sustainability

MDPI

Article

SH-SecNet: An Enhanced Secure Network Architecture for the Diagnosis of Security Threats in a Smart Home

Saurabh Singh, Pradip Kumar Sharma and Jong Hyuk Park *

Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 01811, Korea; singh1989@seoultech.ac.kr (S.S.); pradip@seoultech.ac.kr (P.K.S.)

* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702

Academic Editor: Sehyun Park
Received: 18 February 2017; Accepted: 27 March 2017; Published: 28 March 2017

Abstract: The growing demand for an independent and comfortable lifestyle has motivated the development of the smart home, and providing security is a major challenge for developers and security analysts. Enhancing security in the home environment has been recognized as one of the main obstacles to realizing the vision of creating energy-efficient smart homes and buildings. Understanding the risks associated with the use and potential exploitation of information about homes, end-users, and partners, as well as forming techniques for integrating security assessments into the design, is not straightforward. To address this challenge, we propose enhanced secure network architecture (SH-SecNet) for the diagnosis of security threats in the smart home. In our architecture, we use the Multivariate Correlation Analysis (MCA) technique to analyze the network flow packet in the network layer, as this classifies the network traffic by extracting the correlation between network traffic features. We evaluated the performance of our architecture with respect to various parameters, such as CPU utilization, throughput, round trip time, and accuracy. The result of the evaluation shows that our architecture is efficient and accurate in detecting and mitigating attacks in the smart home network with a low performance overhead.

Keywords: smart home; Internet-of-Things; security; threat diagnosis; Multivariate Correlation Analysis

1. Introduction

With the development of Wireless Sensor Network (WSN) and Radio Frequency (RF) technology, many Internet of Things (IoT) applications have been deployed in smart home systems over the past few years. The purpose of a smart home is to create an environment where the inhabitants can live comfortably, with minimal effort, and realize their preferred home environment [1]. A smart home is the application of ubiquitous computing that involves incorporating smartness into a home for comfort, safety, security, and energy saving [2]. Muhammad Raisul Alam et al. [3] reviewed the associated technologies of the past and present smart home and presented a concrete guideline for future research, to follow the practical development and sustainable smart home. IoT is the most promising paradigm, as the integration of several technologies applied to the smart home system [2]. Luigi Atzori et al. [4] surveyed the enabling technologies and illustrated the major benefits of the spread of this paradigm in everyday life. Smart home technology has advanced beyond essential accommodation functionality, such as self-controlling lights, automatic door features, advanced water sensors, and advanced energy metering systems for energy saving [5].

Smart home communication still exhibits security vulnerabilities that give rise to many security threats via attacks such as a Man-in-the-Middle (MITM) attack, replay, eavesdropping, impersonations, and a Denial of Service (DoS) attack [6,7]. An attacker can manipulate these devices and compromise the network, which can cause personal, financial, and physical damages [8–10]. These attacks also affect the communication and networking system in the smart grid. The smart grid also displays network vulnerability while communicating with the smart home system. Wenye Wang et al. [11] presented a comprehensive survey of cyber security issues and challenges of the smart grid. Smart metering for residential places, which provides homes with smart grids, is a necessary component of this since it transforms these spaces into energy-efficient, controlled smart homes [12]. Recent statistics show that about 40% of gross power consumption and 36% of CO_2 emissions in the European Union can be attributed to homes and buildings [13]. Domestic appliances need to be smarter, secure, safer, and energy-efficient; they should provide secure communication between other devices, have the leverage to secure smart homes and smart metering systems, and provide power consumption control leveraging to the grid.

Therefore, there is a need for reliability, scalability, manageability, and an eco-friendly smart home environment. In addition, it is necessary for an intelligent grid (smart grid) that is compatible with smart homes to provide energy-efficient infrastructure that is scalable and flexible. When the communication vulnerabilities of the smart home are exploited, they can seriously damage the entire infrastructure, give rise to financial issues for the consumer, wield a negative impact on smart home societies, and increase the probability of people losing their lives. Thus, security is still a primary concern in the smart home network. This has motivated us to conduct research on smart home network security issues and provide an efficient, secure solution.

Considering all of the aspects of existing research on security threats and attacks on smart homes, the idea of the paper is to develop a security system to protect smart home network communication. When more devices are linked to the system, more security flaws are revealed. Nowadays, DoS/DDoS attacks, MITM, eavesdropping, interception, and hijacking are related to both privacy and cyber security threats in the smart home. To deal with these attacks and challenges, we propose the SH-SecNet architecture to analyze the smart home network. The SH-SecNet architecture utilizes MCA detection analysis to detect DoS attacks in the real-time network traffic of the smart home. The technique extracts the geometric correlation hidden in the individual pairs of two distinct features within each traffic record, which offers accurate traffic behaviors. Moreover, the proposed architecture utilizes the cryptographic technique Elliptic Curve Digital Signature Algorithm ECDSA and keyed-Hash Message Authentication Code (HMAC), as well as applying a watermarking technique to the message, in order to fulfill the security parameters.

The rest of this paper is organized as follows: Section 2 discusses the challenges and security issues in a smart home environment and existing research; Section 3 proposes SH-SecNet architecture and discusses it in detail; Section 4 provides a description of our performance evaluation and experimental results; Section 5 presents the conclusion of our research.

2. Related Works

2.1. Benefits That Occur from Smart Home

Recently, energy-aware smart home technologies have effectively treated the home environment and workplaces comprised of separate and detached units. The integration of smart homes and smart grids introduces a holistic idea for smart homes that are placed and wisely managed within their wider environment. This may lead to successfully accomplishing the major goal of smart homes and smart grids. In this section, we discuss some of the advantages that result from these interactions [14].

2.1.1. Request Response Programs

This is a contract between the utility and its clients, promising the customer a decrease in duties or the promise of electricity bill rebates at the end of the month, on the condition that he or she consents to decrease his or her power consumption. The essential idea is that when all customers living in a smart home conserve energy, there will be sufficient power for everybody [15]. Nowadays, there are several different demand response programs which promote these policies, such as penalties, prizes, consumer cooperation, and notification policies. These programs can lower electricity costs in the market and maintain the supply and demand balance. This will help to develop a greener smart home, and, as a result, the smart grid becomes more reliable.

2.1.2. Load Shedding Programs

Koen Kok et al. described a procedure that is carried out by the electric utility operator in a centralized manner [16]. In an emergency, the power supply to the grid is switched off, to protect the grid from permanent damage. Also, in an emergency situation, load shedding management generally incorporates a shortage in supply that requires an instantaneous drop in demand, before the occurrence of an imbalance in the demand for supply puts the stability of the smart grid at risk and power becomes unavailable in the smart home [17].

2.1.3. Effective Feedback

The effectiveness of feedback on power consumption is an impressive rate of electric power wastage of every domestic unit that can be associated with the lack of a proper response or feedback [18]. The author refers to the monthly eccentricity bill as an example. In spite of the fact that it specifies the total consumption and the amount of money that the household is charged for it, it appears that power charge alone cannot help us to save energy because it does not reveal how the majority of power was spent.

Undoubtedly, a stable relationship between smart grids and energy conscious smart homes will allow for more viable feedback. For smart homes, the price setting signal is displayed at any time, and the device instantly provides details about energy consumption in terms of money. This kind of detailed information on electricity usage will deepen our understanding of energy usage and will support better-decision making of the grid.

2.1.4. Peak Shaving Capabilities

The advantage of the similarity profitability provided by smart homes and smart grid communications is the foundation for or the structure of a dynamic pricing scheme, which allows charging energies according to time and demand.

2.2. Attacks in Smart Home-Smart Grid

2.2.1. Man-In-The-Middle (MITM) Attack

The attacker impersonates the conveying party, for example, a smart home and smart grid controller, in the next gathering. It then inserts, modifies, and drops the packets. This kind of attack is directed at changing the functionalities of the smart grid, for example, the demand response, load shedding, and electric bills, and brings about financial losses to both sides of the parties involved [17].

2.2.2. Man-In-The-Browser (MITB) Attack

This is an internet-related threat in which a malicious program, such as Trojan, is involved in the attack. It takes control of the data entered by a client or the information recovered from the web server displayed by the browser. This attack can create damage for the client by showing false measurements about his or her power consumption, and not the accurate perceptions provided by the original reading of the smart meter [19].

2.2.3. Denial of Service (DoS) Attack

A DoS attack aims to make service inaccessible, and it could make a real-time charge inaccessible. The smart home system prompts similar attacks, and the grid-related operations cannot be accessed at the victim's smart home [20].

2.2.4. Attack against Home Monitoring and Control

As shown in Figure 1, the Energy System Interface (ESI) and Energy Management System (EMS) represent the inside environment of the smart home [21,22]. ESI is the interface between the smart home and smart grid. Threats in this type of scenario could incorporate an impersonation by an attacker to the client, a message modification attack, a replay attack, and much more. For instance, an attacker imitating the customer's cloud [23] that sends a message to HAN/ESI and requests it to turn on all of the home appliances for increasing the electricity bill or causes it to switch off the lights in a smart home, allowing the attacker to threaten the safety of those inside the house [24]. Also, message modification and a replay attack could have a significant impact on the smart home. For example, for the replay signal that operates the washing machine, the attacker could command it to repeatedly wash the clothes. This is known as a low-impact attack. On the other hand, in a message modification attack, a customer might want to remotely keep the temperature of the oven at 120 °C, but an attacker could modify this to 240 °C, which would automatically risk the lives of those inside the home. This is a high-impact attack.

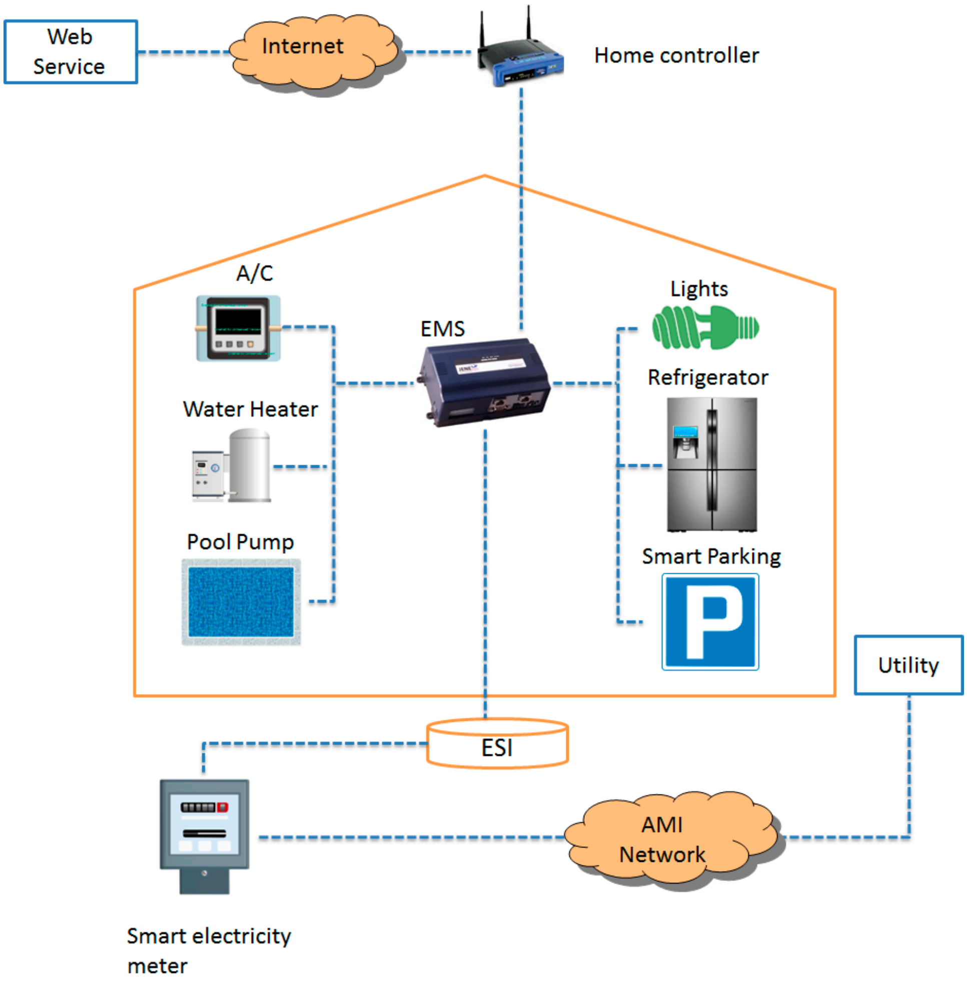

Figure 1. Smart home architecture.

2.3. *Security Challenges and Issues in Smart Home-Smart Grid*

In this section, we discuss the threat issues that initially affect the smart home, take control of the entities, and consequently affect the smart grid.

2.3.1. Threatening of Energy Consumption Reporting

A smart meter within the smart grid provides detailed information on smart home power consumption [25]. It might be threatened by an attacker who decides to change the meter information [26].

2.3.2. Attack Aiming the Demand Response Signal

In this scenario, HAN/ESI is impersonated by an attacker, to intercept the demand-response (DR) signal and replace it using a reply attack, or by modifying the signal by using a modification attack [5].

2.3.3. Issues with the Load Shedding Signal for ESI/HAN

This kind of issue first generates within the smart grid and then affects the smart home. Once in a while, as the demand for electricity increases, the available and planned spply are both interrupted in the form of load shedding [27]. As such, issues must be solved with a specific end goal to prevent instability in the smart home network, as this could harm the grid. This kind of issue is created by a DoS attack.

2.3.4. Issue against NAN Aggregator

The issue generated under this situation includes both the passive interception of information exchanged between ESI/HAN and the smart meter, and also the active modification of new data in the smart grid [28]. The attacker plans and carries out a meter impersonation by injecting false traffic into the grid, with a known result.

2.4. Existing Researches

Gergely Acs et al.'s research [29] presented a new scheme for privacy by preserving the smart metering system. It guarantees the customer's privacy by using holomorphic encryption and avoids involving a trusted third party by exploiting the perturbation algorithm. In this scheme, an electric supplier can periodically gather information from smart meters and determine the total statistics, instead of learning about the exercise of families. Their encryption algorithm is defined as the encryption key and modulo of the large prime number.

Yi Huang et al. proposed a defense mechanism to protect against injection attacks on a control center [30]. They proposed a cumulative sum (CUSUM) algorithm, which is recurrent in nature. It quickly detects attacks with a minimum number of observations.

Yue Li et al. introduced a lightweight key by establishing a protocol for smart home energy [31]. They came up with this because of the development of IoT applications in the smart home creating a security issue in the smart home energy management system. Their proposed scheme uses the Elliptic Curve Cryptography (ECC)-based model of the key establishment protocol.

Mohamed Nabeel et al. proposed a method based on the Physically Unclonable Function (PUF), to provide better hardware authentication for a smart meter [32]. They utilized effective key management to ensure integrity and confidentiality between the smart meter and utility. They utilized the PUF devices based on a one-way function to produce and reproduce a symmetric key and access level password for smart meters in the smart home.

Eun-Kyu Lee et al.'s research [33] suggested a frequency Quorum Rendezvous (FQR) that utilizes a random spectrum-based wireless communication for protecting against powerful attacks. It also prevents jamming attacks. IDS are also deployed to protect against a DoS attack.

Qian Huang et al. introduced high performance technology to be utilized in a smart home or intelligent building. The new technology is Li-Fi, which stands for Light-Fidelity. Li-Fi is a new kind of wireless communication system using light as a medium instead of traditional radio-frequency electromagnetic radiation. Li-Fi technology adopts an energy harvesting method to supply power in wireless sensors. Li-Fi enables a very high transmission speed compared to conventional Wi-Fi technology. Therefore, the energy harvest could easily and rapidly deliver an environmental parameter for control purposes [34].

Qian Huang et al. proposed a Wi-Fi-based indoor localization technology that greatly improves the indoor positioning accuracy with the help of Li-Fi-assisted coefficient calibration [35]. The proposed new technology leverages the existing indoor Li-Fi lighting and Wi-Fi infrastructure, to provide a cost-effective, accurate, and easy-to-use indoor localization framework.

Samrat Vikramaditya Tiwari et al.'s research [36] presented a model for smart home network technology based on multi-device bidirectional Visible Light Communication (VLC). The author described a typical indoor environment in which the proposed bidirectional VLC is evaluated for multiple devices in the smart home network. The author utilizes the color beams from RGB LEDs to transmit the data and also synchronizes multi-device transmission.

Samrat Vikramaditya Tiwari et al. [37] suggested a new modulation scheme known as color coded multiple access for multiuse VLC in smart home technologies. The authors use RGB Light Emitting Diodes (LEDs) for downlinking and Phosphorous-LED for uplinking, to establish bidirectional communication. The proposed scheme also provides flicker-free illumination that would lend itself to a multiuser VLC system for smart home applications.

2.5. Multivariate Correlation Analysis (MCA)

MCA, which plays an important role in the field of data analysis, is an artificial intelligence-based feature extraction technology for original data and legitimate data. MCA is used to characterize accurate network traffic by extracting the geometric correlation between the features of network traffic [38–40]. As shown in Figure 2, the detection process consists of three major steps:

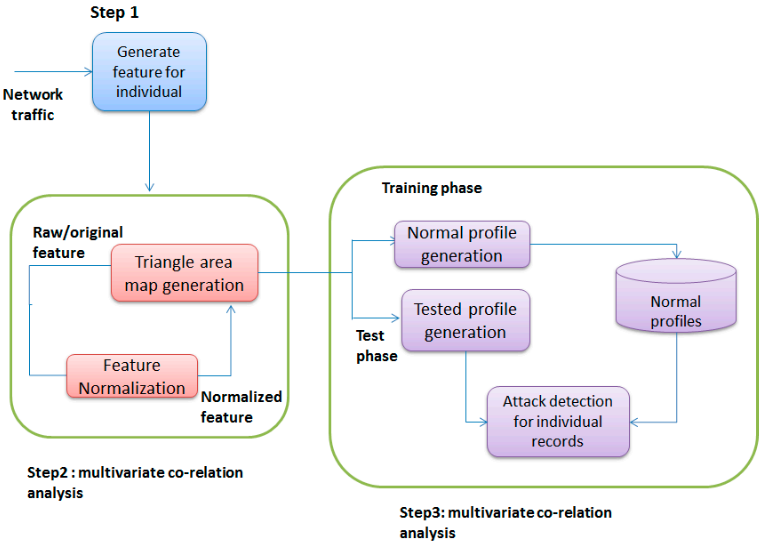
Step 1
Network traffic
Generate feature for individual
Raw/original feature
Triangle area map generation
Feature Normalization
Normalized feature
Step2 : multivariate co-relation analysis
Training phase
Normal profile generation
Normal profiles
Tested profile generation
Test phase
Attack detection for individual records
Step3: multivariate co-relation analysis

Figure 2. MCA system.

Step 1: The basic function is generated from the input network traffic to the internal network, where the protected server resides and is used to form traffic records of a definite time interval. The monitoring and analysis of the destination network reduces the overhead of detecting malicious activity by only concentrating on relevant inbound traffic. As a result, detectors are being developed for fewer network services than legitimate traffic profiles.

Step 2: MCA appiesthe "Generate Triangle Region Map" module to extract the correlation between two different features in each traffic record coming from the first step or extracts the correlation between the normalized profiles by the "feature normalization" module of the Multivariate Correlation Analysis step for extracting traffic records. The occurrence of the intrusion of the network causes these correlation changes, and the change can be used as an index for identifying intrusive activity. All extracted correlations, i.e., triangle areas stored in Triangle Area Maps (TAM), represent traffic records by replacing the original base feature or normalized feature. This provides more sophisticated identifying information to distinguish legitimate and illegal traffic records.

Step 3: An abnormality-based detection mechanism is adopted for decision-making. It facilitates the detection of all DoS attacks, without requiring knowledge related to attacks. In addition, frequent updating of the attack signature database in the case of a labor-intensive attack analysis and misuse-based detection is avoided. On the other hand, attackers need to generate attacks that match the normal traffic profile built by a specific detection algorithm, thus increasing the robustness of the proposed detector and making it difficult to avoid. However, this is a labor-intensive job, and it requires expertise in targeted detection algorithms.

3. Proposed SH-SecNet Architecture

Based on the analysis of existing research on the threats and challenges in a smart home and smart grid environment provided in Chapter 2, we propose a security architecture SH-SecNet in this chapter. The proposed architecture secures the smart home network by considering the security parameter and countering a DoS/DDoS attack.

3.1. SH-SecNet Architecture Overview

Figure 3 illustrates the architecture for securing the smart home network environment, and is comprised of four component layers, which are as listed below.

Application layer: The smart home integrates different kinds of applications, such as monitoring the home, remote access control, transport services, and emergency services. Also, a smart home helps to integrate the intelligence behind it. The proposed model contributes to, provides, and delivers all of the applications in a secure and energy-efficient manner to the end users.

Home gateway: The home gateway which acts as middleware in the smart home provides a high performance and flexibility. It can control and transfer the information between the home network and end users. It can also be used for data processing, and is easy and inexpensive to use. The home gateway in the proposed model is energy-efficient. It is based on energy harvesting techniques, such as solar, thermal, Radio Frequency (RF), and mechanical-based energy harvesting [41].

Network technology: The role of networking is to connect the home devices and to allow them to share information with each other. The two network technologies (wired and wireless) aggregate and control the information. In a smart home, the network is composed of the technologies as described below.

- Wired: This includes many traditional transmission infrastructures, such as electric wiring, coaxial cables, optical fibers, and telephones lines. HomePlug is widely adopted for power line communication and is mostly used for high-speed communication. Some other wired technology standards are X10, KNX, LonWorks, MoCA, and Insteon [42,43].
- Wireless: Two kinds of wireless technology are used in the smart home. The first is based on IEEE standards such as Bluetooth, WiFi, and ZigbeeOver. It is not based on any standardized methods such as PHY or MAC layers. These technologies include Z-wave, SimpliciTI, EnOcean, and Wavenis [42,44].
- Security layer: In SH-SecNet, the security mechanism is composed of many security attributes, which we have applied to our model. The security mechanism is used to analyse and protect the home network. It analyses the request and response data between home devices such as a health care system, multimedia, and an energy management system, and network technologies like those which are wired and wireless.

We used the cryptographic techniques ECDSA [45] and HMAC [46] to achieve confidentiality and authentication, as well as a watermarking technique [47,48], to provide integrity. Also, the model uses public key infrastructure [49] for inter-home device authentication. The MCA technique is applied to detect the DoS attack in the home network using triangle area map generation.

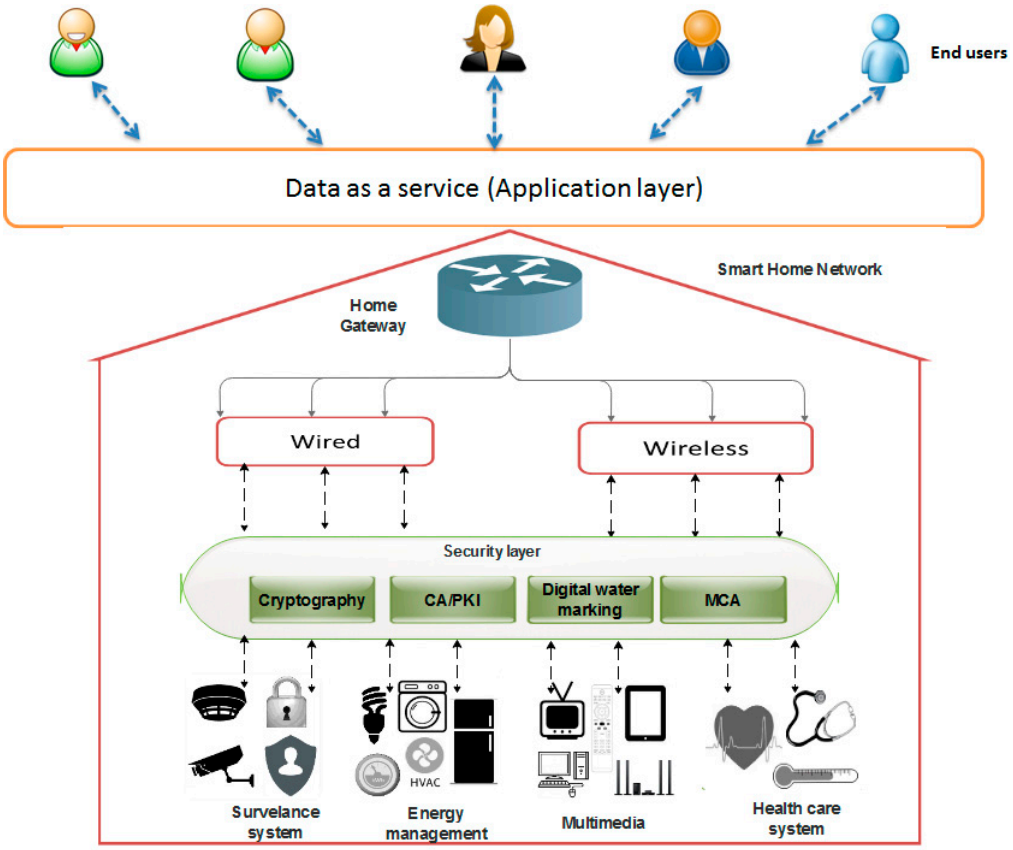

Figure 3. SH-SecNet home network overview.

3.2. Threat Analysis Flow

In this section, we analyze the anomaly-based network detection system in a smart home. Basically, SH-SecNet provides a network attack detection and reaction system in the smart home. The existing research provides detailed discussions on DDoS detection, but there is very limited work on the reaction option. In fact, even in the present work on DDoS security for today's Internet, the reaction choices are extremely basic and deficient, because the post-taking care of the method of reasoning requires the switches to be able to work for all things which are considered distributed. We will now present the detection and prevention attack algorithms that we implemented, as shown in Figure 4.

In SH-SecNet, the new packet arrives at the home gateway. After receiving notification checks, the operating system of the network controller determines whether the packet belongs to the flow or whether it is nonexistent. The new packet will be forwarded to the anomaly detection mechanism, which uses the Multivariate Correlation Analysis (MCA) algorithm and the known attack database. If the query result shows an attack packet, it will create an alert, and send the alert and packet information for further analysis. Otherwise, it first updates the home gateway and then forwards the packet for intelligence security analysis. The intelligence system's security creates the Data Flow Diagrams (DFDs) and analyzes the vulnerability using a vulnerability template. If it is a true vulnerability, it drops the packet, updates the rule, and stores its basic attack pattern information in a known attack DB to detect a similar pattern attack. Otherwise, it updates the home gateway and forwards the packet to the network.

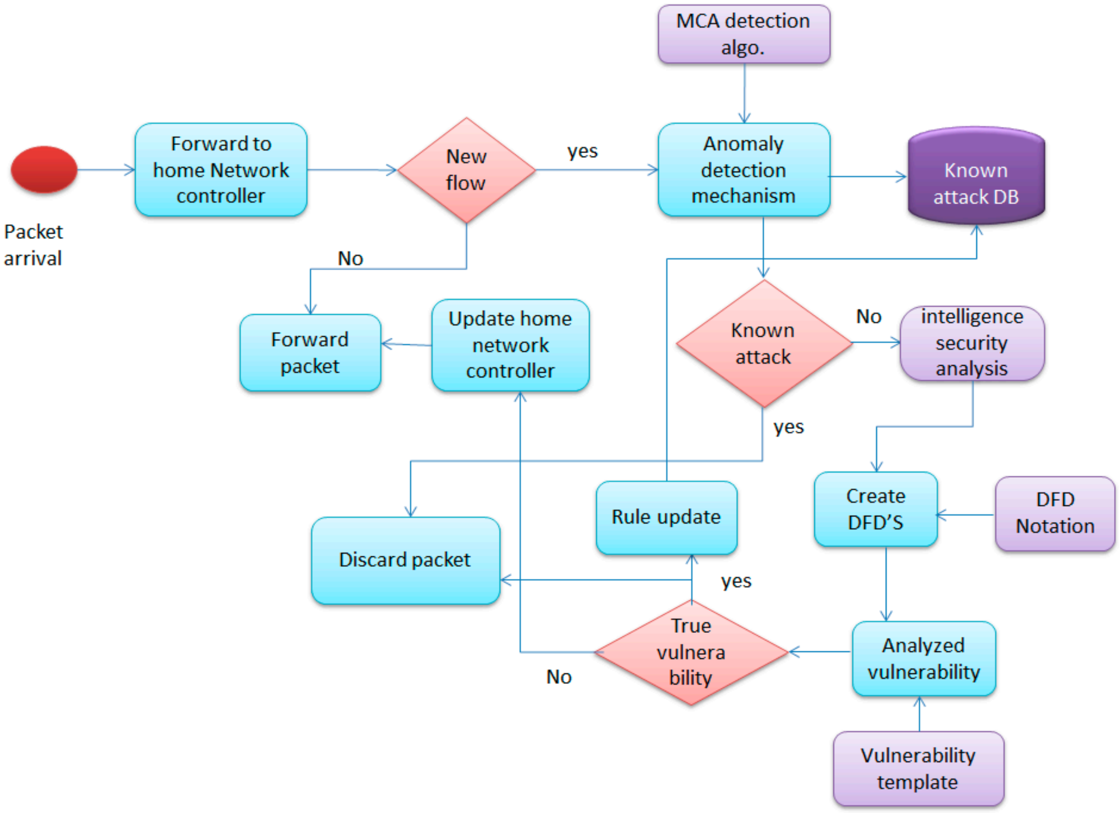

Figure 4. Smart home threat analysis flow diagram.

3.3. MCA Detection Analysis

To ensure the availability of our proposed network architecture against a DoS attack, we applied the MCA approach to our system for traffic classification by extracting the correlation between network traffic features. The MCA approach employs Triangle Area Map generation (TAM) [24]. The approach extracts the correlated data between features in an observed data object, such as network traffic records.

The arbitrary data set is given by: $D = \{d_1, d_2, = \{d_m\}$, where $d_i = \left[f^i_1\, f^i_2 \ldots\ldots f^i_n\right]^T$, $(1 \le i \le m)$ represent i-th n-dimensional traffic records. To find the correlation between the p-th and q-th feature in the vector d_i we utilize the concept of triangle area map generation. First, the vector d_i is projected onto a (p, q)-th two-dimensional Euclidean space

$$S_{i,p,q} = \left[\varepsilon_p,\ \varepsilon_q\right]^T x_i = \left[f^i_p\ f^i_q\right]^T, \text{ where}$$
$$(1 \le i \le m,\ 1 \le\ p \le n,\ 1 \le q \le n,\ p \ne q)$$

The two vectors $\varepsilon_p = \left[e_{p,1}\, e_{p,2} \ldots e_{p,n}\right]^T$ and $\varepsilon_q = \left[e_{q,1}\, e_{q,2} \ldots e_{q,n}\right]^T$ have m number of elements with a zero value, except (p, p) and (q, q), which have a value of one in ε_p and ε_q, respectively. The $S_{i,p,q}$ can be defined as a Cartesian coordinate system, and it is depicted as a two-dimensional Euclidean subspace, with the Cartesian coordinate point $(f^i_p,\ f^i_q)$. The triangle formed with the origin is $\Delta\ f^i_p O\ f^i_q$. Moreover, its area is defined as in Equation (1).

$$Tr^i_{p,q} = \left(\| \left(f^i_p,\ 0\right) - (0,\ 0)\| \times \| \left(0,\ f^i_q\right) - (0,\ 0)\ \|\right)/2 \qquad (1)$$

where: $1 \le i \le m,\ 1 \le\ p \le n,\ 1 \le q \le n,\ p \ne q$

To correctly and accurately conduct an analysis, we need to calculate all of the triangle areas on vector d_i. A triangle map area is constructed when all of the triangle areas are arranged in relation to their indexes. For instance, the map TAM^i is $n \times n$ in size, and the $Tr^i_{p,q}$ is coordinated on the p-th rows and k-th column. Moreover, the diagonal value is $Tr^i_{p,q} = 0,\ if\ p = q$. TAM^i is a symmetric matrix with a zero value of elements present in diagonal places.

When the two TAMs are compared, the differences can be easily identified on the upper or lower triangles because they are symmetrical in nature. Therefore, to investigate the TAMs, we chose either the upper triangle or lower triangle. So, the correlation which exists in the traffic record can be represented by the upper or lower triangles of their TAM^i. For the sake of consistency, we used the lower triangle for both TAMs. Therefore, the new correlation vector is denoted in Equation (2).

$$TAM^i_l = \left[Tr^i_{2,1}\ Tr^i_{3,1}\ \ldots\ Tr^i_{n,1}\ Tr^i_{3,2}\ Tr^i_{4,2}\ \ldots\ Tr^i_{n,2} \ldots Tr^i_{n,n-1}\right]^T \tag{2}$$

where l denotes the lower triangle. So, as previously mentioned, for data set D, its geometrical multi-correlation expression can be represented as seen in Equation (3).

$$D_{TAM_l} = \left\{TAM^1_l,\ TAM^1_l,\ \ldots\ldots\ldots\ldots TAM^m_l\right\} \tag{3}$$

When put into practice, the computation of $Tr^i_{p,q}$ in Equation (1) can be simplified, because the value of $Tr^i_{p,q}$ is eventually equal to half of the multiplication of the absolute value of f^i_p and f^i_q. Therefore, the transformation can be eliminated and the simplified version of Equation (1) is denoted in Equation (4).

$$Tr^i_{p,q} = \left(\left|f^i_p\right| \times \left|f^i_q\right|\right)/2 \tag{4}$$

As explained above, the MCA approach provides the following benefits for data analysis: first, it does not require a historical knowledge of data; second, it results in a lower latency in decision making; and, third, it provides a geometrical analysis.

Detection mechanism: This section presents threshold-based anomaly detectors that use legitimate network traffic records to generate regular profiles and are used for future comparisons with newly received investigated traffic records. The difference between the new incoming traffic record and each normal profile is checked by the proposed detector. If the dissimilarity is greater than the predetermined threshold, the traffic record is flagged as an attack. Otherwise, it is displayed as a legitimate traffic record. Clearly, normal profiles and thresholds directly influence the performance of the detector based on the threshold. Lower quality regular profiles cause incorrect characterization of legitimate network traffic. In this way, we apply the proposed triangulation area-based MCA method first, analyze legitimate network traffic and use the generated TAM to provide high-quality features for normal profile generation.

Normal Profile Generation: Assume l number of legitimate traffic records $R^{normal} = \left\{r^{normal}_1,\ r^{normal}_2,\ \ldots,\ r^{normal}_l\right\}$ are analyzed by the MCA approach using triangle area map generation. In TAM the lower part of the triangle of l, the number of legitimate traffic records is denoted as $R^{normal}_{TAM_{lower}} = \left\{TAM^{normal,\,1}_{lower},\ TAM^{normal,\,2}_{lower},\ \ldots,\ TAM^{normal,\,l}_{lower}\right\}$.

Maharanobis distance (MD) is adopted to measure the difference between traffic records. This is because MD has been successfully and widely used in cluster analysis, classification, and multivariate outlier detection technology. The Euclidean distance and Manhattan distance are different, and the distance between the two multivariate data objects is evaluated by considering the correlation between the variables and eliminating dependency on the measurement scale under calculation.

Threshold Selection: To differentiate the attack from the legitimate traffic, the threshold selection is defined as:

$$Threshhold = \beta + \rho \times \lambda$$

where α ranged from 1 to 3 in a normal distribution. This means the detection decision varies from 67% to 99% with a certain level of confidence in association with a certain level of confidence, in association with the different value of selecting λ. Therefore, if the MD is between observed traffic records $r^{observed}$ and their normal profile is greater than the threshold, then it is considered as an attack.

Attack Detection: For DoS attack detection, the lower triangle ($TAM_{lower}^{observed}$) of the TAM of a perceived record wants to be produced by using the proposed TAM-based MCA approach. Then, the md between $TAM_{lower}^{observed}$ and TAM_{lower}^{normal} stored in the respective pre-generated normal profile Pr is computed using Equation (4). The detailed detection algorithm based on Mahalanobis distance is as follow:

- Step1. Requirement of Observed traffic record $r^{observed}$, normal profile Pr : $(N(\beta,\ \rho^2),\ \overline{TAM_{lower}^{normal}},\ Crv)$ and Parameter λ
- Step2. Generate $TAM_{lower}^{observed}$ for the observed traffic record $r^{observed}$
- Step3. $md^{observed} \leftarrow md(TAM_{lower}^{observed},\ \overline{TAM_{lower}^{normal}})$
- Step4. If $(\beta - \rho \times \lambda) \leq md^{observed} \leq (\beta + \rho \times \lambda)$ then
- Step5. Return normal
- Step6. else
- Step7. Return attack
- Step8. End if

3.4. Security Analysis of Proposed Architecture

3.4.1. Confidentiality

There are many cryptographic techniques for achieving confidentiality. Modern cryptography uses private and public key cryptography. In our proposed model, we applied Elliptic Curve Cryptography (ECC), which has a smaller key size than RSA. ECC uses a popular algorithm called ECDSA. A signature-based algorithm is used to authenticate the communicating device that sends and receives the messages. ECDSA is a substitute for the Digital Signature Algorithm (DSA), which operates in the elliptic curve group of public key cryptography. Both messages sent from the source to the destination, from A to B, must match the elliptic curve region parameter. Device A is a randomly chosen integer that is less than n and n has a key pair consisting of a secret private key d_A, which is the degree of the curve and the public key $Q_A = d_A \times$ G (G is the generator point). The process of signature generation and verification of ECDSA is as detailed below:

(1) Signature generation

To sign a message 'm' by device A, using A's private key d_A

1. Compute e = H (m). Here, 'H' is a cryptographic hash function like SHA $-$ 1.
2. Select a random integer n from [1, z $-$ 1]
3. Compute r = p1 (mod z), here (p1, q1) = n $\times$ G. If r = 0, go to step 2.
4. Compute s = n $-$ 1(e + d_A $\times$ r) (mod z). If s = 0, go to step 2
5. The signature is the pair (r, s)

(2) Signature verification

For device 'B' to authenticate A's signature, B must have A's public key Q_A

1. Prove that r and s are integers in [1, z $-$ 1]. If it is not, the signature is invalid
2. Estimate e = H (m)
3. Estimate k = s $-$ 1 (mod z)
4. Compute t1 = ek (mod z) and t2 = rk (mod z)
5. Calculate (p1, q1) = G + t2 $\times$ Q_A
6. The signature is valid if p1 = r (mod z), invalid otherwise

3.4.2. Integrity by Digital Watermarking

Digital watermarking is a special kind of information concealment technology used to detect illegal copies. Digital watermarks are transmitted in a digitized form, with an information embedded identity.

The digital watermarking technology is suitable for data-centric wireless sensor networks. Rational watermarking algorithms can guarantee data security at low operational costs and effectively tolerate the impact of data processing. Using watermarking technology to solve the security problem of the network is a practical and effective solution.

The digital watermark algorithm consists of three basic procedures: watermark generation, watermark embedding, and watermark extraction or detection. The main idea of the watermarking algorithm is to generate watermarks and then embed them in the data collected by the sensor node. Watermark information is stored in the memory of the sensor node, before the data in this node is transmitted. The destination node activates watermark detection for the specified key and parameters. Only data with the correct watermark can be considered reliable. In the meantime, it must be subject to storage and transfer. Otherwise, it is considered a counterfeit, and is directly damaged and discarded.

Digital watermarking is used for ensuring data integrity and authenticating the embedding of digital data inside a meter reading. In the smart home and smart grid environment, the smart meter is a vulnerable point that can be moved to a non-secure location. The water marking technique that we applied to our approach is completely secure. In Figure 5, the home device sends a message 'm,' which is embedded with a watermark that is sent to the network channel. The extraction algorithm extracts the watermarked print and identifies it. If the watermark is changed, this means that the data is tempered and the system sends a request to the device to resend the watermark. If not, it means that the message has been received.

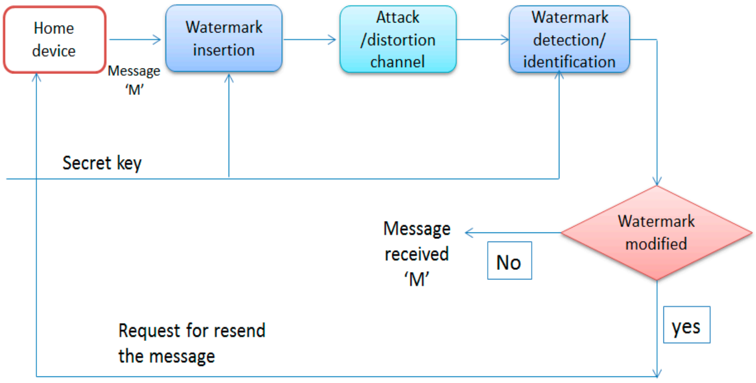

Figure 5. Ensuring integrity by water marking.

3.4.3. Ensuring Authenticity and Non-repudiation

ECC can be used to send a signed message request for authentication, just like with HMAC authentication. Here, the Diffi-Helman and hash-based authentication code are used for authentication. The two devices of A and B communicate with each other. First, device A will select a random number 'P^N' and encrypt the signal message with B's public key. The encrypted message A || B || P^N is sent to B. Similarly, device B generates P^M, decrypts the message, and sends the response A || B || P^N || P^M to A using A's public key. Both side devices can calculate P^{MN} and obtain the shared session key.

4. Experimental Results and Analysis

We carried out an in-depth performance assessment of the SH-SecNet architecture under various scenarios. Using real-time network traffic, we ran an identification precision test on our attack discovery model. SH-SecNet detects the DoS/DDoS attack by analyzing the network of a smart home and smart grid. The results of the evaluation are presented in this section.

4.1. Evaluation Dataset

To evaluate our module's ability to detect attacks, we used the CASAS dataset [50,51]. The CASAS dataset is a smart home based dataset. CASAS is a research project at Washington State University (WSU). Different kinds of sensors, like temperature, motion, and binary sensors are deployed at different locations in the smart home. These sensors are placed on various objects of the smart home, like doors, the fridge, TV, kitchen burner, and meter. Testing the approach on this dataset contributed to a compelling evaluation and allowed us to compare it with other methods. Through the assessment process, only 10% of the labeled data from the CASAS dataset is used, including legitimate traffic, such as TCP, UDP, and ICMP, as well as smart home specific protocol like ZigBee and Z-wave traffic.

4.2. Evaluation Process

Our general evaluation process was as follows. The initially proposed triangulation-based MCA approach is evaluated for its ability to describe network activity. Second, a tenfold mutual acknowledgment is derived for evaluating the detection performance of our proposed MCA-based detection system, and the entire separated information subset is utilized as part of this procedure. In the preparation phase, only the standard records are used. Regular profiles are built with various types of legitimate traffic, using trusted systems. Third, we used parameters such as the True Negative Rate (TNR), false positive rate (FPR), and accuracy (accurately classified sample percentage) for our detection system. We have also used energy consumption-based parameters that prove that our architecture is energy-efficient. In the detection method proposed by the present inventors, a high detection accuracy is required for it to be considered a good candidate.

4.3. Performance Comparisons

True Positive Rate (TPR): This is the ratio between the number of events that have been accurately classified as positive and the total number of events that can be categorized as positive. The denominator is the sum of the True Positive (TP) and False Negative (FN).

$$TPR = \frac{TP}{TP + FN}$$

where TP is the number of events that are properly identified and FN is the number of events that are incorrectly rejected.

False Positive Rate (FPR): This is the ratio between the number of events that were considered positive but should have actually been labeled as negative and the number of events that were properly rejected. The denominator is the sum of the False Positive (FP) and True Negative (TN).

$$FPR = \frac{FP}{FP + TN}$$

where FP is the number of misidentified events and TN is the number of events that have been properly rejected.

Receiver Operating Characteristics (ROC) Curve: This is a very popular technique for measuring the relationship between the TP and FP rates of the anomaly detection system. The ROC curve uses a function of the FP rate wherein the TP rate is plotted for different points, as shown in Figure 6. The closer the value of the ROC area is to one, the better it is; when it is closer to 0.0, it is poor. In Figure 6, the relationship between TPR and FPR is clearly shown in the ROC curve. In theory, TPR increases when a large number of FPRs are tolerated. Moreover, Figure 6 shows the comparison between our model SH-SecNet with TRW-CB and MaxEnt algorithms [52]. We can clearly see that our model has a higher accuracy than the others.

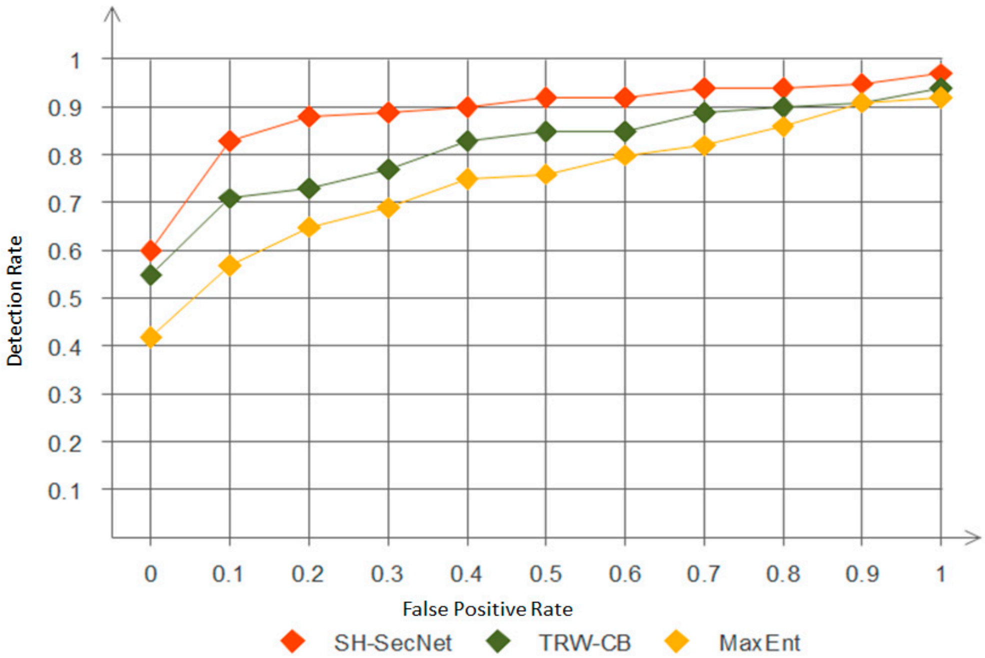

Figure 6. ROC curve between FPR vs. TPR for analyzing network data.

CPU utilization: This refers to a computer system's use of processing resources, handled by the CPU. Figure 7 shows two scenarios of CPU utilization before an attack and during an attack. As can be seen in Figure 7, in a normal case, the CPU workload behaves uniformly, but after an attack, the CPU workload increases exponentially, and when the security system is applied to the network, it gradually decreases after some time. Because the security system detects and discards the anomaly packets, no further analysis of the packet in the network occurs and this decreases the possibilities of congestion in the network, which causes a decrease in CPU utilization.

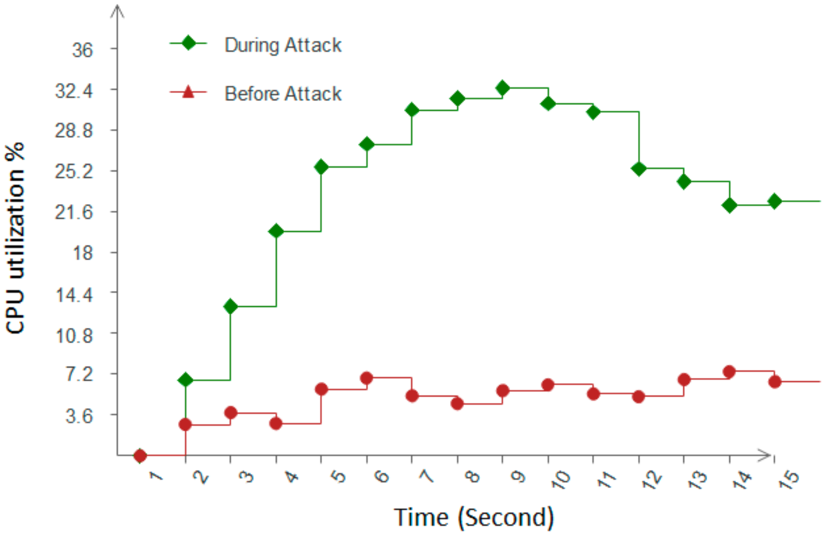

Figure 7. CPU Utilization.

Throughput: System throughput is the data transferred by the system. In Figure 8, initially before an attack, the throughput of the SH-SecNet, TRW-CB, and MaxEnt algorithms is approximately 90–96 Mbps. Initially, we can see that the proposed system has a slightly higher throughput than the other algorithms. After an attack is launched on the network, the throughputs of all three algorithms exponentially decrease until 3–5 s and behave uniformly. At the 4th second, the throughput is at a minimum level, which is below 20 Mbps. From 4 to 10 s, the throughput of the proposed system increases and recovers at a certain level, but the throughput of TRW-CB and MaxEnt remains below 20 Mbps. We can also say that a system with high throughput is more reliable and vice versa.

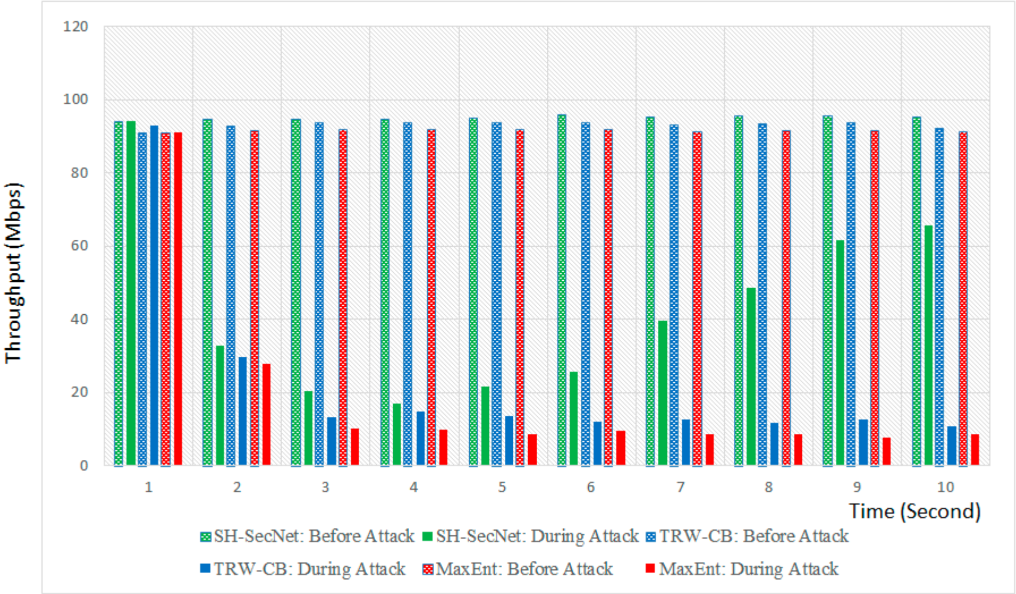

Figure 8. Throughput of the system.

Round Trip Time (RTT): This is the total time required for any packet to travel from the source to the destination and back to the source. To calculate RTT, we also added a packet delay. Figure 9 shows the RTT value with regard to the number of runs. As we know, a system with a low RTT value is more efficient. From the graph, initially before the attack, the RTT value is lower; gradually, however, the RTT value of all three algorithms increases, because of the delay in the network. If we compare the two algorithms TRW-CB and MaxEnt with the proposed model SH-SecNet, the latter is more efficient than the first two.

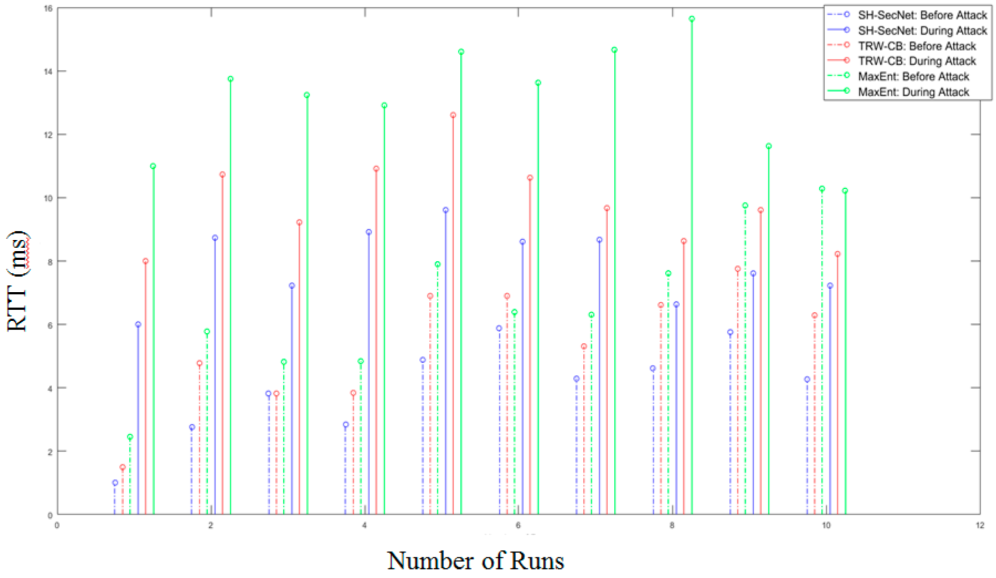

Figure 9. Round trip time.

4.4. Comparison with Existing Researches and Discussions

This section provides an analysis of our proposed SH-SecNet model, so as to compare it with existing research. The analysis is based on the security parameters of confidentiality, integrity, privacy, authentication, and availability in the smart home and smart grid environment.

Gergely Acs et al. proposed a scheme for privacy by preserving the smart metering system. The scheme utilizes homomorphic encryption, which results in the confidentiality and privacy of smart meters [29]. Moreover, the integrity of messages and authentication for smart homes is achieved by proposing a defense mechanism using the smart phone by Teddy Mantoro et al. [53]. They utilize the Diffie-Hellman key and RC4-based hash function to secure authentication and assure the integrity of messages between the central hub and remote devices. In addition, Mohamed Nabeel et al. proposed a method based on the Physically Unclonable Function (PUF), to provide better hardware authentication for a smart meter [32]. Moreover, Eun-Kyu Lee et al. provide availability using a Frequency Quorum Rendezvous (FQR) technique [33].

In Komal K More et al.'s research [40], they use MCA analysis for detecting a DoS attack in the network. They provide the availability for protecting against an DoS attack, but do not provide another security parameter like integrity, confidentiality, and authentication.

SH-SecNet utilizes MCA correlation analysis for analyzing the smart home network and preventing a DoS attack. SH-SecNet architecture applied the cryptographic techniques ECDSA and HMAC to achieve confidentiality and authentication, and achieved integrity using the watermarking technique.

As shown in Table 1, our proposed model covers all of the security parameters, unlike other existing works. Thus, it can be concluded that the SH-SecNet network architecture is more secure than that in existing research on the smart home and smart grid environment. Table 2 presents the quantitative analysis between the proposed model and existing algorithms. Specifically, Table 2 summarizes the percentage improvement obtained with our proposed scheme SH-SecNet compared to existing algorithms TRW-CB and MaxENT, for the various performance matrices.

Table 1. Comparison of security parameters with existing researches.

	Confidentiality	Integrity	Privacy	Authentication	Availability
[29]	✓		✓		
[32]	✓	✓			
[33]					✓
[40]					✓
[52]		✓		✓	
SH-SecNet	✓	✓	✓	✓	✓

Table 2. Percentage improvement with SH-SecNet over TRW-CB and MaxENT.

Parameter	Percentage Improvement
Accuracy	10%–15%
Throughput	47%–55%
RTT	24%–65%

5. Conclusions

In this paper, enhanced secure network architecture for diagnosing security threats in the smart home was presented. The network architecture has been adopted as middleware to ensure the security of various resource-constrained smart home devices in the home area network. The purpose of our proposed architecture is to analyze network packets and classify the network traffic by extracting the correlation between network traffic features using the triangle area-based MCA detection algorithm. The detection mechanism applied legitimate network traffic records to generate regular profiles and these are used for future comparisons with newly received investigated traffic records. We used the concept of an ECC-based signature algorithm to achieve the confidentiality. The digital watermarking algorithm is used to generate watermarks, which are embedded in the data by the sensor node. To assess the performance, we conducted an evaluation study using the CASAS dataset, to verify the effectiveness and performance of the proposed system. The threat analysis of the proposed model showed that when addressing new attack challenges, our SH-SecNet architecture is more efficient and accurate. The detection algorithm is also quite fast, with a high detection accuracy rate.

Acknowledgments: This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-H8601-16-1009) supervised by the IITP (Institute for Information & Communications Technology Promotion).

Author Contributions: Saurabh Singh: Research for the related works, analysis, design, meliorating the proposed model and drafting the article. Pradip Kumar Sharma: Acquisition of data, analysis, and interpretation of related works, conception, and design of and meliorating the complete model. Jong Hyuk Park: Total supervision of the paperwork, review, comments, assessment, etc.

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

References

1. Ahvar, E.; Daneshgar-Moghaddam, N.; Ortiz, A.M.; Lee, G.M.; Crespi, N. On analyzing user location discovery methods in smart homes: A taxonomy and survey. *J. Netw. Comput. Appl.* **2016**, *76*, 75–86. [CrossRef]
2. Toschi, G.M.; Campos, L.B.; Cugnasca, C.E. Home automation networks: A survey. *Comput. Stand. Interfaces* **2017**, *50*, 42–54. [CrossRef]
3. Alam, M.R.; Reaz, M.B.I.; Ali, M.A.M. A review of smart homes—Past, present, and future. *IEEE Trans. Syst. Man Cybern.* **2012**, *42*, 1190–1203. [CrossRef]
4. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
5. Siano, P.; Graditi, G.; Atrigna, M.; Piccolo, A. Designing and testing decision support and energy management systems for smart homes. *J. Ambient Intell. Humaniz. Comput.* **2013**, *4*, 651–661. [CrossRef]
6. Sun, X.; Men, S.; Zhao, C.; Zhou, Z. A security authentication scheme in machine-to-machine home network service. *Secur. Commun. Netw.* **2015**, *8*, 2678–2686. [CrossRef]
7. Wang, W.; Xu, Y.; Khanna, M. A survey on the communication architectures in smart grid. *Comput. Netw.* **2011**, *55*, 3604–3629. [CrossRef]
8. Xu, L.D.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inf.* **2014**, *10*, 2233–2243. [CrossRef]
9. Ng, H.S.; Sim, M.L.; Tan, C.M. Security issues of wireless sensor networks in healthcare applications. *BT Technol. J.* **2006**, *24*, 138–144. [CrossRef]
10. Yoon, S.; Park, H.; Yoo, H.S. Security issues on smarthome in IoT environment. In *Computer Science and Its Applications*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 691–696.
11. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371. [CrossRef]
12. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [CrossRef]
13. Bin, S.; Jun, L. Building Energy Efficiency Policies in China: Status Report. Available online: http://www.gbpn.org/reports/building-energy-efficiency-policies-china-status-report (accessed on 25 March 2017).
14. SmartHouse/SmartGrid. Available online: http://cordis.europa.eu/pub/fp7/ict/docs/sustainable-growth/fp7-smarthouse_en.pdf (accessed on 24 November 2016).
15. Siano, P. Demand response and smart grids—A survey. *Renew. Sustain. Energy Rev.* **2014**, *30*, 461–478. [CrossRef]
16. Kok, K.; Karnouskos, S.; Nestle, D.; Dimeas, A.; Weidlich, A.; Warmer, C.; Strauss, P. Smart houses for a smart grid. In Proceedings of the 20th International Conference and Exhibition on Electricity Distribution-Part 1, CIRED, Prague, Czech Republic, 8–11 June 2009; IET: Hertfordshire, UK, 2009; pp. 1–4.

17. Kamilaris, A.; Tofis, Y.; Bekara, C.; Pitsillides, A.; Kyriakides, E. Integrating web-enabled energy-aware smart homes to the smart grid. *Int. J. Adv. Intell. Syst.* **2012**, *5*, 15–31.
18. Zhao, H.; Magoulès, F. A review on the prediction of building energy consumption. *Renew. Sustain. Energy Rev.* **2012**, *16*, 3586–3592. [CrossRef]
19. Dougan, T.; Curran, K. Man in the browser attacks. *Int. J. Ambient Comput. Intell.* **2012**, *4*, 29–39. [CrossRef]
20. Jacobsson, A.; Boldt, M.; Carlsson, B. A risk analysis of a smart home automation system. *Future Gener. Comput. Syst.* **2016**, *56*, 719–733. [CrossRef]
21. Amer, M.; Naaman, A.; M'Sirdi, N.K.; El-Zonkoly, A.M. Smart home energy management systems survey. In Proceedings of the 2014 International Conference on Renewable Energies for Developing Countries (REDEC), Beirut, Lebanon, 26–27 November 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 167–173.
22. Han, J.; Choi, C.; Park, W.; Lee, I.; Kim, S. Smart home energy management system including renewable energy based on ZigBee and PLC. *IEEE Trans. Consum. Electron.* **2014**, *60*, 198–202. [CrossRef]
23. Singh, S.; Jeong, Y.S.; Park, J.H. A survey on cloud computing security: Issues, threats, and solutions. *J. Netw. Comput. Appl.* **2016**, *75*, 200–222. [CrossRef]
24. Zhou, B.; Li, W.; Chan, K.W.; Cao, Y.; Kuang, Y.; Liu, X.; Wang, X. Smart home energy management systems: Concept, configurations, and scheduling strategies. *Renew. Sustain. Energy Rev.* **2016**, *61*, 30–40. [CrossRef]
25. Longe, O.M.; Ouahada, K.; Rimer, S.; Harutyunyan, A.N.; Ferreira, H.C. Distributed Demand Side Management with Battery Storage for Smart Home Energy Scheduling. *Sustainability* **2017**, *9*, 120. [CrossRef]
26. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 21–38. [CrossRef]
27. Keles, C.; Alagoz, B.B.; Kaygusuz, A. A note on demand side load management by maximum power limited load shedding algorithm for smart grids. In Proceedings of the 2015 3rd International Istanbul on Smart Grid Congress and Fair (ICSG), Istanbul, Turkey, 29–30 April 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–5.
28. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88. [CrossRef]
29. Acs, G.; Castelluccia, C. Dream: Differentially private smart metering. *arXiv*, **2012**. arXiv:1201.2531.
30. Huang, Y.; Li, H.; Campbell, K.A.; Han, Z. Defending false data injection attack on smart grid network using adaptive cusum test. In Proceedings of the 2011 45th Annual Conference on Information Science and System (CISS), Baltimore, MD, USA, 23–25 March 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 1–6.
31. Li, Y. Design of a key establishment protocol for smart home energy management system. In Proceedings of the 2013 Fifth International Conference on Computer Intelligence Communication System and Network (CICSyN), Madrid, Spain, 5–7 June 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 88–93.
32. Nabeel, M.; Kerr, S.; Ding, X.; Bertino, E. Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communication (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 324–329.
33. Lee, E.; Oh, S.Y.; Gerla, M. Frequency quorum rendezvous for fast and resilient key establishment under jamming attack. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **2011**, *14*, 1–3. [CrossRef]
34. Huang, Q.; Li, X.; Shaurette, M. Integrating Li-Fi wireless communication and energy harvesting wireless sensor for next generation building management. *arXiv*, **2014**, arXiv:1602.07399.
35. Huang, Q.; Zhang, Y.; Ge, Z.; Lu, C. Refining Wi-Fi based indoor localization with Li-Fi assisted model calibration in smart buildings. *arXiv*, **2016**, arXiv:1602.07399.
36. Tiwari, S.V.; Sewaiwar, A.; Chung, Y.H. Smart home multi-device bidirectional visible light communication. *Photonic Netw. Commun.* **2016**, *33*, 1–8. [CrossRef]
37. Tiwari, S.V.; Sewaiwar, A.; Chung, Y.H. Color coded multiple access scheme for bidirectional multiuser visible light communications in smart home technologies. *Opt. Commun.* **2015**, *353*, 1–5. [CrossRef]
38. Tan, Z.; Jamdagni, A.; He, X.; Nanda, P.; Liu, R.P. A system for denial-of-service attack detection based on multivariate correlation analysis. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 447–456.
39. Tevari, G.M.; Goudar, R.H. Multivariate Correlation Analysis: An Approach to Detect DDoS Attacks in FTP. *Serv. Int. J. Sci. Technol. Eng.* **2016**, *2*, 424–427.
40. More, K.K.; Gosavi, P.B. A Real Time System for Denial of Service Attack Detection based on Multivariate Correlation Analysis Approach. In Proceedings of the International Conference on Electrical, Electronics,

and Optimization Techniques (ICEEOT 2016), Chennai, India, 3–5 March 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1125–1131.

41. Lu, X.; Wang, P.; Niyato, D.; Kim, D.I.; Han, Z. Wireless networks with RF energy harvesting: A contemporary survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 757–789. [CrossRef]
42. DP Mendes, T.; Godina, R.; MG Rodrigues, E.; CO Matias, J.; PS Catalão, J. Smart home communication technologies and applications: Wireless protocol assessment for home area network resources. *Energies* **2015**, *8*, 7279–7311. [CrossRef]
43. Vanus, J.; Smolon, M.; Martinek, R.; Koziorek, J.; Zidek, J.; Bilik, P. Testing of the voice communication in smart home care. *Hum.-Centric Comput. Inf. Sci.* **2015**, *5*, 1–22. [CrossRef]
44. Spadacini, M.; Savazzi, S.; Nicoli, M. Wireless home automation networks for indoor surveillance: Technologies and experiments. *EURASIP J. Wirel. Commun. Netw.* **2014**, *2014*, 1–17. [CrossRef]
45. Barenghi, A.; Bertoni, G.M.; Breveglieri, L.; Pelosi, G.; Sanfilippo, S.; Susella, R. A fault-based secret key retrieval method for ECDSA: analysis and countermeasure. *ACM J. Emerg. Technol. Comput. Syst.* **2016**, *13*, 8–23. [CrossRef]
46. Chandrakala, A.; Rao, S.B. Providing security by HMAC algorithm in P2P reputation management using distributed identities and decentralized recommendation chains. *Int. J. Innov. Res. Dev.* **2015**, *4*, 1–4.
47. Yan, X.; Zhang, L.; Wu, Y.; Luo, Y.; Zhang, X. Secure smart grid communications and information integration based on digital watermarking in wireless sensor networks. *Enterp. Inf. Syst.* **2017**, *11*, 223–249. [CrossRef]
48. Lalani, S.; Doye, D.D. A novel DWT-SVD canny-based watermarking using a modified torus technique. *J. Inf. Process. Syst.* **2016**, *12*, 681–687.
49. Im, H.; Kang, J.; Park, J.H. Certificate less based public key infrastructure using a DNSSEC. *J. Converg.* **2015**, *6*, 26–33.
50. Cook, D. CASAS Smart Home Project. [Online]. 2012. Available online: http://www.ailab.wsu.edu/casas/ (accessed on 1 January 2017).
51. Synnott, J.; Nugent, C.; Jeffers, P. Simulation of smart home activity datasets. *Sensors* **2015**, *15*, 14162–14179. [CrossRef] [PubMed]
52. Mehdi, S.A.; Khalid, J.; Khayam, S.A. Revisiting traffic anomaly detection using software defined networking. In Proceeding of International Workshop on Recent Advances in Intrusion Detection, Menlo Park, CA, USA, 20–21 September, 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 161–180.
53. Mantoro, T.; Ayu, M.A.; Binti Mahmod, S.M. Securing the authentication and message integrity for Smart Home using smart phone. In Proceeding of 2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, Morocco, 14–16 April 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 985–989.