ECDSA-based Broadcast Authentication Scheme for Smart Home Environments

Dae-Hwi Lee, Im-Yeong Lee
Department of Computer Science and Engineering, Soonchunhyang University, Asan, Korea
leedh527@sch.ac.kr

***Abstract*— Recently, smart home has become the most important IoT service, consistent with the increased interest in IoT. The smart home service is connected with the user's residence and provides various life-friendly services. In a smart home environment, smart devices inside a smart home communicate with users through a home gateway. However, the security update for gateways and smart devices inside the smart home is not yet considered. It only provides security updates for user's smartphone applications. If there is no security for the security update message, the attacker will be able to access the smart home network by forging the message. In this paper, we propose a ECDSA-based broadcast authentication scheme to update message of service provider in smart home environments.**

***Index Terms*— Broadcast Authentication; IoT; Message Authentication; Smart Home.**

I. INTRODUCTION

As the IoT (Internet of Things) environment evolves, smart home becomes more integrated into our lives. In fact, many home appliances already have had internet addresses and maintained connections with one another. Smart home allows user to access smart home network through a smartphone application, and control home appliances and electronic products within the home from the outside. In smart home, communication is carried out using wireless communication technologies such as Z-wave, Zigbee, Bluetooth and WiFi. Although smart home has been commercialized, research in security of smart home is still lacking in this area. System hacking and personal privacy leakage have been identified as risk factors for security threats [1]. Most smart home services are not designed for security. In particular, the main security weaknesses in smart home are user authentication and message authentication. Further, the smart home has yet to provide security updates to its internal home gateways and smart devices. It only provides updates for the user's smartphone applications. If security vulnerability is detected within a smart home environment, security updates are essential for home gateways, smart devices, and smartphone applications. This indicates message authentication technology is required.

Figure 1: Structure of Smart Home

Therefore, in this paper, we propose a broadcast authentication scheme based on ECDSA, in order to transmit security update messages more securely and efficiently in smart home .

II. RELATED RESEARCHES

A. Broadcast Authentication

Broadcast authentication technology has been proposed to enable efficient message authentication in wireless sensor network environments [2,3]. Generally, to provide message authentication when a sender communicates with multiple recipients, the sender generates a message authentication code (MAC) for each recipient. A sender can use his/her respective keys to provide a certain degree of integrity. Broadcast authentication technology is a technique by which a sender can generate a message and MAC or signature, and send the same broadcast message to recipients, to maintain the message's integrity. This can greatly reduce the message computation on the sender's side, thus providing efficiency in environments, in which one sender and multiple receivers may communicate, such as wireless sensor networks or IoT environments. In a wireless sensor network or IoT environment, an attacker can easily inject malicious data such as malicious code into a message or change the contents of a message. Therefore, authentication mechanisms for messages are essential, and broadcast authentication is one such mechanism. If a sender do not have broadcast authentication, he/she should rely on 1:1 communication between devices.

There are three broad categories of broadcast authentication technologies. First, there is a symmetric-key-based broadcast authentication method in which a MAC is first transmitted and a key is delayed. Second, there is a one-time signature for a message and a message, and a broadcast authentication method based on an OTS (One-Time Signature). Finally, there is a broadcast authentication method using public key signatures.

TESLA is a typical broadcast authentication scheme proposed by transmitting MAC together. A. TESLA proposed by Perrig uses a method of transmitting a key and a message after a certain delay time after transmitting the MAC first. It is very simple to use as it only uses simple MAC. Although it requires additional time synchronization

with delay time, it is impossible to prevent non-repudiation. In recent years, the computation capabilities of devices and

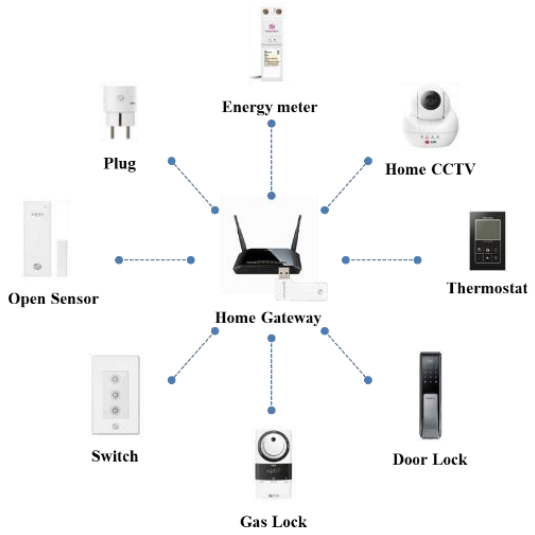

Figure 2: Smart Home Appliances

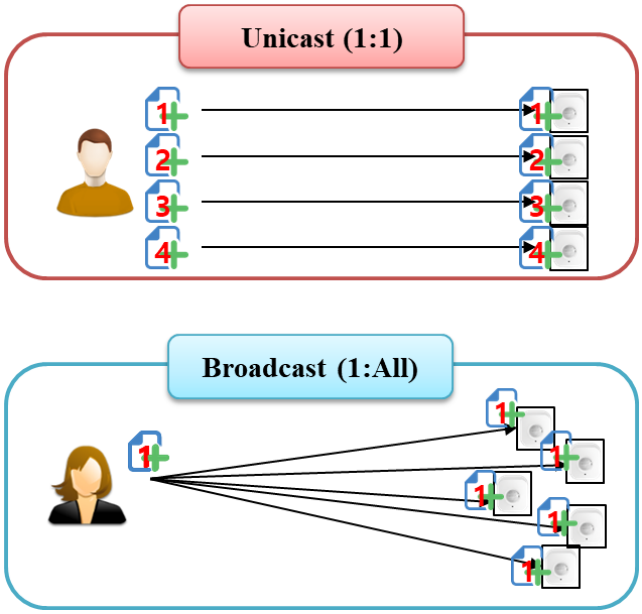

Figure 3: Unicast and Broadcast

sensors have increased, public authentication schemes as ECDSA based public key signatures have been proposed [4-8].

B. Existing Broadcast Authentication Schemes

Huang et al. proposed DREAM, a DSA - based broadcast authentication scheme. This scheme is designed to tolerate DoS attacks using forward-first and authentication-first policies. Each packet can be verified or delivered at each node, and the node that receives the packet supports multiple transmissions that can forward packets to other nodes. However, the sender authentication is not provided because only the signature of the message is verified, without the process of verifying that the sender of the packet is a participating member after receiving the packet. Therefore, there is a problem that the packet can be continuously retransmitted. [4]

Ren et al. proposed a Bloom-filter based Authentication Scheme (BAS) based on Certificate-based Authentication Scheme (CAS) and Direct-storage based Authentication Scheme (DAS). BAS using a counting bloom filter can perform sender authentication via a bloom filter. It is designed to reduce the communication overhead using a method of recovering from the signature without sending additional messages to the transport packet. In the IoT environment, devices with low memory capacity are difficult to apply because they are difficult to store Bloom filters [5].

Liu et al. proposed a broadcast authentication scheme based on ECDSA using a signature block and a message packet chain. However, this method does not provide authentication immediately because the entire message cannot be verified until all the message packets are received. In addition, since all packets must be received and stored, it causes a lot of overhead [6].

Shim et al. proposed EIBAS, a broadcast authentication scheme using ID-based signatures. When a signature and an ID including a part of a message are transmitted using an ID as a public key, the original message can be recovered from the signature and verified through the ID. It is designed to reduce the communication overhead by using the method of recovering the message from the signature similar to the method of Ren. However, since the receiver must store all the IDs of other network participants, the memory overhead is very large [7].

Xu et al. proposed a fast broadcast authentication scheme based on ECDSA to increase the computation speed in the Ren scheme. The basic structure such as the use of the counting bloom filter is similar to that of Ren, but the verification speed is reduced by efficient computational design. However, it is difficult to apply it to a lightweight device in an IoT environment as in the case of a Ren or the like [8].

III. Security Requirements

This section analyzes the security requirements for ECDSA-based broadcast authentication scheme design to provide authentication of alarm messages or update messages in a smart home environment. For a smart home environment, where various devices are connected, the broadcast authentication technology should provide integrity and prompt authentication, as well as provide user identification for valid sender identification. Additionally, it should have a small overhead for the IoT environment [9].

A. Message Integrity

Integrity must be provided to prevent tampering with security update messages sent at an updated time. If an attacker can tamper with the messages used in the communication, it can make the smart home a zombie PC by planting malicious code in the security update, or prevent normal operation.

B. Immediate Authentication

In IoT environments where immediate response is required, the latency of verification should be minimized. If a transmission of an alarm message to be transmitted is delayed in the event of an intrusion or fire in a home, this may cause a serious problem.

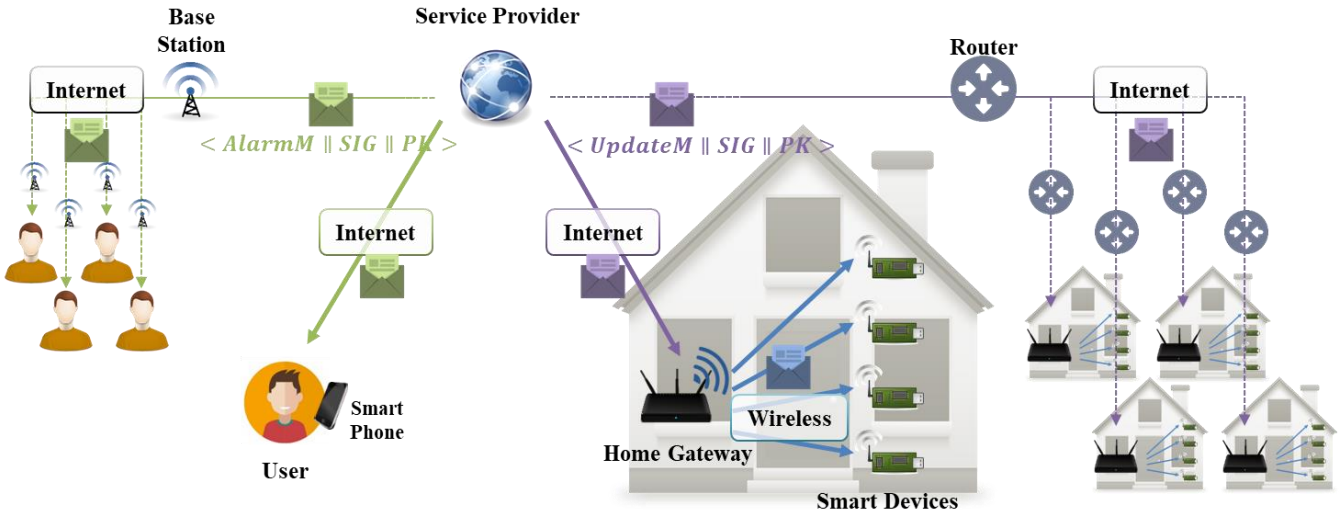

Figure 4: Message Transfer Scenario in Smart Home

C. Prevention of Replay Attack

When an alarm message or an update message is transmitted or received, an attacker can intercept data and disguise it as a legitimate message through a retransmission attack. Only legitimate user's mobile devices and legitimate smart devices need to be authenticated and designed so that they cannot be authenticated even if the attacker retransmits them.

D. Prevention of DoS Attack

Broadcast authentication should be considered safe for DoS attacks such as flooding and jamming. There are home gateways and smart devices that receive messages in a smart home. Because smart devices have very low computational complexity, they must have a DoS attack prevention function for such lightweight devices.

E. Source Authentication

It is very important to verify the identity of the sender to whom the message was sent. Only a legitimate user or service provider can generate a broadcast message and be able to adequately verify this.

F. Memory Overhead

Memory overhead occurs when the buffering time for a message is very long or when storage is used heavily. In a MAC-based broadcast authentication protocol such as TESLA, a message must be kept in the buffer for a long time for the key release delay. This can be addressed by providing authentication immediately and minimizing the size of messages and signatures for lightweight appliances.

IV. Proposed Scheme

The proposed method consists of 5 phases in total. The smart home service provider generates and publishes parameters for ECDSA and broadcast authentication at the Setup phase. In the Home gateway registration phase, the user's home gateway is registered in the service provider, and in the Smart device registration phase, the smart device is registered in the home gateway. In the Service provider message broadcast and authentication phase, the service provider broadcasts an update message to the home gateway, and the home gateway authenticates the message. In the Home gateway message broadcast and authentication phase, the home gateway broadcasts the message to the smart device and ends the authentication of the message.

A. System Parameters

· E : An elliptic curve over the finite field F_q
· P : An ECC point that generates the subgroup of order q
· PU_*, PR_* : Public key and private key pair of $*$
· s : Master secret key generated by service provider
· V_{SP} : Counting Bloom-filter between service provider and home gateways
· KC_G : Authentication keychain in smart home networks
· n : The overall size of the authentication keychain KC_G

B. Setup Phase

Step 1. The service provider generates an elliptic curve E on the finite field F_q, and select a generator P with a prime number p.

Step 2. The service provider randomly selects the master secret key s to generate its public key $PU_{SP} = sP$.

Step 3. The service provider publishes the system parameters $< E_q, E, p, P, PU_{SP} >$. Then, the counting bloom-filter V_{SP} is generated through the bit vector of $h(ID_{SP} \| PU_{SP})$.

C. Home Gateway Registration Phase

Step 1. The home gateway selects the private key PR_G and registers the public key $PU_G = PR_G \cdot P$ to register the service. The home gateway transmits the generated public key PU_G, together with the identifier ID_G, to the service provider.

Step 2. The service provider adds the bit vector of $h(ID_G \| PU_G)$ to the counting bloom-filter V_{SP} using the transmitted ID_G, PU_G.

Step 3. The service provider sends its identifier ID_{SP} and V_{SP} to the home gateway, which stores the received ID_{SP}, V_{SP}.

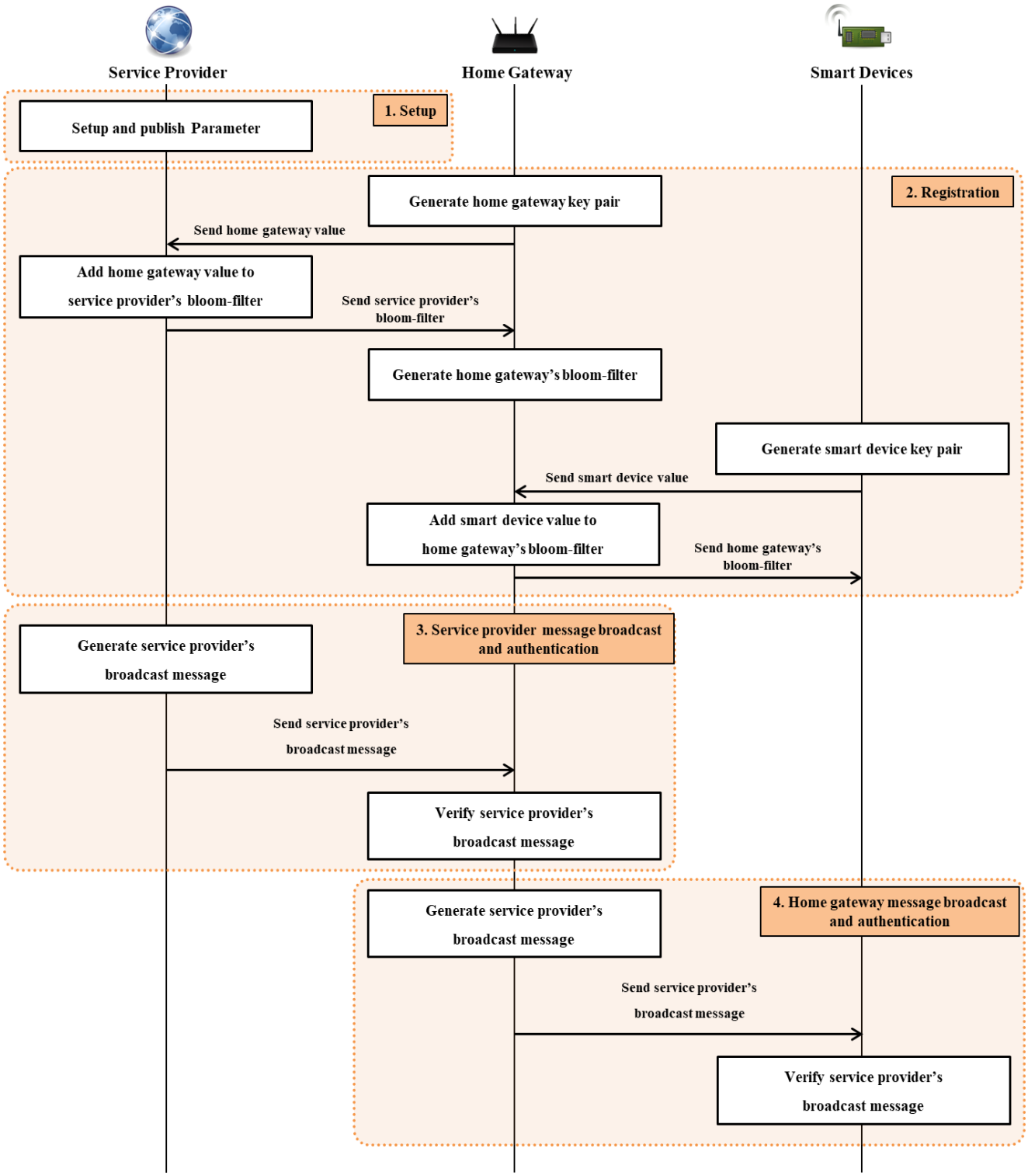

Figure 5: Structure of Proposed Scheme

Smart Device Registration Phase

Step 1. The smart device transmits its identifier ID_D to the home gateway for registration in the smart home.

Step 2. The home gateway selects an arbitrary R and generates a one-way authentication keychain $KC_G = \left(h^1(R), h^2(R), \dots, h^n(R)\right)$ according to the number n overall size of keychain.

Step 3. The home gateway sends ID_G, V_G, and $h^n(R)$ to the smart device, and stores the received value.

D. Service Provider Message Broadcast and Authentication Phase

Step 1. The service provider generates a time stamp tt_1 to transmit the message m_{SP}, and divides the message into the form $M_1 \parallel M_2 =< m_{SP} \parallel tt_1 \parallel ID_{SP} > (|M_1| \leq 10B)$.

Step 2. An arbitrary key pair (k, K) is generated, to be used for signature generation $(K = kP = (x_1, y_1),\ x_1\ mod\ q \neq 0)$.

Step 3. Redundancy is added to the modulo operation with modulus q to generate f_1.

Step 4. $c = I + f_1 \, mod \, q$ is computed by hashing K to integer I. Furthermore, $f_2 = h(M_2)$ is calculated using message M_2 to calculate $d = k - s(c + f_2) \, mod \, q$. Then, the signature σ_{SP} is $\sigma_{SP} = (c, d)$.

Step 5. The service provider generates a broadcast message $BM_{SP} =< M_2 \parallel \sigma_{SP} \parallel PU_{SP} \parallel tt_1 >$ and transmits it to the home gateway.

Step 6. The home gateway discards the message if tt_1 is invalid or $c, d = 0$ for authentication of BM_{SP}.

Step 7. It is confirmed that the bit vector of $h(ID_{SP} \parallel PU_{SP})$ is included in the counting bloom filter V_{SP} for identifying the service provider.

Step 8. After calculating $f_2 = h(M_2)$ for message recovery, the $X = dP + (c + f_2) \cdot PU_{SP} = (x_1', y_1')$ hash is calculated to convert to integer I.

Step 9. $f_1 = c - I \, mod \, q$ is calculated, redundancy checked, and M_1 recovered from f_1 if correct. Then, the entire message $M_1 \parallel M_2 =< m_{SP} \parallel tt_1 \parallel ID_{SP} >$ is restored.

E. Home Gateway Message Broadcast and Authentication Phase

Step 1. The home gateway extracts the message m_D from m_{SP}, to be transmitted to smart devices in the smart home.

Step 2. The home gateway generates a broadcast message $BM_G =< m_D \parallel h^{n-1}(R) \parallel ID_G \parallel tt_2 >$ and transmits it to the smart devices.

Step 3. The smart device receiving the BM_G checks the validity of the time stamp tt_2, and discards the message if it is invalid.

Step 4. After validating the time stamp, the smart device performs a hash operation once on the received $h^{n-1}(R)$ value and compares it with $h^n(R)$ that it has stored. If the values match, approve message m_D and store $h^{n-1}(R)$ for subsequent message verification. Finally, the smart device executes the message m_D.

V. ANALYSIS OF PROPOSED SCHEME

This section compares and analyzes existing schemes and proposed scheme, and confirms the six security requirements presented in Section 3 for the ECDSA based broadcast authentication scheme for smart home environment. Among them, the security requirements to be considered in the smart home environment are the prevention of replay attack, prevention of DoS attack, source authentication, and memory overhead.

A. Prevention of Replay Attack

In the proposed scheme, the service provider or the home gateway includes a time stamp in the broadcast message to prevent replay attack. This confirms time validity and prevents same message from being used after a certain period of time. The service provider can verify the validity of the message by using the ECDSA signature. In the home gateway, the message can be verified only at the corresponding stage through the key chain shared with the smart devices. Therefore, if an attacker intercepts an intermediate broadcast message and sends it to the home gateway or smart device, it cannot positively expose the message. In addition, the attacker cannot confirm the whole message because it is designed so that part of the message can be included in the signature in the process of signing the message with ECDSA so that it can be restored when verifying.

Table 1
Analysis of Proposed Scheme

	Y. Huang[4]	**K. Ren[5]**	**Y. Liu[6]**	**K.A. Shim[7]**	**J. Xu[8]**	**Proposed Scheme**
Base System	DSA	ECDSA	ECDSA	IBS	ECDSA	ECDSA
Message Structure	Message, Signature, Public Key	Partial Message, Signature, Public Key	EB_0(Signature) EB_i(Message Chain)	Signature, ID(Public Key)	Partial Message, Signature, Public Key	Partial Message, Signature, Public Key
Prevent Packet Loss (Integrity)	O	O	O	O	O	O
Prevent Replay Attack	X	O	O	O	O	O
Immediate Authentication	O	O	X	O	O	O
Support Multiple Transfers	O	X	X	X	X	O
Source Authentication	X	O Counting Bloom Filter	O Counting Bloom Filter	O ID-based Signature	O Counting Bloom Filter	O Counting Bloom Filter, Hash Chain
Memory Overhead	Low	Medium	High	High	Medium	GW: Medium Node Devices: Low

B. Prevention of DoS Attack

When a home gateway receives a broadcast message from someone, it verifies the time validity by checking the time stamp to prevent a replay attack. Then, the public key and the identifier included in the message are hash computed, and the result is retrieved from the counting bloom filter V_{SP} to confirm that the message sender is a legitimate service provider. In this case, since only one hash operation and bloom filter search operation are performed in the home gateway, the process of confirming that the sender is a legitimate sender is performed very quickly. In addition, since unnecessary operations are not performed, a DoS attack can be prevented. Likewise, a smart device can verify a time validation and perform a hash operation to verify and create an authentication keychain value, thereby preventing a DoS attack.

C. Source Authentication

As shown in the prevention of DoS attack, when a home gateway or a smart device receives a broadcast message, there is a process of checking who is transmitting the message. The home gateway identifies the value dependent on the sender's public key PU_{SP} and the identifier ID_{SP} in the counting bloom filter V_{SP}, and the smart device identifies the sender via the authentication keychain. For important messages such as update messages or emergency notifications, authentication to the sender is essential.

D. Memory Overhead

The smart home environment has been commercialized in the IoT environment. Nevertheless, there are smaller products such as wall outlets and gas valves that have lower computing power and memory capacity than large home appliances such as refrigerators and TVs. Since the home gateway can be supplied with sufficient power in the form of a router designed for a smart home, it is not a big problem to apply a security protocol having a high computational complexity. However, it provides efficiency in protocol design for smart devices such as small products. In the proposed scheme, communication is divided into service provider - home gateway, home gateway - smart device so that various security requirements can be satisfied.

VI. Conclusion

Due to the development of IoT, various services for IoT environment are being released, and security technology is continuously being developed. In particular, smart home is closely related to our daily lives, so if security is not taken into consideration, not only economic loss but also risk of injury may occur. In order to prevent this, it is necessary to authenticate the transmitted messages in the smart home, and it has been studied as a method of improving the broadcast message authentication technology used in the existing wireless sensor network environment according to the smart home environment. In this paper, an ECDSA-based broadcast authentication scheme is used to provide sender efficiency and update message integrity, thus aiding in forming a secure smart home environment. In particular, it is designed to prevent DoS attacks and reduce memory overhead so that it can work well in lightweight devices. Recently, public key signature-based broadcast authentication schemes using ECDSA have been studied in order to increase efficiency. In the future, it will be necessary to study authentication techniques that can reduce overhead while utilizing the public key signature scheme.

Acknowledgement

This research was supported by the MSIT(Ministry of Science, ICT), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2017-2015-0-00403) supervised by the IITP (Institute for Information & communications Technology Promotion).

References

[1] M. H. Kim and Y. T. Shin, "A Study on The Smart Home Service Security Threat," *Conference of the KICS*, pp. 1069-1070, 2016.

[2] D. H. Lee and I. Y. Lee, "ECDSA-based Broadcast Authentication Scheme for Smart Home Environments," *Conference of the APIC-IST*, 2017.

[3] A. Perrig, R. Canetti, J. D. Tygar and D. Song, "Efficient authentication and Signing of Multicast Streams Over Lossy Channels," *Security and Privacy*, 2000, pp. 56-73.

[4] Y. Huang, W. He and K. Nahrstedt, "DoS-resistant Broadcast Authentication Protocol with Low End-to-End Delay," *Presented in IEEE INFOCOM Workshops*, 2008.

[5] K. Ren, S. Yu, W. Lou and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 8, 2009, pp. 4554-4564.

[6] Y. Liu, J. Li and M. Guizani, "PKC based Broadcast Authentication using Signature Amortization for WSNs," *IEEE Transactions on Wireless Communications*, Vol. 11, 2012, pp.2106–2115.

[7] K. Shim, Y. Lee and C. Park, "EIBAS: an Efficient Identity-based Broadcast Authentication Scheme in Wireless Sensor Networks," *Ad Hoc Networks*, Vol. 11, 2012, pp.182-189.

[8] J. Xu and L. Dang, "Multi-User Broadcast Authentication Protocol in Wireless Sensor Networks against DoS Attack," *The Open Cybernetics & Systemics Journal*, Vol. 8, 2014, pp. 944-950.

[9] K. Grover and A. Lim, "A Survey of Broadcast Authentication Schemes for Wireless Networks," *Ad Hoc Networks*, Vol. 24, 2015, pp.288-316.