

A Secure Multimedia System in Emerging Wireless Home Networks

Nut Taesombut, Richard Huang, and Venkat P. Rangan

Department of Computer Science and Engineering
University of California, San Diego
La Jolla, CA 92093-0114, USA
{ntaesomb,ryhuang,venkat}@cs.ucsd.edu

Abstract. With their availability of high-bandwidth and extensive transmission range, Wireless Local Area Networks (WLANs) become a compelling technology for developing next-generation home entertainment systems. In the near future, home multimedia systems will rely on wireless networks in lieu of typical wired networks in interconnecting media appliances. Wireless connectivity will enable many novel and advanced features to entertain and comfort a home user. However, before systems are viable and widely acceptable, there are security and copyright protection problems that need to be addressed. Since the system relies on wireless communication, privacy of streaming media content becomes a great concern among media content owners and legitimate consumers who wish to protect their intellectual property against illegal use. In this paper, we present a gateway-based architecture for secure wireless home multimedia systems. We have developed a protocol to ensure secure bootstrap registration of new media devices and protect communication within a wireless home network. We have built the system prototype to evaluate the timing overhead of the device registration process and identify the bottleneck.

1 Introduction

In the past, the lack of high speed and broad transmission range was a main obstacle that hindered the widespread deployment of wireless communication technologies. With an advanced “third generation” (3G) mobile phone, a user can exchange only non-bursty-traffic information, such as a voice, a small image and a short video clip. Nonetheless, the recent advancements in the IEEE 802.11 standard [1] yield a new paradigm for considerably higher bandwidth communication over a wireless medium. As a consequence, multimedia streaming which generally requires a bandwidth up to several megabits per second becomes feasible in a wireless network. Such advanced wireless technology has catalyzed the development of digital multimedia systems for homes and small enterprises today. It allows media appliances and conventional computers to communicate with each other using a radio signal rather than through a wired cable. One key advantage of adopting WLAN in implementing multimedia systems over

its wired counterpart is that all wiring difficulty during system installation and adjustment can be eliminated. Furthermore, a device can be relocated unrestrictedly and seamlessly within the wireless network, thus allowing more flexibility and convenience for a user to use the system. In the near future, WLANs are expected to increasingly replace wired networks in interconnecting media appliances in homes and small workplaces. We envision next-generation home entertainment systems built from off-the-shelf media devices that can be automatically recognized by the system (plug and play) and communicate with each other wirelessly.

The Internet has revolutionized the way digital media content is produced, distributed and consumed. Varying kinds of media content, such as movies and songs, are now available online and can be delivered to home users at low cost. Nevertheless, not all media content are available for public consumption; some are for sale or controlled by other restriction rules. In a wireless network, which relies on a broadcast medium, one can easily intercept streaming media content from a network neighborhood and illegally forward it to his display device. Due to the digital nature of today's media content, once compromised, unlimited number of copies can be made and redistributed. This has posed a great concern to media content owners who wish to protect their intellectual property against online piracy. Therefore, to make such wireless home multimedia systems viable, there are significant digital media content protection and security challenges that need to be addressed.

It has been shown that a wireless network based on the IEEE 802.11 standard is untrustworthy. Even though there are a few techniques that provide authentication, privacy and access control in wireless LANs [1,2], in practice these security mechanisms are ineffective and usually not enabled by default. In addition, several flaws have been found in the design and implementation of WLAN [3,4,5]. A smart attacker can eavesdrop an on-going communication in, obtain an unauthorized access from, and inject a bogus message into the wireless network. For this reason, the existing security mechanisms should not be counted on to provide a reliable communication in WLAN.

In this paper, we present a gateway-based architecture of the wireless home media network and develop a secure registration protocol for it. The primary goal of our proposed architecture is to secure a wireless home network as well as facilitate digital rights management (DRM) for media content protection. The protocol aims to ensure secure bootstrap registration of new media appliances. It provides mechanisms for mutual authentication and trust establishment between media appliances and a home gateway. At the end of the protocol, session keys will be generated and distributed to the participating gateway and media appliance. We demonstrate an application of these keys with a lightweight video encryption algorithm to encrypt video streams. The major challenge in the design and implementation of the system is the resource constraints of a lightweight media appliance. A media appliance, such as TV and DVD player, generally has limited processing capabilities and memory resources. We overcome such limitations by avoiding computationally expensive operations at a

media appliance. We expect our full-fledged system to provide a strong security and content protection guarantee for wireless home multimedia networks.

The remainder of this paper is organized as follows: In Section 2, we describe the gateway-based architecture of the wireless multimedia system followed by its components and advantages. In Section 3, we present the secure registration protocol and its security analysis. In Section 4, we illustrate an application of the generated session keys to protect the privacy of digital video. In Section 5, we present the system prototype built to evaluate the performance of the device registration process. In Section 6, we discuss the future work and conclude the paper.

2 Wireless Home Multimedia System

This section presents a gateway-based architecture of the wireless home media network. The proposed architecture is illustrated in Figure 1. The secure multimedia system can be viewed as two connected networks: (1) a wireless home network and (2) a wired global network. All communication across these two networks is managed through a master gateway. The wireless home network is based on the WLAN technology. It provides a hosting environment to media appliances (e.g. TVs, DVD players and speakers). As communication within WLAN is untrustworthy, when a media appliance first emerges in the network it does not trust any other device. On the other hand, the wired global network is the well-known Internet in which an authentication server and media content providers reside. In contrast to that in WLAN, any communication between two parties in the Internet is assumed to be trusted using SSL. The rest of this section will describe the system components and the advantages of the gateway-based approach.

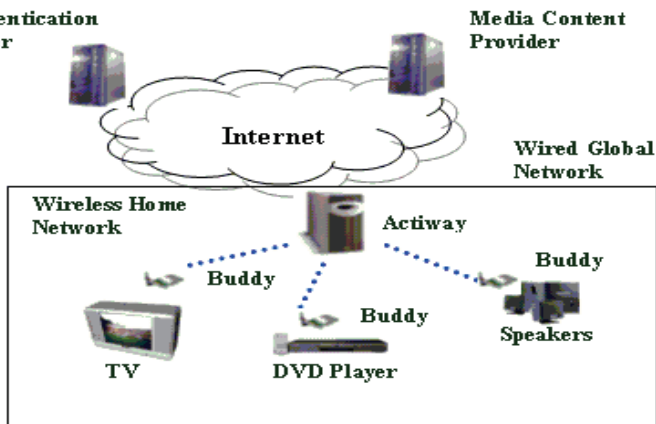


Fig. 1. Architecture of Wireless Home Multimedia System

2.1 System Components

The wireless home multimedia system comprises of four main components: namely (1) media device; (2) active gateway; (3) media content provider; and (4) authentication server. The detail of each component is given in this section.

Media Device. Each media appliance connects to the home WLAN through a lightweight interface called *Buddy* [6]. The buddy is equipped with an encoder and/or decoder that corresponds to the media types that the device is capable of playing. However, as the buddy is designed to be a simple and inexpensive attachment, it does not include any user interface and cannot perform processing-intensive cryptographic operations. For convenience, a media appliance together with its buddy will be referred to as a *media device*.

Active Gateway. A master gateway called *Actiway* (*Active gateway*) is a resourceful gateway located between the wireless home network and the Internet. Connectivity to the Internet via the gateway allows media content providers to deliver media content to remote devices. The gateway maintains a record of all the devices owned by the user, enforces access control and copyrights policy as well as mediates communication among media devices. Since the system aims to support varying kinds of media devices, many of which may have their specific data formats, the gateway also functions as a media switch, capable of performing necessary media type conversion and streaming media content from multiple sources to multiple playback devices.

Media Content Provider. A media content provider is a storage server that contains multimedia presentations, such as movies, songs, etc. These documents can be accessed from a media device in the wireless home network. If the media content is available for public consumption, a home user can download the content via the gateway to his display device and replay it many times. On the other hand, a user may be required to pay for the content before he can get access to it.

Authentication Server. An authentication server (or AS) is a trusted server and may be specific to device manufacturer. It maintains a secured database that contains a unique ID, embedded keys and an access key of each genuinely manufactured device. When the device first emerges in the network, the device and gateway do not trust each other. The AS mediates the establishment of trust and a secure channel between them.

2.2 System Advantages

We have chosen to use the gateway-based architecture for the wireless home multimedia system. In this architecture, the gateway is a master controller over all media devices in the wireless home network. This section summarizes the benefits resulting from using the gateway-based approach.

Media Switching. In a multimedia-based network, communicating information is inherently media content. Multiple media sources can simultaneously deliver media content to multiple media sinks. With the gateway as a central media switch, media content can be appropriately forwarded to media sinks and conversion between different types of media format can be efficiently managed.

Media Synchronization. When a media source streams media content to more than one media sink, the emergence of asynchrony among the different media sinks is imminent due to an unreliable nature of a wireless network. The gateway can perform as a conductor to ensure synchrony over all media sinks. Using adaptive feedback techniques for media synchronization and continuity as described in [7], the media sinks can periodically send synchronization information back to the gateway and the gateway can use this information to dynamically adapt media streaming rate appropriate for individual media sink.

Centralized Access Control. As an access controller, the gateway controls which media devices can enter the wireless network and participate in the home multimedia system. All communication between media devices and other machines in the Internet and among the devices themselves in the home network must be through the gateway. A device will not be allowed to communicate with any other device in the system unless it can properly identify and prove itself as trusted (authentic) one.

Digital Rights Management. The gateway-based architecture of the wireless home multimedia system facilitates the concept of Digital Rights Management (DRM). Instead of streaming media content to (possibly dishonest) media devices directly, the media content provider delivers the content through the gateway. The gateway can enforce media rights policies provided by a media content provider. The protected media content are buffered at the gateway and then forwarded to the media device in a manner corresponding to the restriction rule. The gateway ensures that the content will never be copied or distributed illegally.

3 Secure Registration Protocol

In this section, we present the Secure Registration Protocol (SRP) for the wireless home multimedia system. Here, we provide only an overview of the protocol. The detailed description can be found in our previous paper [8]. The primary goals of the protocol are to provide a secure bootstrap registration for a new media device and to establish a secure communication channel between the device and the home gateway.

3.1 Protocol Overview

We now present a high-level description of the protocol. Figure 2 illustrates all messages exchanged in the protocol¹. There are three main stages in the protocol as summarily described below.

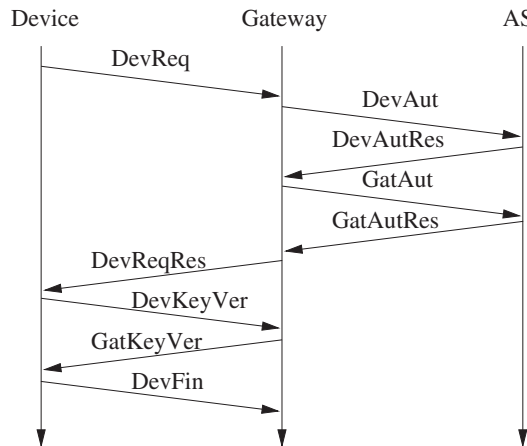


Fig. 2. Secure Registration Protocol

Authentication of Media Device to Authentication Server. The device needs to identify and authenticate itself to the authentication server in order to show that it is genuine. When manufactured, the device is associated with a globally unique ID (*DeviceID*) and embedded with two secret keys (*KE, KMAC*) – the former is used as a key for encryption functions and the later is used a key for message authentication code (MAC) generation functions. These keys are known only to the device itself and the authentication server. Therefore, to authenticate, the device creates a new request message, called *DevReq*, with HMAC record signed by *KMAC* and broadcasts it over the WLAN to the gateway. The gateway then copies all information in the received message together with its *GatewayID* into a new message, called *DevAut*, and forwards it to the authentication server via a secure channel. Since the authentication server also knows *KMAC*, it can check whether the device is authentic by re-computing the HMAC record. If both HMACs match, the authentication server accepts and trusts the device. The server then notifies the gateway with *DevAutRes* that the device can be trusted.

¹ See Appendix for the detailed message format and the notations we use.

Authentication of Gateway to Authentication Server. The gateway also has to prove itself to the authentication server that it is authorized to control the device. At the time of purchase, the user will be given a device together with its *access key*². The user can delegate his access rights to the device to the gateway by entering the access key into the gateway. The gateway sends the hashed value of the access key as a certificate in *GatAut* to the authentication server.

Session Key Distribution. If the access key is valid and the corresponding device has never been associated with any other gateway, the authentication server associates the device with the requesting gateway. The server then grants a ticket³ to the gateway in the *GatAutRes* message. Next, the authentication server generates a master key and securely distributes it to the device and gateway (via *GatAutRes* and *DevReqRes* messages). At this point, both the device and gateway use the master key to generate two session keys (*SKE, SKMAC*) with which they will use to establish a secure communication channel. However, before they start the secure session, they need to verify that their derived keys are matched (with *DevKeyVer*, *GatKeyVer* and *DevFin* messages).

3.2 Protocol Analysis and Security Considerations

The goals of the protocol and the secure system are security of a wireless network and copyright protection of communicating media content. This section shows how these security properties can be achieved.

Preventing Unauthorized Devices from Entering a Home Network. If an unauthorized device attempts to connect to a home network, it needs to supply the authentication server with its private KMAC key that has not been previously associated with any other gateway. Since this key is securely embedded with the device and has never been exposed, it could not be compromised. In addition, the user needs to supply a device's access key in the authentication process. If an unauthorized device requests to join the network, the user can observe the emergence of this device from the gateway's user interface. Either of these processes will fail for an unauthorized device.

Preventing Eavesdropping and Message Forgery over Device-Gateway Communication. Following a successful registration, all communication between device and gateway is either encrypted or noise-modulated with *SKE* that is generated from the confidential master key known only to the gateway, the participating device and the authentication server. Without knowledge of this key, an attacker cannot derive any intelligible information from an obscured

² The access key is a credential that its possessor can claim as a rightful controller of the device.

³ Possession of the ticket proves to the device that the gateway is authorized to control the device. See M_2 in Table 4 for the detail of the ticket.

communication in the wireless home network. To verify the integrity of messages transmitted over the wireless home network and the identity of its sender, every message is attached with HMAC digest generated using the secret key *SKMAC*. Unless this digest is valid, the received message is rejected and discarded. Therefore, an attacker cannot impersonate a trusted entity or inject a counterfeit message into the home network.

4 Lightweight Video Encryption

At the end of the SRP protocol, session keys (*SKE*, *SKMAC*) are generated and distributed to the device and the gateway. These session keys will be used to establish a secure communication path between the two parties, which guarantees communication privacy and message authentication. This section presents an application of the session keys, a lightweight video encryption which appropriate for resource-constrained devices.

4.1 Background

MPEG (Moving Picture Experts Group) standards, including MPEG-1, MPEG-2, MPEG-4, and MPEG-7, are widely used in multimedia applications. MPEG standards consist of three parts: audio, video, and the interleaving of the two streams. In this paper, we consider MPEG-1 video, although similar operations can be applied to the other MPEG models.

An MPEG sequence consists of units called Group Of Pictures (GOPs). Each GOP contains I (intracoded) frames, P (predicted) frames, and B (bidirectionally-predicted) frames. Motion estimation in MPEG operates on Macroblocks. We're interested in the intracoded macroblocks. They can occur in P and B frames in addition to I frames. This is important because some selective methods encrypt only the I frames, but leaves I blocks in P and B frames unencrypted. This is not sufficiently effective because I blocks usually contain the most important aspect of a frame.

4.2 Lightweight Video Encryption

By making the observation that P and B frames are interpolated from I frames, we decided to encrypt only I frames with the 128 bit session keys. We experimented with encrypting a combination of Y, U, and V blocks. Encrypting any of Y, U, or V blocks by itself does not fully make the frames unrecognizable. Encrypting Y and one of U or V is sufficient to result in an unrecognizable picture. Our lightweight video encryption works by applying DES to the AC components of the Y and V blocks of the I frames. However, to provide a higher level security, we can optionally encrypt the I blocks within the P and B frames. Another possibility would be to encrypt only I blocks in all frames. Figure 3 shows the result of encrypting.

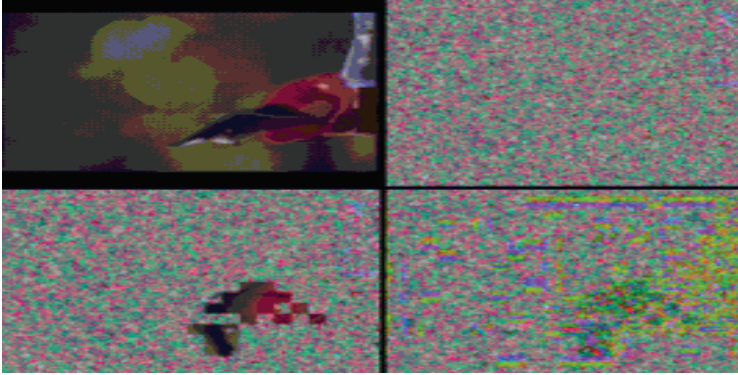


Fig. 3. From upper-left to bottom right, unencrypted I frame, encrypted I frame, P frame from encrypted I frame and unencrypted I blocks, and P frame from encrypted I frame and encrypted I blocks

5 System Prototype

This section focuses on the system prototype we have built to demonstrate the potential of the proposed architecture. We give an overview of the prototype and present its implementation. Here, we also describe the experiment we performed to evaluate the performance of the device registration process.

5.1 Implementation

The main objective of implementing the prototype is to illustrate and evaluate the secure device registration process of the system. Figure 4 shows the physical structure of the prototype.

As can be seen, the prototype consists of a media device, a gateway, an authentication server and a wireless access point. The gateway, the authentication server and the access point are connected through a 10 Mbits/sec speed LAN, while the media device connects to the access point via a 11 Mbits/sec speed WLAN. The system specification is as follows: the media device is a 500 MHz Pentium III Dell Inspiron 7500 with 192 MB RAM and a Lucent WaveLan 10/100 PC card; the gateway is a 1.8 GHz Pentium 4 Sony PCG-GRS100P with 512 MB RAM and a Inter(R) PRO/100 VE Network Connector card; and the authentication server is a 800 MHz Celeron HP desktop with 128 RAM and a Linksys NC100 Fast Ethernet adapter. All machines operated on RedHat 8.0 with kernel version 2.4.18-14 and all processes were written in GNU C. The authentication server had a database management system (DBMS) running on it. The DBMS we used is MySQL version 3.23 (www.mysql.com). The database stored records of each genuinely manufactured device comprising of *DeviceID*, embedded secret keys and the current value of device counter. The SSL and cryptographic library is the OpenSSL library version 0.9.7 (www.openssl.org). The

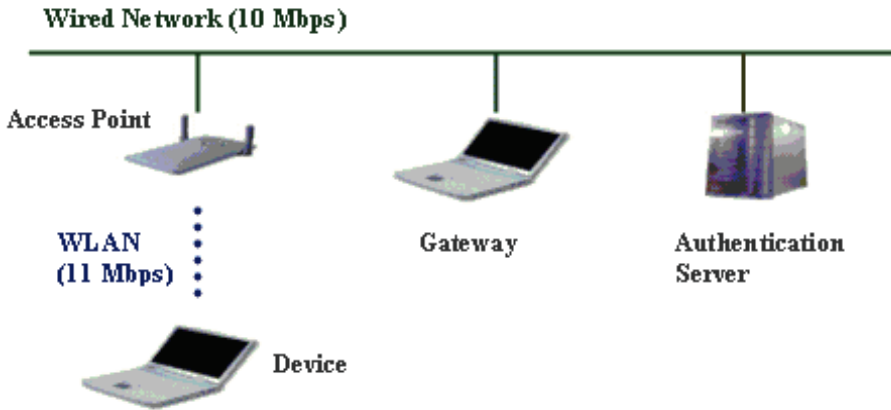


Fig. 4. System Prototype

key-hashing function and the symmetric key encryptions we used are HMAC [9] and AES [10] respectively.

5.2 Performance of Secure Registration Process

We used the setup as described above to perform an experiment. The main goal of the experiment is to measure the timing overhead of the secure registration process of the system and to identify the bottleneck. The overhead includes the processing time of the process at each device and the communication time among them.

The experiment we performed is as described below: Initially, the gateway had established a secure communication with the authentication server using SSL and it was listening for a new request from the device. We then started running the device process. We measured the total elapsed time in the secure registration process starting from the time the device sent the *DevReq* message until when the gateway received the *DevFin* message. Note that during the time the experiment was performed no other nodes were active. Therefore, we assume that there is no interference with our experimental results.

Table 1 shows the average elapsed time for the secure registration process to complete. The total elapsed time for the entire process is approximately 303.6 msec. As can be seen, the communication time dominates the processing time, accounting for 96.5 percent of the total elapsed time. Specifically, most of the communication time was spent in the conversation between the gateway and the authentication server (230.6 msec), as compared to that between the device and the gateway (62.5 msec).

Next we consider the processing-time overhead of the secure registration process. Unfortunately, due to our resource limitations, the machines we used to perform the experiment had different processing capabilities. The gateway

Table 1. Average elapsed time for SRP protocol

	Time(msec)
Total elapsed time	303.6
Processing time	10.5
- at device	1.0
- at gateway	2.0
- at auth server	7.5
Communication time	293.1
- between device and gateway	62.5
- between gateway and auth server	230.6

Table 2. Processing time for each category of operations at the device

	Time(msec)
Key-hashing function (HMAC)	0.5
Encryption function	0.1
Other operations	0.4

process, which was run on the fastest machine (1.8 GHz), would take longer time to finish when it was run on the other machines in the experiment. Nonetheless, as can be observed in Table 1, the process at the authentication server incurs the highest overhead. From our detailed analysis, this was a consequence of the time for the AS process to make a query to the database system.

In our experiment, we were specifically interested in the processing-time overhead at the media device since in practice only the device would have limited processing resources. Table 2 shows the processing time of each category of operations executed at the device. As we expected, the types of operations that dominated the others were cryptographic operations, including keyed-hashing functions and symmetric key encryptions. Although such operations are computationally expensive, they are required for our system to meet its security goals. In fact, the processing-time overhead would have been much higher, if we instead used public key encryptions and digital signatures.

Since the communication time results in the largest portion of the total elapsed time, minimizing the number of exchanged messages would greatly reduce the timing overhead. It is possible to combine the device authentication process and the gateway authentication process by merging the *DevAut* and *GatAut* and sending them together. Another possibility of optimization is to start performing session key verification process at the gateway rather than at the device. The gateway can generate a random number, encrypt it and send the outcome with the *DevReqRes* message to challenge the device. Only two additional messages (*DevKeyVer* and *GatKeyVer*) are required to complete the entire verification process and the protocol. As a result, one roundtrip time be-

tween the gateway and the authentication server and one-trip time between the device and the gateway can be eliminated.

6 Conclusion and Future Work

We have presented the design and implementation of our gateway-based architecture that aims to secure a communication in wireless home networks and protect digital media content from online piracy. A major service provided by the system is a secure registration where new media devices can be securely registered at the master gateway. In addition, we have developed the system prototype and performed the experiment to investigate the timing overhead of the registration process. The results we got are promising; it takes approximately 0.3 second to complete the entire registration process and the processing resource used at the device is minimized.

The next step of our project is to design and implement a lightweight communication protocol suitable for other multimedia-based applications and apply the Digital Rights Management (DRM) technology to our prototype.

References

1. L.M.S.C. of the IEEE Computer Society: Wireless LAN Medium Access Control. IEEE Standard 802.11, 1999.
2. Lucent Orinoco: User's Guide for the ORiNOCO Manager's Suite, November 2000.
3. W. A. Arbaugh, N. Shankar, and Y. J. Wan: Your 802.11 Wireless Network Has No Clothes, <http://www.cs.umd.edu/waa/wireless.pdf>.
4. J. Walker: Unsafe at Any Key Size: Analysis of the WEP Encapsulation. Technical Report 03628E, 802.11 Committee, March 2002.
5. Intercepting Mobile Communications: The Insecurity of 802.11. in Proceedings of the 7th Conference on Mobile Computing and Networking, March 2002.
6. I. Ramani, R. Bharadwaja, and P. V. Rangan: Location Tracking for Media Appliances in Wireless Home Networks. in Proceedings of the IEEE International Conference on Multimedia and Expo (ICME'03), July 2003.
7. S. Ramanathan and P. V. Rangan: Adaptive Feedback Techniques for Synchronized Multimedia Retrieval over Integrated Networks. in IEEE/ACM Transaction on Networking, 1993.
8. N. Taesombut, V. Kumar, R. Dubey, and P. V. Rangan: A Secure Registration Protocol for Media Appliances in Wireless Home Networks: in Proceedings of the IEEE International Conference on Multimedia and Expo (ICME'03), July 2003.
9. M. Bellare, R. Canetti, and H. Krawczyk: Message Authentication Code Using Hash Functions: The HMAC Construction. in Proceedings of the 23rd International Cryptology Conference (CRYPTO'96), March 1996.
10. J. Daemen and V. Rijmen: AES Proposal: Rijindael. in Proceedings of the 1st AES Conference, August 1998.

Appendix

Table 3 shows all notations and terms used in the paper and Table 4 illustrates the detailed format of the messages involved in the secure registration protocol.

Table 3. Notations and terms used in the paper.

M_1, M_2	Concatenation of two messages M_1 and M_2
$DeviceID$	Device's identification
$GatewayID$	Gateway's identification
N	Random number for key verification
$Dcount$	Counter maintained by device
$Scount1, Scount2$	Two separate counters maintained by authentication server
$AccKey$	Device's access key
$MasterKey$	Master key
KE	Embedded key for encryption function shared between device and authentication server
$KMAC$	Embedded key for HMAC function shared between device and authentication server
SKE	Session key for encryption function shared between device and gateway
$SKMAC$	Session key for HMAC function shared between device and gateway
$HMAC_k()$	Keyed-hashing function for message authentication code using key k
$H()$	One way hashing function
$E_k()$	Encryption function using key k
$DevAcc$	Pre-determined number indicating that the device authentication is successful
$GateAcc$	Pre-determined number indicating that the gateway authentication is successful
$Finish$	Pre-determined number indicating that the protocol is complete

Table 4. Detail of messages exchanged in the SRP protocol.

$DevReq$ (Device \rightarrow Gateway)	$M_1, HMAC_{KMAC}(M_1)$ where $M_1 = DeviceID, Dcount$
$DevAut$ (Gateway \rightarrow AS)	$GatewayID, M_1, HMAC_{KMAC}(M_1)$
$DevAutRes$ (AS \rightarrow Gateway)	$DevAcc, GatewayID, DeviceID, Scount1$
$GatAut$ (Gateway \rightarrow AS)	$GatewayID, DeviceID, Scount1, h(AccKey, Scount1)$
$GatAutRes$ (AS \rightarrow Gateway)	$GateAcc, M_2, MasterKey, HMAC_{KMAC}(M_2)$ where $M_2 = GatewayID, DeviceID, E_{KE}(MasterKey), Scount2, Dcount$
$DevReqRes$ (Gateway \rightarrow Device)	$M_2, HMAC_{KMAC}(M_2)$
$DevKeyVer$ (Device \rightarrow Gateway)	$M_3, HMAC_{SKMAC}(M_3)$ where $M_3 = GatewayID, DeviceID, E_{SKE}(N)$
$GatKeyVer$ (Gateway \rightarrow Device)	$M_4, HMAC_{SKMAC}(M_4)$ where $M_4 = GatewayID, DeviceID, E_{SKE}(N - 1)$
$DevFin$ (Device \rightarrow Gateway)	$M_5, HMAC_{SKMAC}(M_5)$ where $M_5 = Finish, DeviceID, GatewayID$