symmetry

MDPI

Article

Design of a Symmetry Protocol for the Efficient Operation of IP Cameras in the IoT Environment

Jaeseung Lee [1], Jungho Kang [2], Moon-seog Jun [1] and Jaekyung Han [3,*]

[1] Department of Computer Science and Engineering, Soongsil University, Seoul 07027, Korea; ljs0322@ssu.ac.kr (J.L.); mjun@ssu.ac.kr (M.-s.J.)
[2] Department of Information Security, Baewha Women's University, Seoul 03039, Korea; kjh7548@naver.com
[3] Department of Construction Legal Affairs, The Graduate School of Construction Legal Affairs, Kwangwoon University, Seoul 01890, Korea
* Correspondence: hjk1014@kw.ac.kr; Tel.: +82-29-405-788

Received: 8 January 2019; Accepted: 28 February 2019; Published: 11 March 2019

Abstract: The rapid development of Internet technology and the spread of various smart devices have enabled the creation of a convenient environment used by people all around the world. It has become increasingly popular, with the technology known as the Internet of Things (IoT). However, both the development and proliferation of IoT technology have caused various problems such as personal information leakage and privacy violations due to attacks by hackers. Furthermore, countless devices are connected to the network in the sense that all things are connected to the Internet, and network attacks that have thus far been exploited in the existing PC environment are now also occurring frequently in the IoT environment. In fact, there have been many security incidents such as DDoS attacks involving the hacking of IP cameras, which are typical IoT devices, leakages of personal information and the monitoring of numerous persons without their consent. While attacks in the existing Internet environment were PC-based, we have confirmed that various smart devices used in the IoT environment—such as IP cameras and tablets—can be utilized and exploited for attacks on the network. Even though it is necessary to apply security solutions to IoT devices in order to prevent potential problems in the IoT environment, it is difficult to install and execute security solutions due to the inherent features of small devices with limited memory space and computational power in this aforementioned IoT environment, and it is also difficult to protect certificates and encryption keys due to easy physical access. Accordingly, this paper examines potential security threats in the IoT environment and proposes a security design and the development of an intelligent security framework designed to prevent them. The results of the performance evaluation of this study confirm that the proposed protocol is able to cope with various security threats in the network. Furthermore, from the perspective of energy efficiency, it was also possible to confirm that the proposed protocol is superior to other cryptographic protocols. Thus, it is expected to be effective if applied to the IoT environment.

Keywords: IP camera; IP camera security; NVR security; video security

1. Introduction

As Internet technology has developed rapidly, and its penetration rate has increased greatly in recent years, the Internet environment now has a closer relationship with humans, and technology related with the so-called Internet of Things (IoT) is becoming increasingly widespread. However, as IoT technology develops and demand for it increases, various types of security incidents are taking place due to exploitation of the growing number of security vulnerabilities.

As the meaning of the IoT implies, the more devices that are connected to the network, the greater the number of network-based security attacks. Furthermore, the application of existing security solutions such as vaccines and firewalls—hitherto applied to PCs, servers and networks—to the IoT environment, has raised awareness of several limitations. Consequently, there is a growing need for device security that fits the IoT environment. As an example of a major security incident, numerous IoT devices were infected and exploited by a large-scale DDoS attack on the Internet domain service provider Dyn, which for several hours made it impossible to access dozens of popular websites such as The New York Times, Twitter, Netflix, and Amazon. The DDoS attack is not a new type of attack, but it is one that has been used most frequently to exploit and abuse the existing PC environment by attacking and infecting PCs beforehand and then exploiting them. By examining cases of such attacks, it was possible to confirm that smart devices used in the IoT environment, including DVRs, tablets, CCTVs (Closed Circuit Televisions) and other everyday smart devices, can be used for network attacks [1,2]. In addition, IoT devices connected to Internet Explorer can be hacked and exploited for attacks. A recent example of this attack was identified by Imperva, a company dedicated to security [3]. The attack was found to be a traditional HTTP flaw attack used in attacks on the Internet environment of existing PCs, which aimed to overload resources on the cloud service. However, what is particularly noteworthy about this attack is that it came from an IP camera rather than a traditional computer botnet. Imperva explained that this attack made up to 20,000 requests per second by exploiting about 900 CCTV cameras, using the embedded version of Linux and the BusyBox toolkit [4,5]. The attackers exploited the software vulnerabilities and the social engineering methods used to infect computers for attacks in the existing environment, but this attack was performed in an environment that could be attacked easily by accessing the Internet through Telnet and SSL [6]. Also, to attack the IoT devices, "root" and "admin", and "admin" and "password" were mainly used as the ID and password combinations, respectively. These combinations could be used to exploit the fact that the product default values had not been changed. In order to prevent the problems that can occur in the IoT environment, it is necessary to apply a security solution to the devices, but the situation is not easy to handle. In the IoT environment, it is difficult to install and execute security solutions due to the features of small devices with limited memory space and computational power, and it is also difficult to protect certificates and encryption keys due to easy physical access [7]. Therefore, in this paper, we discuss the trends and security problems of IP cameras used in the above cases in the IoT environment, and propose a secure method of communication by configuring the NVR network security design system.

2. Related Works

2.1. Internet of Things

The "Internet of Things" refers to intelligent technologies and services that can connect innumerable devices scattered widely across different areas to a single network to facilitate the exchange of information through communication. The technological concept that enables autonomous communication between humans and objects, as well as between objects, through human intervention, and provides services by analyzing the surrounding environment, is considered to be the leading technology of the digital revolution.

Since Kevin Ashton, the founder of the MIT Auto-ID Center, proposed both the concept of the IOT and the term itself in 1999, it has been undergoing continuous development and it now easy to encounter the IoT as many devices and services which have been developed accordingly.

Currently there is a wide range of IT products that use the IoT in the market. The IP camera field, which is the environment proposed in this paper, and many IoT services and devices are under development with a view to applying IOT technology in the fields of crime and disaster prevention. Objects must be able to communicate with each other in such an environment, and machine-to-machine communication is the base technology that supports such interaction.

However, most IoT services and devices currently operate only within the domain of the same manufacturer or service. Therefore, a standardized mode is essential to establish machine-to-machine communication, especially secured communication, between objects that are made by different manufacturers and used in different business domains. Moreover, the existing method of communication requires SSL and RSA security protocols, which were developed for the existing network environment, and these may not be efficient in an environment such as the IP camera network, which has certain battery and storage limitations. Therefore, this paper proposes a protocol that is both stable and more energy efficient than existing security protocols, and hence is applicable to the IP camera environment.

2.2. IP Camera Trends

As the term Closed-Circuit Television implies, existing CCTV systems have their own closed configurations for the purpose of security. Therefore, it is common to install CCTV cameras in a specific area to monitor captured images at predetermined locations, and to store and retrieve them when necessary. On the other hand, the development of information technology (IT) has led to the emergence of IP cameras, which have the advantage of being open, scalable and flexible, unlike conventional CCTVs, by utilizing the concept of transmitting images based on the networks. Because they are linked to the Internet via a network connection, IP cameras have a great feature in that they can be used anytime and anywhere, provided that the Internet is available [8]. This feature is advantageous in that the installation and configuration of a network is both simple and inexpensive in the present era, and in many cases networks have been installed and configured in most places, so that it is relatively easy to use IP cameras for everyday purposes at no additional cost. In addition, while conventional analog CCTV cameras capture video only, the latest IP cameras are equipped with functions for compressing and transmitting video and audio at the same time, and most IP cameras also support voice recording and transmission. This not only makes it possible to expand from conventional simple video surveillance to the communication function, but also makes it possible to utilize them for security surveillance using voice [9].

If one looks at the types of IP cameras currently being released, they are very different from conventional CCTV cameras. First, they typically come in special shapes such as the box, dome, bullet, and flat rectangular types. Furthermore, they can be classified into fixed pan & tilt, zoom and high-speed dome types according to camera module movement, and into vandal-proof, weather-proof and waterproof types according to their proofing function. In addition, they usually feature an infrared (IR) light emitting diode (LED), which is either fitted on the front of the camera or attached separately for operation in nighttime and low-light environments. In addition, WDR (Wide Dynamic Range), is also becoming more common. In the early stage of transition from CCTVs to IP cameras, the terminology was not yet established, so the term IP camera was used along with web camera and network camera. In this paper, the target device is also referred to as a "network camera", but in recent years this has almost been unified with the term "IP camera", while "web camera" specifically indicates a product composed only of a camera module connected to a PC via a USB [10].

2.3. IP Camera Market Trends

The global video surveillance market was worth $17.2 billion in 2017, and is expected to grow at an average annual rate of 7.2% to reach $22.7 billion by 2021. Both economic growth and demand for security in emerging countries are expected to continue rising as a key driving force in the growth of the global video surveillance market. The most direct cause is related to attacks by global terrorism and the resulting increase in civilian deaths. Since 2012, the number of people killed by terrorism has steadily increased in the international community. In 2015, the number of terrorist attacks worldwide came to 11,770 and the death toll reached 28,320, representing increases of 14.5% and 26.0% respectively compared to 2012. To prevent these problems, demand for video surveillance systems by governments in each country is increasing, and governments and intelligence agencies are increasingly deploying such systems to curb criminal activity and control hostile situations.

This trend is also associated with the development of IoT technology, which is making system installation and management much easier. IoT-based connection devices are being applied to video surveillance systems, and the number of connected devices in the world is expected to increase sharply from 8.7 billion in 2012 to 22.9 billion in 2016. As the numbers of IoT-connected devices and IoT access control solutions are increasing explosively, the related video surveillance market is expanding accordingly [11].

In addition, the world's urban population increased from 3.94 billion in 2012 to 4.02 billion in 2016, and this increase has led to a greater need for advanced safety products and services to ensure a safer urban life, prevent crime and promote disaster and incident preparedness. Also, as the urban population increases, the need for high-tech safety products is being widely emphasized. As a result, the demand for associated services is increasing and improvements in the quality and performance of safety products and services are rapidly progressing [12].

We can explain the cause of this increase in terms of the social environment as well as technology. The number of Internet users worldwide is expected to increase to 3.48 billion in 2016, up 42.0% from the 2.45 billion recorded in 2012. The increase in the number of users of wired and wireless Internet is also expected to facilitate the increasing demand for IP cameras. The improved accessibility of computers and mobile devices to wired and wireless networks has increased the Internet usage rate and the number of Internet users, and this increase is a key factor in the rising demand for IP cameras.

Worldwide per capita GDP in 2016 was $10,337, up 5.7% from $9781 in 2012, and economic growth in both developed and developing countries is driving investment in video surveillance products and services. The growth of global GDP has resulted in an increase of consumer purchasing power for video surveillance products and services, and an increase in demand for security and safety related products and services, and is leading to the growth of worldwide video surveillance markets [13].

2.4. Cases of IP Camera Security

The growth of the IP camera market has not only had a positive impact in such areas as anti-terrorism, crime prevention, disaster and incident monitoring, but also a negative impact. Over the past several years, malicious attacks on IP cameras have caused plenty of problems. Austrian security researchers have identified more than 80 backdoors to Sony's IP cameras, while Israeli security experts have found vulnerabilities in IP camera models. SEC Consult, an Austrian security company, has found two different kinds of backdoors in Sony's IPELA Engine IP cameras. According to this company, it is possible to remotely control "primana" and "debug" via Telnet, so their users are recommended to update the firmware through the SNC Toolbox to fix the vulnerabilities.

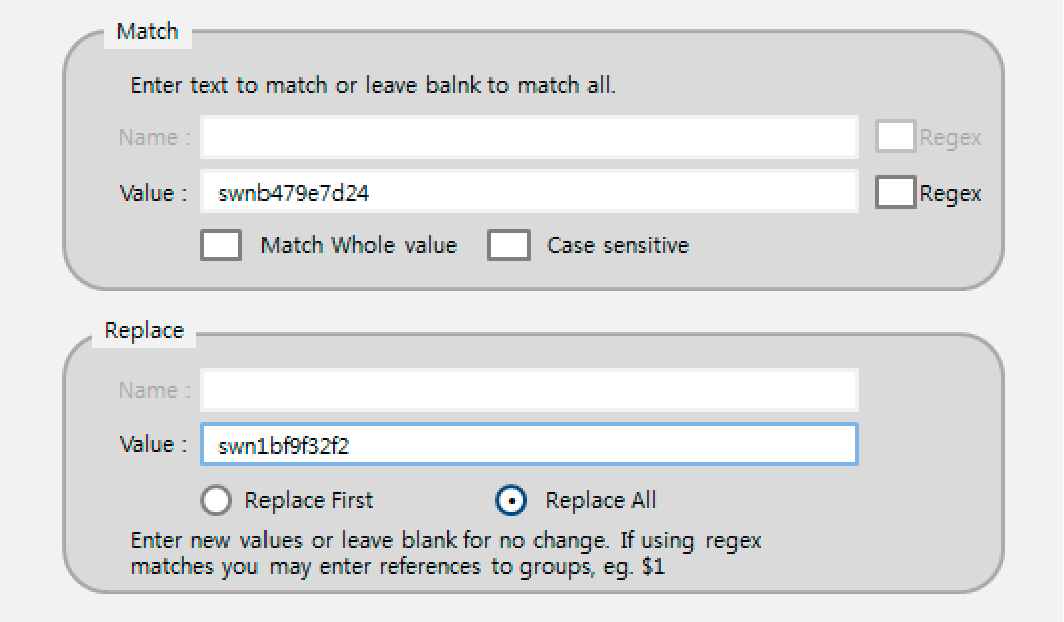
In addition, Cybereason purchased twelve types of IP cameras from eBay and Amazon, and found that all the passwords for the purchased devices were "888888", which made it difficult to defend their firewalls against attackers. It was a vulnerable situation, in which the companies that made such IP cameras had not updated the firmware.

Security vulnerability has also been detected in SWANN's cameras, which showed that they can intercept messages sent from OzVision's computer server to the Swann camera app with a free tool commonly used in the security industry. The Swann Camera app is used to view images taken by the camera on a smartphone. The intercepted message includes a serial number for each camera given by the factory. By changing the serial number, a research group composed of five European security consultants was able to acquire the images from other cameras. The researchers succeeded in acquiring the images simply by inserting the serial number of the camera they had purchased. During this process, they did not have to enter the ID or password of another user account. They also found a way to identify the serial number used by Swann's camera. Figure 1 is a program action screen that changes the actual serial number. Theoretically, it is possible to steal images quickly from any account, causing a major problem with personal image information leakage.

There was also a case in which a DDoS attack used IP cameras. On 21 October 2016, the DNS service provider Dyn was subjected to a massive Distributed Denial of Service (DDoS) attack, which resulted in the simultaneous paralysis or delay of seventy-six sites including Twitter, Netflix, and The New York Times (NYT).

According to the Bryan Krebs blog (Krebs on Security) analysis, it was confirmed that the cause of the DDoS attack was a vulnerable IoT device (i.e., a device whose factory default ID/PW was not reset), infected with the Mirai malicious code, which executed the DDoS attack initiated by hackers. Most IoT devices are connected online with a weak factory default ID/PW configuration, making them vulnerable to attacks. Therefore, the number of attempts to infect malicious code targeting such devices has been increasing every year, making security measures essential. Moreover, the Mirai malicious codes used in the abovementioned example of large-scale DDoS attacks have been made public, thus enabling anyone to make a malicious code easily, by simply changing the source codes. As a result, we are faced with the possibility not only of large-scale DDoS attacks, but also an Internet crisis in which IoT devices are exploited by new malicious codes capable of using the source codes [14,15].

The manufacturers of IoT equipment (IP cameras, Internet routers, set-top boxes, etc.) use various CPUs (ARM, MIPS, PowerPC, SuperH, etc.) and adopt the Linux operating system, which is suitable for such a CPU environment. Based on the Linux operating system, the source codes are made to be executable in various CPU environments through cross-compilation. On this account, almost all IoT equipment is subject to attacks. We can confirm that the malicious codes actually found had the same functionality, but were designed to run in various CPU environments such as ARM, MIPS, and PowerPC [16].



Match

Enter text to match or leave balnk to match all.

Name : □ Regex

Value : swnb479e7d24 □ Regex

□ Match Whole value □ Case sensitive

Replace

Name :

Value : swn1bf9f32f2

○ Replace First ◉ Replace All

Enter new values or leave blank for no change. If using regex matches you may enter references to groups, eg. $1

Figure 1. Picture of the serial number change program.

2.5. Network Attack Methods

2.5.1. DDoS

The Distributed Denial of Service attack is a method of performing multiple DOS attacks in parallel. It consists of creating a Denial-of-Service situation to prevent users from using a given service by generating heavy traffic that cannot be accommodated in the operating servers and network equipment of the company providing the service. The main characteristic of the DDoS attack is that the principal objective is to stop a system service for a certain period of time in order to prevent it from being provided to users, rather than hacking, information leakage or taking control of the server systems to acquire the highest privileged account [17,18].

The target servers attacked by an attacker are not damaged by the deletion, modification, leakage or destruction of data, but there may arise file system or other damage due to the system attack. This implies that if used in combination with other types or methods of attack, it can be a pre-work of system paralysis for effective intrusion. It is difficult to trace the cause of a DDoS attack and the attacker. In the case of a DoS attack, there are many ways to falsify the attack sources, and for a distributed DoS attack, even if it is possible to track an attack host, it is still difficult to find out when the host was occupied or what unexpected route was used for the takeover, and to keep track of them, and so on.

2.5.2. Sniffing and Spoofing

Sniffer was originally a registered trademark of Network Associate, but is now used as a general term, like PC or Kleenex. It is a tapping device that eavesdrops on traffic flows within the computer network. In the case of a sniffing attack, it has become a very threatening type of attack for companies, such as web hosting service providers and IDC centers connected in the same network. If an attack on a single system succeeds, the attacker will be able to intercept the entire data flow on the network through the system and thereby acquire sensitive information, such as user IDs and passwords [19].

In the case of the Ethernet, all hosts in the local network share the same communication line, which means that any computer on the same network can observe every different computer's traffic. However, if one's computer allows all traffic passing through the Ethernet, it must deal with irrelevant and unnecessary traffic, which is inefficient and results in poor network performance. Therefore, an Ethernet interface should have a filtering function that ignores irrelevant traffic that does not include the user's own MAC address, thus processing only traffic that has the user's own MAC address. Nevertheless, the user can set a function to observe all traffic on the Ethernet interface. This is called the promiscuous mode. The sniffer will set the Ethernet interface to the promiscuous mode and thus be able to eavesdrop on all traffic going through the local network.

Spoofing is a method of hacking used by malicious attackers who build a fake website and induce users to visit it, and thereby obtain the system privileges of users who access the real website and steal their information by exploiting the structural flaws of the Internet Protocol (TCP/IP). ARP Spoofing is an attack scheme that exploits flaws in the ARP protocol to cheat its MAC address as the MAC addresses of other users. By exploiting the vulnerability of ARP Request Broadcasting, attackers can obtain accurate information about all Host IP-MAC address mappings on the network [20,21].

2.6. DVR and NVR

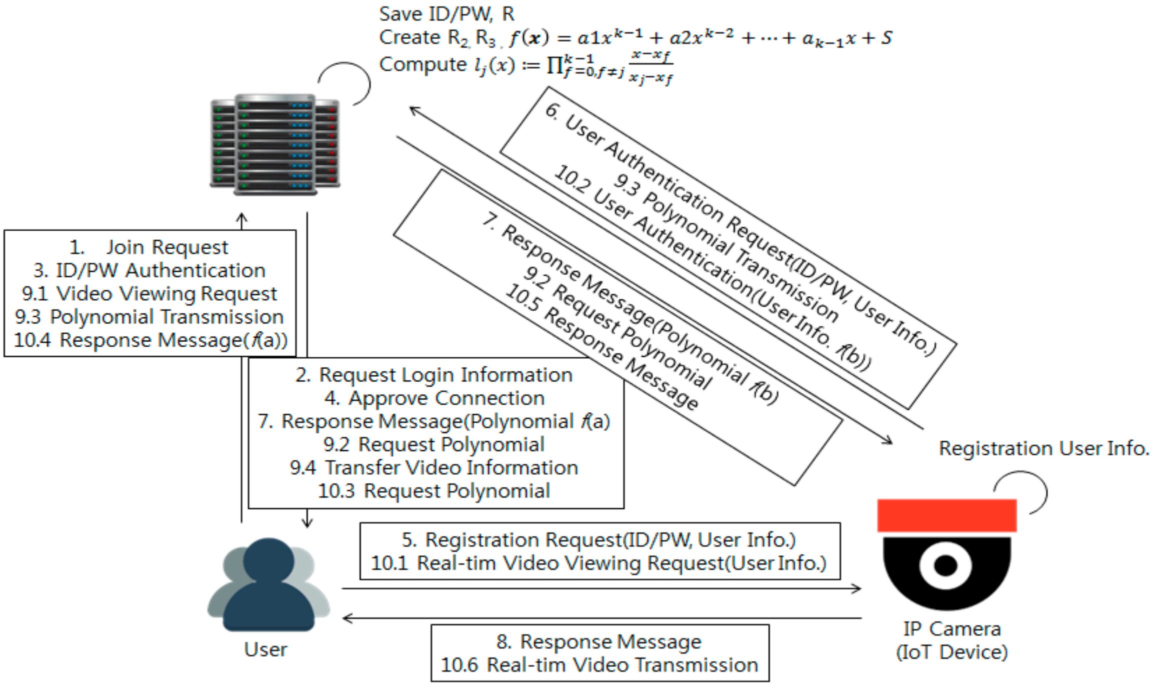
The DVR (Digital Video Recorder) is a device that converts image data input from an analog camera into high-quality digital images using a capture board and stores them on a hard disk. The DVR converts recorded images into digital images and stores them on the hard disk semi-permanently, allowing users to search them according to their recorded data condition (event, date, etc.). It is also a multifunctional digital recording and monitoring device equipped with an image transmission function that can search recorded images and monitor screens in real time using LAN, MODEM, ADSL, etc. at a remote place from a long distance [22,23].

The NVR (Network Video Recorder) is a system that receives and stores video data from the cameras, videos, and servers installed on a network. It has both networking and the ability to store received video data in real time, and to decode and output them to a monitor [24,25]. The number of connected cameras can be limited according to the resolution of the received image. The NVR performs recording and playback simultaneously. Video data recorded on a single device can be remotely viewed by several authorized operators scattered throughout the network. They are independent and do not affect each other. In addition, it is easy to expand the number of NVR units, and even if you have plenty of NVR units throughout the system, you only have to connect it to the network to add one more NVR. In this paper, we propose a security system that is based on the NVR system [26,27].

3. Contents of the Proposed System

This chapter presents a design method of a control center to cope with security threats and to operate IP cameras effectively. As they are connected to the network, IP cameras combined with the NVR system described above are vulnerable to various security threats such as user authentication and access security threats that can occur in the network. IP cameras are currently being used not only in numerous homes and offices, but also in disaster, incident and crime prevention. ID/PW authentication can be taken easily by indiscriminate insertion attacks. As such, this paper proposes a secure authentication protocol using the user code, random data, and the real-time request time value from the standpoint of IP camera users and the control center.

In this paper, the procedure is divided into the following three steps: First, the user registers an IP camera. In order to utilize an IP camera, its ID/PW-based registration procedure for user registration is performed in the control center. During this process, a transfer process is performed for the serial number and random value of the product as well as the polynomial expression to be used in the authentication process later on. The second step involves a procedure for viewing the images stored in the control center to be performed. After proceeding to the authentication of the user, the control center and the IP camera, viewing is allowed if the user is judged to be suitable. The third step consists of the real-time monitoring of IP cameras. The user is proved to be a legitimate user to connect an IP camera and receives video images in real time. The proposed protocol applies the group key method between the devices, the control center and the users, to enable secure communication. In addition, the proposed protocol is designed in such a way that the more IoT devices (including IP cameras) are connected to the network, the more reliable the authentication procedure becomes. Thus, a strong authentication system is constructed to reflect the current tendency to use multiple IoT devices. The proposed entire protocol procedure is as shown in Figure 2, Table 1 is the meaning of Notation where Protocol is used.



Save ID/PW, R
Create R_2, R_3, $f(\boldsymbol{x}) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$
Compute $l_j(x) := \prod_{f=0,f\neq j}^{k-1} \frac{x-x_f}{x_j-x_f}$
6. User Authentication Request(ID/PW, User Info.)
9.3 Polynomial Transmission
10.2 User Authentication(User Info. f(b))
7. Response Message(Polynomial f(b)
9.2 Request Polynomial
10.5 Response Message
1. Join Request
3. ID/PW Authentication
9.1 Video Viewing Request
9.3 Polynomial Transmission
10.4 Response Message(f(a))
2. Request Login Information
4. Approve Connection
7. Response Message(Polynomial f(a)
9.2 Request Polynomial
9.4 Transfer Video Information
10.3 Request Polynomial
Registration User Info.
5. Registration Request(ID/PW, User Info.)
10.1 Real-tim Video Viewing Request(User Info.)
8. Response Message
10.6 Real-tim Video Transmission
User
IP Camera
(IoT Device)

Figure 2. Protocol composition diagram.

Table 1. Proposed Notation.

Notation	Meaning
E_k(plaintext)	Encrypt a using key k
D_k(ciphertext)	Encrypt ciphertext using key k
R	Random Number
ID	Identification for authentication
PW	Password for authentication
f(k)	Polynomial for secret sharing
SN	Serial Number
l_j(x)	Formula for secret combinations

3.1. Internal Connection Protocol

This paper proposes a method of distributing keys and allowing the restoration of a key to retrieve an image only if a certain number of keys are in agreement when an image viewing request is sent internally. In the process of exchanging keys, the group key is used, and it is renewed periodically so as to secure it.

3.2. Registration Procedure

This step is a user registration procedure, and the detailed structure is shown in Figure 3.

- The user sends a joint request for registration to the control center.
- The control center sends a response message to the user, and the user proceeds to the membership subscription process based on the ID/PW, generates a random value, and transmits them together.
- The control center stores the user's subscription information in the database and finishes.
- The user sends a connection request to the IP camera through the network to register the desired IP camera.
- The IP camera requests the user's information, and the user transmits the ID/PW and the random value generated in the control center registration procedure in response to the request.
- The IP camera sends a request to the control center for the product to confirm the validity of the user.
- The control center determines the suitability of the user (i.e., the process of requesting the user to provide the serial number of the associated IP camera and the receipt of the response to the request), and sends the polynomial to the user for authentication later. The polynomial key distribution method is presented in Section 3.2.2.
- Finalizing the registration procedure of the user and the IP camera.

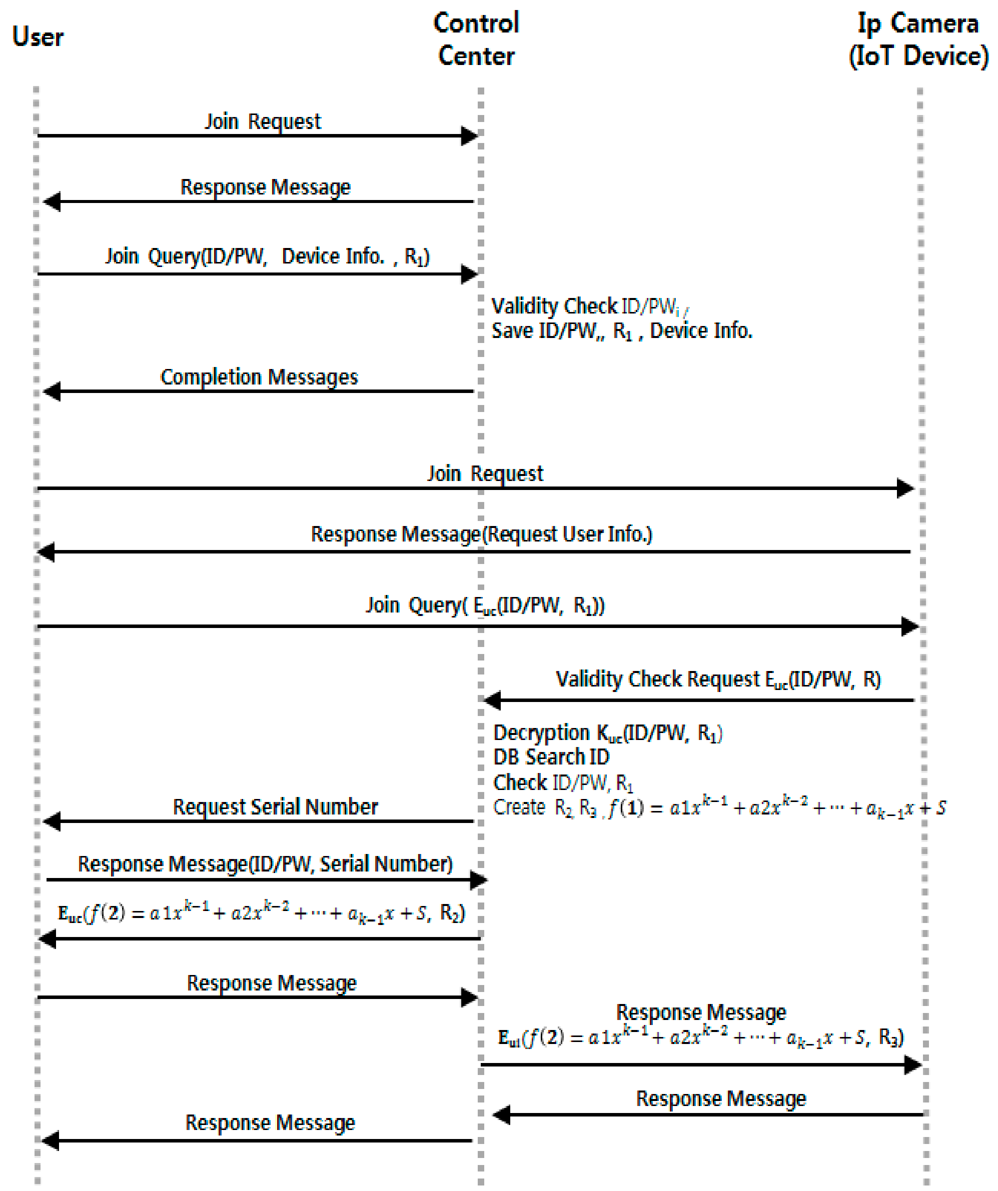

User
Control Center
Ip Camera (IoT Device)
Join Request
Response Message
Join Query(ID/PW, Device Info. , R_1)
Validity Check ID/PW$_i$ /
Save ID/PW,, R_1 , Device Info.
Completion Messages
Join Request
Response Message(Request User Info.)
Join Query(E_{uc}(ID/PW, R_1))
Validity Check Request E_{uc}(ID/PW, R)
Decryption K_{uc}(ID/PW, R_1)
DB Search ID
Check ID/PW, R_1
Create R_2 R_3 , $f(1) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$
Request Serial Number
Response Message(ID/PW, Serial Number)
$E_{uc}(f(2) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$, R_2)
Response Message
Response Message
$E_{ui}(f(2) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$, R_3)
Response Message
Response Message

Figure 3. Registration Process Protocol.

3.2.1. Overview of Image Viewing

- The user transmits an image viewing request message.
- In this study, the user is allowed to view an image when more than an n number of devices, user and control center information, are collected. Each device determines the suitability of the user request and then transmits the polynomial information owned by the device to the operation server if it is determined to be appropriate.
- If a certain number of polynomial key values are collected, the operation server allows access to the image.

3.2.2. Polynomial Key Distribution and Transmission Method

The key distribution method uses $k - 1$ order polynomials. This paper gives an example of the simplest structure based on the three following elements: user, control center, and IP camera. Therefore, the protocol is configured by setting n to 3 and k to 2.

- The control center selects the k-1th order polynomial f(k) with the constant s.

- The control center decides the value of j and transmits f(j). In this paper, j is designated as 1 for user, 2 for control center, and 3 for IP camera, and these are encrypted using the group key transmitting.
- When the control center sends the key to the operation server, they encrypt it using the group key and transmit it.
- The control center decrypts the original key using the Lagrange polynomial if k or more distribution keys are collected.

3.2.3. Exchange of Keys to Secure Safety

An attacker may take a cipher text sent from the control center and use it as it is. In this paper, it is designed to prevent situations in which a cipher text is used as it is by using it after generating and using random values in the encryption process, and designed to mutually authenticate each other.

3.3. Video Image Monitoring

This step is a monitoring process step and the detailed structure is shown in Figure 4.

- In order to monitor a video image, the user requests to connect to the IP camera, encrypts the ID/PW and the polynomial key value using the group key, and then transmits them.
- The IP camera requests the polynomial key value of the received login information from the control center and nearby devices according to the level of security requirement.
- If the polynomial key value is confirmed to be suitable, an image is transmitted to the user in real time.

When the user ends the session, the polynomial key value is discarded, and the polynomial key value is updated according to a predetermined period.

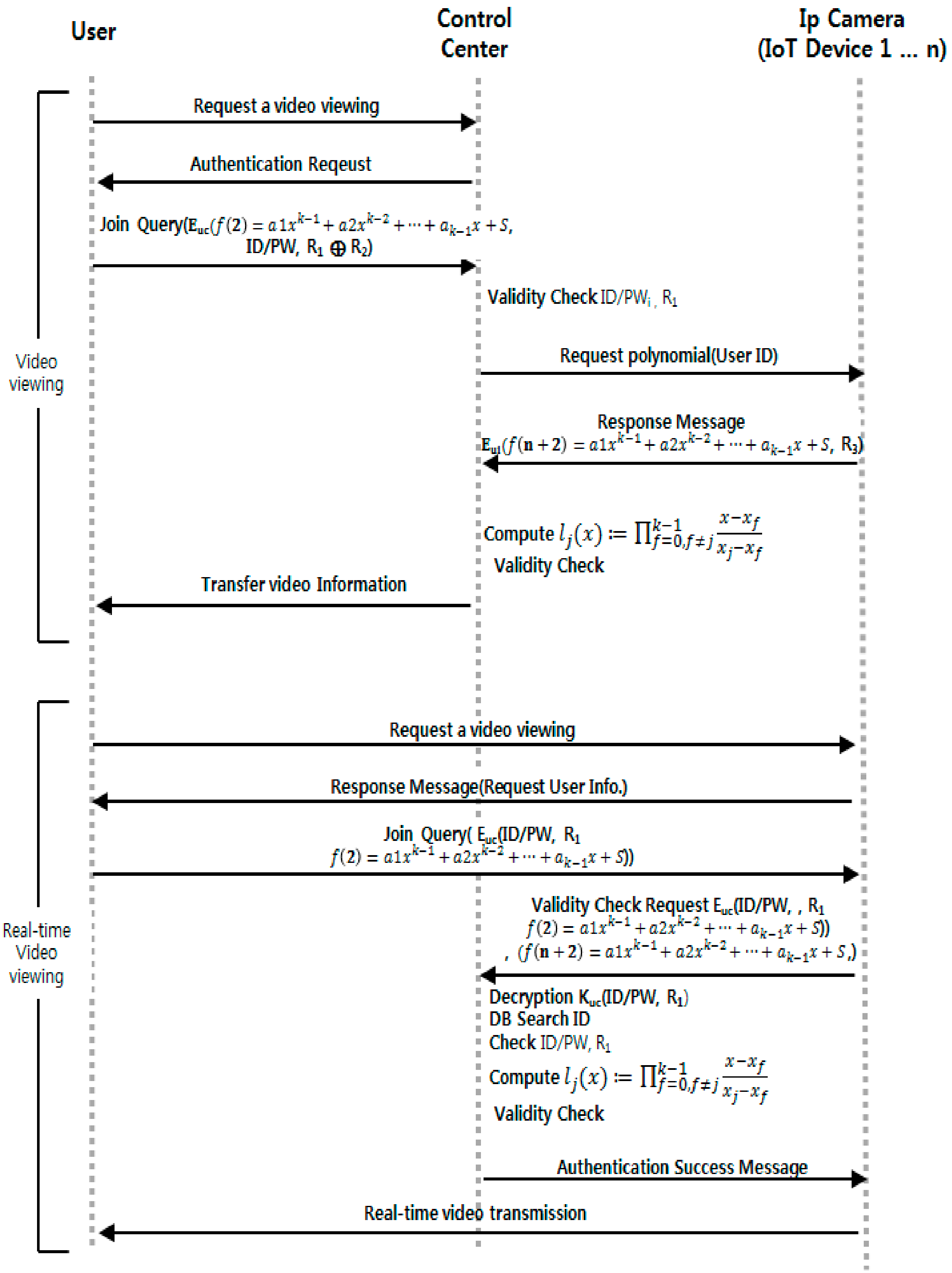

User
Control Center
Ip Camera (IoT Device 1 ... n)
Request a video viewing
Authentication Reqeust
Join Query(E$_{uc}$($f(2) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$, ID/PW, R$_1$ ⊕ R$_2$)
Validity Check ID/PW$_i$, R$_1$
Request polynomial(User ID)
Response Message
E$_{ul}$($f(\mathrm{n}+2) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$, R$_3$)
Compute $l_j(x) \coloneqq \prod_{f=0,f\neq j}^{k-1} \frac{x-x_f}{x_j-x_f}$
Validity Check
Transfer video Information
Video viewing
Request a video viewing
Response Message(Request User Info.)
Join Query(E$_{uc}$(ID/PW, R$_1$ $f(2) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$))
Validity Check Request E$_{uc}$(ID/PW, , R$_1$ $f(2) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$)) , ($f(\mathrm{n}+2) = a1x^{k-1} + a2x^{k-2} + \cdots + a_{k-1}x + S$,)
Decryption K$_{uc}$(ID/PW, R$_1$)
DB Search ID
Check ID/PW, R$_1$
Compute $l_j(x) \coloneqq \prod_{f=0,f\neq j}^{k-1} \frac{x-x_f}{x_j-x_f}$
Validity Check
Authentication Success Message
Real-time video transmission
Real-time Video viewing

Figure 4. Monitoring process protocol.

4. Performance Evaluation

4.1. Security Evaluation

IoT environment inherits existing security threats and weaknesses of existing information and communication networks. Therefore, the performance evaluation will evaluate the safety of the proposed protocol on the security threats and additional security threats of existing information networks. The following is the result of evaluating the safety of the security threats that can occur in the information communication network.

In addition, as a result of security strength analysis, it satisfies all the security requirements defined in the OneM2M standard among the existing IoT environment standard documents, and is expected to be immediately applicable to the IoT environment.

4.1.1. Mutual Authentication

In this paper, we performed the ID/PW registration procedure using the encryption method to join the control center. In this process, it exchanges random values, which are later used to update the key and authentication values. In the control center, a polynomial f(k) is transmitted to the user and the IoT Device respectively for the subsequent authentication process. After the initial authentication, mutual authentication can be carried out by performing the verification procedure using the polynomial value. In the direct authentication process of users and IP cameras, the authentication center can perform the role of an authentication center, thus enabling secure authentication.

4.1.2. Reuse Attack

The reuse attack is a method of attack in which an unauthorized attacker can steal a message sent between each node and reuse it. To address this problem, even if a message is stolen, it is possible to authenticate it so as to prevent an attacker from using the previous transmission value by exchanging random numbers continuously. Also, in this paper, since the time stamp is assumed to be transmitted during the authentication procedure, it is possible to verify information sent the previous time.

4.1.3. Message Forgery Attack

This is a method of attack in which an unauthorized attacker seizes a message sent between each node and sends a forged message to the receiver for a desired purpose. This study confirms that data transmission is safe from message forgery attacks unless the attacker steals the key, since cipher text is generated through an encryption key before it is transmitted.

4.1.4. Sniffing

This method of attack consists in "sniffing" transmitted messages. This study confirms that it is safe from sniffing attacks because the messages between the nodes are transmitted only after applying the encryption using the inter-node secret key, which is continuously updated. Even if sniffing attempts are made in order to peek into a message, it is safe because the sniffer will only be able to see the cipher text.

4.1.5. Spoofing

This is a method of attack in which an attacker deceives the other party by changing the information that may reveal them on the network without permission. This study confirms that it is safe against spoofing attacks because the nodes have already been mutually authenticated, and the attackers will not be able to get the secret key between the nodes that have been initially shared.

4.1.6. Side-Channel Attack

This is a method of attacking through ancillary constituents such as processing time, energy usage, and electromagnetic waves. This study confirms that it is safe against side-channel attacks because it always transmits the same size message regardless of the volume of the transmitted data.

4.2. Performance Evaluation

For the performance analysis, we sequentially configured the IoT devices numbering between 3 and 40 and placed them randomly in an area measuring 45 × 45 m. We then positioned the control center in a specific location with consideration to the placement of the devices. All of the IoT devices were situated within 70 m of the control center. To confirm the efficiency regardless of the random distribution of the devices, we tested them more than 20 times under the same conditions. The following table shows the average values, while Table 2 shows the test environment in detail.

Figures 5 and 6 are simulations that compare and analyze the energy consumption of protocols in the server and client areas, respectively. Energy consumption varies depending on where the server and client are set up and is the average for more than 20 test results.

For simulated device performance, clients were based on Raspberry PI b+. In addition, for servers, PC with sufficient computational power is defined, and detailed performance is shown in Table 3. Tables 4 and 5 represent the detailed values of the simulation results.

Table 2. Assessment Environment.

Simulation Initial Settings	
Number of Device	3~40
Placement Area	45 m × 45 m
Control Center Location	X = 60 m, y = 30
Device Initial Energy	1.0
ETX, ERX	50 nanoJ
Packet Size	6000 bit

Table 3. Simulation Environment.

Sortation	Client	Server
Process	ARM1176JZF-S 700 MHz Single Core	3.5 GHz Intel Core i5-4690
Memory	512 MB	16 GB
storage medium	Micro SD Card, 8 GB	SSD 512 GB

Table 4. Compare Rates According to the Number of IoT Device (Server). (Unit: ms).

Number	ECC	RSA	SSL	Kerberos	Proposed
3	18.74498	30.77373	59.15496	0.09947	26.85049
5	31.24164	51.28955	98.59160	0.165781	44.75081
10	68.731608	112.83701	216.90153	0.364719	98.451782
20	137.46322	225.67402	433.80306	0.72944	196.90356
30	203.69549	334.40787	642.81727	1.08089	291.77528
40	281.17476	461.60595	887.32445	1.49203	402.75729

Table 5. Compare Rates According to the Number of IoT Device (Client). (Unit: ms).

Number	ECC	RSA	SSL	Kerberos	Proposed
3	12.99786	25.59363	59.44896	1.17664	0.09490
5	21.66311	42.65605	99.08161	1.96106	0.15816
10	48.95862	96.40267	223.92443	4.43201	0.35744
20	93.58461	184.27414	428.03254	8.47179	0.68325
30	134.31125	264.46751	614.30596	12.15859	0.98059
40	181.97008	358.31082	832.28549	16.47293	1.32854

In the proposed protocol, the clients perform only simple hash computation for the energy efficiency of devices with various hardware computing capabilities in the IoT environment, and the authentication protocol is proposed so that the computation is concentrated in the control center, such as encryption, decryption and polynomial computation. This feature is expected to be applicable not only to simple IP cameras but also to ultra-light devices which cannot be installed with encryption modules in the heterogeneous IoT environment, which is a limitation of lightweight security technology in the existing IoT and smart home environments.

This paper's performance analysis confirms that the proposed authentication framework is lighter than the previously well-known security authentication technology. It also confirms that it has been significantly improved in terms of security and energy efficiency due to its low energy consumption compared to the existing authentication technology. In conclusion, it is confirmed that the proposed authentication protocol is superior in terms of performance compared to the security schemes for which the existing documents are designed.

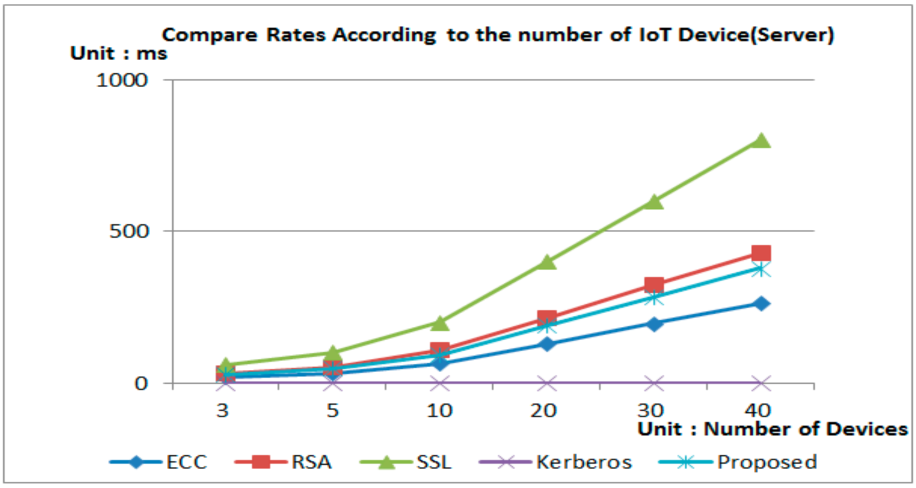


Figure 5. Energy performance evaluation(Server).

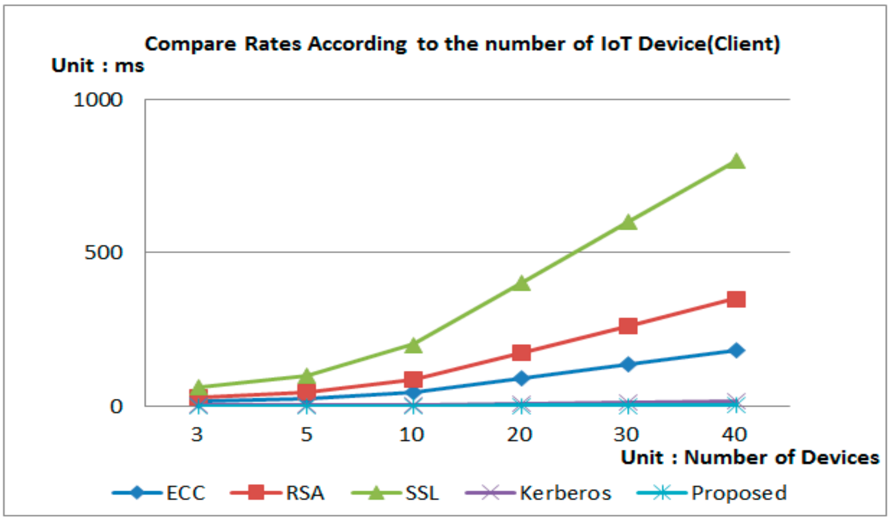


Figure 6. Energy performance evaluation(Client).

5. Conclusions

In the proposed protocol, concerning the energy efficiency of devices in IoT environments with various hardware computing abilities, only a simple hash operation was performed for the clients, while for the encryption and decryption of polynomials, the authentication protocol was proposed in order to allow the calculation to be concentrated in the control center. In addition to simple IP cameras, in a heterogeneous IoT environment, which is the limiting point of lightweight security technologies in existing IoT and smart home environments, it is expected to be utilized on all ultra-lightweight devices that cannot be equipped with encryption module.

For the authentication framework proposed through the performance analysis it was confirmed that it was lighter than the well-known security authentication technology on the client side, and in terms of devices, it can be seen that the energy consumption is significantly improved in terms of security and energy efficiency compared to the existing authentication technology.

Author Contributions: J.L. designed the protocol; J.K. researched related work; J.L. and M.-s.J. performed and analyzed the data; and J.H. and J.L. wrote the paper.

Funding: This research received no external funding.

Acknowledgments: The present Research has been conducted by the Research Grant of Kwangwoon University in 2017.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
2. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in internet-of-things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]
3. Williams, C. Today the Web Was Broken by Countless Hacked Devices—Your 60-Second Summary. Available online: www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained (accessed on 21 October 2016).
4. Imperva Breaking Down Mirai: An IoT DDoS Botnet Analysis. Available online: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html (accessed on 26 October 2016).
5. Brass, I.; Tanczer, L.; Carr, M.; Blackstock, J. Regulating IoT: Enabling or Disabling the Capacity of the Internet of Things? *Risk Regul.* **2017**, *33*, 12–15.
6. Burke, D. Preventing DDOS Attacks against IoT Devices. Ph.D. Thesis, Utica College, Utica, NY, USA, 2018.
7. Frank, C.; Nance, C.; Jarocki, S.; Pauli, W.E. Protecting IoT from Mirai botnets; IoT device hardening. In Proceedings of the Conference on Information Systems Applied Research, Austin, TX, USA, 5 November 2017; p. 1508.
8. Popovic, G.; Arsic, N.; Jaksic, B.; Gara, B.; Petrovic, M. Overview, characteristics and advantages of IP Camera video surveillance systems compared to systems with other kinds of camera. *Int. J. Eng. Sci. Innov. Technol.* **2013**, *2*, 356–362.
9. Kang, J.; Han, J.; Park, J.H. Design of IP camera access control protocol by utilizing hierarchical group key. *Symmetry* **2015**, *7*, 1567–1586. [CrossRef]
10. Fularz, M.; Kraft, M.; Schmidt, A.; Kasiński, A. The architecture of an embedded smart camera for intelligent inspection and surveillance. In *Progress in Automation, Robotics and Measuring Techniques*; Springer: Cham, Switzerland, 2015; pp. 43–52.
11. Tekeoglu, A.; Tosun, A.S. Investigating security and privacy of a cloud-based wireless IP camera: NetCam. In Proceedings of the 2015 24th International Conference on Computer Communication and Networks (ICCCN), Las Vegas, NV, USA, 3–6 August 2015; pp. 1–6.
12. Bangali, J.; Shaligram, A. Design and Implementation of Security Systems for Smart Home based on GSM technology. *Int. J. Smart Home* **2013**, *7*, 201–208. [CrossRef]
13. Baran, R.; Ruść, T.; Rychlik, M. A smart camera for traffic surveillance. In *International Conference on Multimedia Communications, Services and Security*; Springer: Cham, Switzerland, 2014; pp. 1–15.
14. Krebs on Security. Researchers Find Fresh Fodder for IoT Attack Cannons. Available online: https://krebsonsecurity.com/2016/12/researchers-find-fresh-fodder-for-iot-attack-cannons/KrebsonSecurity (accessed on 16 December 2016).
15. Rio Kellyan, Tech Desk Editor. The Video of the Home Security Camera Was Hacked. Available online: https://www.bbc.com/korean/news-44962424 (accessed on 7 July 2018).
16. Korea Internet & Security Agency. 2016 Mirai Malicious Code Trends. Available online: https://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=24864&queryString=cGFnZT0xJnNvcnRfY29kZT0mc2VhcmNoX3NvcnQ9dGl0bGVfbmFtZSZzZWFyY2hfd29yZD1taXJhaSZ4PTAmeT0w (accessed on 12 December 2016).
17. Peng, T.; Leckie, C.; Ramamohanarao, K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Comput. Surv. (CSUR)* **2007**, *39*, 3. [CrossRef]
18. Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput. Commun. Rev.* **2004**, *34*, 39–53. [CrossRef]

19. Jeon, W.; Kim, J.; Lee, Y.; Won, D. A practical analysis of smartphone security. In *Symposium on Human Interface*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 311–320.
20. Ramachandran, V.; Nandi, S. Detecting ARP spoofing: An active technique. In Proceedings of the International Conference on Information Systems Security, Kolkata, India, 19–21 December 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 239–250.
21. Chomsiri, T. Sniffing packets on LAN without ARP spoofing. In Proceedings of the Third 2008 International Conference on Convergence and Hybrid Information Technology, Busan, Korea, 11–13 November 2008; pp. 472–477.
22. Lin, C.F.; Yuan, S.M.; Leu, M.C.; Tsai, C.T. A framework for scalable cloud video recorder system in surveillance environment. In Proceedings of the 2012 9th international conference on Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), Fukuoka, Japan, 4–7 September 2012; pp. 655–660.
23. Lipton, A.J.; Clark, J.I.; Zhang, Z.; Venetianer, P.L.; Strat, T.; Allmen, M.; Severson, W.; Haering, N.; Chosak, A.; Frazier, M.; et al. Video Analytic Rule Detection System and Method. U.S. Patent 8,564,661, 22 October 2013.
24. Liu, H.; Chen, S.; Kubota, N. Intelligent Video Systems and Analytics: A Survey. *IEEE Trans. Ind. Inform.* **2013**, *9*, 1222–1233.
25. Lindsey, S.L.; Call, S.J. Devices, Systems, and Methods for Remote Video Retrieval. U.S. Patent Application No 14/451,067, 4 February 2016.
26. Liu, J.K.; Au, M.H.; Susilo, W.; Liang, K.; Lu, R.; Srinivasan, B. Secure sharing and searching for real-time video data in mobile cloud. *IEEE Netw.* **2015**, *29*, 46–50. [CrossRef]
27. Costin, A. Security of CCTV and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, Vienna, Austria, 28 October 2016; pp. 45–54.