Advances in Computer, Signals and Systems (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2022.060106
ISSN 2371-8838 Vol. 6 Num. 1

A Lightweight Remote Mutual Authentication Scheme for Smart Home Environments

Shaomin Zhang[a,*], Yincai Zhang[b] and Baoyi Wang[c]

School of Control and Computer Engineering, North China Electric Power University, China
a. zhangshaomin@126.com, b. zhangyincai0628.@163.com, c. wangbaoyiqj@126.com
**corresponding author*

Keywords: smart home, mutual authentication, lightweight, security

Abstract: Based on IoT technology, smart home owners can access smart devices remotely and enjoy convenient and efficient services. However, sensitive data collected by smart devices are vulnerable to attacks such as eavesdropping and impersonation when transmitted over untrusted channels. The security of resource-constrained smart devices is low, and attackers may use the controlled devices to further execute malicious behaviors. In order to solve the above existing security problems, a lightweight remote mutual authentication scheme is designed in this paper, which can be applied in resource-constrained smart home environments. Compared with related schemes, this scheme has lower computation overhead and communication overhead.

1. Introduction

In recent years, IoT technology has developed rapidly, and more and more smart sensors and wireless communication devices are connected to traditional devices, which greatly facilitate people's lifestyles. According to statistics, the number of IoT devices will increase to 3.5 billion by 2024, and the global data space will grow to 163 ZB by 2025, of which the data generated by IoT devices will account for more than 50% [1,2]. With the maturity of IoT technology, concepts such as smart city, smart healthcare, and smart home have been proposed one after another [3]. Take smart home as an example, it integrates modern communication technology and home services into different smart devices, and manages and controls smart devices through wireless networks to improve people's quality of life. Smart devices have many built-in sensor elements, and users can control smart homes remotely through their smartphones. For example, before leaving work in winter, users can remotely turn on the heating system at home in advance, or log into smart cameras or set alarm triggering mechanisms to monitor the situation at home in real time. In short, based on the IoT environment, users can interact with various devices in the smart home and enjoy convenient services in real time.

As described in the literature [4], to provide more accurate and high-quality services, third-party service providers need to collect log data of devices for defect analysis and service updates. However, these log data contain a large amount of highly personal behavioral data and user privacy information, and lawbreakers may infer users' daily behavioral habits by analyzing log data, which seriously affects users' personal safety and property security. For example, after an attacker gains control of a sensor, he can pass a malicious plug-in into the device, and once the malicious plug-in is activated, the

attacker can capture sensitive user information [5]. In addition to this, smart devices have limited resources to resist most attacks against sensors, which further aggravates the security risk during smart home operation. Therefore, it is urgent to find a way to protect the data security and user privacy of smart devices.

To address the above security issues, researchers have proposed different solutions. Chang and Le [6] proposed a password and smart card-based authentication scheme for IoT environment. The scheme uses only XOR operations and one-way hash functions for resource-constrained sensor devices. Das et al [7] proved that literature [6] is not resistant to session key compromise attacks. To eliminate the security problems of literature [6], a new authentication and key negotiation scheme based on ECC was proposed in literature [7]. Kumar et al [8] proposed a lightweight authentication scheme suitable for smart home environment, where smart devices establish session keys by using authentication tokens and home gateways. However, the scheme cannot provide mutual authentication among user, smart device, and home gateway. Shuai et al [9] proposed an elliptic curve cipher (ECC) based anonymous authentication scheme for smart home environment, which uses random number method to resist replay attacks and avoid clock synchronization problem. The literature [10] performed a cryptanalysis of Shuai et al.'s [9] scheme and pointed out that the scheme is vulnerable to attacks such as insider attacks and replay attacks. The literature [11] proposed a remote user authentication key establishment protocol in a smart home environment, like the literature [6], the scheme uses only one-way hash functions, XOR operations and symmetric encryption/decryption.

In summary, the main contributions of this paper are as follows: a lightweight remote mutual authentication scheme is designed for smart devices, home gateways, and visitors (users and service providers) in a smart home environment. Based on the literature [8], the designed scheme enables mutual authentication among smart devices, home gateways, and visitors, and prevents malicious gateways and visitors from launching collusive attacks on smart devices.

The rest of the thesis is structured as follows: the second part describes the relevant technologies. The third part introduces the model architecture of the scheme. The fourth part introduces the specific implementation process of the scheme. The fifth part analyzes the performance of the scheme. The sixth part concludes the whole paper and looks at the future research directions.

2. Related technology

2.1. One-way hash functions

One-way hash function (also known as hash function) is a basic algorithm in cryptography for generating message digests and key encryption, which converts arbitrarily long messages into shorter, fixed-length output strings.

Definition: A function $f:\{0,1\}^n \to \{0,1\}^{l(n)}$ is $(t(n),\varepsilon(n))$ one-way if f is polynomial time computable and there is always $Pr_{y\leftarrow f(U_n)}[A(1^n,y)\in f^{-1}(y)] \le \varepsilon(n)$ for any probabilistic algorithm A with running time $t(n)$.If $\varepsilon(n) = 1/t(n)$,then f is said to be $\varepsilon(n)$-hard. f is a one-way function if there exists some negligible function $\varepsilon(n)$ such that the function f is $\varepsilon(n)$-hard.

3. Scheme design

3.1. Design ideas

Smart devices in smart home systems are resource-constrained and vulnerable to attacks such as illegal access, eavesdropping, tampering, and collusion, which seriously affect user privacy and security. Therefore, the design idea of this paper is:

When a visitor accesses the smart home system, first the home gateway and the visitor verify each other's identity, then the home gateway and the smart device verify each other's identity, and finally the smart device and the visitor verify each other's identity. Only the authenticated entities are eligible to participate in the subsequent data transmission process.

3.2. Scheme model

The model architecture of the scheme is shown in Figure 1. Each smart home system consists of several sensors, and the user or service provider accesses the smart home system through the home gateway. The functions of each entity are described below. Table 1 introduces the meaning of each symbol.

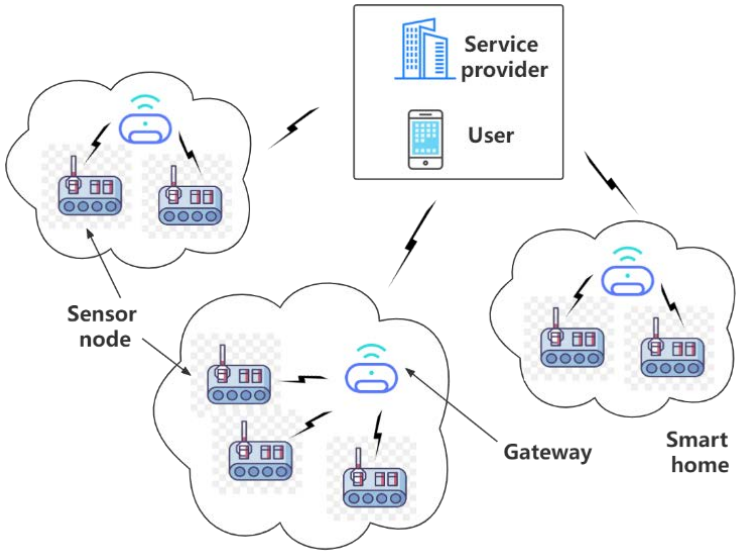

Figure 1: Model structure diagram.

Home Gateway (Hg): The home gateway is an online home server that accesses and manages numerous resources in smart devices. When a visitor uses a wireless device such as a smartphone to communicate remotely with the home gateway over the Internet, the home gateway verifies the visitor's identity and verifies the access history.

Smart devices (Sd): Sensors in smart devices collect log data of the device and record the daily usage of the device, while sensors generate relevant data based on the user's usage habits of the device. The smart device provides the requested data to the authenticated visitors.

Visitors (U_i): Visitors include residential users and service providers. The user accesses the data in the smart device to understand the operation of the device. The service provider accesses the data in the smart device, analyzes the user's device usage habits, and provides personalized services tailored to the user.

Table 1: List of symbols.

Hg	Home gateway	Sd	Smart device	U_i	Visitors
K_i	Private key for entity i	K_{i-j}	Shared key for i and j	ID_i	Identifier of entity i
$\oplus$	Exclusive or operation	II	Connection operation	H (·)	Hash function

4. Scheme implementation

4.1. System initialization

Step1. ID_{hg} is the home gateway identifier, ID_{hg} selects a random number r and computes $K_{hg} = h(ID_{hg}||r)$, K_{hg} is the private key of ID_{hg}.

Step2. ID_{sd} is the smart device identifier, compute $K_{sd-hg} = h(ID_{sd}||r)$, K_{sd-hg} is the shared key of smart device and home gateway.

Step3. $\{ID_{sd}, K_{sd-hg}\}$ is saved in ID_{sd}, $\{ID_{hg}, K_{hg}, ID_{sd}, K_{sd-hg}\}$ is saved in ID_{hg}.

4.2. Registration

Step1. User selects unique identity ID_i, secret value PSW_i, random number x_1, calculate $H_{psw} = h(x_1 \oplus PSW_i)$, send $\{ID_i, H_{psw}\}$ to home gateway ID_{hg}.

Step2. ID_{hg} selects the random number x_2 and computes $H_1 = h(H_{psw}||T_1)$, $H_2 = h(H_{psw}||ID_{hg})$, $H_3 = h(H_1||x_2||K_{hg}) \oplus h(H_{psw}||T_1)$, T_1 is the timestamp.

Step3. ID_{hg} stores $\{ID_{hg}, T_1, x_2, H_1, H_2, H_3\}$, and sends it to the user.

Step4. The user calculates $H_{ID} = h(PSW_i||ID_i) \oplus x_1$, sends H_{ID} to the home gateway ID_{hg}.

4.3. Login

Step1. The user logs into the home gateway and enters $\mathrm{ID_i}$ and $\mathrm{PSW_i}$. The home gateway calculates $x_1' = \mathrm{H_{ID}} \oplus h(\mathrm{PSW_i}||\mathrm{ID_i})$, $\mathrm{H'_{psw}} = h(x_1'||\mathrm{PSW_i})$, $\mathrm{H_2'} = h(\mathrm{H'_{psw}}||\mathrm{ID_{hg}})$. If $\mathrm{H_2'} = \mathrm{H_2}$, the user authentication is successful.

Step2. The user chooses random number x_3 and computes $\mathrm{M_1} = \mathrm{H_3} \oplus h(\mathrm{H_{psw}}||\mathrm{T_1}), \mathrm{M_2} = h(\mathrm{T_2}||x_3||\mathrm{M_1}||\mathrm{ID_{hg}})$, $\mathrm{M_3} = (x_3||\mathrm{T_2}) \oplus \mathrm{M_1}$, send $\{\mathrm{ID_{sd}}, \mathrm{M_2}, \mathrm{M_3}\}$ to the Hg.

4.4. Authentication

Step1.When the home gateway receives a user login request, it calculates $\mathrm{M_1'} = \mathrm{H_3} \oplus \mathrm{h(H_{psw}||T_1)} = \mathrm{h(H_1||x_2||K_{hg})}$, $\mathrm{M_1' \oplus M_3} = (\mathrm{x_3'||T_2'})$.

Step2. The home gateway calculates $\mathrm{M_2'} = \mathrm{h(T_2'||x_3'||M_1'||ID_{hg})}$, checks whether $\mathrm{M_2'} = \mathrm{M_2}$ holds, and if it does, the user is authenticated successfully.

Step3. The home gateway selects the random number $\mathrm{x_4}$ and computes $\mathrm{H_4} = \mathrm{h(ID_{sd}||H_1||K_{sd-hg}||x_4||T_3)}$, $\mathrm{H_5} = (\mathrm{x_3'||T_3||x_4}) \oplus \mathrm{K_{sd-hg}}$, $\mathrm{H_6} = \mathrm{H_1} \oplus \mathrm{h(ID_{sd}||h(x_4)||x_3')}$.

Step4. The home gateway sends $\{\mathrm{ID_{sd}}, \mathrm{H_4}, \mathrm{H_5}, \mathrm{H_6}\}$ to the smart device.

Step5.The smart device calculates $(\mathrm{x_3''||x_4'||T_3'}) = \mathrm{H_5} \oplus \mathrm{K_{sd-hg}}$, calculates $\mathrm{H_1'} = \mathrm{H_6} \oplus \mathrm{h(ID_{sd}||h(x_4')||x_3'')}$, $\mathrm{H_4'} = \mathrm{h(ID_{sd}||H_1'||K_{sd-hg}||x_4'||T_3')}$. The smart device checks whether $\mathrm{H_4'} = \mathrm{H_4}$ holds, and if it does, it means the smart device authenticates the home gateway successfully.

Step6. The smart device selects the random number $\mathrm{x_5}$ and calculates $\mathrm{S_{ki}} = \mathrm{h(H_1'||x_3''||x_4'||x_5)}$, $\mathrm{N_1} = \mathrm{h(T_4||x_5||K_{sd-hg}||ID_{sd}||T_3||S_{ki})}$, $\mathrm{N_2} = \mathrm{h(x_5||T_4)} \oplus \mathrm{x_4'}$, send $\{\mathrm{N_1}, \mathrm{N_2}\}$ to the home gateway.

Step7. The home gateway calculates $(\mathrm{x_5'||T_4'}) = \mathrm{N_2} \oplus \mathrm{x_4}, \mathrm{N_1'} = \mathrm{(x_5'||T_4'||K_{sd-hg}||ID_{sd}||T_3'||S_{ki})}$. Check whether $\mathrm{N_1'} = \mathrm{N_1}$ holds, and if it does, it means the home gateway authenticates the smart device successfully.

Step8. The home gateway calculates $\mathrm{H_7} = \mathrm{h(S_{ki}||H_1||x_4||T_5||H_4)}$, $\mathrm{H_8} = \mathrm{h(x_5'||x_4||T_5)} \oplus \mathrm{x_3'}$,

sends $\{H_4, H_7, H_8\}$ to the user.

Step9. The user computes $(x_5''||x_4'||T_5') = H_8 \oplus x_3$, $H_7' = h(S_{ki}||H_1||x_4'||T_5'||H_4) = h(S_{ki}||h(H_{psw}||T_1)||x_4'||T_5'||H_4)$, if $H_7' = H_7$, then the user authenticates the home gateway and smart device successfully.

5. Performance analysis

5.1. Computational cost analysis

Table 2 shows the comparison of computational cost of several schemes. We use T_{exp},T_h,T_{XOR} to denote the time cost of elliptic curve dot product, hash function, and XOR operation. Where T_{exp}= 0.4276ms and T_h= 0.0052ms, the time cost of the XOR operation is negligible compared to the elliptic curve dot product and hash function [9].

Table 2: Computational cost comparison with lightweight protocols.

Schemes	Total cost	Total execution time(ms)
Ref. [6]	$20T_h$	0.104ms
Ref. [7]	$4T_{exp} + 31T_h$	1.8196ms
Ref. [9]	$3T_{exp}$+$16T_h$	1.366ms
Our scheme	$21T_h$	0.1092ms

Table 3: Communication cost comparison with lightweight protocols.

Schemes	Total cost (bits)	Smart decice cost (bits)
Ref. [7]	2752bits	1408bits
Ref. [9]	1728bits	320bits
Our scheme	1664bits	320bits

5.2. Communication cost analysis

Table 3 shows the comparison of the communication cost of several schemes, and the total communication cost is the number of bits required for transmission in the login and authentication phases. As described in the literature [9], the lengths of each entity identity, timestamp, ECC point multiplication, ciphertext block, and hash function are assumed to be 32bit, 32bit, 320bit, 256bit, and 160bit, respectively. The results show that the communication cost of this scheme is low and can keep the smart home system stable for a long time.

6. Conclusion

In this paper, a lightweight remote mutual authentication scheme for smart home environments is proposed. The scheme uses only one-way hash functions and XOR operations, with low computational and communication costs, and is suitable for resource-constrained smart home systems. In the future, we will further improve the process of secure data transmission after successful authentication.

References

[1] *K. Sikder, G. Petracca, H. Aksu, T. Jaeger and A. S. Uluagac, A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications, in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1125-1159, Second quarter 2021.*

[2] *Data age 2025: The evolution of data to life-critical, [Online]. Available: https://www.import.io/wp-content/uploads/2017/04/Seagate-WP-DataAge2025-March-2017, accessed: Nov. 29, 2021.*

[3] *S. P. Mohanty, U. Choppali, and E. Kougianos, everything you wanted to know about smart cities, IEEE Consum. Electron. Mag., vol. 5, no. 3, pp. 60-70, Jul. 2016.*

[4] *S. Sendra, L. Parra, J. Lloret, and J. Tomas, Smart system for children chronic illness monitoring, Information Fusion, vol. 40, pp. 76-86, Mar 2018.*

[5] *R. Wijewickrama, A. Maiti, and M. Jadliwala, deWristified: Handwriting inference using wrist-based motion sensors revisited, in Proc. 12th Conf. Security Privacy Wireless Mobile Netw., 2019, pp. 49-59.*

[6] *C.-C. Chang and H.-D. Le, A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks, IEEE Trans. Wireless Commun., vol. 15, no. 1, pp. 357-366, Jan. 2016.*

[7] *A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, provably secure user authentication and key agreement scheme for wireless sensor networks, Secur. Commun. Netw., vol. 9, no. 16, pp. 3670-3687, 2016.*

[8] *P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, Lightweight and Secure session-key establishment scheme in smart home environments, IEEE Sensors J., vol. 16, no. 1, pp. 254-264, Jan. 2016.*

[9] *Shuai, M., Yu, N., Wang, H., Xiong, L., Anonymous authentication scheme for smart home environment with provable security. Computers & Security 86, 132-146, 2019.*

[10] *Damandeep Kaur, Devender Kumar, Cryptanalysis and improvement of a two-factor user authentication scheme for smart home, Journal of Information Security and Applications, Volume 58, 2021.*

[11] *M. Wazid, A. K. Das, V. Odelu, N. Kumar and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 391-406, 1 March-April 2020.*