D2D Group Key Agreement Scheme for Smart Devices in HANs

*Qingru Ma, Haowen Tan**

School of Information Science and Engineering, Zhejiang Sci-Tech University, China
maqingru0njfu@163.com, tan_halloween@foxmail.com

Abstract

The home area network (HAN) is one of the most widely researched areas in recent years. HANs integrate 5G/6G networks and artificial intelligence technology to provide data services for home users. The devices in HANs collect and transmit data relating to users' daily activities for analysis by remote service providers. These data often contain a large number of users' personal privacy. The disclosure of these data could have far-reaching consequences for the privacy of the individuals involved. Some researchers are dedicated to investigating the authentication of smart devices by the system. However, the increased frequency of interactions between devices and gateways, as well as between devices themselves, is a defining characteristic of HANs. In this paper, a device-to-gateway (D2G) authentication scheme is proposed. Based on the authentication result, a partial key is generated for smart devices and the gateway. Finally, a device-to-device (D2D) group key agreement scheme is presented. The security and efficiency of the proposed scheme are proved according to the analysis.

Keywords: D2D authentication, Group key agreement, Home area networks (HANs)

1 Introduction

Artificial intelligence and future Internet technologies are continuously evolving, resulting in a desire for a more intelligent life. New technological advances have led to the development of new environments, such as vehicular ad hoc networks, smart grids, e-health systems, and smart homes, which have become an integral part of people's lives, providing more opportunities for a convenient life [1-2]. Home area networks (HANs) [3] are the primary application scenario for smart homes and smart grids and they are closely connected with individuals and their daily lives. In a HAN, smart devices like voice assistants, intelligent door locks, air conditioners, sweeping robots, etc. are networked together in the home [4]. The HAN is powerful and transformative because it can be accessed by voice or other bio-information to create the possibility for home activity management [5-6]. As can be seen in Figure 1, in a home area network with smart devices, a variety of smart devices are integrated into an information interaction platform through wired and wireless connections. Smart devices such as a smart fan, a sweeping robot, a temperature and humidity monitor, a camera, and a smart door lock complete home services for users by receiving information and executing instructions, which are very important for social networks [7]. In the system shown in Figure 1, the camera is used to monitor the situation near the home, and the temperature monitor is used to monitor the indoor temperature. If the camera detects an unauthorized intrusion, the system will send an alarm message to the police, who can then investigate the situation or confirm it to the residents. If the temperature monitor detects abnormally high data, the fire center will be notified. The fire center can make an emergency response after verifying that there is a fire.

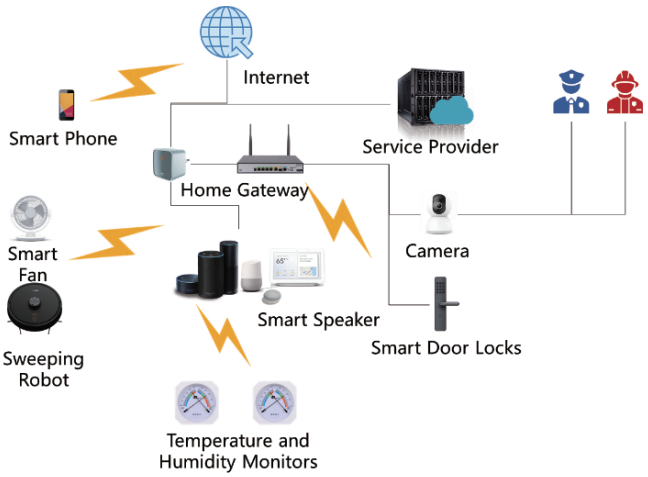

Figure 1. Home area networks with smart devices

The information interaction in HANs is mainly divided into two categories: device-to-gateway (D2G) and device-to-device (D2D). D2G communication requires the device to authenticate the identity to the gateway node and transmit the collected data to the gateway. The gateway will send the data to the remote service provider to obtain appropriate instructions or analysis feedback. These instructions or analyses will be fed back to intelligent devices to perform corresponding operations. D2D communication is faster and more intelligent. D2D communication enables smart devices to form an ad hoc network and intelligently communicate between devices with the help of edge servers. For example, when someone is at home, once the indoor temperature detector detects that the room temperature exceeds a certain temperature, it will send instructions to the air conditioner to reduce the indoor temperature and keep the residents comfortable.

*Corresponding Author: Haowen Tan; E-mail: tan_halloween@foxmail.com
DOI: 10.53106/160792642023052403011

The motivation of our work: However, the security issues in HAN are also very important for the promotion and application. The security concerns associated with HAN are significant and warrant careful consideration. For example, HANs are frequently accessed remotely and are thus vulnerable to security attacks. In HANs, a large number of smart devices need to communicate with each other. If the devices in a group can have a common secure session channel, the cooperation between these devices can provide users with better intelligent services. External attackers are often interested in the information in the group. An attacker may masquerade as a legitimate group device to obtain user privacy data shared within the group. Researchers mainly focus on the communication between devices and gateway nodes in HANs, and pay less attention to the interaction between devices. The lack of security information interaction channel between smart devices may cause the leakage of privacy information to home users.

Our contributions:

The contributions of this paper are listed as follows:

A D2G authentication method is presented for the verification of new smart device. In this paper, we first propose an authentication method for the smart devices and the gateway. A smart device signs its pseudo-identity and the gateway verify the signature.

A D2D group key agreement scheme is proposed for group devices in HANs. Based on the authentication, a D2D group key agreement scheme is given to support devices to communicate in a group. This scheme helps smart devices in HANs easily collaborate with each other to provide an intelligent life for individuals.

The scheme Is proved to be secure and efficient for HANs. In the security analysis, the correctness of the designed scheme is first proved. Then, the unforgeability of the signature in D2G authentication is also proved. In addition, the scheme is proved to be semantic secure under the BDH assumption. The simulation indicates that the scheme is efficient for HAN environment.

2 Related Work

A number of studies have been undertaken in the area of home area networks in recent years [8-10]. Satam et al. [11] provide a home area automated intrusion detection system with the assistance of wireless sensors. Semantic names are utilized to achieve device-to-device communication over wireless broadcast media in [12]. Many new technologies have been applied to HANs, such as automated firmware analysis, machine learning, and blockchain technology [13]. The work by McAuley et al. [14] considers the new challenges of cyber-security in HANs. Scott et al. [15] provide a secure recommendation scheme for AI-empowered home area networks. Pillai et al. [16] focus on the user-defined device interaction rules in HANs. Manandhar et al. [17] discuss the policies for the collection and sharing of device data. Aïvodji et al. [18] show a possibility of secured and privacy-preserving smart home architecture based on federated learning. There are also some studies focus on group authentication and key agreement [19].

All the above-mentioned schemes rarely considered the device-to-device group key agreement for the home area networks.

3 Preliminaries

In this phase, some significant preliminaries are presented in this section.

3.1 Bilinear Pairing

Let G_1 and G_2 be groups with prime order q. G_1 and G_2 are multiplicative groups. The mapping relationship can be described as follows:

Bilinearity. $e(g^a, g^b) = e(g, g)^{ab}$, $a, b \in Z_p^*$.

Non-degeneracy. If g is a generator of G_1, and $e(g, g)$ is a generator of G_2, we have $e(g, g) \neq 1$.

Computability. e is efficiently computable.

3.2 DL Assumption

Discrete logarithm assumption (DL assumption) can be defined as: Let G be a multiplicative group, g be the generator of G, and $g^a \in G$. $a \in Z_p$. It is difficult to compute for an adversary, which can be demonstrated as:

$$Adv_A^{DL}(K) = \Pr[A(g, g^a) \rightarrow a] = \epsilon_{DL}$$

3.3 CDH Assumption

Computational Diffie-Hellman assumption (CDH assumption) can be defined as: Let G be a multiplicative group, g be the generator of G, and g^a, $g^b \in G$. a, $b \in Z_p$. It is difficult to compute g^{ab} for an adversary, which can be demonstrated as:

$$Adv_A^{CDH}(K) = \Pr[A(g, g^a, g^b) \rightarrow g^{ab}] = \epsilon_{CDH}$$

4 System Model and Security Model

In this section, the system model and the security model are introduced in detail.

4.1 System Model

The system mentioned in this paper is in the environment of home area networks with smart devices trying to communicate with each other in a group. The system model is illustrated by Figure 2.

There are three entities in the presented system: the registration center (RC), the home gateway (GW), and all the smart devices (SD). The roles of these three entities are introduced as follows:

Registration center (RC): An RC is used for the registration of a new home gateway or a new smart device. The setup phase is implemented by the RC offline. The calculation on the RC can be considered as not affecting the efficiency of the scheme.

Gateway (GW): A GW in the room is to authenticate smart devices and assist devices to communicate with each other. In this system, a GW, as one of the members

participating in information sharing in a HAN, is allowed to share a session key with intelligent devices.

Smart devices (SD): SDs are devices equipped with multiple IoT sensors. These devices receive or execute the instructions issued by residents to achieve various functional features in the smart home environment.

4.2 Security Model

The security model of this proposal can be described in the following aspects:

Unforgeability of the D2G signature: The signature generated in the D2G authentication phase may be forged by an unregistered adversary. The adversary may participate in the key generation phase with a forged signature. The unforgeability of the D2G signature means that the signature generated in the D2G authentication phase cannot be forged by any adversaries.

D2D group session key security: External attackers may obtain the encrypted data of group members by rebuilding the group key. According to the rebuilt group key, the attackers may have the advantage to obtain the information transmitted in the smart device group of the HAN. The D2D group session key security means that the group key generated in the D2D group key generation phase cannot be distinguished from a random value.

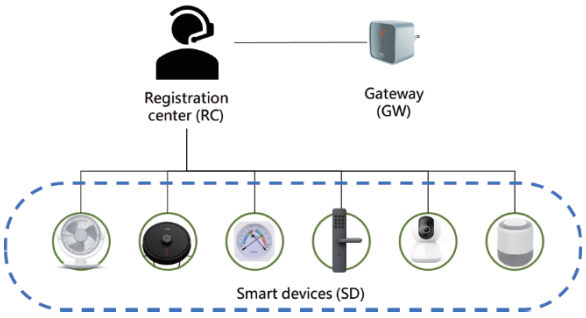

Figure 2. The system model of the proposal

5 Main Idea

In this section, the main idea of our proposed scheme is described in detail. Firstly, an overview of the scheme is given to show a brief introduce of the scheme. Then, the detailed scheme is demonstrated in for phases.

5.1 Overview of the Proposed Scheme

An overview of the proposed scheme is given in this subsection. This scheme is composed of four phases: setup phase, D2G authentication phase, partial key generation phase, and D2D group key generation phase. In the setup phase, the system generates some necessary parameters. The gateway GW and the devices generate their public keys and secret keys. In the D2G authentication phase, smart devices generate signatures for verification. In the partial key generation phase, a smart device generates a partial parameter and a partial key. In the D2D group key generation phase, the GW sends back parameters generated by the partial keys of the smart devices. The smart devices establish their group key agreement.

5.2 Setup Phase

The secret key of the GW is chosen as z. The public key of the GW is $h_G = g^z$. The smart device SD_i chooses a secret value $x_i \leftarrow Z_p$. Then SD_i computes $A_i = g^{x_i}$. The pair of secret key and public key (pk_i, sk_i) of this smart device is listed as follows:

$$\begin{aligned} pk_i &= (A_i, f) \\ sk_i &= x_i. \end{aligned} \tag{1}$$

A pseudo-identity PID_i is generated by the smart device SD_i.

5.3 D2G Authentication Phase

The D2G authentication phase is implemented between the smart device and the home gateway GW.

The smart device SD_i chooses a random value $r_i \leftarrow Z_p$. According to its pseudo-identity, SD_i computes σ_i.

$$\sigma_i = (\sigma_{i_1}, \sigma_{i_2}) = \left(r_i, f^{\frac{1}{x_i + H(PID_i, r_i)}} \right). \tag{2}$$

The value of σ_i is sent to the home gateway GW. The GW verify σ_i by the following equation.

$$e\left(\sigma_{i_2}, A_i g^{H(PID_i, \sigma_{i_1})}\right) = e(f, g). \tag{3}$$

If Eq. (3) stands, the device can join in this HAN. Otherwise, the request will be refused.

5.4 Partial Key Generation Phase

The device SD_i generates a partial parameter $B_i = h_G^{x_i}$. A partial key is generated as Eq. (4).

$$k_{x_i 2G} = H_1(B_i, \sigma_{i_1}, \sigma_{i_2}, f, PID_i). \tag{4}$$

According to the device's public key, the GW can also generate this value.

5.5 D2D Group Key Generation Phase

The GW computes Eq. (5) and sends M_i to SD_i.

$$M_i = g^{\prod_{y=0}^{I\setminus\{i\}} k_{x_y 2G}}. \tag{5}$$

The devices in the group are sequenced. The device SD_i computes Eq. (6) as its group session key.

$$SK_i = H_2(M_i^{k_{x_i 2G}}, \{PID_i\}_{[I]}). \tag{6}$$

6 Security Analysis

The correctness and security of the proposed scheme is proved in this section.

6.1 Correctness

The correctness of the D2G authentication can be proved by Eq. (7).

$$\begin{aligned}
&e\left(\sigma_{i_2}, A_i g^{H(PID_i,\sigma_{i_1})}\right)\\
&= e\left(f^{\frac{1}{x_i+H(PID_i,r_i)}}, A_i g^{H(PID_i,\sigma_{i_1})}\right)\\
&= e\left(f^{\frac{1}{x_i+H(PID_i,r_i)}}, g^{x_i} g^{H(PID_i,\sigma_{i_1})}\right)\\
&= e\left(f^{\frac{1}{x_i+H(PID_i,r_i)}}, g^{x_i} g^{H(PID_i,r_i)}\right)\\
&= e\left(f^{\frac{1}{x_i+H(PID_i,r_i)}}, g^{x_i+H(PID_i,r_i)}\right)\\
&= e(f,g)^{\frac{1}{x_i+H(PID_i,r_i)}x_i+H(PID_i,r_i)}\\
&= e(f,g). \qquad \textbf{(7)}
\end{aligned}$$

The partial key $k_{x_i 2G}$ can be correctly generated by the GW, which can be proved by Eq. (8).

$$\begin{aligned}
&k_{x_i 2G}\\
&= H_1(B_i, \sigma_{i_1}, \sigma_{i_2}, f, PID_i)\\
&= H_1(h_G^{x_i}, \sigma_{i_1}, \sigma_{i_2}, f, PID_i)\\
&= H_1(g^{zx_i}, \sigma_{i_1}, \sigma_{i_2}, f, PID_i)\\
&= H_1(A_i^z, \sigma_{i_1}, \sigma_{i_2}, f, PID_i). \qquad \textbf{(8)}
\end{aligned}$$

The same session key SK_i can be generated by each smart device, which can be proved by Eq. (9).

$$\begin{aligned}
&SK_i\\
&= H_2(M_i^{k_{x_i 2G}}, \{PID_i\}_{[I]})\\
&= H_2(g^{\prod_{i=0}^{I} k_{x_i 2G}}, \{PID_i\}_{[I]}). \qquad \textbf{(9)}
\end{aligned}$$

6.2 Security

In this subsection, the security of the proposed scheme is analyzed from the following aspects.

Theorem 1: Unforgeability of the D2G signature. The signature generated in the D2G authentication can be proved to be unforgeable.

Proof:

The signature is designed as $\sigma_i = (\sigma_{i_1}, \sigma_{i_2}) = \left(r_i, f^{\frac{1}{x_i+H(PID_i,r_i)}}\right)$.

In this signature, $\sigma_{i_1} = r_i$ is a random value chosen by the device. $\sigma_{i_2} = f^{\frac{1}{x_i+H(PID_i,r_i)}}$ is computed by the device with its secret value. The adversary can know nothing about the secret value with an advantage of ϵ_{D2G}. If the value can be computed, then the adversary can also solve the DL problem with advantage at least $\epsilon_{DL} \geq \epsilon_{D2G}$. However, according to the security model, the advantage ϵ_{DL} is negligible. So, the advantage ϵ_{D2G} is also negligible, and the D2G signature is unforgeable.

Theorem 2: D2D group session key security. The group key generated by group devices in the D2D group key agreement phase can be proved to be secure.

Proof:

The group key $Sk_i = H_2\ (M_i^{k_{x_i 2G}}, \{PID_i\}_{[I]})$, where $M_i = g^{\prod_{y=0}^{I\setminus\{i\}} k_{x_y 2G}}$.

The value can only be calculated by the device i and the GW. This is because $k_{x_y 2G} = H_1(B_i, \sigma_{i_1}, \sigma_{i_2}, f, PID_i)$, where $B_i = h_G^{x_i} = g^{zx_i}$. The adversary can obtain g^z and g^{x_i}. But it can hardly calculate g^{zx_i}. If the adversary can generate this value in the value of ϵ_{D2D}, it can solve the CDH problem with advantage at least $\epsilon_{CDH} \geq \epsilon_{D2D}$. Since ϵ_{CDH} is negligible, the advantage ϵ_{D2D} is also negligible, and the D2D key agreement is secure. The message encrypted with SK_i is also secure.

7 Performance Analysis

The operations implemented by SD and GW are listed as Table 1.

Table 1. The operations of SD and GW

D2G	D2GVerif-GW	Partial Key	D2D-GW	D2D-SD
1H+1E	1H+1P	1E+1H	*I*E+*I*H	1E+1H

H is denoted as the anti-collision hash function. is the exponential operation. P is the pairing operation. The number I is the total number of the smart devices.

As can be seen in Table 1, the GW takes over most of the calculation operations. The calculation burden on the resource limited entities (the smart devices) are relatively low.

The simulation of the scheme is implemented on the platform Ubuntu. The smart devices are simulated on Raspberry Pi 4 Computer Model B with 2G RAM. The GW is simulated on a laptop with 8G RAM.

As is shown in Figure 3, the time costs of each phase in views of an SD and a GW are illustrated in Figure 3. The simulation results show that most of the time cost are on the GW side. The algorithms on the SD side are efficient.

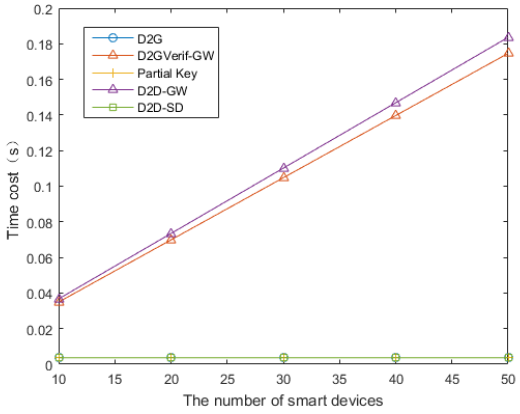

Figure 3. The time cost of different phases

8 Conclusion

In this paper, a D2D key agreement scheme is proposed for the home area networks (HANs) with smart devices. This scheme can support D2G authentication. Based on the authentication, with a partial key generated by the smart devices, a group key can be generated by devices with the assistance of the home gateway. According to our assistance, the scheme is secure and efficient for the application in HANs.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grants No. 61922045, No. U21A20465, No. 62172292, and Science Foundation of Zhejiang Sci-Tech University (ZSTU) under Grants No. 22222266-Y.

References

[1] W. Wang, Z. Han, M. Alazab, T. R. Gadekallu, X. Zhou, C. Su, Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps, *IEEE Transactions on Industry Applications*, Vol. 58, No. 5, pp. 5616-5623, September-October, 2022.

[2] B. D. Deebak, F. H. Memon, S. A. Khowaja, K. Dev, W. Wang, N. M. F. Qureshi, In the Digital Age of 5G Networks: Seamless Privacy-Preserving Authentication for Cognitive-Inspired Internet of Medical Things, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 12, pp. 8916-8923, December, 2022.

[3] B. L. R. Stojkoska, K. V. Trivodaliev, A review of Internet of Things for smart home: Challenges and solutions, *Journal of cleaner production*, Vol. 140, pp. 1454-1464, January, 2017.

[4] D. Marikyan, S. Papagiannidis, E. Alamanos, A systematic review of the smart home literature: A user perspective, *Technological Forecasting and Social Change*, Vol. 138, pp. 139-154, January, 2019.

[5] I. Cvitić, D. Peraković, M. Periša, B. Gupta, Ensemble machine learning approach for classification of IoT devices in smart home, *International Journal of Machine Learning and Cybernetics*, Vol. 12, No. 11, pp. 3179-3202, November, 2021.

[6] M. Ammi, S. Alarabi, E. Benkhelifa, Customized blockchain-based architecture for secure smart home for lightweight IoT, *Information Processing & Management*, Vol. 58, No. 3, Article No. 102482, May, 2021.

[7] S. A. Khowaja, P. Khuwaja, K. Dev, I. H. Lee, W. U. Khan, W. Wang, N. M. F. Qureshi, M. Magarini, A Secure Data Sharing Scheme in Community Segmented Vehicular Social Networks for 6G, *IEEE Transactions on Industrial Informatics*, Vol. 19, No. 1, pp. 890-899, January, 2023.

[8] H. Tan, An efficient IoT group association and data sharing mechanism in edge computing paradigm, *Cyber Security and Applications*, Vol. 1, Article No. 100003, December, 2023.

[9] D. Liu, Z. Li, C. Wang, Y. Ren, Enabling secure mutual authentication and storage checking in cloud-assisted IoT, *Mathematical Biosciences and Engineering*, Vol. 19, No. 11, pp. 11034-11046, August, 2022.

[10] S. Ji, Y. Yuan, J. Shen, C. F. Lai, B. Chen, An Efficient Three-Party Authentication and Key Agreement Protocol for Privacy-Preserving of IoT Devices in Mobile Edge Computing, *Journal of Internet Technology*, Vol. 23, No. 3, pp. 437-448, May, 2022.

[11] S. S. Satam, H. El-Ocla, Home Security System Using Wireless Sensors Network, *Wireless Personal Communications*, Vol. 125, No. 2, pp. 1185-1201, July, 2022.

[12] Z. Zhang, T. Yu, X. Ma, Y. Guan, P. Moll, L. Zhang, Sovereign: Self-contained Smart Home with Data-centric Network and Security, *IEEE Internet of Things Journal*, Vol. 9, No. 15, pp. 13808-13822, August, 2022.

[13] I. Antzoulis, M. M. Chowdhury, S. Latiff, IoT Security for Smart Home: Issues and Solutions, *IEEE International Conference on Electro Information Technology (eIT)*, Mankato, MN, USA, 2022, pp. 568-574.

[14] D. McAuley, J. Chen, T. Lodge, R. Mortier, S. Piasecki, D. A. Popescu, L. Urquhart, *Human-centred home network security*, March, 2022, https://arxiv.org/abs/2203.14109.

[15] E. Scott, S. Panda, G. Loukas, E. Panaousis, Optimising user security recommendations for AI-powered smart-homes, *2022 IEEE Conference on Dependable and Secure Computing (DSC)*, Edinburgh, UK, 2022, pp. 1-8.

[16] M. M. Pillai, A. Helberg, Improving Security in Smart Home Networks through user-defined device interaction rules, *IEEE AFRICON*, Arusha, Tanzania, 2021, pp. 1-6.

[17] S. Manandhar, K. Kafle, B. Andow, K. Singh, A. Nadkarni, Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage, *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, USA, 2022, pp. 3521-3538.

[18] U. M. Aïvodji, S. Gambs, A. Martin, IOTFLA: A secured and privacy-preserving smart home architecture implementing federated learning, *2019 IEEE Security*

and Privacy Workshops (SPW), San Francisco, CA, USA, 2019, pp. 175-180.

[19] H. Tan, D. Choi, P. Kim, S. Pan, I. Chung, An efficient hash-based RFID grouping authentication protocol providing missing tags detection, *Journal of Internet Technology*, Vol. 19, No. 2, pp. 481-488, March, 2018.

Biographies

Qingru Ma has received the B.E. degree from Nanjing Forestry University, Nanjing, China, in 2020. She is currently pursuing the Ph.D. degree at Zhejiang Sci-Tech University, Hangzhou, China. Her research interests include smart home security, and intelligent factory security.

Haowen Tan received the B.S. and M.S. degrees from Nanjing University of Information Science and Technology, China, in 2013 and 2016, respectively, and the Ph.D. degree from Chosun University, Korea, in 2020. He is currently working at Zhejiang Sci-Tech University, Hangzhou, China. His research interests include network security, and VANETs.