit secret key \( K_{GWN-SD_j} \) of GWN for \( SD_j \), and computes the corresponding temporal credential \( h(ID_{SD_j}, K_{GWN-SD_j}) \) and stores \( \{ID_{SD_j}, h(ID_{SD_j}, K_{GWN-SD_j})\} \) in the memory of \( SD_j \). The RA further randomly generates the unique GWN’s identity \( ID_{GWN} \) and a unique random 1024-bit secret key \( K_{GWN-U_i} \) of GWN for each user \( U_i \) (\( i = 1, 2, \ldots, m \)), and also selects the temporary identity \( TID_i \) corresponding to each user \( U_i \)’s identity \( ID_i \) into the memory of the GWN after \( U_i \)’s successful registration phase described in Section 4.2. Finally, the GWN and \( SD_j \) contain the information \( \{\{TID_i, ID_i, K_{GWN-U_i}\}|i = 1, 2, \ldots, m\}; \{\{ID_{SD_j}, K_{GWN-SD_j}\}|j = 1, 2, \ldots, n\} \), and \( \{ID_{SD_j}, h(ID_{SD_j}, K_{GWN-SD_j})\} \) for each user \( U_i \) and smart device \( SD_j \), respectively.

### 4.2 User Registration Phase

To access the services from a particular smart device \( SD_j \), a user \( U_i \) first needs to register with the \( RA \) securely (for example, in person). The following steps are required for the \( U_i \)’s registration, which are also summarized in Fig. 2.

**Step REG1.** \( U_i \) chooses a unique identity \( ID_i \), and a password \( PW_i \), and generates 160-bit random secrets \( a \) and \( r \) \( U_i \) also imprints his/her biometrics \( BIO_i \) to the sensor of \( SP_i \). The \( SP_i \) applies the fuzzy extractor probabilistic generation function \( Gen(\cdot) \) to generate secret biometric key \( \sigma_i \) and public parameter \( \tau_i \) as \( Gen(\cdot) = (\sigma_i, \tau_i) \) [31], [32], [33]. The \( SP_i \) of \( U_i \) calculates the masked password \( RPW_i = h(PW_i, |\sigma_i|, a) \oplus r \), and sends the registration request \( \langle TID_i, RPW_i \rangle \) to the RA using a secure channel. Note that a privileged-insider user of the RA being an adversary knows the registration information \( \{ID_i, RPW_i\} \) to mount the privileged-insider attack.

**Step REG2.** After receiving \( \langle ID_i, RPW_i \rangle \) from \( SP_i \), the RA first generates a 1024-bit secret key \( K_{GWN-U_i} \) of GWN for \( U_i \), and calculates \( A_i = h(ID_i, |K_{GWN-U_i}|) \oplus RPW_i \). RA also generates a temporary identity \( TID_i \) corresponding to \( ID_i \) for \( U_i \) as discussed in the GWN registration phase (Section 4.2). Finally, \( RA \) sends the registration reply with information \( \{A_i, TID_i\} \) to \( U_i \) securely. Note that the privileged-insider user of the RA being an adversary does not know the information \( \{A_i, TID_i\} \) as these information are computed online by the RA.

**Step REG3.** After receiving \( \langle A_i, TID_i \rangle \) from the RA, \( SP_i \) of \( U_i \) computes base points \( B_1 = h(ID_i)|\sigma_i| \oplus a, RPW_i = h(PW_i, |\sigma_i|, a) \), and \( A_2 = A_i \oplus h(ID_i, |K_{GWN-U_i}|) \oplus RPW_i = h(ID_i, K_{GWN-U_i}) \oplus h(PW_i, |\sigma_i|, a) \). Finally, \( SP_i \) stores the information \( \{TID_i, A_1, B_1, C_i, \tau_i, h(\cdot), Gen(\cdot), Rep(\cdot), t\} \) in its memory, where \( t \) is the error tolerance parameter used by the fuzzy extractor \( Rep(\cdot) \) function.

At the end of this phase, the user \( U_i \) erases \( A_1 \) from his/her smart phone \( SP_i \) in order to avoid the privileged-insider attack as explained in Section 5.3.3. In addition, the RA also deletes \( A_1 \) and \( RPW_i \) from its database.

![Fig. 2. User registration phase](image-url)

### 4.3 Login Phase

The login process of \( U_i \) is performed as per the following steps:

**Step UL1.** \( U_i \) first provides his/her identity \( ID_i \) and password \( PW_i^* \) into the interface of the smart phone \( SP_i \), and also provides his/her biometrics \( BIO_i^* \) to the sensor of \( SP_i \). \( SP_i \) extracts the biometric key \( \sigma_i^* \) as \( \sigma_i^* = Rep(BIO_i^*, \tau_i) \) with the constraint that the Hamming distance between the original biometrics \( BIO_i \) at the time of registration and entered current \( BIO_i^* \) is less than or equal to \( t \). \( SP_i \) further computes \( a^* = B_1 \oplus h(ID_i, |\sigma_i^*|) \), \( RPW_i^* = h(PW_i^*, |\sigma_i^*|, a^*) \), and \( C_i^* = h(ID_i, |RPW_i^*|, |\sigma_i^*|) \). \( SP_i \) then checks whether \( C_i^* = C_i \). If it is valid, \( U_i \) passes both password and biometric verification. Otherwise, the session is terminated immediately.

**Step UL2.** \( SP_i \) calculates \( M_1 = A_1^* \oplus RPW_i^* = h(ID_i, |K_{GWN-U_i}|) \). Then \( SP_i \) generates a random nonce \( r_{U_i} \), and the current timestamp \( T_1 \), and calculates parameters \( M_2 = M_1 \oplus r_{U_i} \), and \( M_3 = h(M_2|T_1|) \oplus TID_i \oplus r_{U_i} \). Finally, \( SP_i \) sends the login request message \( \langle TID_i, M_2, M_3, T_1 \rangle \) to GWN via an open channel.

### 4.4 Authentication and Key agreement Phase

On receiving the login request \( \langle TID_i, M_2, M_3, T_1 \rangle \) from \( SP_i \), following steps are performed by \( U_i / SP_i, GWN \) and an accessed...
Fig. 3. Summary of login, and authentication and key agreement phases

smart device $SD_j$ to establish a session key between $U_i$ and $SD_j$ for later secure communication:

**Step AUKA1.** GW $N$ first checks the timeline of $T_1$ by condition $|T_1 - T_1^*| \leq \Delta T$, where the maximum transmission delay is denoted by $\Delta T$ and $T_1^*$ is the reception time of the message $(TID_1, M_2, M_3, T_1)$. If the condition matches, the GW $N$ searches the received $TID_1$ in its database and if it is found in the database, the GW $N$ extracts $ID_1$ and $K_{GW\text{--}U_i}$ corresponding to $TID_1$ from its database, and calculates $M_4 = h(ID)|K_{GW\text{--}U_i}| = M_1$ using the extracted $ID_1$ and $K_{GW\text{--}U_i}$, $r_{SD_i} = M_2 \oplus M_4 = M_2 \oplus M_1$, $M_5 = h(M_2||T_1)||ID_1||TID_1||T_1^*$. 

**Step AUKA2.** GW $N$ checks if $M_5 = M_3 \oplus M_2$ holds. If it does not match, it terminates the authentication process. Otherwise GW $N$ generates a random nonce $r_{GW\text{--}N}$ and timestamp $T_2$, and calculates parameters $M_6 = h(|ID_2||K_{GW\text{--}N\text{--}SD_i}|)$, $M_7 = E_{M_6}(ID_2, ID_{GW\text{--}N}, r_{GW\text{--}N}, h(M_4))$, $M_8 = h(ID_2||T_2)||ID_2||ID_{GW\text{--}N}||r_{GW\text{--}N}$. For computing $M_7$, if we use the stateless CBC of AES-128 (AES-CBC) symmetric encryption scheme, then the GW $N$ needs to set the IV of CBC as $IV = h(M_6||T_2)$ so that it is random for each message in a particular session. Then $GW\text{--}N$ sends the authentication request message $(M_7, M_8, T_2)$ to $SD_j$ via an open channel.

**Step AUKA3.** After receiving the message $(M_7, M_8, T_2)$ from $GW\text{--}N$, $SD_j$ checks the timelines of $T_2$ by the criteria $|T_2 - T_2^*| \leq \Delta T$, where $T_2^*$ is the reception time of the message $(M_7, M_8, T_2)$. If condition holds, $SD_j$ decrypts $M_7$ using the stored key $h(ID_2||K_{GW\text{--}N\text{--}SD_i})$ as $(ID_2, ID_{GW\text{--}N}, r_{GW\text{--}N}, h(M_3)) = D_{h(ID_2||K_{GW\text{--}N\text{--}SD_i}}[M_7]$. For decrypting $M_7$, $SD_j$ also needs to set the IV of CBC as $IV = h(ID_2||K_{GW\text{--}N\text{--}SD_i})|T_2| = h(M_4||T_2)$.

**Step AUKA4.** $SD_j$ calculates $M_9 = h(ID_2||K_{GW\text{--}N\text{--}SD_i})|T_2| ||ID_2||ID_{GW\text{--}N}||r_{GW\text{--}N}$ and checks the condition $M_9 = M_8$. If it does not match, it terminates the authentication process. Otherwise, $SD_j$ generates a random nonce $r_{SD_j}$ and the current timestamp $T_3$, and computes the session key as $SK_{ij} = h(ID_2||ID_{SD_j}||ID_{GW\text{--}N}||r_{SD_j}||r_{GW\text{--}N}|r_{SD_j}||h(M_4)||h(ID_2||K_{GW\text{--}N\text{--}SD_i})|T_3|)$. After that, $SD_j$ computes parameters $M_{10} = h(ID_2||K_{GW\text{--}N\text{--}SD_i})|T_3| \oplus r_{SD_j}$, $M_{11} = h(SK_{ij}|T_3)$ and $M_{12} = h(ID_2||ID_{GW\text{--}N}||r_{GW\text{--}N}|r_{SD_j}||ID_{SD_j}||ID_{GW\text{--}N}||T_3)$. Then $SD_j$ sends the authentication reply message $(M_{10}, M_{11}, M_{12}, T_3)$ to the GW $N$ via an insecure channel.

**Step AUKA5.** Upon receiving authentication request message, GW $N$ checks the timelines of $T_3$ by applying the criteria $|T_3 - T_3^*| \leq \Delta T$, where $T_3^*$ is the reception time of the message $(M_{10}, M_{11}, M_{12}, T_3)$. If condition matches, GW $N$ computes $r_{SD_j} = M_{10} \oplus h(ID_2||ID_{GW\text{--}N\text{--}SD_i})|T_3|$ and $M_{13} = h(ID_2||ID_{GW\text{--}N}||ID_{SD_j}||T_3)$. The GW $N$ checks the condition $M_{13} = M_{12}$. If it does not match, the GW $N$ aborts the message. Otherwise, GW $N$ computes $M_{14}$ using previously computed $M_4 = h(ID_2||K_{GW\text{--}N\text{--}U_i})$ as $M_{14} = E_{M_6}(r_{GW\text{--}N}, r_{SD_j}, ID_{GW\text{--}N}, h(M_6))$. For encrypting the information in $M_{14}$ using the key $M_6$, we also use the stateless CBC of AES-128 (AES-CBC) symmetric encryption scheme and thus, the GW $N$ needs to set the IV of CBC as $IV = h(M_4||T_3)$ so that it is random for each message in a particular session. The GW $N$ chooses current timestamp $T_4$ and generates a new temporary identity $TID_{new}^\text{GW\text{--}N}$ corresponding to $ID_2$. The GW $N$ further computes $M_{15} = TID_{new}^\text{GW\text{--}N} \oplus (h(TID_1||M_4||T_3||T_4)$
and $M_{16} = h(M_{11} || T_4 || \tau_i^4)$. The GWN sends the message $(M_{14}, M_{15}, M_{16}, T_3, T_4)$ to $U_i$ via insecure channel.

**Step AUKA6.** After receiving the message $(M_{14}, M_{15}, M_{16}, T_3, T_4)$, $SP_i$ of $U_i$ first checks the timeliness of $T_4$ with the condition $|T_3 - T_4| \leq \Delta T$, where $T_4$ is the reception time of the message. If condition matches, $U_i$ decrypts $M_{14}$ using precomputed $M_1$ as $D_{M_1} [M_{14}] = (r_i^U, r_i^{GW\text{N}}, r_i^{SD_j}, ID_{SD_j}, ID_{GW\text{N}}, h(M_6))$. For decrypting $M_{14}$, $SD_j$ also needs to set the IV of CBC as $IV = h(M_1[T_4]) (= h(M_4[T_4]))$.

Then $SP_i$ checks if $r_i^U = r_i^U$. If they do not match, $SP_i$ terminates the authentication process. Otherwise, it computes the session key $SK_i = h(ID_j || ID_{SD_j} || ID_{GW\text{N}} || T_4 || T_4)$. Then it checks the condition $C_{i,j}^{\text{new}} = C_i$. If they do not match, $SP_i$ terminates the session and discards the session key. Otherwise, message comes from the valid source and the computed session key $SK_i$ is authentic. Finally, $SP_i$ computes the new temporary identity as $TI_{i,j}^{\text{new}} = M_{15} \oplus h(TI_{i,j} || M_1 || T_3 || T_4)$ and replaces $TI_{i,j}$ with $TI_{i,j}^{\text{new}}$ in its memory.

The login, authentication and agreement phases are summarized in Fig. 5.

**4.5 Password and Biometric Update Phase**

The proposed scheme provides password and biometric update facility through which a legitimate user $U_i$ can update his/her password and biometrics for security reasons at any time after user registration phase without further involving the RA. Note that the biometric information of a given user $U_i$ is unique and unchanged as compared to the chosen password by that user $U_i$. However, we suggest the user $U_i$ to update his/her biometric information in the proposed scheme, if he/she desires to do so. This is required to protect strongly the offline password guessing attack to be considered in this phase as described by Huang et al. [14], which is discussed in detail in Section 5.3.11. This phase needs the following steps:

**Step PBU1.** $U_i$ provides his/her identity $ID_i$, old password $PW_{\text{old}}$ to interface of the $SP_i$, and current his/her biometrics $BIO_{\text{old}}$ to the sensor of the $SP_i$. $SP_i$ then computes $\sigma_{i,j}^{\text{old}} = \text{Rep}(BIO_{\text{old}}, \tau_i)$, $a'_i = B_i \oplus h(ID_i || \sigma_{i,j}^{\text{old}})$, $RPW_{\text{old}} = h(PW_{\text{old}} || \sigma_{i,j}^{\text{old}} || a'_i)$ and $C_{i,j}^{\text{old}} = h(ID_j || RPW_{\text{old}} || \sigma_{i,j}^{\text{old}})$. $SP_i$ checks the condition $C_{i,j}^{\text{old}} = C_i$. If it matches, $U_i$ is the actual user; otherwise, the phase is terminated immediately.

**Step PBU2.** $SP_i$ asks $U_i$ to enter a new password $PW_{\text{new}}$ and also imprint new biometrics $BIO_{\text{new}}$. The $SP_i$ then calculates $\text{Gen}(BIO_{\text{new}}) = (\sigma_{i,j}^{\text{new}}, \tau_i^{\text{new}})$, $RPW_{\text{new}} = h(PW_{\text{new}} || \sigma_{i,j}^{\text{new}} || a'_i)$, $B_{\text{new}} = h(ID_i || \sigma_{i,j}^{\text{new}} || \tau_i^{\text{new}})$, $C_{\text{new}} = h(ID_i || RPW_{\text{new}} || \sigma_{i,j}^{\text{new}})$ and $A_{\text{new}} = A_i \oplus RPW_{\text{old}} || RPW_{\text{new}}$, $h(ID_j || KG_{GW\text{N} - U_i}) \oplus RPW_{\text{new}} = h(ID_j || KG_{GW\text{N} - U_i}).$

Finally, $SP_i$ replaces $\tau_i, A_i, B_i, C_i$ with $\tau_i^{\text{new}}, A_{\text{new}}, B_{\text{new}}$ and $C_{\text{new}}$ in its memory, respectively.

The password and biometric update phase is also summarized in Fig. 4.

**4.6 Dynamic Smart Device Addition Phase**

To deploy a new smart device $SD_j^{\text{new}}$ in the existing smart home network, the RA performs the following steps offline:

**Step DA1.** RA first assigns a unique new identity $ID_{SD_j}^{\text{new}}$ and also generates a new secret key $KG_{GW\text{N} - SD_j^{\text{new}}}$ of GWN for $SD_j^{\text{new}}$. RA further computes the temporal credential of $SD_j^{\text{new}}$ as $h(ID_{SD_j^{\text{new}}} || KG_{GW\text{N} - SD_j^{\text{new}}})$.

**Step DA2.** RA stores the information $\{ID_{SD_j^{\text{new}}}, h(ID_{SD_j^{\text{new}}} || KG_{GW\text{N} - SD_j^{\text{new}}})\}$ into the memory of $SD_j$ before its deployment in the smart home. RA also sends the information $\{ID_{SD_j^{\text{new}}}, KG_{GW\text{N} - SD_j^{\text{new}}}\}$ to the GWN securely, which are then stored in the database of the GWN.

Finally, RA also needs to inform the existing users in the network about the deployment of the new smart device $SD_j^{\text{new}}$ so that they can access the services from $SD_j^{\text{new}}$, if needed.

**5 Security Analysis**

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

**5.1 Formal Security Analysis using Real-Or-Random Model**

The widely-accepted Real-Or-Random (ROR) model [14] is used for formal security analysis of the proposed scheme.

**5.1.1 ROR Model**

We follow the Abdalla et al.’s ROR model [14] for formal security analysis as done in [25]. Under our scheme, we have three participants in the smart home: smart device $SD_j$, user $U_i$ and GWN.

**Participants.** Let $\Pi_1^{SD_j}, \Pi_2^{SD_j}$ and $\Pi_3^{GW\text{N}}$ be the instances $t$, $u$ and $v$ of $SD_j$, $U_i$ and GWN, respectively. These are called oracles [25].

**Accepted state.** An instance $\Pi^t$ is known to be accepted, if upon receiving the last expected protocol message, it goes into an accept state. The ordered concatenation of all communicated (sent and received) messages by $\Pi^t$ forms the session identification (sid) of $\Pi^t$ for the current session.

**Partnering.** Two instances $\Pi^t$ and $\Pi^u$ are said to be partnered if the following three conditions are fulfilled simultaneously: 1) both $\Pi^t$ and $\Pi^u$ are in accept state; 2) both $\Pi^t$ and $\Pi^u$ mutually authenticate each other and share the same sid; and 3) $\Pi^t$ and $\Pi^u$ are mutual partners of each other.

**Freshness.** The instance $\Pi_3^{GW\text{N}}$ or $\Pi_1^{SD_j}$ is fresh, if the session key $SK_{ij}$ between $U_i$ and $SD_j$ has not revealed to an adversary $A$ using a Reveal($\Pi^t$) query given below [25].

**Adversary.** It is assumed that $A$ has full control over all the
communications in a smart home. $A$ has the ability to read, modify the exchanged messages, or can fabricate new messages and inject them into the network. Furthermore, $A$ has access to the following queries [25].

Execute($\Pi_1^b, \Pi_1^b, \Pi_1^b$): $A$ can execute this query to obtain the messages exchanged between three legitimate participants $U_1$, $GW$ and $SD_j$, which is further modeled as an eavesdropping attack.

Reveal($\Pi_1^b$): This query reveals the current session key $SK_{ij}$ generated by $\Pi_1^b$ (and its partner) to an adversary $A$.

Send($\Pi_1^b, msg$): $A$ runs this query to send a message, say $msg$, to a participant instance $\Pi_1^b$, and also receives a response message. It is modeled as an active attack.

CorruptSmartPhone($\Pi_1^b$): It represents the smart phone $SP_i$ lost/stolen attack, which outputs the information stored in $SP_i$.

CorruptSmartDevice($\Pi_1^{SD}$): This represents an attack in which secret $h(ID_{SD}||K_{GW-N-SD})$ is disclosed to $A$, which is applied to verify the security of the proposed scheme. As mentioned in [26], both CorruptSmartPhone and CorruptSmartDevice queries ensure the weak-corrupption model in which temporary keys and the internal data of the participant instances are not corrupted.

Test($\Pi_1^b$): It represents the semantic security of a session key $SK_{ij}$ between $U_i$ and $SD_j$ following the indistinguishability in the ROR model [13]. An unbiased coin $b$ is flipped before start of the experiment, and its result is only known to $A$ which is used to decide the output of the Test query. If $A$ runs this query, and the established session key $SK_{ij}$ is also new, then $\Pi_1^b$ returns $SK_{ij}$ in case $b=1$ or a random number for $b=0$; otherwise, it outputs ⊥ (null).

Note that we impose a restriction that the adversary $A$ has access to only limited number of CorruptSmartPhone($\Pi_1^b$) and CorruptSmartDevice($\Pi_1^{SD}$) queries, whereas he/she can access the Test($\Pi_1^b$) query many times. According to the threat model described in Section [13], the $GW/N$ is trusted. Thus, $A$ does not have any access to a corrupt query related to the $GW/N$.

Semantic security of session key. According to the requirements of the ROR model [13], $A$ needs to distinguish between an instance’s real session key and a random key. $A$ can make several Test queries to either $\Pi_1^{SD}$, or $\Pi_1^b$. The output of Test query should be consistent with respect to the random bit $b$. After the experiment is finished, $A$ returns a guessed bit $b'$ and he/she can win the game if the condition $b'=b$ is met. Let $SUCC$ be an event that $A$ wins the game. The advantage $Adv_{b'}^{AKE}$ of $A$ in breaking the semantic security of our authenticated key agreement (AKE) scheme, say $\mathcal{P}$ against deriving the session key $SK_{ij}$ between $U_i$ and $SD_j$ is given by $Adv_{b'}^{AKE} = [2Pr[SUCC] - 1]$. In the ROR sense, $A$ is secure if $Adv_{b'}^{AKE} \leq \psi$, where $\psi > 0$ is a sufficiently small real number.

Random oracle. As mentioned in [26], all communicating participants as well as $A$ have access to a collision-resistant one-way cryptographic hash function $h(\cdot)$. $h(\cdot)$ is modeled by a random oracle, say $HO$.

5.1.2 Security Proof

Theorem 1 provides the semantic security of our proposed scheme under the widely-accepted ROR model [26], [35].

Theorem 1. Let $A$ be an adversary running in polynomial time $t$ against our scheme $\mathcal{P}$ in the random oracle, $D$ a uniformly distributed password dictionary and $l$ the number of bits present in the biometrics key $\sigma_1$. The advantage of $A$ in breaking semantic security of our scheme is estimated as $Adv_{b'}^{AKE} \leq \frac{q_{send}^2}{|Hash|} + \frac{q_{send}}{|D|} + 2Adv_{\Pi_1^{SD}}^{IND-CPA}(k)$, where $q_{send}$, $q_{send}$, $|Hash|$, $|D|$ and $Adv_{\Pi_1^{SD}}^{IND-CPA}(k)$ or $Adv_{\Pi_1^{SD}}^{IND-CPSA}(k)$ are the number of HO queries, the Send queries, the range space of $h(\cdot)$, the size of $D$, and the advantage of $A$ in breaking the IND-CPA secure symmetric cipher $\Omega$ (provided in Definition 2), respectively, and $Adv_{\Pi_1^{SD}}^{IND-CPA}(k) = Adv_{\Pi_1^{SD}}^{IND-CPSA}(k)$.

Proof. The proof is similar to that presented in the schemes [26], [35]. The sequence of five games, say $GM_i$, are defined in the security analysis, where $i = 0, 1, 2, 3, 4$. Assume that $SUCC_i$ be an event wherein an adversary $A$ can guess the random bit $b$ in $GM_i$ correctly.

$GM_0$: This game corresponds to a real attack performed by $A$ against our scheme $\mathcal{P}$ in the ROR sense. The bit $b$ is chosen at the beginning of $GM_0$. Hence, it follows that

$$Adv_{b'}^{AKE} = |2Pr[SUCC_0] - 1|.$$ (1)

$GM_1$: This game represents an eavesdropping attack performed by the single/multiple eavesdropper $SE/ME$, say $A$, where $A$ can query Execute($\Pi_1^b, \Pi_1^b, \Pi_1^b$) oracle. At the end of the game, $A$ makes queries to the $Test$ oracle. The output of $Test$ oracle determines whether it is the actual session key $SK_{ij}$ or a random number. Note that the session key $SK_{ij}$ is calculated by both $U_i$ and $SD_j$ as $SK_{ij} = h(ID_i||ID_{SD}, ||ID_{GW-N}||r_{GW-N}||r_{SD}, ||h(M_i)||h(h(ID_i, ||K_{GW-N-SD})))$, where $M_i = h(ID_i, ||K_{GW-N-SD})$. To calculate $SK_{ij}$, $A$ must have $M_i$ and $h(ID_{SD}, ||K_{GW-N-SD})$, which further involve secret keys $K_{GW-N-SD}$, $K_{GW-N-SD}$, $A$ also requires $ID_i, ID_{SD}, ID_{GW-N}, r_{U_i}, r_{GW-N}$ and $r_{SD}$, for calculating $SK_{ij}$, which are unknown to him/her. As a consequence, the chance of winning the game $GM_1$ for $A$ is not increased by eavesdropping attack. It is then obvious that

$$Pr[SUCC_0] = Pr[SUCC_1].$$ (2)

$GM_2$: By adding the simulations of the $Send$ and $HO$ oracles are added into $GM_1$. $GM_1$ is transformed into $GM_2$, which represents an active attack. In this game, the objective of $A$ is to fool a participant to accept a modified message. $A$ is permitted to make different $HO$ queries to examine the existence of the hash collisions. All the exchanged messages $(TI_1, M_2, M_3, T_1, \langle M_7, M_8, T_2, \rangle, \langle M_{10}, M_{11}, M_{12}, T_3, \rangle)$ and $(\langle M_{14}, M_{15}, M_{16}, T_3, T_4 \rangle)$ during the login and authentication phase contain the participant’s identity, random nonce and timestamps. Hence, there is no collision when the $Send$ oracle is queried by $A$. The results of the birthday paradox give

$$Pr[SUCC_1] - Pr[SUCC_2] \leq \frac{q_{send}^2}{2|\text{Hash}|}.$$ (3)

$GM_3$: $GM_2$ is transformed into $GM_3$ by adding the simulation of CorruptSmartPhone oracle. $A$ can choose low-entropy passwords, and using the information stored into $SP_i$, he/she may try to acquire the user’s password using the dictionary attack. Again, $A$ may try to acquire the biometrics key $\sigma_1$ from the information stored in $SP_i$. We have used a strong fuzzy extractor in our scheme $\mathcal{P}$, which is capable to extract at most $l$ random bits and the guessing probability of $\sigma_1 \in [0, 1]^l$ by $A$ is approximately $\frac{1}{2^l}$ [31]. It is also assumed that the system allows...
the limited number of wrong password inputs. Thus, we have the following result,
\[
|Pr[SuccC2] - Pr[SuccC3]| \leq q_{send}/(2^l|D|). \tag{4}
\]

GM4: GM4 is transformed into GM4e, where GM4e is the last game. It models an attack in which \( \mathcal{A} \) physically capture (compromise) a smart device \( \mathcal{D}_j \) by adding the simulation of CorruptSmartDevice oracle. \( \mathcal{A} \) then knows the information \( \{ID_{SDj}, h(ID_{SDj}) [K_{GW\text{-}N\text{-}SDj}] \} \) which is stored in \( \mathcal{D}_j \).

Let \( \mathcal{A} \) also have all the eavesdropped messages \( \langle ID_i, M_i \rangle \). Decryption by \( \mathcal{A} \) using \( h(ID_{SDj}) [K_{GW\text{-}N\text{-}SDj}] \) as \( h(ID_{SDj}) [K_{GW\text{-}N\text{-}SDj}] \), \( \mathcal{A} \) can not decrypt \( M_i \) as \( M_i \) is unknown to \( \mathcal{A} \) since \( M_i \in E_{M} [r_{SDj}^1, r_{GW\text{-}N}, r_{SDj}^2, ID_{SDj}, ID_{GW\text{-}N}, h(M_0)] \). This implies that without having \( M_0 \) \( \mathcal{A} \) can not decrypt \( M_i \). But, \( \mathcal{A} \) can extract the information including \( r_{SDj} \) and \( M_0 \) due to the IND-CPA secure symmetric cipher used in the proposed scheme for encryption/decryption. This concludes that

\[
|Pr[SuccC2] - Pr[SuccC3]| \leq Adv^{IND\text{-}CPA}_{\mathcal{A}}(k). \tag{5}
\]

In GM4, all the random oracles are simulated. \( \mathcal{A} \) is only left to guess the bit \( b \) for winning the game after querying the Test oracle. It is clear that \( Pr[SuccC4] = 1/2 \).

From Equation (1), we get \( \frac{1}{2} Adv^{AKE}_{\mathcal{A}} = Pr[SuccC4] = 1/2 \).

Using the triangular inequality, we have \( Pr[SuccC1] \leq Pr[SuccC4] \leq Pr[SuccC2] + Pr[SuccC3] \). Using Equations (2) and (3), we have,

\[
Pr[SuccC0] - 1/2 \leq \frac{q_{h^2}^2}{2^l|\text{Hash}|} + \frac{q_{send}^2}{2(|D|)} + Adv^{EC\text{-}DDH}_G(t).
\]

Finally, Equation (1) yields the required result:

\[
Adv^{AKE}_{\mathcal{A}} \leq \frac{q_{h^2}^2}{|\text{Hash}|} + \frac{q_{send}^2}{2^l|D|} + 2 Adv^{IND\text{-}CPA}_{\mathcal{A}}(k). \tag{6}
\]

5.2 Formal Security Verification using AVISPA

The proposed scheme is simulated for the formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool to exhibit that the proposed scheme withstands replay and man-in-the-middle attacks.

AVISPA integrates four backends that implement different state-of-the-art automatic analysis mechanisms: (i) OFMC; (ii) CL-AtSe; (iii) SATMC; and (iv) TA4SP. The detailed description and functionality of these backends are available in [15, 25, 30, 37, 33]. A security protocol requires to be implemented in the High Level Protocols Specification Language (HLPSL) [39], which is converted into intermediate format (IF) using the HLP $$2$$IF translator. The IF is then given as input to one of the four backends to produce output, which has various sections highlighting whether the designed scheme is safe or unsafe against an adversary.

The registration, login, authentication and session key agreement phases of our scheme are implemented in HLPSL. In our implementation, four basic roles are defined: registration authority, user, gateway node and smart device for representing the RA, a user \( \mathcal{U}_i \), the GW\( \text{N} \) and a smart device \( \mathcal{S}_D \), respectively. The HLPSL role specification \( \mathcal{U}_i \) is given in Fig. 5. \( \mathcal{U}_i \) as an initiator receives the start signal, updates its state from 0 to 1, and sends the registration request \( \langle ID_i, RP_{Wi} \rangle \) to the RA using \( Snd() \) channel securely. The RA accepts the registration request of \( \mathcal{U}_i \), and sends information \( \langle A_0, TID_0 \rangle \) to \( \mathcal{U}_i \) using \( Snd() \) channel securely. \( \mathcal{U}_i \) then receives information \( \langle A_1, TID_1 \rangle \) using \( Rcvi() \) channel securely. \( \mathcal{U}_i \) sends the login request \( \langle TID_1, M_2, M_3, T_3 \rangle \) to the GW\( \text{N} \) using public channel. The GW\( \text{N} \) further sends the authentication request \( \langle M_7, M_8, T_2 \rangle \) to \( \mathcal{S}_D \) using public channel. The \( \mathcal{S}_D \) also sends reply message \( \langle M_{11}, M_{15}, M_{16}, T_3 \rangle \) to the GW\( \text{N} \) using public channel. Both \( Snd() \) and \( Rcvi() \) public channels use Dolev-Yao threat model type [39]. So, an intruder (always denoted by (i)) can read, modify or delete the contents of exchanged messages. Similarly, we also have specified the roles for RA, GW\( \text{N} \) and \( \mathcal{S}_D \) in our HLPSL implementation.

In the session role specified in Fig. 5, all the basic roles are started with concrete arguments. Fig. 6 also consists of top level environment role, which is the starting point for the execution. At the end, in the goal section, four authentication goals and two secrecy goals are specified.

The declaration witness(\( \mathcal{U}_i, \mathcal{G}W\text{N}, \mathcal{U}_{gw\text{-}n\_f}, T1' \)) says that \( \mathcal{U}_i \) has freshly generated the current timestamp \( T3 \) for
GWNN. The declaration request(GWNN,U1, gw u1 t4,T4) expresses U1’s acceptance of timestamp T4 generated for U1 by GWNN. The declaration secret({ PWi, A*, R'}, sr1,U1) also says that the information PWi, a and r are only known to U1. This is specified with protocol id sr1 in the goal section (given in Fig. 6).

Fig. 6. The results of the analysis using OFMC and CL-AtSe backends.

We have simulated our scheme using the widely-used OFMC and CL-AtSe backends. The executability check on non-trivial HLPSL specifications, replay attack check, and Dolev-Yao model check are verified in the proposed scheme. For more details on these verifications, one can refer to [31], [40]. The simulation results shown in Fig. 7 depicts that the proposed scheme is secure against replay as well as man-in-the-middle attacks.

Fig. 7. The results of the analysis using OFMC and CL-AtSe backends

5.3 Informal Security Analysis

The informal security analysis shows that the following other possible known attacks are prevented.

5.3.1 Traceability

In many applications, it is desirable that a user authentication should not allow an adversary to trace a user during login and authentication phases. Therefore, it also becomes important that the identity of the user should not be revealed to an adversary to preserve the privacy of that user in a network, especially in a smart home environment. The login request (TID1, M2, M3, T3) sent by U1 to the GWNN is different each time due to the following reason. The smart phone SP1 of U1 computes M1 = A* ⊕ RPW* = h(IDt || KGWNN−U1), M2 = M1 ⊕ rU1, and M3 = h(M1) || T1 || IDt || PID1 || rU1, where T1 is current timestamp and rU1 random nonce of U1. The involvement of T1 and rU1, ensures that M2 and M3 are distinct for each session. Moreover, other exchanged messages (M7, M8, T2, (M10, M11, M12, T3) and (M14, M15, M16, T3, T4) are also different for each session due to the use of timestamps and random nonces. In addition, our scheme allows to update old TID1 with a new TIDnew for each session while the message (M14, M15, M16, T3, T4) is sent to U1 by the GWNN. After receiving the message, SP1 of the user U1 calculates TID1new = M15 ⊕ h(TID1, || M1 || T3 || T1) and replaces TID1 with TID1new in its memory. Due to this, TID1 in the login request messages are different for distinct sessions. Thus, our scheme avoids traceability of U1 and SD1 by an attacker.

5.3.2 Anonymity

Prior to sending the login request (TID1, M2, M3, T3) to the GWNN, U1 hides its identity IDt in M1 = A* ⊕ RPW* = h(IDt || KGWNN−U1) M2 and M3. The GWNN also hides the identities of U1 and SD1 as it computes M6 = h(IDSD || KGWNN−SD1) M7 = EMe1(IDt, IDGWNN, rU1, TGWNN, h(M4)) and M8 = h(M6) || T2 || IDSD || IDGWNN || TGWNN. If attacker intercepts all the messages during login and authentication phases, he/she is unable to identify IDt and IDSD, as these are protected by symmetric encryption and one-way cryptographic hash function h(·). Therefore, the user and smart device anonymity are preserved in our scheme.

5.3.3 Privileged-Insider Attack

Suppose A is a malicious insider user of the RA, who knows IDt and RPWt, which were sent to RA by U1 during his/her registration phase. Note that RPWt = h(PWt || [σ1 || a] ⊕ r). We assume that A obtains the smart phone SP1 of U1 only after the user registration phase is finished. A can then extract all the information { TID1, A*, B1, C1, τ1, h(·), Gen(·), Rep(·), t} stored in SP1 using the power analysis attacks [41]. Note that the user U1 already deleted the information A1 from its smart phone SP1 at the end of the user registration phase described in Section 4.2. Hence, without having A1, it is computationally hard for A to derive the secret r as r = A* ⊕ A1. As a result, without r, A cannot derive h(PWt || [σ1 || a] ⊕ r). Furthermore, without knowing a, it is computationally infeasible to derive the biometric key σ1 as h(ID1 || σ1) = B1 ⊕ a. As a consequence, without having a, σ1, and KGWNN−U1, it is also computationally hard for A to guess correctly the password PWt of U1 from C1 = h(IDt || RPWt || σ1) = h(IDt || h(IDt || KGWNN−U1) ⊕ h(PWt || σ1 || a)) || σ1. In summary, it is computationally hard for A to guess and verify correctly PWt and σ1 from RPWt, A*, B1 and C1 due to the collision resistant property of h(·). Therefore, our scheme is secure against the privileged-insider attack.
5.3.4 Stolen Smart Phone Attack

Suppose the smart phone $S_P$ of $U_i$ is lost or stolen by an attacker $A$. $A$ can then extract all information $\langle TID_i, A_*, B_1, C_1, \tau_i, h(\cdot), Gen(\cdot), ReP(\cdot), t \rangle$ stored in $S_P$ using the power analysis attacks [41]. Note that $B_i = h(ID_i \| \sigma_i) \oplus a \| RPW_i = RPW_i \oplus r \equiv (WP_i \| \sigma_i \| a, \sigma_i = h(ID_i \| \| RPW_i \| \sigma_i)$ and $A_i' = A_i \oplus r = h(ID_i \| K_{GW-N-U_i}) \oplus RPW_i$. To correctly guess $ID_i$ and $PW_i$ from $B_i$ and $C_i$ respectively, $A$ needs to know both $a$ and $r$. Again, to know $a$ from $B_i$, $A$ needs both $ID_i$ and $PW_i$. Thus, it is computationally infeasible for $A$ to correctly guess both $ID_i$ and $PW_i$ as $ID_i$ and $PW_i$ are protected by the one-way hash function $h(\cdot)$. Therefore, our scheme is secure against such an attack.

5.3.5 Session Key Security

The session key $SK_{ij} = h[ID_i \| ID_{SD_i} \| ID_{GW_N} \| r_{U_i} \| r_{GW_N} \| T_{SD_i} \| T_{GW_N} \| T_{i} \| (m_A) \| h(h(ID_{SD_i} \| K_{GW-N-SD_i}) \| T_{3} \| T_{j} \| T_{GW_N})]$ is calculated by both $U_i$ and $SD_i$. The message $\{M_{10}, M_{11}, M_{12}, T_{3}\}$ sent by $SD_i$ to $GW_N$ contains session key $SK_{ij}$ as $M_{11} = h(SK_{ij} \| T_{3})$. Suppose an attacker $A$ intercepts this message and tries to compute the session key $SK_{ij}' = h[ID_i \| ID_{SD_i} \| ID_{GW_N} \| RU_i \| T_{GW_N} \| T_{i} \| (m_A) \| h(hID_{SD_i} \| K_{GW-N-SD_i}))$ by generating the random nonces $r_{U_i}, r_{GW_N}, r_{SD_i}, \text{ and timestamp } T_{3}$. However, the computation of $SK_{ij}'$ is not possible for $A$ because he/she does not know the various identities $ID_i, ID_{SD_i}, \text{ and } ID_{GW_N}$. Without the knowledge of these parameters, and due to the collision resistance property of $h(\cdot)$, it is very difficult for $A$ to obtain $SK_{ij}$. Therefore, our scheme preserves the session key security.

5.3.6 User Impersonation Attack

Suppose there is an adversary $A$, who has the lost/stolen smart phone $S_P$ of a legal user $U_i$, and knows all the information stored in $S_P$ by the help of power analysis attacks [41]. Assume that $A$ intercepts $U_i$’s login request $\langle TID_i, M_{12}, M_{13}, T_{1} \rangle$ and tries to create another valid login request, say $\langle TID_i, M_2', M_3', T_{1} \rangle$ on behalf of $U_i$. Let us assume the current timestamp $T_{1}$ of his/her system. To compute $M_2', M_3'$ required to compute to $M_2 = A_\epsilon \oplus RPW_{U_i}' = h(ID_i \| K_{GW-N-U_i})$. Suppose $A$ generates a random nonce $r_{U_i}'$. To compute $M_2' = M_2 \oplus r_{U_i}'$, and $M_3' = h(M_2') \| T_{1} \| ID_{i} \| T_{1} \| T_{SD_i} \| T_{GW_N} \| (m_A) \| h(ID_{SD_i} \| K_{GW-N-SD_i})$, $A$ needs $ID_i$ and $K_{GW-N-U_i}$, which are infeasible for $A$ to obtain them. Due to the one-way hash function $h(\cdot)$, it is computationally infeasible for $A$ to create valid login request $\langle TID_i, M_2', M_3', T_{1} \rangle$ on behalf of $U_i$, even he/she knows the all information from the lost/stolen $S_P$. So, it is clear that our scheme is secure against the user impersonation attack.

5.3.7 GWN Impersonation Attack

Suppose an adversary $A$ intercepts the messages $\{M_7, M_8, T_{2}\}$ and $\{M_{14}, M_{15}, M_{16}, T_{3}, T_{4}\}$, and attempts to create other valid messages, say $\{M_7', M_8', T_{2}'\}$ and $\{M_{14}', M_{15}', M_{16}', T_{3}', T_{4}'\}$ on behalf of the GWN, where $M_7 = EM_{GW} [ID_i, ID_{GW_N}, r_{U_i}, r_{GW_N}, h(M_A)]$, $M_8 = h(ID_{SD_i} \| K_{GW-N-SD_i})$, $M_4 = h(ID_i \| K_{GW-N-U_i})$, and $M_8 = h(M_6) \| T_{2} \| ID_{i} \| ID_{SD_i} \| ID_{GW_N} \| r_{GW_N}$, $M_{14} = EM_{GW} [r_{U_i}, r_{GW_N}, r_{SD_i} \| ID_{SD_i}, ID_{GW_N}, h(M_6)]$, $M_{15} = TID_{GW} \oplus h(ID_{GW_N} \| T_{3} \| T_{4})$, $M_{16} = h(M_{11}) \| T_{4} \| (r_{U_i}')$. Suppose $T_{2}, T_{3}$, and $T_{4}, r_{GW_N}, r_{SD_i}'$, are the current timestamps and different random nonces generated by $A$. To compute $M_7', M_8', M_4$, and $M_8'$, the secret key $K_{GW-N-SD_i}$, and various identities $ID_i, ID_{SD_i}, \text{ and } ID_{GW_N}$ are required. To compute $M_{14}', M_{15}', M_{16}', T_{3}'$ the secret key $K_{GW-N-U_i}$, and various identities $TID_i, ID_i, ID_{SD_i}, \text{ and } ID_{GW_N}$ are required. Moreover, the messages are protected by the one-way hash function $h(\cdot)$. Thus, $A$ is not able to create other valid messages $\{M_7', M_8', T_{2}'\}$, $\{M_{14}', M_{15}', M_{16}', T_{3}'\}$ on behalf of the GWN. Therefore, the proposed scheme is secure against the GWN impersonation attack.

5.3.8 Smart Device Impersonation Attack

Suppose an adversary $A$ intercepts the messages $\{M_{10}, M_{11}, M_{12}, T_{3}\}$ and attempts to create another valid message, say $\{M_1', M_{12}', T_{3}\}$ on behalf of the smart device $SD_j$, where $T_{3}$ is the current timestamp of $A$’s system when this message is created. Note that $M_{10} = h(ID_{SD_i} \| K_{GW-N-SD_i}) \| T_{3} \| T_{j} \| T_{GW_N}, M_{11} = h(SK_{ij} \| T_{3}), SK_{ij} = h(ID_i \| ID_{SD_i} \| ID_{GW_N} \| T_{i} \| T_{GW_N} \| T_{i} \| T_{GW_N}, r_{U_i}', r_{GW_N}, r_{SD_i}' \text{ and timestamp } T_{3}$. The secret keys $K_{GW-N-SD_i}$, and $h(ID_i \| ID_{GW_N})$, and various identities $ID_i, ID_{SD_i}$, and $ID_{GW_N}$ are necessary. Therefore, $A$ is not able to create another valid message $\{M_{10}', M_{11}', M_{12}', T_{3}\}$ on behalf of $SD_j$. This confirms that the proposed scheme is secure against this attack.

5.3.9 Resilience against Smart Device Capture Attack

Suppose a smart device $SD_j$ is physically captured by an attacker $A$. Each $SD_j$ contains the information $\{ID_{SD_j}, h(ID_{SD_j} \| K_{GW-N-SD_j})\}$. Since each $K_{GW-N-SD_j}$ is distinct, $h(ID_{SD_j} \| K_{GW-N-SD_j})$ is also distinct for each $SD_j$. If $A$ tries to extract $K_{GW-N-SD_j}$ from $h(ID_{SD_j} \| K_{GW-N-SD_j})$ using $ID_{SD_j}$, it is difficult task for $A$ to compute $K_{GW-N-SD_j}$ as $K_{GW-N-SD_j}$ is a long 1024-bit secret key. However, $A$ can know the session key $SK_{ij}$ shared with the legal user $U_i$, which is stored in $SD_j$’s memory. Thus, compromise of this particular smart device $SD_j$ in the smart home network does not lead to compromise of the session keys between that $U_i$ and other non-compromised smart devices $SD_j$’s as the stored $h(ID_{SD_j} \| K_{GW-N-SD_j})$ is distinct for $SD_j$. The proposed scheme is then unconditionally secure against this attack.

5.3.10 Gateway Bypass Attack

In our scheme, both $U_i$ and $SD_j$ can not bypass the GWN due to the following argument. $U_i$ can only send the login request through the GWN, and $SD_j$ can send the authentication response only through the GWN. Both $U_i$ and $SD_j$ also establish the session key $SK_{ij}$ through the GWN. When the GWN receives login request from $U_i$, it computes $M_1 = EM_{GW} [ID_i, ID_{GW_N}, r_{U_i}, r_{GW_N}, h(M_A)]$ and $M_8 = h(M_6) \| T_{2} \| ID_{i} \| ID_{SD_i} \| ID_{GW_N} \| r_{GW_N}$ and sends $\langle M_1, M_2, T_{2}\rangle$ to $SD_j$, where $M_6 = h(ID_{SD_i} \| K_{GW-N-SD_i})$, and $T_{2}$ is the current timestamp generated by $U_i$. $U_i$ cannot compute $M_6$ as he/she does not know $K_{GW-N-SD_i}$, and it is only known to the GWN. Therefore, $U_i$ is not able to compute $M_2$ and $M_6$. When the GWN receives authentication reply from $SD_j$, it computes $M_{14} = EM_{GW} [r_{U_i}, r_{GW_N}, r_{SD_i}' \| ID_{SD_i}, ID_{GW_N}, h(M_6)]$, $M_{15} = TID_{GW} \oplus h(ID_{GW_N} \| T_{3} \| T_{4})$, $M_{16} = h(M_{11}) \| T_{4} \| r_{U_i}'$ and sends the message $\langle M_1, M_2, T_{3}, T_{4}\rangle$ to $U_i$. $SD_j$ cannot compute $M_6$ as he/she does not know $K_{GW-N-U_i}$. Therefore,
5.3.11 Offline-Dictionary Attack

We consider an interesting attack scenario in our proposed scheme as illustrated by Huang et al. [34] to verify whether an adversary A can derive the password of a legal user $U_i$ or not. As in [34], we also consider the following attacking scenario as follows.

- At time $T_1$, suppose $U_i$ invokes the password and biometric update phase to change the password to $PW_{i1}$. At the end of this phase, the smart phone $SP_i$ of $U_i$ contains the information $(TD_i, A_i^*, B_i, C_i, \tau_i, h(\cdot), Gen(\cdot), Rep(\cdot), t)$, where $A_i^* = h(ID_i || KGW_N - U_i) \oplus h(PW_{i1} || \sigma_{i1}) || \sigma_{i1}$ and $\sigma_{i1}$ is the biometric key derived from the new biometrics $BIO_{i2}$ entered by $U_i$ at this time.

- At some time later (say, $T_2$), $U_i$ again changes his/her password to a new password $PW_{i2}$. At the end of this phase, the $SP_i$ of $U_i$ contains the information $(TD_i, A_i^{**}, B_i, C_i, \tau_i, h(\cdot), Gen(\cdot), Rep(\cdot), t)$, where $A_i^{**} = h(ID_i || KGW_N - U_i) \oplus h(PW_{i2} || \sigma_{i2}) || \sigma_{i2}$ and $\sigma_{i2}$ is the biometric key derived from the new biometrics $BIO_{i2}$ entered by $U_i$ at this time $T_2$.

- A passive adversary A with a smart phone can obtain the data stored in the smart phone at time $T_1$ and $T_2$. Now, given $(A_i^*, A_i^{**})$, A can calculate $A_i^* \oplus A_i^{**} = h(PW_{i1} || \sigma_{i1} || a) \oplus h(PW_{i2} || \sigma_{i2} || a)$. By testing all password pairs in the password dictionary, A can try to find at least one pair $(pw_{i1}, pw_{i2})$ such that $A_i^* \oplus A_i^{**} = h(pw_{i1} || \sigma_{i1} || a) \oplus h(pw_{i2} || \sigma_{i2} || a)$. However, to satisfy this condition, A further needs to guess correctly the biometric keys pair $(\sigma_{i1}, \sigma_{i2})$. In addition, A also needs the random secret $a$ which is only known to $U_i$. To derive $a$, A requires to guess the biometric key too. Thus, without having the biometric keys pair $(\sigma_{i1}, \sigma_{i2})$ and random secret $a$, it is computationally infeasible problem for A to verify whether the guessed passwords pair $(pw_{i1}, pw_{i2})$ is correct or not. As a result, the proposed scheme has the ability to protect the offline-dictionary attack described in [34].

6 PRACTICAL PERSPECTIVE: NS2 SIMULATION

The proposed scheme is simulated using the widely-accepted networking simulation tool, NS2 2.35 simulator [16] on Ubuntu 14.04 LTS platform.

6.1 Simulation Parameters

The various simulation parameters are given in Table 2. The network coverage area is taken as $400 \times 200$ m². The communication ranges of the gateway nodes (GW) and smart devices (SDs) are taken as 200 m and 50 m, respectively. The network simulation time is taken as 1800 seconds (30 minutes). The traditional Ad hoc On-Demand Distance Vector (AODV) routing protocol is used as the routing protocol. Two types of users are taken in the simulation: first type consists of the static users, who do not move (for example, some smart home users seat on the chair and access SD), while the second type has moving users (for example, somebody is walking in the garden and accessing SD, or somebody is driving the card and accessing SD). The speeds for these smart home users are considered as 2, 10 and 15 mps, respectively.

6.2 Simulation Environment

We have considered the following three network scenarios in the simulation. For all the scenarios, we have taken one GW and 50 SDs.

- Scenario 1. In this case, we have taken two users ($U_i$s): one is static and other one is moving with 2 mps.

- Scenario 2. In this case, we have taken three users ($U_i$s): one is static and other two are moving with the speeds of 2 mps and 15 mps, respectively.

- Scenario 3. In this case, we have taken eight users ($U_i$s): four are static and other four are moving with the speeds of 2 mps, 2 mps, 10 mps and 15 mps, respectively.

Moreover, we assume that the bit lengths of the identity, hash output (if we use SHA-1 hash algorithm) and random number/nonce are 128, 160 and 128 bits, respectively. In each scenario, we have considered the following messages between different network entities: $(TD_i, M_5, M_3, T_1), (M_7, M_8, T_2), (M_{10}, M_{11}, M_{12}, T_3)$ and $(M_{14}, M_{15}, M_{16}, T_3, T_4)$ of sizes 480 bits, 960 bits, 512 bits and 1280 bits, respectively.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Ubuntu 14.04 LTS</td>
</tr>
<tr>
<td>Network coverage area</td>
<td>$400 \times 200$ m²</td>
</tr>
<tr>
<td>Network scenarios</td>
<td>1, 2 and 3</td>
</tr>
<tr>
<td>Number of users ($U_i$)</td>
<td>2, 3, 8 for scenarios 1, 2, 3</td>
</tr>
<tr>
<td>Number of gateway nodes (GW)</td>
<td>1 for all scenarios</td>
</tr>
<tr>
<td>Number of smart devices (SD)</td>
<td>50 for all scenarios</td>
</tr>
<tr>
<td>Mobility</td>
<td>2 mps, 10 mps, 15 mps</td>
</tr>
<tr>
<td>Simulation time</td>
<td>1800 seconds</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Communication range of GW</td>
<td>200 m</td>
</tr>
<tr>
<td>Communication range of SD</td>
<td>50 m</td>
</tr>
</tbody>
</table>

6.3 Simulation Results and Discussions

The network performance parameters, such as end-to-end delay (in seconds) and throughput (in bps) are calculated during the simulation.

6.3.1 Impact on End-to-end Delay

The end-to-end delay (EED) is calculated as the average time taken by the data packets to arrive at the destination from the source. The EEDs of our scheme for different scenarios are given in Fig. 3(a). The EEDs are 0.29832, 0.29687 and 0.28637 seconds for the network scenarios 1, 2 and 3, respectively. Note that the EED decreases in the scenarios 2 and 3, because in these scenarios we have considered more number of mobile users who are traveling towards the gateway node as compared to the scenario 1. For this reason, the EED reduces as the distance between the gateway node and mobile users decreases which affects the reducibility of the EEDs accordingly.
6.3.2 Impact on Throughput

The throughput is measured as the number of bits transmitted per unit time. Fig. 8(b) depicts the network throughput (in bps) of our scheme under different network scenarios. The throughput values are 197.56, 303.87, and 793.78 bps for the scenarios 1, 2, and 3, respectively. Note that the throughput increases with an increase in the number of users. Due to the large number of users, more number of messages are exchanged in the network, and as a result, the throughput also increases.

7 Performance Comparison

In this section, the proposed scheme is compared with related existing schemes of Kumar et al. [5], Vaidya et al. [21], Kim and Santoso-Vun et al. [25], and Jeong et al. [20]. During the login, and authentication and key agreement phases. Since the registration, and password and biometric update phases are not available in Kim-Kim’s scheme. Kumar et al. provide formal security proof under the ROR model and formal security verification using A VISPA are also available in our scheme. The schemes of Kumar et al., Kim-Kim and Jeong et al. provide formal security proof under the ROR model and formal security verification using A VISPA are not available in their scheme.

Finally, the functionality and security features comparison among our scheme and other schemes is shown in Table 5. The scheme of Vaidya et al. is insecure against privileged-insider, password guessing, and smart device capture attacks, and it does not have the traceability, user anonymity and smart device anonymity properties. Moreover, the dynamic smart device addition phase, offline smart device registration phase, formal security proof under standard model and formal security verification using AVISPA are not supported in their scheme. Kim-Kim’s scheme is vulnerable to password guessing attack, password change attack, privileged-insider attack, user impersonation attack through privileged-insider attack and smart device capture attack, and it does not have traceability, user anonymity and smart device anonymity properties. Additionally, the dynamic smart device addition phase, offline smart device registration phase, formal security proof under the ROR model and formal security verification using AVISPA are not available in Kim-Kim’s scheme. Kumar et al. does not support traceability and gateway anonymity properties and it does not provide formal security proof under the ROR model. The schemes of Kumar et al., Jeong et al. and Santoso-Vun also lack the functionality features, which are shown in Table 5. In summary, our scheme provides significantly better security and functionality features compared to those for other existing schemes.

8 Conclusion

This paper presents a new scheme to address the user authentication issue in a smart home environment. The proposed scheme...
TABLE 5

<table>
<thead>
<tr>
<th>Functionality features</th>
<th>[5]</th>
<th>[21]</th>
<th>[22]</th>
<th>[20]</th>
<th>[25]</th>
<th>Our</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFF1:</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF2:</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF3:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF4:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF5:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF6:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF7:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF8:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF9:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF10:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF11:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF12:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF13:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF14:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF15:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF16:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF17:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF18:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF19:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF20:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF21:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF22:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF23:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF24:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SFF25:</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Note: SFF1: mutual authentication between GW N and smart device; SFF2: mutual authentication between user and smart device; SFF3: mutual authentication between user and GW N; SFF4: key agreement; SFF5: traceability property; SFF6: password guessing attack; SFF7: password change attack; SFF8: dynamic smart device addition phase; SFF9: user anonymity property; SFF10: GW N anonymity property; SFF11: smart device anonymity property; SFF12: replay attack; SFF13: privileged-insider attack; SFF14: man-in-the-middle attack; SFF15: stolen smart phone/smart card attack; SFF16: user impersonation attack; SFF17: smart device impersonation attack; SFF18: GW N bypassing attack; SFF19: DoS attack; SFF20: resilient against smart device capture attack; SFF21: offline smart device registration phase; SFF22: password change phase; SFF23: biometric update phase; SFF24: formal security proof under ROR model; SFF25: formal security verification using AVISPA.

✓: the scheme is secure or supports a particular functionality/security feature; ×: the scheme is not secure or does not support a particular functionality/security feature. N/A: not applicable in the scheme.

Table 5 provides additional functionality features. The proposed scheme is secure against several known attacks, which are shown through random oracle model, informal security and AVISPA tool. The practical implementation of the proposed scheme is also demonstrated though the widely-accepted NS-2 simulator. Overall, the proposed scheme provides a better trade-off between security and functionality features provided in Table 5 and overheads as compared to other existing related schemes.

ACKNOWLEDGMENTS

We thank the anonymous reviewers and the Associate Editor for providing constructive and generous feedback. This work was supported by the Information Security Education & Awareness (ISEA) Phase II Project, Department of Electronics and Information Technology (DeitY), India.

REFERENCES

Mohammad Wazid (S’17) received the M.Tech. degree in computer network engineering from Graphic Era University, Dehradun, India and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology (IIIT), Hyderabad, India. His current research interests include security in wireless sensor network, vehicular adhoc network, Internet of Things (IoT) and cloud computing. He has published over 145 papers in international journals and conferences in the above areas.

Ashok Kumar Das (M’17) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently an Assistant Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. His current research interests include security in wireless sensor network, vehicular ad hoc networks, smart grid, Internet of Things (IoT) and cloud computing. He has authored over 445 papers in international journals and conferences. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is in the editorial board of KSI Transactions on Internet and Information Systems, and the International Journal of Internet Technology and Secure Transactions (Inderscience).

Vanga Odelu received the M.Tech. degree in computer science and data processing and Ph.D. degree from IIT Kharagpur, India. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Indian Institute of Information Technology, Sri City, India. His research interests include user authentication, security in cloud computing and smart grid. He has authored over 40 papers in international journals and conferences.

Neeraj Kumar (M’16) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra (J&K), India, in 2009. He was a Post-Doctoral Research Fellow at Coventry University, Coventry, U.K. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has authored more than 160 technical research papers published in leading journals and conferences from the IEEE, Elsevier, Springer, John Wiley, including IEEE TIE, IEEE TDS, IEEE TIFS, IEEE TCE, IEEE Network, IEEE Com, IEEE WC, IEEE IoTJ, IEEE SJ, FGCS, JNCA, and ComCom. He is in the editorial board of JNCA (Elsevier) and UCJS (Wiley).

Willy Susilo (SM’02) received the Ph.D. degree in computer science from the University of Wollongong, Australia. He is currently a Professor and the Head of the School of Computing and Information Technology with the University of Wollongong, Australia. He is also the Director of the Centre for Computer and Information Security Research with the University of Wollongong. He has been awarded the Prestigious ARC Future Fellow by the Australian Research Council. His main research interests include cloud security, cryptography, and information security. He has served as a Program Committee Member in many international conferences including Asiacrypt and CT-RSA. He is the Editor-in-Chief of the Information Journal. He is also an Associate Editor of the IEEE Transactions on Information Forensics and Security, Computer Standards & Interfaces and International Journal of Information Security.