sustainability

MDPI

Article

Dynamic Group Management Scheme for Sustainable and Secure Information Sensing in IoT

Hyungjoo Kim [1] and Jungho Kang [2,*]

[1] Convergence Laboratory, Korea Telecom Research & Development Center, 151 Taebong-ro, Seocho-gu, Seoul 06763, Korea; hyungjoo.kim@kt.com

[2] Department of Computer Science and Engineering, Soongsil University, 369 Sangdo-ro, Dongjak-gu, Seoul 06978, Korea

* Correspondence: kjh7548@naver.com; Tel.: +82-2-826-6526; Fax: +82-2-822-2071

Academic Editors: James J. Park and Han-Chieh Chao

Received: 7 August 2016; Accepted: 13 October 2016; Published: 24 October 2016

Abstract: The services provided to users in the environment associated with the Internet of Things (hereinafter referred to as IoT) begin with the information collected from sensors. It is imperative to transmit high-quality sensor data for providing better services. It is also required to collect data only from those authenticated sensors. Moreover, it is imperative to collect high-quality data on a sustainable and continuous basis in order to provide services anytime and anywhere in the IoT environment. Therefore, high-quality, authenticated sensor networks should be constructed. The most prominent routing protocol to enhance the energy consumption efficiency for the sustainable data collection in a sensor network is the LEACH routing protocol. The LEACH routing protocol transmits sensor data by measuring the energy of sensors and allocating sensor groups dynamically. However, these sensor networks have vulnerabilities such as key leakage, eavesdropping, replay attack and relay attack, given the nature of wireless network communication. A large number of security techniques have been studied in order to solve these vulnerabilities. Nonetheless, these studies still cannot support the dynamic sensor group allocation of the LEACH routing protocol. Furthermore, they are not suitable for the sensor nodes whose hardware computing ability and energy resources are limited. Therefore, this paper proposed a group sensor communication protocol that utilizes only the four fundamental arithmetic operations and logical operation for the sensor node authentication and secure data transmission. Through the security analysis, this paper verified that the proposed scheme was secure to the vulnerabilities resulting from the nature of wireless network communication. Moreover, this paper verified through the performance analysis that the proposed scheme could be utilized efficiently.

Keywords: dynamic group management; distance-bounding; group authentication; IoT; sustainable sensing; LEACH routing protocol; sensor network

1. Introduction

The Internet of Things (IoT) tries to connect with all objects based on the communication network and provide people with the intellectual technologies and services that communicate between person and object, or object and object. For this purpose, IoT devices process various kinds of information at different service fields. At this time, the IoT environment is analyzed from various perspectives such as environment, economy, and infrastructure, among others, and the device is deployed depending on the analysis results. The deployed devices can sense and process simple ambient information such as temperature or humidity, or they can process personal information such as the position of an individual. In the case of handling simple ambient information, priority may be placed on service sustainability rather than security for energy efficiency. However, even when only simple ambient

information is processed, it is hard for services such as smart energy or smart vehicles to place priority solely on energy efficiency, as they are closely related to the public and individual's security.

Therefore, IoT devices shall provide people with a service environment in which both sustainability and security shall be achieved. Especially, the sensor that collects information at the front line shall be ensured of sustainability and security. This is because sustainability and security at the sensor ultimately leads to the service provided to the users. The characteristics of IoT service are as follows.

The IoT environment provides users context rich services based on user experience. At this time, user experience is based on the information collected from various objects that are available around users. Moreover, the most fundamental object among these diverse objects providing information is a sensor [1,2].

The quality of service to be provided to users through IoT shall be determined based on the quality of information to be collected and analyzed. That is to say, the quality of service to be provided through IoT shall be determined when it is possible to collect information from an authenticated sensor securely through a sensor network [3,4].

A sensor network infrastructure consists of the sensor nodes that synchronize or transmit the information detected through sensing to a server via other wireless network devices. Because of the characteristics of wireless communication, sensor nodes have been vulnerable to attacks such as relay attack, replay attack, and eavesdropping. The vulnerable authentication and management of the key may lead to infection by malicious codes such as Stuxnet, or an attack by malicious firmware updates, which in turn could develop into IoT device-based distributed denial-of-service (DDoS) by the second attack. Eavesdropping may expose the privacy of an individual who uses the IoT device to others, and an attack of retransmission may cause damages such as unfair penalty.

Thus, security protocols and schemes have been adapted. Even the sensor node supporting the encryption such as RC5 and public key was developed [5–7].

However, those sensor nodes whose hardware computing power and energy resources are very limited compared to the other sensor nodes are not suitable for the use of encryption and secure communication requiring a high degree of computing power, which are used in the existing schemes and protocols. In addition, the studies to prevent relay attack have tried to detect transmission device location on wireless network topology using radio frequency signal analysis. On that account, it is not appropriate to utilize it in a sensor with mobility or a sensor whose energy is relatively limited compared to the other sensors [8–10].

The quality of intelligent services in the IoT environment can be enhanced when the information is collected mainly from users on a continuous basis. That is to say, it is imperative to collect and transmit data continuously from a sensor [1,2]. The reason why sustainability is important is because an individual's life and the company's business are more closely dependent on IoT. After the development of the smart phone, many and various lives and businesses were re-conducted through the smart phone. As such, once an IoT environment is completely constructed, lives and business would continue based on IoT. It means that in this case, if there were even one disconnection in the continuity of information, there would be grave damage. In the smart factory environment, if even one piece of information does not arrive on time, the manufacturing process may be stopped or destroyed. In the smart automobile environment, if the sensor fails to collect the information even once, it could cause a traffic accident. Therefore, it is not optional but mandatory for IoT to provide sustainability.

The most adequate sensor network routing protocol for the continuous collection and transmission of data is the LEACH routing protocol [11]. The LEACH protocol has a better efficiency of data transmission energy since it allocates cluster headers and sensor groups dynamically based on energy efficiency analysis. However, it is not adequate to utilize the LEACH protocol for the application of the existing group management technique because it allocates groups dynamically.

Therefore, in this paper, the goal is to develop the secure authentication protocol which has high energy efficiency and whose service is sustainable in the IoT environment. For this purpose, this paper designs and proposes a group sensor secure communication protocol that solves the security vulnerabilities to which the existing sensor nodes are threatened, by utilizing the four kinds of fundamental arithmetic operations such as ADD operator and logical operations such as AND operator. The proposed secure communication protocols are also secure to a relay attack by using the distance-bounding technique between sensor nodes during the proposed authentication process. Also, this paper proposes the scheme to authenticate simultaneously all the sensor nodes in the ever-changing sensor group and to allocate group keys dynamically.

2. Related Work

2.1. LEACH Routing Protocol

The LEACH protocol introduced the cluster-based routing protocol that allowed the sensor nodes to consume power equally with communication distance by taking advantage of the fact that the power of sensor nodes would increase in proportion with communication distance [11].

The nodes arbitrarily elect cluster headers in the LEACH routing protocol and they form each cluster through those elected cluster headers. Furthermore, the sensor groups are formed based on the consumption rate of energy generated when communicating with the cluster headers. Therefore, the groups are formed dynamically based on the elected cluster headers in the LEACH routing protocol. The group-based communication shall be conducted accordingly.

Those nodes included in a cluster collect data and transmit these collected data to a cluster header. A cluster header organizes the data transmitted by nodes, transfers it to the base station in the end, and communicates with the base station. On this account, they consume more energy compared to the other nodes. Also, there might be an adverse effect on the entire sensor network when a majority of tasks are concentrated on a particular node. The LEACH routing protocol prevents the phenomenon that tasks are concentrated on a particular node through the method of electing a new cluster header in each round in order to distribute energy consumption that is otherwise concentrated on a particular node.

The LEACH routing protocol elects a cluster header among the nodes that have not become a cluster header. These newly elected cluster headers form a new cluster with the remaining nodes. Herein, the time of forming and disbanding a new cluster is expressed as "round". A round is repeated periodically; thus, all the nodes in a region are selected once as a cluster header. As a result, they distribute the energy consumption that is concentrated on the cluster headers. After all the nodes have become a cluster header, all the nodes are again qualified to become a cluster header. This cycle is called "group of round". In regard to the time of LEACH routing protocol, all the nodes in a network should be synchronized.

The LEACH routing protocol elects a cluster header through a probability-based algorithm. In the process of electing a cluster header, those sensor nodes that have never become a cluster header in a group of round take part. No special message is utilized in the process of electing a cluster header in the LEACH routing protocol. The purpose of the LEACH routing protocol is to enhance the energy efficiency of sensor networks and increase the overall lifetime of networks by allowing for equal energy consumption through distributing the energy consumption concentrated on a particular cluster-forming node.

The LEACH routing protocol elects a new cluster header for each round in order to consume energy equally, which would otherwise be concentrated on a particular node. At this time, those cluster headers that have been elected in the current group of round are not able to participate. Therefore, the probability of being elected as a cluster header will increase after each round.

2.2. Group Sensor Network and Distance Bounding Work

Management techniques in group sensor network topology are classified into the following three types [12]. The first management technique is the centralized group management technique. This technique allows only one group administrator to manage all group members. Moreover, headers are generated with an increase in the number of group sensor nodes. The second management technique is the decentralized management technique. It allows several group administrators to manage their own group sensor nodes. There might be an overload when modifying group confidential information or changing group members. Lastly, the contribution type management technique enables all sensor nodes to cooperate to maintain groups without a specific administrator. It has the problem associated with the optimization of group size.

Authentication protocols and management schemes for group sensor networks have been proposed by many researchers (Carlo Blundo et al. [13], Wensheng Zhang et al. [14], etc.). Nonetheless, there are many vulnerabilities such as replay and relay attack and the session key duplication problem. Moreover, the existing group sensor management studies have designed management plans without taking into account the modification of cluster header. As a result, they are not suitable for the environment in which cluster headers are changed continuously.

There are some measures secure to the relay attack that implement authentication via data connection between transmission devices such as sensor or cluster header. Some of these measures are the wireless network topology analysis using radio frequency signal-based method proposed by Guoqiang Mao, Loukas Lazos et al. [15] and the distance verification-based method proposed by Dave Singelee et al. [16]. The method using distance validation is more efficient than the wireless network topology analysis using radio frequency signal-based method. Because of only focusing on the simple distance validation, mafia attack has a high success rate.

3. Secure Dynamic Group Management Scheme

This section proposes a secure communication scheme that can conduct simultaneously mutual authentication between group sensor nodes and validate the distance between group sensor nodes by using the four kinds of fundamental arithmetic operations, substitution, logical operation, and challenge-response technique. The proposed scheme is made with four protocols that contain cluster header authentication and group authentication. During the authentication, the seed value which is required for generating and confirming the key is securely transmitted with the use of the multiplication, addition, and logistic XOR or $||$ only.

Figure 1 is a conceptual diagram of the secure dynamic group management scheme. Once the cluster header is selected, it will obtain a certain value for the group authentication from BS, and the sensor group will conduct the group authentication using that value. It is assumed that base station and secret key were shared when distributing sensor nodes. Also, it is assumed that the filter function was shared for the reduction of bit stream as shown in Figure 2. The process of filter function action is as follows. If a series of bit streams is put in the function, the values of bits located in the specified position would be selected for first filtering. Then, the values of bits, which are located in the specification positions, are kept among those that are filtered in unit of block while others would be removed. Lastly, only one bit is selected which is located as a specified position. The filter function continues to act until it gets the bit steam of the specified size while the dual values are designed not to come out by changing the input values or the position of filtering. For example, assuming that the seed is x in the size of 48 bits, x undergoes the FA and FC filtering functions in the first layer and is then divided into 5-bit values. In addition, one output value is obtained through the FC filtering function in the second layer. In addition, if there is more than 1-bit value, the filtering shall be repeated from first layer to only 1-bit value is left. The used symbols are explained in Table 1.

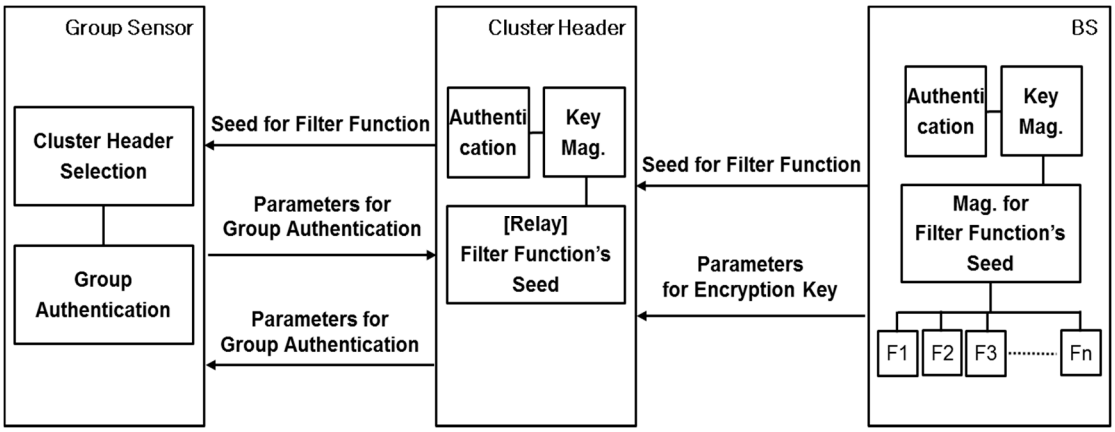

Figure 1. Proposed Scheme's Concept.

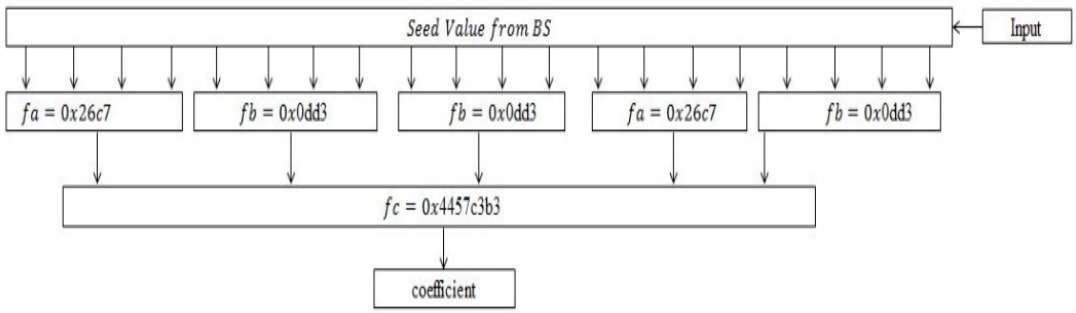

Figure 2. Filter Function.

Table 1. The symbols used in the scheme.

Symbols	Explanation
RN	Random Number
S-Box	Substitution-Box (S-box having no inverse matrix)
ID	Identification
K	Secret Shared Key
RB	Redundancy Bits

3.1. Cluster Header Authentication and Encryption Key's Elements Transmission

Figures 3 and 4 show the process of transmitting the filter function seed values, which the elected cluster headers (hereinafter referred to as CH) and the base station (hereinafter referred to as BS) will use for authentication and information transmission in mutual authentication and sensor group. The process thereof consists of the two rounds. The first round carries out the mutual authentication between BS and CH and the process of generating secret key. The second round is the process of transmitting filter function seed value for generating secret key and group sensor node secret key.

BS and CH exchange RN_{CH_1} and RN_{BS_1} and generate $4n$ bits stream $\{0, 1\}^n$ by utilizing the expansion substitution-box operator. The generated bits stream is separated into n bits stream, while the CH generates the second random number. The second random number and ID of CH are transmitted to BS using the challenge/response process. BS measures the time of the challenge/response process and verifies the distance between BS and CH.

The n bits stream is conducted r^0, r^1, ad, and lr. Afterwards, ID_{CH}' is derivate. BS generates different n bits stream, called 'c'. 'c' and ad are used to derivate challenge bits 'C'. When 'C' is derivate, lr is used as reference point. If lr_i is zero, 'C' is conducted $c_i || ad_i$. Otherwise, if lr_i is one, 'C' is conducted $ad_i || ad_i$.

After an initial process of challenge/response is run, BS sends challenge bits 'C' to CH. With that process started, BS also measures a time while the challenge/response process and verifies the distance between BS and CH against of relay attack.

For response, CH validates 'C' and operates 'R'. CH also could generate $4n$ bits stream and derivate 'C'. While BS derivates 'C', CH also derivates 'C'. And while BS sends 'C', CH derivates 'R'. 'R' is conducted r^0, r^1, and ID_{CH}'. When 'R' is derivate, there are two rules. The first rule is about a position of ID_{CH}'. If lr_i is zero, ID_{CH}' is positioned behind of r^0 or r^1. Otherwise, if lr_i is one, ID_{CH}' is positioned in front of r^0 or r^1. The second rule is about a value used. If c_i is zero, $r_i{}^0$ is used. Otherwise, if c_i is one, $r_i{}^1$ is used. Based on the two rules, 'R' is derivate and transmitted to BS.

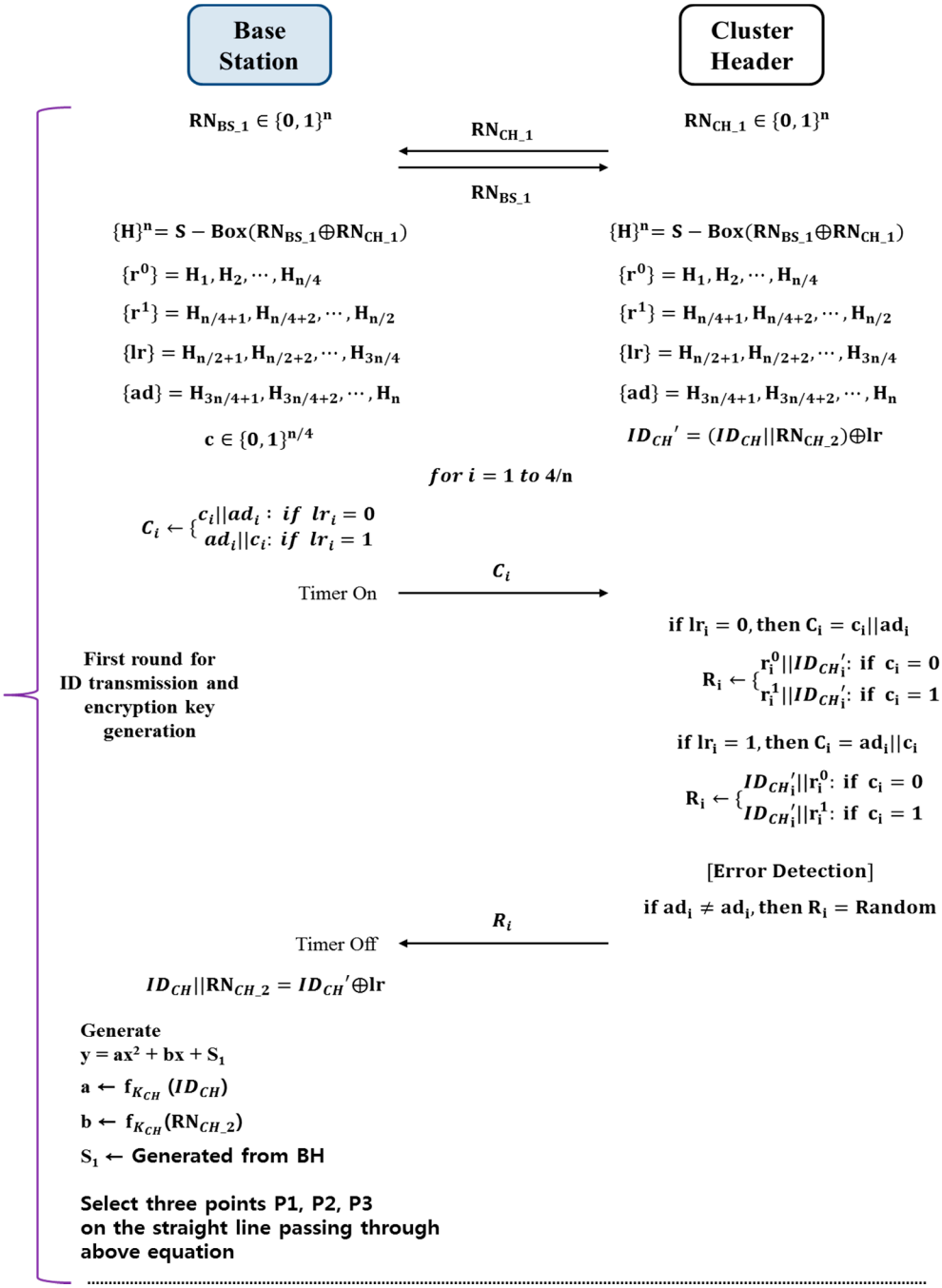

Figure 3. Cluster header authentication and encryption key's elements transmission protocol-1.

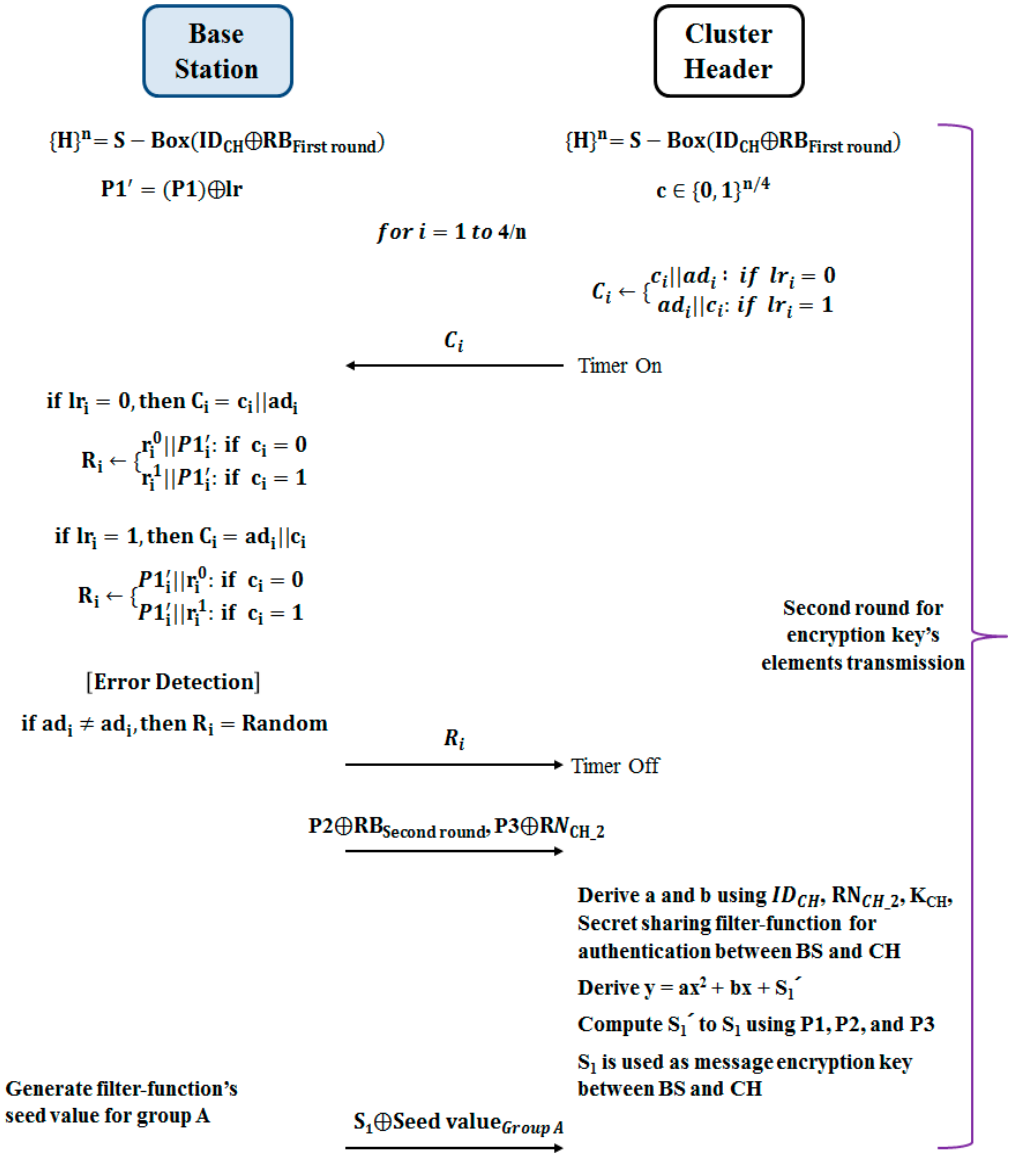

Figure 4. Cluster header authentication and encryption key's elements transmission protocol-2.

After CH's ID is transmitted, the process of generating a session key between BS and CH will begin. BS generates a second order polynomial with S (to be used as a session key) in the constant term. The coefficients of this polynomial will be derived by using ID of CH, which was transmitted in the challenge/response process, and the second random number. BS is the seed value of the filter function that was shared in advance. The resulting value of substituting ID and the random number in the filter function after substituting the secret key of CH is used as a coefficient of the polynomial. Lastly, BS selects the points (P1, P2 and P3) crossing the polynomial graph. In this process, only multiplication and addition is used to create P1, P2 and P3.

For the second round, BS and CH shall create a series of bit streams again. The ID and the result value obtained from the calculation of the remainder bit that is not used during the challenge/response in the first round becomes the bit stream of $4n$ bits, and the bit stream is separated into n bits. In the second challenge/response process, the response time is verified in CH and, through the challenge/response process, the point P1 in the polynomial is transmitted. Once the challenge/response process is finished, the remainder bit not used in the second challenge/response process and the random number, as well as P2 and P3, are XOR calculated and transmitted. Once the

transmission of all seed values is finished, CH obtains the polynomial for the recovery of secret value S. As in the calculation at BS, CH uses the ID, random number, secret key and filter function to create the polynomial. Afterwards, the received P1, P2 and P3 are put into the polynomial to get the secret value S.

The procedure of obtaining the secret value S is as follows. The coefficients in the polynomial of the cluster header are known but not the constants. The polynomial is a second-degree polynomial. So, if the three coordinates passing by are known, one can find out the constants. For this, P1, P2 and P3 are put into the cluster header to get the S, which can jointly meet the requirements.

Lastly, BS transmits CH the filter function seed value to be used in the group sensor nodes belonging to CH.

3.2. Group Sensor Authentication and Secure Sensor Information Transmission

Figures 5 and 6 show the process in which an elected cluster header conducts mutual authentication for all the sensor nodes simultaneously belonging to a group, and also derives a session key value to be used for transmitting sensor information. A process for each sensor node consists of the two rounds.

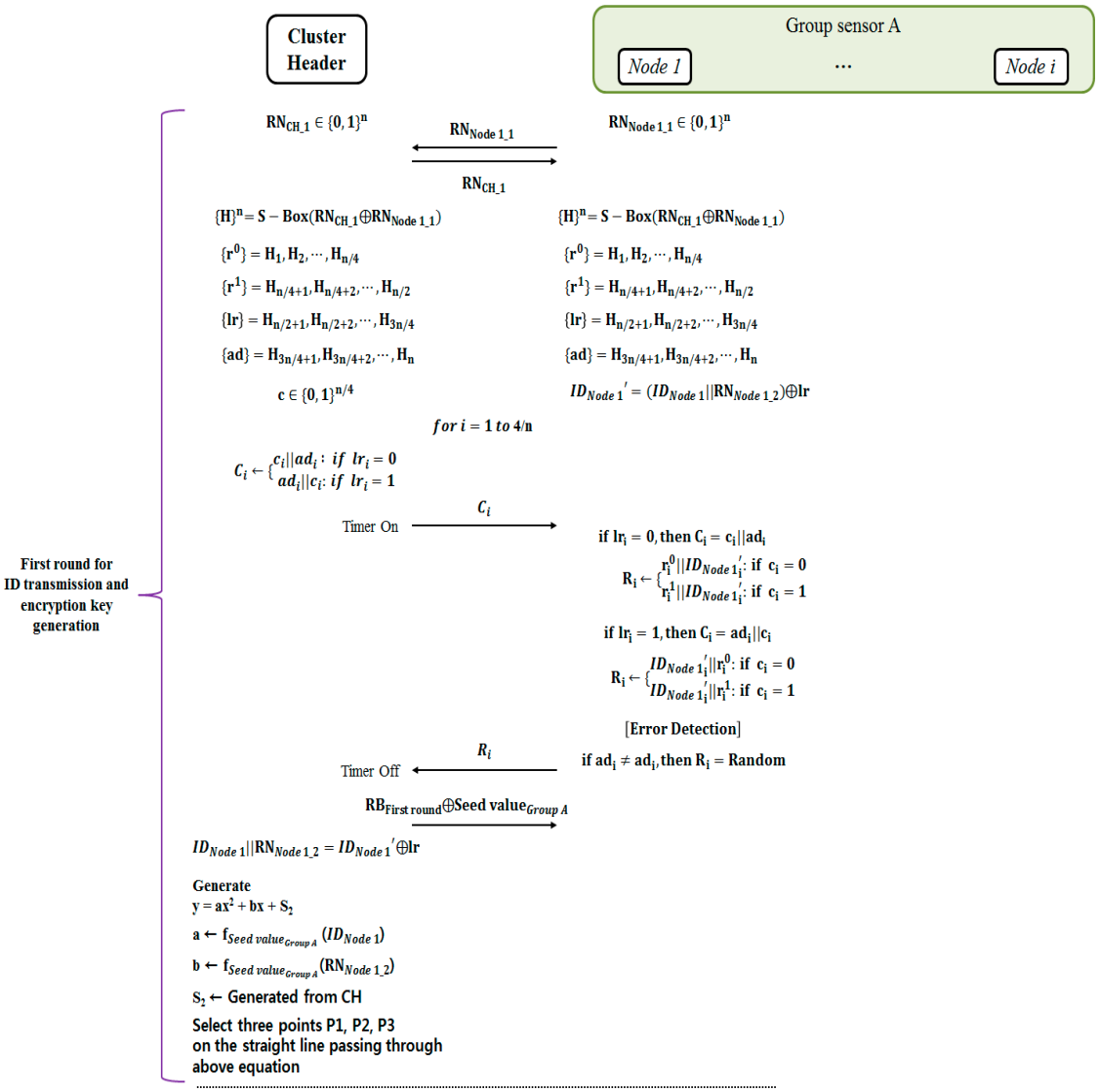

Figure 5. Group sensor authentication and secure sensor information transmission protocol-1.

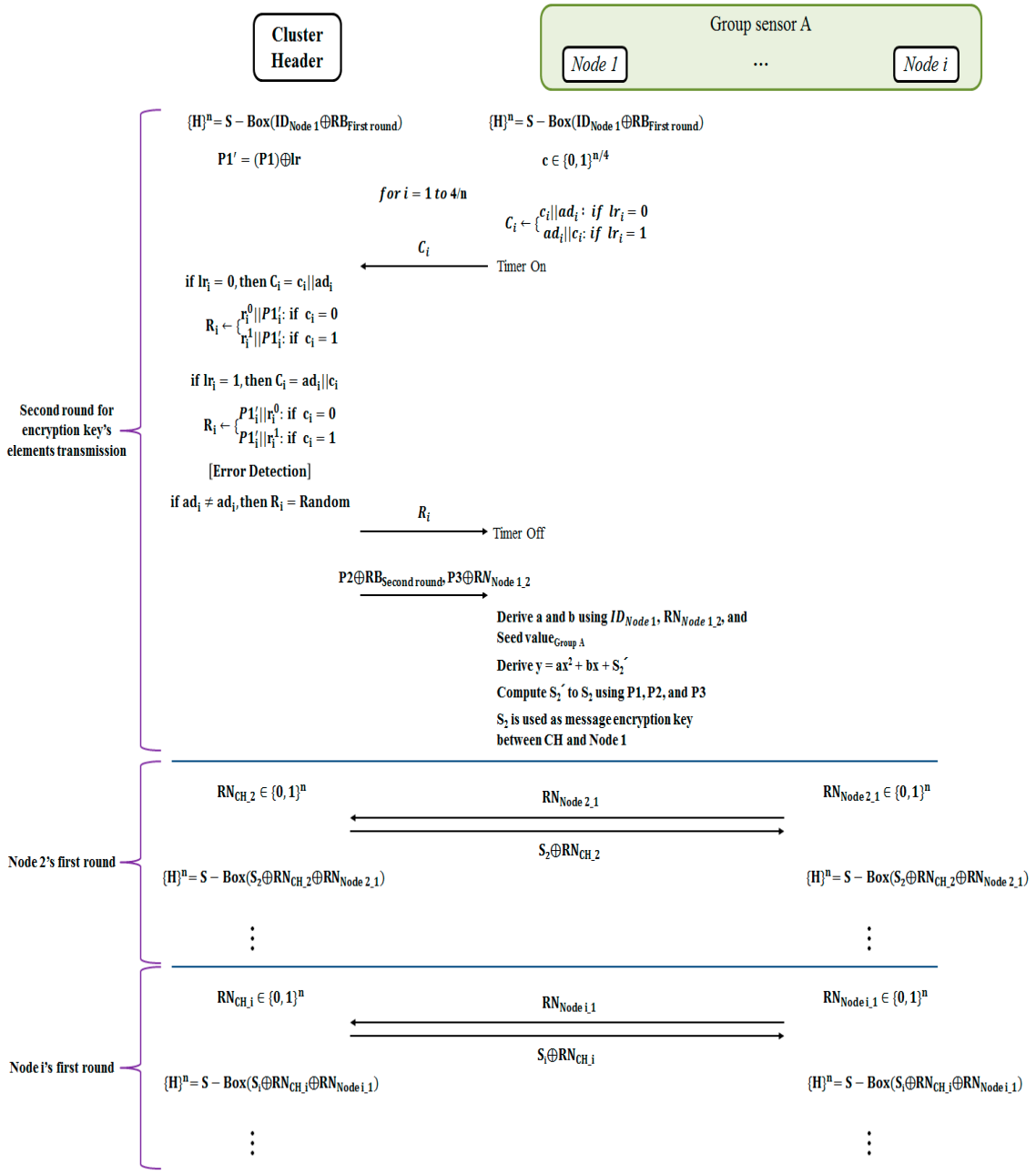

Figure 6. Group sensor authentication and secure sensor information transmission protocol-2.

The first round consists of the mutual authentication between CH and sensor node, the transmission of filter function seed value and the process of generating a session key. The second round is the polynomial transmission process to generate a session key to be used in a group sensor node.

CH and sensor node exchange RN_{CH_1} and $RN_{Node\_1\_i}$ and generate $4n$ bits stream $\{0, 1\}^n$ by utilizing the expansion substitution box operator. The generated bits stream is separated into n bits stream, while the sensor node generates the second random number. The second random number and ID of sensor node are transmitted to CH using the challenge/response process. CH measures a time while the challenge/response process and verifies the distance between CH and sensor node.

The n bits stream is conducted r^0, r^1, ad, and lr. Afterwards, ID_{Node_1}' is derivate. CH generates different n bits stream. And it's called 'c'. 'c' and ad are used to derivate challenge bits 'C'. When 'C'

is derivate, lr is used as reference point. If lr_i is zero, 'C' is conducted $c_i || ad_i$. Else if lr_i is one, 'C' is conducted $ad_i || ad_i$.

After initial process of challenge/response is run, CH sends challenge bits 'C' to sensor node. At that process started, CH also measures the time of the challenge/response process and verifies the distance between CH and sensor node against relay attack.

For the response, sensor node validates 'C' and operates 'R'. Sensor node also could generate $4n$ bits stream and derivate 'C'. While CH derivates 'C', sensor node also derivates 'C'. And while CH sends 'C', sensor node derivates 'R'. 'R' is conducted r^0, r^1, and ID_{Node_1}'. When 'R' is derivate, there are two rules. The first rule is about a position of ID_{Node_1}'. If lr_i is zero, ID_{Node_1}' is positioned behind of r^0 or r^1. Otherwise, if lr_i is one, ID_{Node_1}' is positioned in front of r^0 or r^1. The second rule is about a value used. If c_i is zero, r_i^0 is used. Otherwise, if c_i is one, r_i^1 is used. Based on the two rules, 'R' is derivate and transmitted to CH.

After sensor node's ID is transmitted, the process of generating a session key between BS and CH will begin. At this time, CH executes an operation on the filter function seed value received from BS with the remainder bit occurred in the first challenge/response process and then transmits the result of this operation to a sensor node. After then, CH generates a second order polynomial with S (to be used as a session key) in the constant term. The coefficients of this polynomial are derived through the ID of a sensor node transmitted in the challenge/response process and the second random number. CH substitutes the seed value of the filter function transmitted to a sensor node. The result value of substituting ID and the random number in the filter function is utilized as a coefficient of the polynomial. Lastly, CH selects the points (P1, P2 and P3) crossing the polynomial graph.

For the second round, CH and a sensor node generate a series of bit streams again. The resulting value of calculating ID and the remainder bit stream not used as seed of transmitted value in the challenge/response process of the first round becomes a n bit stream. This bit stream is again sub-divided into a bit stream of each n bits. The second challenge/response process verifies the response time in a sensor node. The point P1 above the polynomial is transmitted via challenge/response process. After the challenge/response process is completed, P2 and P3 undergo an XOR operation with the remainder bit and random number not used in the second challenge/response process and then they are transmitted. After transmitting all the seed values, a sensor node derives a polynomial for restoring the secret value S. As shown in the operation process in CH, a sensor node generates a polynomial by using the ID, random number, secret key and filter function. After this, it derives the secret value S by substituting the received P1, P2 and P3 in the polynomial. The derived S will be utilized as the encryption key to transmit sensor information.

After the first sensor node authentication and key derivation process are completed, the second sensor node will be processed. At this time, the value used in the first sensor node is transmitted to the second sensor node as though it is a random number, in order to guarantee that all the authentication and key derivation processes are continuous.

4. Security and Performance Analysis

4.1. Security Analysis

Table 2 shows the comparative analysis result on the security between the other group sensor management studies and the proposed scheme. As shown in the table, the proposed scheme has an outstanding level of security compared to the existing studies. In addition, it was confirmed that the proposed dynamic group management scheme would not only support for dynamic group allocation but also be secure to all the security vulnerabilities in a wireless sensor network environment by utilizing only the four fundamental arithmetic operations, logical operation and substitution operation.

Table 2. Comparative security analysis.

	Blundo's Protocol	Zhang's Protocol	Singelee's Protocol	Proposed Scheme
Relay attack	Not Secure	Not Secure	Secure	Secure
Replay attack	Not Secure	Not Secure	Not Secure	Secure
Eavesdropping	Secure	Secure	Not Secure	Secure
Leaked key	Not Secure	Secure	Secure	Secure
Sensor nodes anonymity	Not-supported	Not-supported	Not-supported	Supported
Dynamic group management	Not-supported	Not-supported	Not-supported	Supported
Mutual authentication	Not-supported	Supported	Not-supported	Supported
Forward security and Error detection	Not-supported	Supported	Supported	Supported
Mafia attack success probability	-	-	(1/2)^n	2*{1/(4*n-th Node)}^n
Terrorist attack success probability	-	-	(1/2)^n	2*{1/(4*n-th Node)}^(n*n-th Node)

4.1.1. Replay Attack and Relay Attack

A successful rate of mafia attack is 2*{1/(4*n-th Node)}^n, and rate of terrorist attack is 2*{1/(4*n-th Node)}^(n*n-th Node).

For attacks by mafia or terrorist groups to be successful, the attacker has to correctly hit all bits transmitted during the process of challenge/response. As in the general challenge/response process, nit bit shall be hit based on the probability of 50% of hitting 0 and 1, and the formula of (1/2)^n is obtained. In the proposed scheme, as two bits are transmitted to challenge/response, the attacker shall select one value among 00, 01, 10 and 11. This means a probability of 1/4. In addition, in case of group certification, n nodes are used. So, n multiplications are made. As the two challenge/responses are made for each node, the number 2 is further multiplied. As a result, the attacker can hit all bits with the probability of 2*{1/(4*n-th Node)}^n.

In addition, the proposed scheme provides security against replay attack using dynamic seed and transmission values. Base station, cluster head, and sensor node generate random numbers and use these to derivate authentication values, which are dynamic values based on substitution operator and filter function.

4.1.2. Sensor Node Eavesdropping and Anonymity

In the proposed paper, the plain values are the only random number values transmitted by the base station, cluster head, and sensor node. Also, when ID is transmitted, the position of ID is changed reference to random value and $4n$ bits stream. Because of that, an attacker could not analyze and recognize transmission values. In addition, anonymity is provided using an ID position change technique.

4.1.3. Error Detection and Forward Security

The base station, cluster head, and sensor node generate $4n$ bits stream and derivate challenge/response values. As a result, the base station, cluster head, and sensor node can validate the location where the ad value is transferred by the lr value during the distance bounding process. That is, the CH, BS, and sensor node can detect errors in the challenge/response process. If the CH, BS, and sensor node use the secret shared substitution box and if the seed value of the filter function is right, error detection and forward security are worked.

4.1.4. Dynamic Group Management

The proposed dynamic group management scheme supports the dynamic cluster header allocation of LEACH routing protocol. The LEACH routing protocol improves the energy efficiency by forming new groups and changing the cluster headers of a group on a continuous basis. However, the existing studies on sensor management were designed based on the network topology in which cluster headers were dedicated. The proposed scheme is different from the method to manage a group using one single group key. It continues to generate information transmission session keys based on polynomial

operation by receiving field function seed values from BS. As for group authentication, the proposed scheme utilizes simultaneous authentication that mixes information to be used for the authentication and key derivation between group sensors. That is to say, it conducts simultaneous authentication for group authentication in a way that it mixes the values to be used for authentication and the values to be used for key derivation rather than the way of authenticating a group by matching the key values. As a result, the proposed scheme supports the allocation of dynamic cluster headers and groups through the aforementioned way of group authentication.

4.2. Performance Analysis

In a sensor network environment such as smart dust, the light weighted certification hierarchy shall be used on a continual basis. However, the existing studies use algorithms such as hash and AES, which are hard to use in the sensor, having the limited calculation capacity due to the performance of hardware. Accordingly, in this section, the energy efficiency would be measured when the protocol is used, which is suggested for use in the limited sensors such as smart dust. So, here, the energy efficiency would be compared between the leach routing protocol, which is used for maximization of the energy efficiency, and the proposed protocol, without applying the security in the sensor network environment.

For the performance simulation, this study used a hundred-sensor node. The sensor nodes were randomly set. The virtual environment's size is 100 m $\times$ 100 m. The base station was designated in a specific location in consideration of the placement area. The distances between the base station and all sensor nodes are within the range from 50 m to 125 m depending on the placement. Each round was set at 20 s. In overall, the above settings were configured so that they would be equivalent to the existing routing protocol environment.

Figure 7 is the simulation result that analyzed the energy consumption of each routing protocol by increasing the critical distance. As can be seen in the deducted graph, it was confirmed that there was an insignificant difference between the energy consumption of the proposed security scheme and the energy consumption of the basic LEACH routing protocol [11] or LEACHC routing protocol [17].

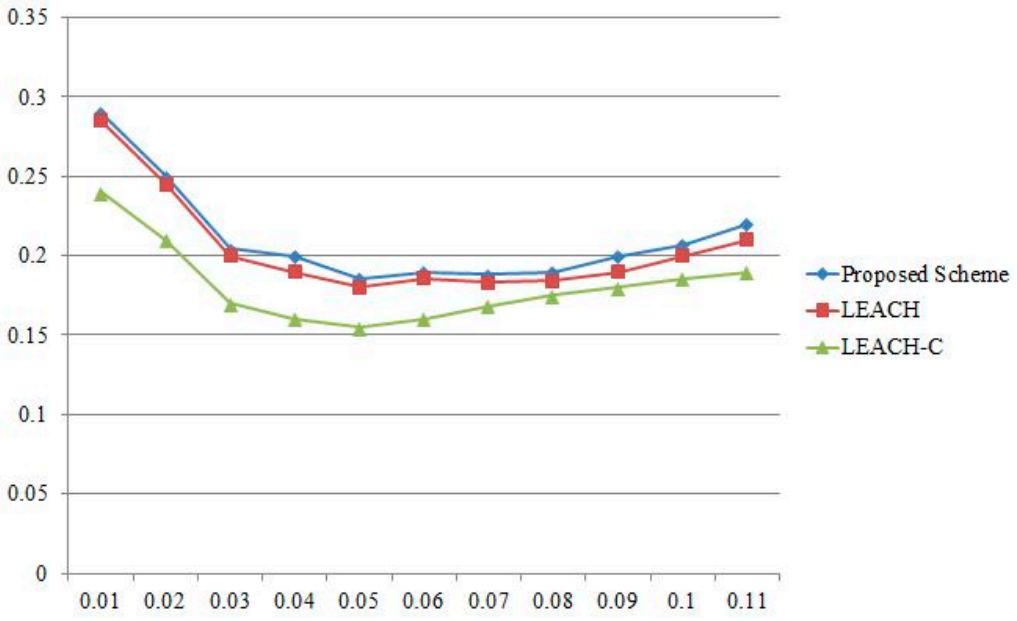

Figure 7. Performance analysis result.

5. Conclusions

This paper provides the measurements to manage the dynamically allocated cluster headers and group securely by utilizing the four kinds of fundamental arithmetic operator, substitution operator, and logical operator. The proposed scheme supports mutual authentication and confidential information transmission in the dynamically allocated cluster headers and groups through authenticating group sensor nodes simultaneously and allocating the keys. Moreover, it can verify the distance between the sensor nodes by utilizing the distance bounding. It is secure to the various vulnerabilities resulting from the nature of wireless sensor network environment.

The security provided by the proposed scheme not only provides logical security, but also physical security. The mutual authentication and e2e encryption communication offers confidentiality in communication in a logical way. If the proposed scheme is applied, actions can be taken against access by malicious users, infections by malicious codes, malicious updates of firmware and eavesdropping.

The dynamic group authentication and the distance-bounding technique contained in the proposed scheme also provide people with physical security. If even one sensor does not participate in authentication, the dynamic group authentication would fail. This kind of security leads to the sensor's function, which detects theft or damage. The distance-bounding technique allows the sensor implementing the authentication to sense the geological existence, thereby providing similar physical security as in a dynamic group authentication.

Also, it was confirmed that the proposed scheme had an insignificant difference in the energy consumption as compared with the existing routing protocols. The IoT environment will be the mesh network environment and the transfer of various kinds of information would happen on a sporadic basis. In addition, the cluster header will continue to transfer the information to servers for the analysis of information based on the cloud computing environment. Therefore, this could ultimately lead to service sustainability since both the demand for calculation at the cluster header and energy consumption is reduced. However, the calculation cannot be reduced for the quality in service. What is necessary is not reduction in energy consumption, but the efficient use of energy. The best routing protocol in terms of efficient energy use is the LEACH protocol. It can be said that the proposed scheme is more efficient than the LEACH protocol, which is the most efficient in energy consumption.

From the abovementioned analysis results, it is believed that the proposed dynamic group management scheme can be utilized as a sustainable and secure sensor node management scheme for providing high-quality intelligent services in the IoT environment [18].

Author Contributions: Hyungjoo Kim designed the proposed scheme; Hyungjoo Kim and Jungho Kang researched related work; Hyungjoo Kim and Jungho Kang performed and analyzed the scheme; Hyungjoo Kim and Jungho Kang wrote the paper.

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

References

1. Lee, E.J.; Kim, C.H.; Jung, I.Y. An Inteligent Gren Service in Internet of Things. *J. Converg.* **2014**, *5*, 4–8.
2. Benlamri, R.; Zhang, X. Context-aware recommender for mobile learners. *Hum. Centric Comput. Inf. Sci.* **2014**, *4*, 12. [CrossRef]
3. Howard, N.; Cambria, E. Intention awareness: Improving upon situation awareness in human-centric environments. *Hum. Centric Comput. Inf. Sci.* **2013**, *3*, 9. [CrossRef]
4. Ibrahim, N.; Mohammad, M.; Alagar, V. Publishing and discovering context-dependent services. *Hum. Centric Comput. Inf. Sci.* **2013**, *3*, 1. [CrossRef]
5. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. *IEEE Commun. Mag.* **2002**, *40*, 102–114. [CrossRef]
6. Degefa, F.B.; Won, D. Extended Key Management Scheme for Dynamic Group in Multi-cast Communication. *J. Converg.* **2013**, *4*, 7–13.
7. Yoon, M.; Kim, Y.K.; Chang, J.W. An Energy-efficient Routing Protocol using Message Success Rate in Wireless Sensor Networks. *J. Converg.* **2013**, *4*, 15–22.

8. Tishita, T.A.; Akhter, S.; Islam, M.I.; Amin, M.R. Spectrum Sensing and Data Transmission in a Cognitive Relay Network Considering Spatial False Alarms. *J. Inf. Process. Syst.* **2014**, *10*, 459–470. [CrossRef]
9. Bae, S. Power Consumption Analysis of Prominent Time Synchronization Protocols for Wireless Sensor Networks. *J. Inf. Process. Syst.* **2014**, *10*, 300–313. [CrossRef]
10. Dubey, T.; Sahu, O.P. Self-Localized Packet Forwarding in Wireless Sensor Networks. *J. Inf. Process. Syst.* **2013**, *9*, 477–488. [CrossRef]
11. Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 1–7 January 2000; pp. 1–10.
12. Ko, H.Y.; Doh, I.S.; Chae, K.J. Mutual Authentication Mechanism for Secure Group Communications in Sensor Network. *KIPS Trans. Part C* **2010**, *17*, 441–450. [CrossRef]
13. Blundo, C.; De Santis, A.; Herzberg, A.; Kutten, S.; Vaccaro, U.; Yung, M. Perfectly-secure key distribution for dynamic conferences. *Infor. Comput.* **1998**, *146*, 1–23. [CrossRef]
14. Zhang, W.; Cao, G. Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboratio-Based Approach. In Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, USA, 13–17 March 2005.
15. Mao, G.; Fidan, B.; Anderson, B.D. Wireless sensor network localization techniques. *Comput. Netw.* **2007**, *51*, 2529–2553. [CrossRef]
16. Singelee, D.; Preneel, B. Location verification using secure distance bounding protocols. In Proceedings of the Second IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS'05), Washington, DC, USA, 7–10 November 2005.
17. Heinzelman, W.B.; Chandrakasan, A.P.; Balakrishnan, H. An application-specific protocol architecture for wireless microsensor networks. *IEEE Trans. Wirel. Commun.* **2002**, *1*, 660–670. [CrossRef]
18. Kim, H. A Study on Authentication and Authority Management Framework Based on Certificateless in Integration IoT and Cloud Computing. Ph.D. Thesis, Soongsil University, Seoul, Korea, 2015.