entropy

MDPI

Article

A Multiple Rényi Entropy Based Intrusion Detection System for Connected Vehicles

Ki-Soon Yu [1], Sung-Hyun Kim [2], Dae-Woon Lim [1] and Young-Sik Kim [3,*]

[1] Major in Information Communication Engineering, Dongguk University, Seoul 04620, Korea; ykscj39@gmail.com (K.-S.Y.); daewoonlim@gmail.com (D.-W.L.)
[2] School of Computing, Korea Advanced Institute of Science and Technology, Daejeon 34141, Korea; harryzzong@kaist.ac.kr
[3] Department of Information and Communication Engineering, Chosun University, Gwangju 61452, Korea; iamyskim@chosun.ac.kr
* Correspondence: iamyakim@chosun.ac.kr; Tel.: +82-62-230-7032

Received: 31 December 2019; Accepted: 3 February 2020; Published: 6 February 2020

Abstract: In this paper, we propose an intrusion detection system based on the estimation of the Rényi entropy with multiple orders. The Rényi entropy is a generalized notion of entropy that includes the Shannon entropy and the min-entropy as special cases. In 2018, Kim proposed an efficient estimation method for the Rényi entropy with an arbitrary real order α. In this work, we utilize this method to construct a multiple order, Rényi entropy based intrusion detection system (IDS) for vehicular systems with various network connections. The proposed method estimates the Rényi entropies simultaneously with three distinct orders, two, three, and four, based on the controller area network (CAN)-IDs of consecutively generated frames. The collected frames are split into blocks with a fixed number of frames, and the entropies are evaluated based on these blocks. For a more accurate estimation against each type of attack, we also propose a retrospective sliding window method for decision of attacks based on the estimated entropies. For fair comparison, we utilized the CAN-ID attack data set generated by a research team from Korea University. Our results show that the proposed method can show the false negative and positive errors of less than 1% simultaneously.

Keywords: connected vehicles; intrusion detection system (IDS); Rényi entropy; Shannon entropy; vehicular network

1. Introduction

In modern cars, dozens of electronic control units (ECUs) are operated together, and they communicate over controller area networks (CANs). The connectivity between cars and the Internet will be further accelerated by the advancement of smart and autonomous vehicles. Increasing connectivity can help improve performance or convenience; however, modern vehicles have become more vulnerable to hacking attacks owing to this. Automotive systems based on CAN bus are already in common use, but no security considerations against hacking have been made since the design of the protocol. Since 2010, many instances of car hacking through the on-board diagnostics II (OBD-II) port for in-vehicle diagnosis and the infotainment system have been reported [1–8]. Thus, security measures for modern cars against hacking threats also have been actively researched [7,9,10]. Because vehicular security is an important issue today, we need a reliable solution to protect vehicles in motion. Here, we also need a lightweight algorithm since the available devices have very constrained computational power. In this paper, we propose a solution for a vehicular intrusion detection system (IDS) with both low complexity and reliability simultaneously.

Related Works

Network IDS (NIDS) is an important piece of network security equipment. Recently, machine learning based IDSs for general networks have been proposed for malware classification [11,12] and intrusion detection [13], which are based on a deep belief neural (DBN) network and can detect unknown attacks up to 97.5% of the time. However, a large dataset is necessary for the training process. For intrusion detection, entropy is also an important measure for anomaly. In [14], several kinds of entropy definitions, such as Shannon entropy, Rényi entropy, and Tsallis entropy, were used to detect intrusion at the same time. Then, it was improved by combining wavelet and principal component analysis with previous entropy measures [15]. In this paper, we focus on Rényi entropy in order to maintain low computational complexity in the vehicular environment. Additionally, a discretized extended feature space (DEFS) model is used for IDS [16], wherein the number of event patterns can be reduced by grouping similar patterns based on feature values. There is a probabilistic-driven ensemble (PDE) approach that operates by using several classification algorithms, whose effectiveness has been improved on the basis of a probabilistic criterion [17]. A series of experiments, performed by using real-world data, show how such an approach outperforms the state-of-the-art competitors, proving its better capability to detect intrusion events with regard to the canonical solutions.

To secure vehicular environments, two different approaches have been considered: security countermeasures based on encryption and authentication for data over vehicular networks, and intrusion detection systems that can detect suspicious activities on the networks [18–27]. In this work, we focus on the intrusion detection system based on the estimation of the Rényi entropy with multiple orders [28]. The Rényi entropy is a generalized notion of entropy that includes the Shannon entropy and the min-entropy as special cases [29].

In 2018, Kim proposed an efficient estimation method for Rényi entropy with arbitrary real order α [28]. In this work, we utilize this method to construct a multiple order Rényi entropy based intrusion detection system (IDS) for vehicular systems with various network connections. The proposed method estimates the Rényi entropies with three distinct orders, two, three, and four, simultaneously, based on the CAN-IDs of consecutively generated frames. The collected frames are split into blocks with fixed numbers of frames, and the entropies are evaluated based on these blocks. For a more accurate estimation against each type of attack, we also propose a retrospective sliding window (RSW) method on the estimated entropy values. For fair comparison, we utilized the CAN-ID attack data set generated by a research team from Korea University [30]. Our results show that the proposed method can show the false negative and positive errors of less than 1% simultaneously.

The rest of the paper is organized as follows. In Section 2, the basic definitions and notion are defined for the understanding of the proposed scheme. Additionally, two main attack models considered in this paper are explained. In Section 3, the theoretical analysis of Rényi entropy with respect to attack rate is presented. In addition, the proposed algorithm to measure multiple order Rényi entropies simultaneously and the improvements based on RSW method are provided. In Section 4, simulation results based on the vehicular attack data set are discussed. Finally, we conclude this paper in Section 5.

2. Preliminaries

The basic principle of an IDS for a vehicular system is the same as that of an IDS for a general network [31]. The first method requires storing pre-specified signatures of external attacks, inspection of transmitted packets, and analyzing whether any pattern matches with the stored signatures. The second method detects abnormalities using statistical characteristics of the normal range of the data generated by the vehicle.

One of the biggest differences between conventional networks and vehicular networks in the viewpoint of IDS is that messages generated and transmitted in intra-vehicular networks have uniform and regular characteristics, because the traffic usually conveys control or status information of the machine, unlike those made by humans over general networks. Because estimation is made by determining whether the abnormal phenomenon is normally deviated from the pattern, the probability of error can

be reduced, compared to general networks. Meanwhile, the computational power of the ECUs used in vehicles is limited compared to general network environments, and thus, complicated algorithms are not adequate in ECU environments. The time required to collect enough packets should also be minimized.

Entropy-based IDSs have been proposed, because the entropy measure can reflect the statistical characteristics of the traffic over networks [10,18]. Entropy based detection methods for intrusions have already been applied to IDSs for general networks, and these possibilities have been considered for vehicular environments. For example, [10] proposed an intrusion detection method using relative distance (RD) and conditional self-information (CSI) for vehicular networks. RD is the probability distribution of two sets of events, and is defined as

$$RD_{p|q}(x) = p(x) \log_2 \frac{p(x)}{q(x)}.$$

As the name suggests, RD can be used as a metric to determine the relative distance between two probability distributions. If $q(x)$ denotes the distribution of the normal intra-vehicular network traffic and $p(x)$ denotes the distribution of the current intra-vehicular network traffic, then the large value of $RD_{p|q}(x)$ gives the distance between $p(x)$ and $q(x)$. That is, it indicates that the current traffic represented by $p(x)$ is far from the normal one.

Entropy can be used as an indicator of abnormality in internal data of vehicles. However, to estimate the entropy of data sets generated in real time, the entropy can be calculated only after collecting enough data sets. This is because the distributions $p(x)$ and $q(x)$ should be available before $RD_{p|q}(x)$ can be calculated. It may not respond immediately to real time attacks since it has a complicated operation to deal with cumulative value of logarithms.

2.1. Shannon Entropy and Rényi Entropy

The first and the most popular definition of entropy for information is Shannon entropy [32]. Let F_2 be the finite field with two elements $\{0, 1\}$. Now, suppose that X is an L-bit output random variable from a random source $\mathcal{S}$. Then, the Shannon entropy is defined as

$$H(X) = -\sum_{b \in F_2{}^L} \Pr(b) \log_2 \Pr(b).$$

In this work, the random source $\mathcal{S}$ corresponds to a CAN system, and X corresponds to the continuously generated CAN-IDs over the network. L is given by $\lceil \log_2 M \rceil$, where M is the total number of used CAN-IDs. Vehicular IDSs based on Shannon entropy have been proposed.

In 1961, a more generalized definition of entropy for information was proposed by Rényi [29]. Because this generalized definition includes the Shannon entropy and the min-entropy (another popular entropy measure) as special cases, it has been utilized in many applications. The Rényi entropy is defined as

$$R_\alpha = \frac{1}{1-\alpha} \log_2 \sum_{b \in F_2{}^L} \Pr(b)^\alpha$$

where $\alpha > 0$ and $\alpha \neq 1$.

2.2. Efficient Estimation of Rényi Entropy

Recently, for real values of the order ($\alpha > 0$ and $\alpha \neq 1$), Kim proposed an efficient estimation of Rényi entropy, based on the distance to the nearest neighbor [28]. For the estimation, he defined a test function $f(s^N)$ for a random sample s^N of length N as

$$f(s^N) = \frac{1}{K} \sum_{n=1}^{K} g(D_n(s^N))$$

where $D_n(s^N)$ is the minimum distance between the current sample and the previous sample with the same CAN-ID as the current one. For the estimation of Rényi entropy of order α, the parameter $g(k)$ of the estimator for a given index distance k is given by

$$g(k) = \begin{cases} 1, & \text{if } k = 1 \\ (-1)^{k-1} P_{k-1}^{\alpha-2}, & \text{if } k \geq 2 \end{cases}$$

where

$$P_{k-1}^{\alpha-1} = \binom{\alpha-2}{k-1} = \frac{(\alpha-2)(\alpha-3)\cdots(\alpha-k)}{(k-1)!}.$$

For $\alpha = 2$, the parameter $g(x)$ is given by

$$g(x) = \begin{cases} 1, & \text{if } k = 1 \\ 0, & \text{otherwise.} \end{cases}$$

For $\alpha = 3$, the parameter $g(x)$ is given by

$$g(x) = \begin{cases} 1, & \text{if } k = 1 \\ -1, & \text{if } k = 2 \\ 0, & \text{oterwise.} \end{cases}$$

Finally, for $\alpha = 4$, the parameter $g(x)$ is presented as

$$g(x) = \begin{cases} 1, & \text{if } k = 1 \\ -2, & \text{if } k = 2 \\ 1, & \text{if } k = 3 \\ 0, & \text{oterwise.} \end{cases}$$

2.3. Attack Models

Originally developed by Bosch in 1983, CAN is a protocol designed for communication between micro-controllers. It was put in vehicles for the first time in 1989. CAN minimizes the cost of intra-vehicular communication, and it was standardized in 1993 by ISO as an international standard (ISO 11898). In vehicular applications, CAN has been used for connections and communications between engine management systems, transmission control systems, on-board controllers, and miscellaneous ECUs. It is possible to connect 2031 devices in a single network simultaneously. The CAN frame size varies from 44 bits to 108 bits, depending on the length of payload. Because the maximum bandwidth of CAN is 1 Mbps, it is possible to transmit 9259 frames in a second when the frame size is fixed as 108 bits.

An open CAN attack data set created by Korea University in 2017 [30] is utilized to evaluate the proposed IDS in the CAN environment. In this data set, two major attack types are considered, the denial of service (DoS) attack and the fuzzy attack. In accordance with CAN specifications, the CAN-IDs with lower values have higher priorities. Therefore, for the DoS attack, high priority CAN-IDs are intentionally injected into the network to prevent transmission of the normal network traffic. In case of the fuzzy attack, randomly generated CAN-IDs are continuously injected along with the normal traffic to interrupt the normal data transmission.

3. Theoretical Analysis of Entropy with Respect to Attack Rate

In this section, we analyze the values of the Rényi entropies theoretically against two attack models, the DoS attack and the fuzzy attack.

3.1. Case 1: DoS Attack

In case of the DoS attack, we assume that the CAN-ID with zero (the highest priority CAN-ID) is used in the attack frame. If the CAN-ID with zero is continuously injected, the other frame does not have any chance to transmit its data, owing to the priority. We first assume that there are K distinct CAN-IDs with distributions $(n_0, n_1, \ldots, n_K)$, each corresponding to CAN-ID 0 to K, in order.

If there is no attack (normal phase), we have $n_0 = 0$. Therefore, the total number of frames injected into the network is $N = \sum_{i=0}^{K} n_i$. Let $(d_0, d_1, \ldots, d_K)$ be the differences between the frequencies of each CAN-ID in the normal phase and in the attack phase. In this setting, if we add all of the differences, we have $\sum_{i=0}^{K} d_i = 0$. Then, we can represent the Rényi entropy $E_A(\beta)$ in the attack phase using the Rényi entropy in the normal phase E, where the attack rate β is given by $\beta = n_0/N$.

Theorem 1. *In the DoS attack scenario, the Rényi entropy with order α is defined as*

$$E(\beta) = -\frac{1}{1-\alpha}\log_2((1-\beta)^\alpha 2^{-(1-\alpha)E} + \beta^\alpha). \tag{1}$$

Proof. In the DoS attack model, the frequency of the attack CAN-ID with the highest priority increases, and the frequencies of the other CAN-IDs decrease. Thus, we have the following relation:

$$d_0 = -\sum_{i=1}^{K} d_i \text{ where } d_0 > 0 \text{ and } d_i < 0 \text{ for } 1 \le i \le K.$$

Then, the relative rates of the CAN-IDs (except for the attack ID) decrease with the attack rate β. Therefore, we have $d_i = -\beta n_i$, for $1 \le i \le K$. Thus, the probability of occurrence for each CAN-ID follows the distribution $(p_0, ..., p_K) = \{\frac{n_0}{N}, \frac{n_1}{N}, \ldots, \frac{n_K}{N}\}$. Thus, the Rényi entropy with order α for the normal phase is given by

$$E = \frac{1}{1-\alpha}\log_2\left(\frac{\sum_{i=0}^{K} n_i^\alpha}{N^2}\right). \tag{2}$$

Similarly, the Rényi entropy with order α for the attack phase is defined as

$$E_A(\beta) = \frac{1}{1-\alpha}\log_2\left(\frac{\sum_{i=0}^{K}(n_i + d_i)^\alpha}{N^2}\right). \tag{3}$$

Then,

$$\sum_{i=0}^{K}(n_i + d_i)^\alpha = \sum_{i=1}^{K}(n_i - \beta n_i)^\alpha + (\beta N)^\alpha \tag{4}$$

$$= (1-\beta)^\alpha \sum_{i=1}^{K} {n_i}^\alpha + N^\alpha \beta^\alpha. \tag{5}$$

Therefore, from the definition of Rényi entropy in (2), we have

$$\begin{aligned}\frac{\sum_{i=0}^{K}(n_i + d_i)^\alpha}{N^\alpha} &= (1-\beta)^\alpha \frac{\sum_{i=1}^{K} n_i^\alpha}{N^\alpha} + \beta^\alpha \\ &= (1-\beta)^\alpha 2^{-(1-\alpha)E} + \beta^\alpha.\end{aligned}$$

Finally, we have

$$E(\beta) = \frac{1}{1-\alpha}\log_2((1-\beta)^\alpha 2^{(1-\alpha)E} + \beta^\alpha).$$

□

3.2. Case 2: Fuzzy Attack

We now assume that the CAN-IDs are generated randomly, according to the uniform distribution. Suppose that the total number of occupied normal CAN-IDs is k. Owing to the randomly generated attack CAN-IDs, the total number of used CAN-IDs increases up to K, where $K \geq k$.

In the normal phase, the distribution of the CAN-IDs is given by $n_1, n_2, \ldots, n_k, n_{k+1}, \ldots, n_K$, where $n_{k+1} = ... = n_K = 0$. Then, we have $N = \sum_{i=1}^{k} n_i$, which corresponds to the total number of frames. Let the numbers of occurrences of individual CAN-IDs in the attack be $(d_1, \ldots, d_K)$, and let β be the attack rate defined by $\beta = \sum_{i=1}^{K} d_i/N$.

Because the CAN IDs injected by the attacker are uniformly and randomly generated, we can assume that $n_i = \frac{\beta N}{K}$ for $1 \leq i \leq K$. Because the attack can interrupt and collide with the normal transmission, we assume the reduced frequency of the normal CAN-IDs due to the attack is given by $c_1, c_2, \ldots, c_K$, such that $c_{k+1} = c_{k+2} = \ldots = c_K = 0$. If we assume that each CAN-ID has similar reduced rates due to the uniform random injection of each CAN-ID, we have $c_i = \beta N_i$. Again, for the Rényi entropy of order α for the normal phases, we have

$$E_\alpha = \frac{1}{1-\alpha}\log_2\frac{\sum_{i=1}^{K} n_i^\alpha}{N^\alpha} = \frac{1}{1-\alpha}\log_2(\frac{\sum_{i=1}^{k} n_i^\alpha}{N^\alpha}).$$

Theorem 2. *For given Rényi entropies E_2, E_3, and E_4 of orders two, three, and four, respectively, in the normal phase, we have the corresponding Rényi entropies in the attack phase, $E_2(\beta)$, $E_3(\beta)$, and $E_4(\beta)$ of orders two, three, and four, with attack rate β as follows:*

(1) For $\alpha = 2$, we have

$$E_2(\beta) = -\log_2\left((1-\beta)^2 2^{-E_2} + \frac{\beta(2-\beta)}{K}\right);$$

(2) For $\alpha = 3$, we have

$$E_3(\beta) = -\frac{1}{2}\log_2\left((1-\beta)^3 2^{-2E_3} + 3\frac{\beta(1-\beta)^2}{K}2^{-E_2} + \frac{\beta^2}{K^2}(3-2\beta)\right);$$

(3) For $\alpha = 4$, we have

$$E_4(\beta) = -\frac{1}{3}\log_2\left((1-\beta)^4 2^{-3E_4} + 4\frac{\beta(1-\beta)^3}{K}2^{-2E_3} + 6\frac{\beta^2(1-\beta)^2}{K^2}2^{-E_2} + \frac{\beta^3}{K^3}(4-3\beta)\right).$$

Proof. For the attack phase, we can represent the Rényi entropy as follows:

$$E_\alpha(\beta) = -\frac{1}{1-\alpha}\log_2\left(\frac{\sum_{i=1}^{K}(n_i + d_i - c_i)^\alpha}{N^\alpha}\right).$$

The inner summation of the logarithm is given by

$$\begin{aligned}\sum_{i=1}^{K}(n_i+d_i-c_i)^{\alpha} &= \sum_{i=1}^{k}(n_i+\frac{\beta N}{K}-\beta n_i)^{\alpha}+(K-k)\left(\frac{\beta N}{K}\right)^{\alpha}\\ &= \sum_{i=1}^{k}((1-\beta)n_i+\frac{\beta N}{K})^{\alpha}+(K-k)\left(\frac{\beta N}{K}\right)^{\alpha}\\ &= \sum_{i=1}^{k}\sum_{j=0}^{\alpha}\binom{\alpha}{j}((1-\beta)n_i)^{j}\left(\frac{\beta N}{K}\right)^{\alpha-j}+(K-k)\left(\frac{\beta N}{K}\right)^{\alpha}\\ &= \left(\frac{\beta N}{K}\right)^{\alpha}\sum_{j=0}^{\alpha}\binom{\alpha}{j}(1-\beta)^{j}\left(\frac{\beta N}{K}\right)^{-j}\sum_{i=1}^{k}n_i^{j}+(K-k)\left(\frac{\beta N}{K}\right)^{\alpha}\\ &= \left(\frac{\beta N}{K}\right)^{\alpha}\left[\sum_{j=0}^{\alpha}\binom{\alpha}{j}\left(\frac{1-\beta}{\beta}\right)^{j}\left(\frac{K}{N}\right)^{j}\sum_{i=1}^{k}n_i^{j}+(K-k)\right]. \end{aligned} \quad (6)$$

By applying $\alpha = 2, 3, 4$ to (6), the statements of this theorem are proven. □

3.3. Proposed Algorithm for Estimation of Rényi Entropies with Orders 2, 3, and 4

The proposed IDS scheme identifies intrusions based on the estimated Rényi entropies and the changing patterns of the estimated entropy values for block-wise data. The continuously produced CAN frames are split into blocks, and the estimated values are updated on the outstanding blocks via the RSW method to quickly produce intermediate entropy values. Based on the estimation method for the Rényi entropies described in Section 2.2 [28], we can formulate Algorithm 1 for estimating Rényi entropies with three distinct orders 2, 3, and 4 simultaneously, using the blocks with fixed lengths N_S, which contain consecutive N_S frames over the CAN.

Algorithm 1: Proposed estimation of Rényi entropy with multiple orders 2, 3, and 4.

Input : Consecutive CAN-IDs r_i obtained from the traffic over CAN
Output: Estimated value of Rényi entropy (R_2, R_3, R_4) for each block

```
begin
    S_2 ← 0; S_3 ← 0; S_4 ← 0; // To accumulate estimated values over blocks
    while True do
        A_2 ← 0; A_3 ← 0; A_4 ← 0; // To count the specific patterns
        L_1 ← 0; L_2 ← 0; L_3 ← 0; // To store the three previous CAN-IDs
        // Calculation over a block
        for i = 1 to N_B do
            r_i ← Current CAN-ID;
            if r_i == L_1 then
                A_2++; A_3++; A_4++;
            end
            else if r_i == L_2 then
                A_3 ← A_3 − 1; A_4 ← A_4 − 2;
            end
            else if r_i == L_3 then
                A_4++;
            end
            L_3 ← L_2; L_2 ← L_1; L_1 ← r_i; // Update the three previous CAN-IDs
        end
        S_2 ← ωS_2 + A_2; S_3 ← ωS_3 + A_3; S_4 ← ωS_4 + A_4;
        R_2 ← −log_2(S_2(1 − ω)/N_B);
        R_3 ← −log_2(S_3(1 − ω)/N_B);
        R_4 ← −log_2(S_4(1 − ω)/N_B);
        return (R_2, R_3, R_4)
    end
end
```

3.4. Improving Accuracy Using a Characterizing Attack Pattern with RSW

In the proposed scheme, attacks can be detected using the Rényi entropies derived from the frequencies of individual CAN-IDs embedded in the CAN frames. In this subsection, we explain the parameters and criteria for the detection, such as block size, acceptable range, and RSW size. Usually, it is not possible to detect intrusions immediately because of the estimation of Rényi entropy. To overcome this shortcoming, we propose a retrospective way of decision-making that can improve the missing probability of the proposed IDS. This will be used to audit and analyze the attack features after the attack or central monitoring server to prevent similar attacks later.

To enhance the accuracy of detection, we can also utilize the characteristics of specific attacks, such as the DoS attack and fuzzy attack. The DoS attack exploits the order of priorities of the CAN frames. Therefore, if the highest order CAN-ID is consecutively inserted into the network, the normal traffic does not have any chance to transmit. However, in this case, the estimated entropy is significantly reduced owing to the reduction in randomness (uncertainty). This can be observed in the sample test data obtained from Korea University, as shown in Figure 1 [30].

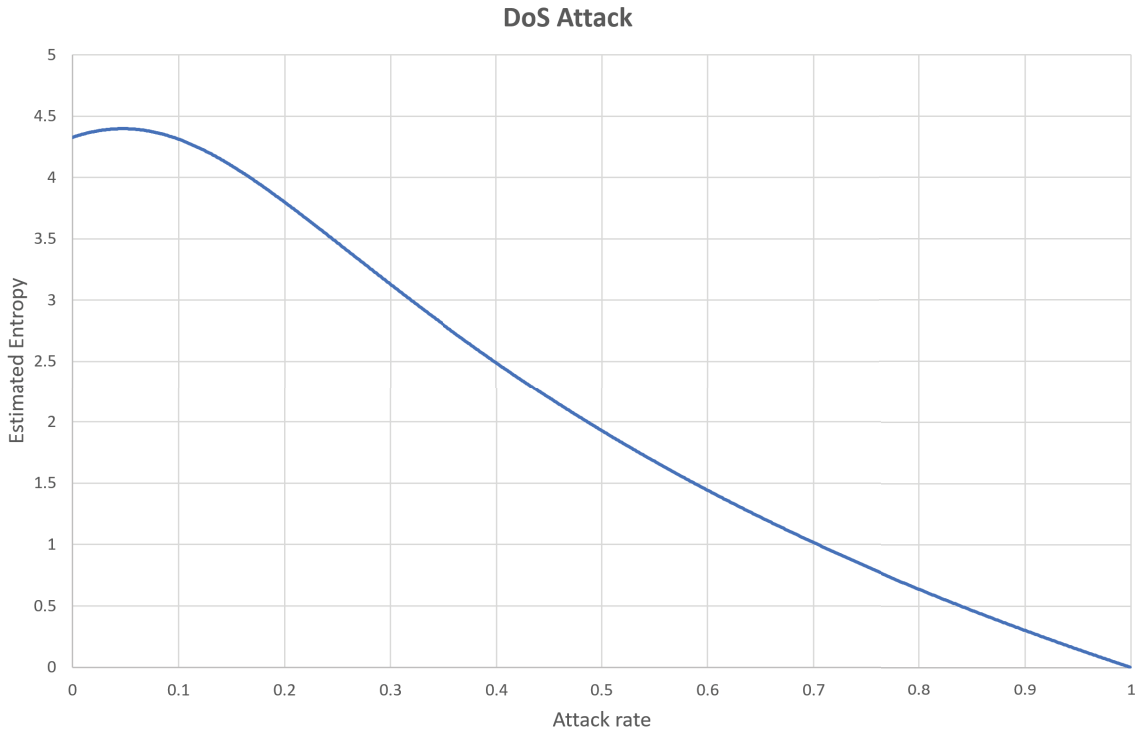

Figure 1. Entropy changes with respect to the attack rate of the denial of service (DoS) attack.

In Figure 1, the x-axis represents the attack ratio (the attack frames with respect to the normal traffic) and the y-axis represents the estimated entropy value. For the normal traffic, the estimated entropy value is around 4.3. However, when the attack is applied, the estimated value increases slightly and is then reduced significantly with the attack rate. If the attack rate is around 5–10% (that is, if new CAN-IDs of 5–10% are inserted), the traffic becomes diverse compared to the normal traffic. This is because the newly inserted CAN-IDs are similar in number to the other CAN-IDs. However, the inserted frames become the majority and reduce the diversity and randomness of the CAN-IDs, because a significant number of CAN-IDs are of the highest priority. The estimated entropy is thus significantly reduced.

Fuzzy attack is another type of attack in which randomly generated CAN frames with random CAN-IDs are inserted into the network. This attack exploits the fact that any ECU will accept any CAN frame with an ID in the proper range. Therefore, the fuzzy attack will increase the estimated entropy, according to the increase in the attack rate. This phenomenon can be observed in Figure 2, which is

based on the same test CAN traffic generated from the data set from Korea University [30]. As can be seen in the figure, the estimated values increase with the attack rate and the range of the CAN-IDs.

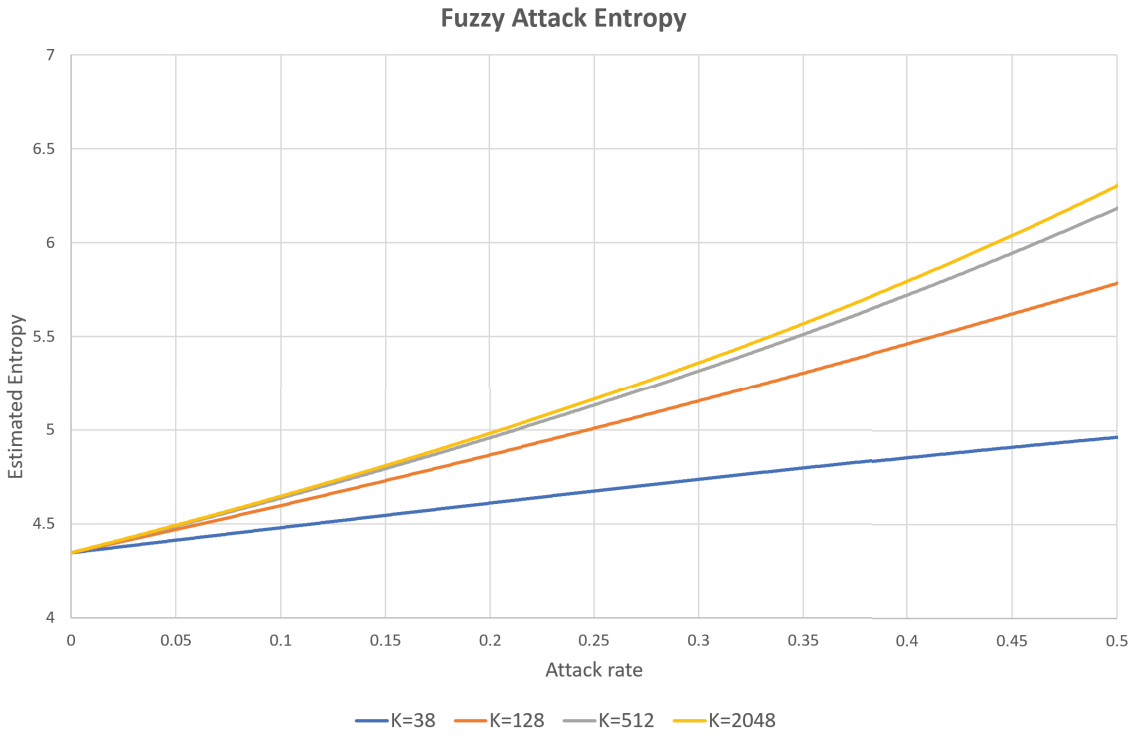

Figure 2. Entropy changes with respect to the attack rate of the DoS attack.

The block size defines the number of CAN frames used in the evaluation of the Rényi entropy, and the indices of CAN frames in a block move according to the RSW method. The Rényi entropy is evaluated using the frequencies of individual CAN-IDs in a block. If the evaluated Rényi entropy is not in the allowed range, it is implied that there is an intrusion.

To reduce false alarms and missing probabilities in DoS and fuzzy attacks, we propose a new method that utilizes the fluctuation of Rényi entropy values after the attack. These values can be used to audit and analyze the attack behavior in a central analysis center to develop a countermeasure to the attack, and to prevent similar future attacks.

Using the dependence of the entropy behavior on the class of attacks, we can reduce the missing and false alarm probabilities simultaneously. The proposed intrusion detection method is described in the following eight steps, which are carried out repeatedly.

Step 1. Generate an i-th block, blk_i, by accumulating CAN-IDs of the sequentially generated N_B frames into the queue of CAN-IDs, que_{id}, where N_B is the size of a block.

Step 2. Entropy h_i related to the frequencies of the individual CAN-IDs accumulated in que_{id} in Step 1 is evaluated.

Step 3. By comparing the estimated entropy h_i in Step 2 with the pre-specified normal entropy H, the first decision of whether blk_i is normal or abnormal is made. Denote $d_i = 0$ for the normal block and $d_i = 1$ otherwise.

Step 4. Find the entropy change information p_i, by comparing h_i with h_{i-1} according to the following rules:

$$p_i = \begin{cases} 0, & \text{if } h_i = h_{i-1} \\ \sigma_0, & \text{if } h_i > h_{i-1} \text{ and } d_i = 0 \\ -\sigma_0, & \text{if } h_i < h_{i-1} \text{ and } d_i = 0 \\ \sigma_1, & \text{if } h_i > h_{i-1} \text{ and } d_i = 1 \\ -\sigma_1, & \text{if } h_i < h_{i-1} \text{ and } d_i = 1, \end{cases}$$

where $\sigma_0 \leq \sigma_1$.

Step 5. p_i is stored in the pattern queue que_{patt}.

Step 6. Check whether the pattern of entropy change information p_is in que_{patt} fits into the rules specified according to the types of attacks, and whether the pattern matches with one of the rules. These blocks are treated as attack patterns, even if the result of the first decision is classified as normal traffic.

Step 7. Otherwise, if there is no matching rule among the P_{size} amount of consecutive p_is, P_{size} blocks are removed from que_{pat}. In this case, the intrusion decision on the output blocks is determined by the results of the first decision.

Step 8. CAN-IDs in the considered block slide (i.e., the number of blocks in a slide multiplied by N_S) are removed from que_{id}.

This process is depicted in Figure 3. Therefore, we can define the entropy change to be a pattern for specific attacks. If pre-specified patterns are observed in the transmitted traffic, the miss rate can be reduced, because we can detect an attack even if the entropy is still in the allowed range.

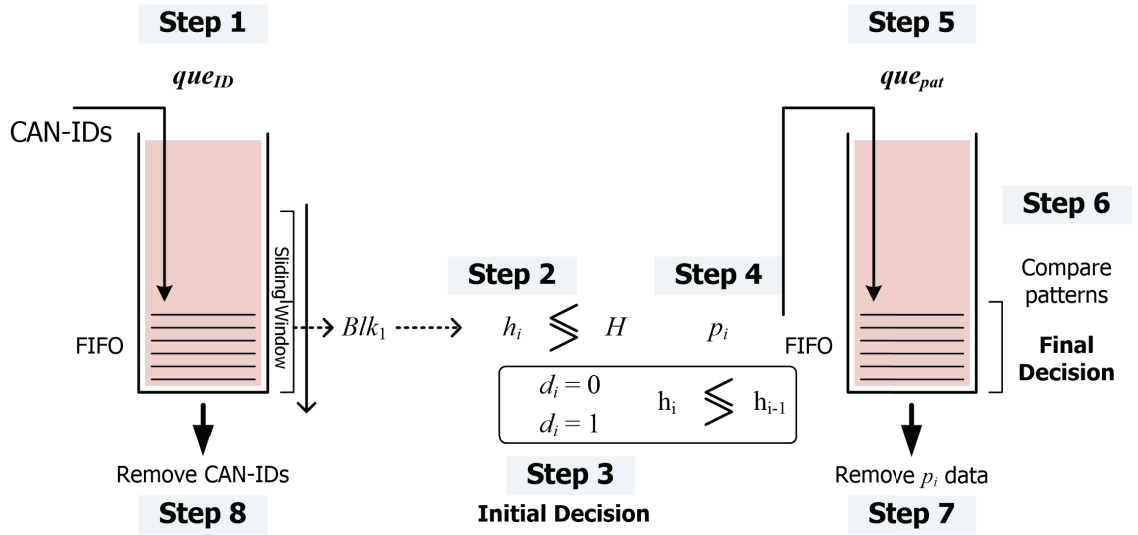

Figure 3. Proposed RSW method based on the estimated entropies.

Because the data over CAN is generated continuously during the operation of the vehicle, the data will be split into blocks with the fixed number of CAN frames. Then, the number of frequencies of individual CAN-IDs in a block will be counted to estimate the Rényi entropy of the generated CAN data. If the estimated Rényi entropy is not in the approved normal range, it will be treated as an abnormal block. In this work, we propose a more accurate method to detect intrusions by distinguishing suspicious blocks that are in the approved range, but may correspond to the initial frames of the attack. This will be determined based on the real-time behavior of the estimated Rényi entropy. Figures 4 and 5 show that the examples of detected abnormal frames in the proposed IDS, based on real-time changes of the Rényi entropy.

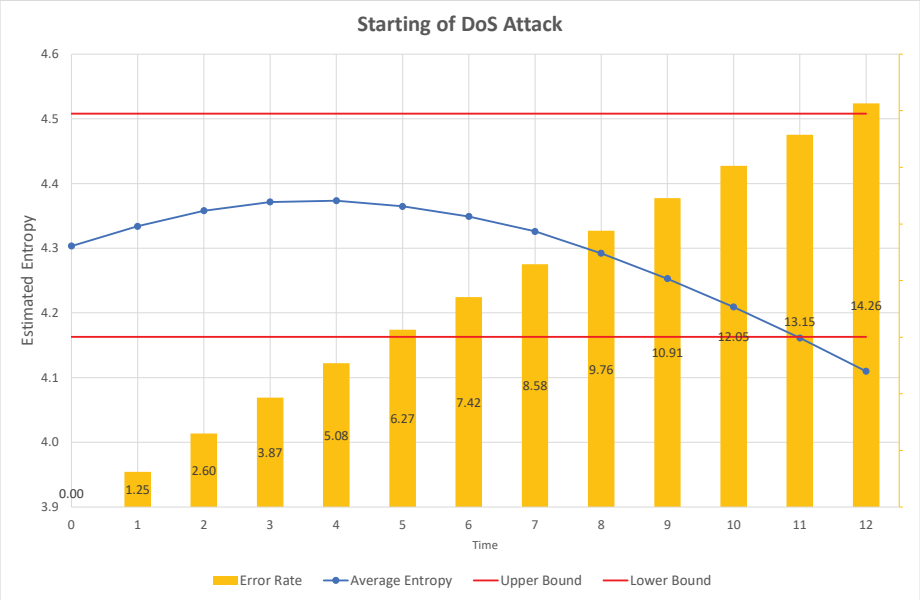

Figure 4. Error rate with respect to the size of the RSW.

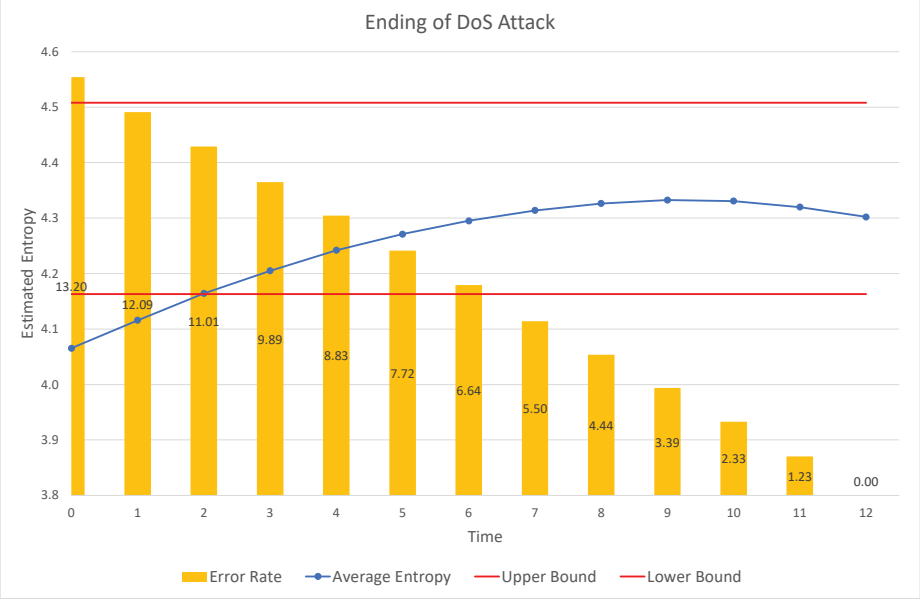

Figure 5. Error rate with respect to the size of the RSW.

4. Numerical Results

In the dataset provided by Korea University [30], the interval without attack and the interval with attack existed together. After splitting data blocks, we calculated attack rate and estimated entropies for individual blocks. Then, the same attack rate values were collected and sorted, and the corresponding

estimated entropy values are presented as in Figures 1, 2, 4, 5, 8 and 9. Contrary to this, Figures 6 and 7 directly use the dataset.

First, the accuracy of the theoretical analysis in Sections 3.1 and 3.2 is depicted in Figures 6 and 7. In these figures, the theoretical expectation is represented as an orange solid line with respect to the attack rate from 0 to 1, and the estimated entropy from the real attack data set is presented as a collection of blue dots. In the real attack data set for the DoS attack, the attack rate is distributed from 0 to 0.6 since the attack rate of 0.5 means that the half of the bandwidth is already occupied by the attacker and the higher attack rate is difficult to see in the real vehicles. Similarly, in the attack data set for the fuzzy attack, the attack rate is distributed from 0 to 0.5. Resultantly, the theoretical expectation and the estimated data from the real attack data set are almost overlapping the entire available range in both attack models.

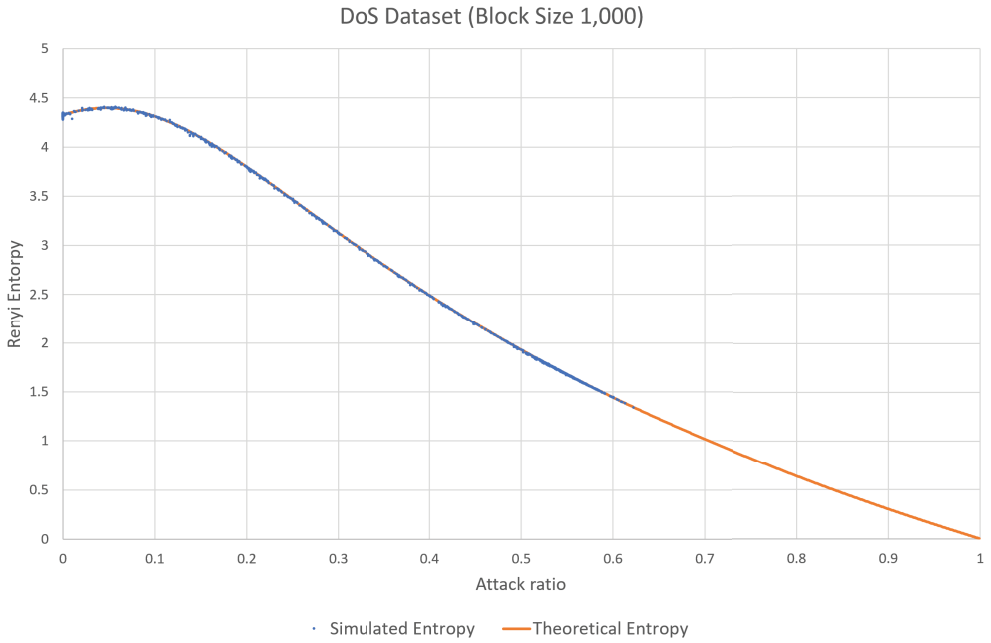

Figure 6. Comparison between the theoretical expectation and the result from the real data set in the DoS attack.

Next, the RSW method is analyzed in Figures 4 and 5. In a DoS attack, the entropy decreases continuously during the elapsed time due to the injection of the same CAN-IDs; i.e., due to reduced randomness. However, at the starting point, the entropy is in the allowed range. Thus, we can determine some CAN-IDs in the allowed range as attack frames, by observing the patterns of the decrease. The problem is in determining how many frames are classified as attack frames. Figure 4 shows the error rate with respect to the depth of the trace back. In this experiment, the attack starts at time 0. Therefore, if we determine the attack or intrusion at time 12, we miss many attack frames injected during time 0 to 12. Based on the movement of curve of estimated values, we can decide on more frames in the allowed range (i.e., time 0 to 12 in this example), so we can reduce the miss rate. For example, at the unit time 12, if we can decide that frames at the time 1 are also classified as attack frames, then the error rate (miss rate) is only 1.25 %. Contrary to this, we can also set the ending point more accurately, as in Figure 5. In this case, we can decide the frames in the time range 0 to 12 are attack frames.

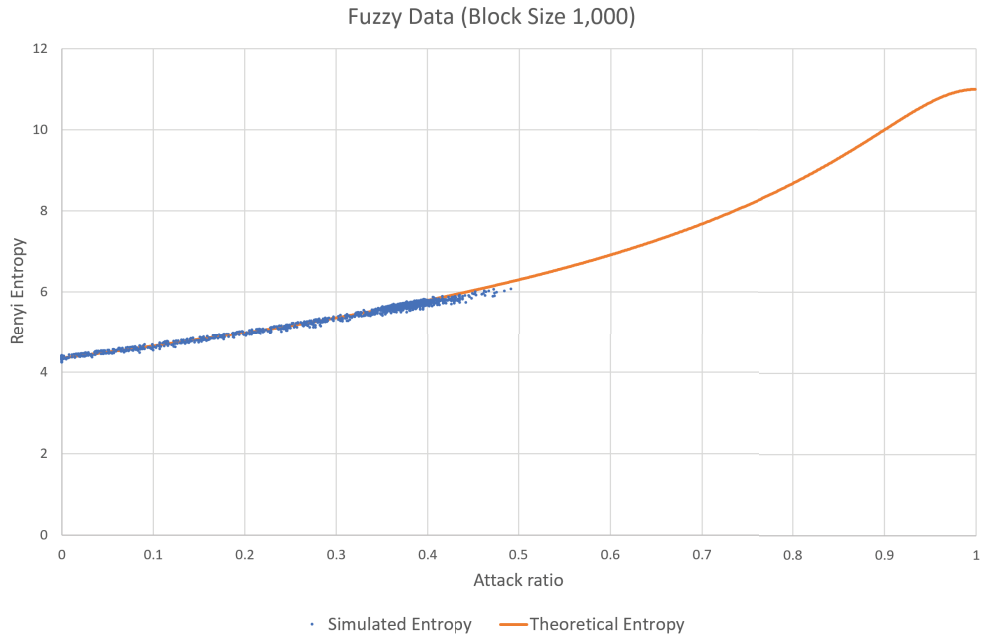

Figure 7. Comparison between the theoretical expectation and the result from the real data set in the fuzzy attack.

In Figures 8 and 9, the multiple estimated values are depicted at the same time by using the same dataset provided by Korea University [30]. We can set the different bounds for each estimated values and then decides whether there is an intrusion or not by observing estimated values. Among three estimated values, if more then two values are in the unallowed ranges and one value is still in the allowed range, then we can decide that there is an intrusion by using the majority vote rule.

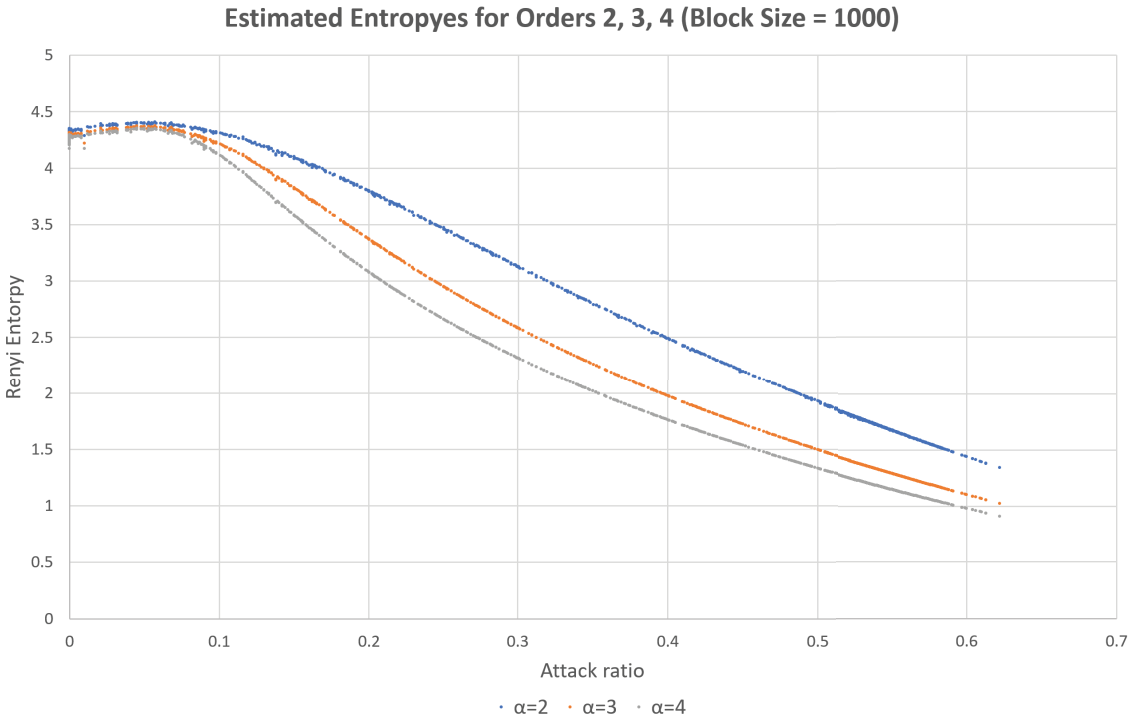

Figure 8. Estimated Rényi entropies with orders 2, 3, and 4 with respect to the attack rate for the DoS attack.

Table 1 compares the false alarm rates and miss rates when we only use the estimated entropy, and utilize both estimated entropy and the entropy change patterns, respectively. It can be seen that the miss rate can be reduced by up to 54.6% and 32.6%, with similar false-alarm rate in DoS attack and fuzzy attack, respectively. This method can influence to increasing false alarm rate slightly because it designates previous frames as attack frames depending on the change patterns of estimated entropies.

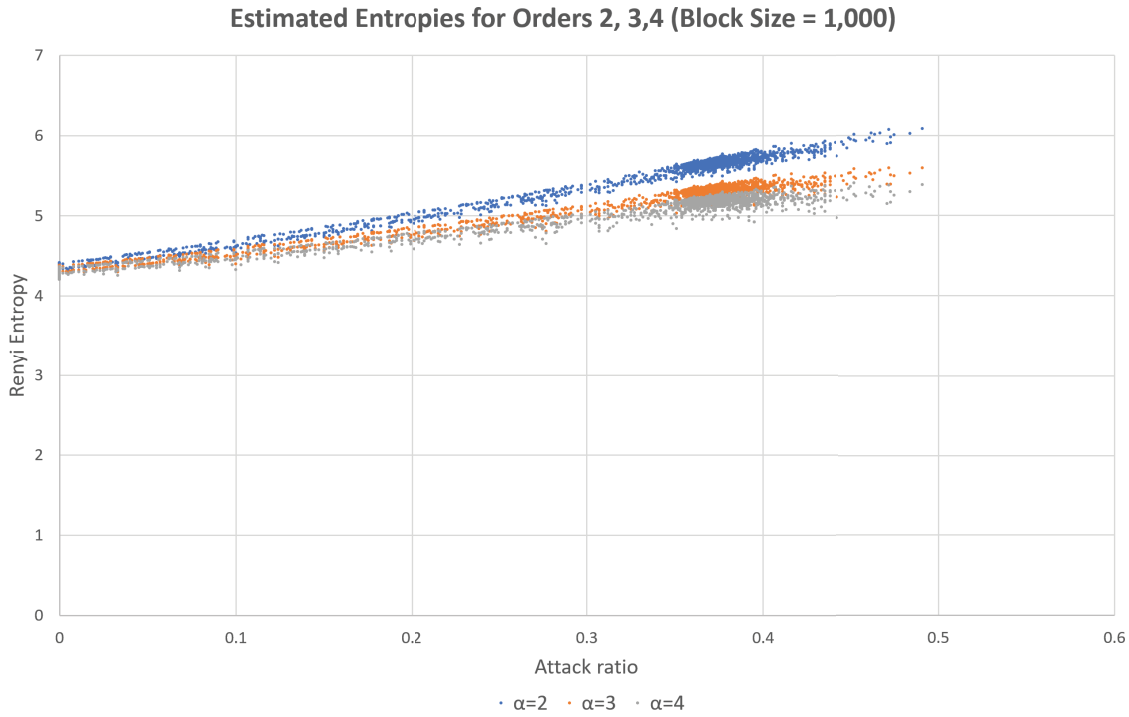

Figure 9. Estimated Rényi entropies with orders 2, 3, and 4 with respect to the attack rate for the Fuzzy attack.

Table 1. False alarm rates and the miss rate for the entropy case and entropy + RSW case with respect to the DoS attack and fuzzy attack.

DoS Attack	**False Alarm**	**Missing**
Entropy	0.78 (100) %	1.08 (100) %
Entropy + RSW	0.79 (101.3)%	0.49 (154.6)%
Fuzzy Attack	**False Alarm**	**Missing**
Entropy	0.39 (100) %	0.86 (100)%
Entropy + RSW	0.41 (105.1)%	0.58 (132.6)%

5. Conclusions

In this work, we tested an IDS for vehicular networks by using multiple order Rényi entropies simultaneously. The proposed IDS considers several orders of Rényi entropy simultaneously. Each Rényi entropy can be estimated simultaneously with very low complexity. Estimated data can be used to detect anomalies in the intra-vehicular network traffics generated by the vehicle. During the estimation the collected frames were split into blocks with fixed number of frames, and the entropies were evaluated based on these blocks. For a more accurate estimation against each type of attack, we also propose a RSW method for decision of attacks based on the estimated entropies. For fair comparison, we utilized the CAN-ID attack data set generated by a research team from Korea University [30]. Our results show that the proposed method can show the false negative and positive errors of less than 1% simultaneously.

As further work, we will study IDS based on machine learning (ML) and improve the performance by applying estimated Rényi entropy to several ML algorithms. In addition, the proposed method was only simulated and validated on the two major attack models in the dataset provided by Korea University. However, it is necessary to verify the validity of the proposed scheme for other attack models, which will be possible after obtaining a valid dataset from an actual vehicular environment. This will be done in the future. Since the proposed method has very low complexity, it can be used for vehicle IDS and contributes to vehicle safety by enabling rapid detection of external attacks.

Author Contributions: Y.-S.K. first proposed using the Rényi entropy. K.-S.Y., D.-W.L., and Y.-S.K. carried out the formal analysis of the proposed attack. K.-S.Y. and D.-W.L. developed a methodology to analyze the proposed scheme. S.-H.K. wrote a program in C and investigated the numerical data. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Institute for Information and Communications Technology Promotion (IITP) grant, which is funded by the Korean government (MSIT) (2017-0-00441, Development of Core Technologies of Intrusion Tolerance System for Autonomous Vehicles).

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

References

1. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T. Experimental security analysis of a modern automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Berkeley/Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
2. Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX Security Symposium, San Francisco, CA, USA, 8–12 August 2011; p. 6.
3. Miller, C.; Valasek, C. *A Survey of Remote Automotive Attack Surfaces*; Tech. Rep. 8; Black Hat USA: Las Vegas, NV, USA, 2014.
4. Petit, J.; Shladover, S.E. Potential cyberattacks on automated vehicles. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 546–556. [CrossRef]
5. Miller, C.; Valasek, C. *Remote Exploitation of an Unaltered Passenger Vehicle*; Tech. Rep. 23; Black Hat USA: Las Vegas, NV, USA, 2015.
6. Fröschle, S.; Stühring, A. Analyzing the capabilities of the can attacker. In Proceedings of the 22nd European Symposium on Research in Computer Security, Oslo, Norway, 11–15 September 2017; Springer: Oslo, Norway, 2017; pp. 464–482.
7. Liu, J.; Zhang, S.; Sun, W.; Shi, Y. In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Netw.* **2017**, *31*, 50–58. [CrossRef]
8. Marchetti, M.; Stabili, D. Read: Reverse engineering of automotive data frames. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1083–1097. [CrossRef]
9. Wu, W.; Li, R.; Xie, G.; An, J.; Bai, Y.; Zhou, J.; Li, K. A Survey of Intrusion Detection for In-Vehicle Networks. *IEEE Trans. Intell. Transp. Syst.* **2019**. [CrossRef]
10. Muter, M.; Asaj, N. Entropy-Based Anomaly Detection for In-Vehicle Networks. In Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV), Baden-Baden, Germany, 5–9 June 2011.
11. Narayanan, B.N.; Djaneye-Boundjou, O.; Kebede, T.M. Performance analysis of machine learning and pattern recognition algorithms for Malware classification. In Proceedings of the 2016 IEEE National Aerospace and Electronics Conference(NAECON) and Ohio Innovation Summit (OIS), Dayton, OH, USA, 25–29 July 2016; pp. 338–342.
12. Kebede, T.M.; Djaneye-Boundjou, O.; Narayanan, B.N.; Ralescu, A.; Kapp, D. Classification of Malware programs using autoencoders based deep learning architecture and its application to the microsoft malware Classification challenge (BIG 2015) dataset. In Proceedings of the 2017 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 27–30 June 2017, pp. 70–75.
13. Alom, M.Z.; Bontupalli, V.; Taha, T.M. Intrusion Detection using Deep Belief Networks. In Proceedings of the 2015 National Aerospace and Electronics Conference, (NAECON), Dayton, OH, USA, 16–19 June 2015; pp. 339–344.

14. Callegari, C.; Giordano, S.; Pagano, M. Entropy-based network anomaly detection. In Proceedings of the 2017 International Conference Computing, Networking and Communications (ICNC), Silicon Valley, CA, USA, 26–29 January 2017; pp. 334–340.
15. Callegari, C.; Giordano, S.; Pagano, M. Anomaly detection: An overview of selected methods. In Proceedings of the 2017 Int. Multi-Conference Engineering, Computer and Information Sciences (SIBIRCON), Novosibirsk, Russia, 18–24 September 2017; pp. 52–57.
16. Saia, R.; Carta, S.; Recupero, D.R.; Fenu, G.; Stanciu, M.M. A Discretized Extended Feature Space (DEFS) Model to Improve the Anomaly Detection Performance in Network Intrusion Detection Systems. In Proceedings of the 11th International Joint Conference Knowledge Discovery, Knowledge Engineering and Knowledge Management, Vienna, Austria, 17–19 September 2019; pp. 322–329.
17. Saia, R.; Salvatore, C.; Recupero, R. A Probabilistic-driven Ensemble Approach to Perform Event Classification in Intrusion Detection System. In Proceedings of the 10th International Joint Conference Knowledge Discovery, Knowledge Engineering and Knowledge Management, Seville, Spain, 18–20 September 2018.
18. Berezinski, P.; Jasiul, B.; Szpyrka, M. An Entropy-Based Network Anomaly Detection Method. *Entropy* **2015**, *17*, 2367–2408. [CrossRef]
19. Lee, H.; Jeong, S.H.; Kim, H.K. OTIDS: A Novel Intrusion Detection System for In-vehicle Network by using Remote Frame. In Proceedings of the 2017 IEEE 15th PST, Calgary, AB, Canada, 28–30 August 2017.
20. Hazem, A.; Fahmy, H. Lcap-a lightweight can authentication protocol for securing in-vehicle networks. In Proceedings of the 10th Escar Embedded Security Cars Conference, Berlin, Germany, 28–29 November 2012; Volume 6, pp. 283–300.
21. Macher, G.; Sporer, H.; Brenner, E.; Kreiner, C. Supporting cyber-security based on hardware-software interface definition. In Proceedings of the European Conference Software Process Improvement, Graz, Austria, 14–16 September 2016; Springer: Graz, Austria, 2016; pp. 148–159.
22. Abbott-McCune, S.; Shay, L.A. Intrusion prevention system of automotive network can bus. In Proceedings of the IEEE International Carnahan Conference Security Technology (ICCST), Orlando, FL, USA, 24–27 October 2016; pp. 1–8.
23. Eric, W.; William, X.; Suhas, S.; Songsong, L.; Kai, Z. Hardware module-based message authentication in intra-vehicle networks. In Proceedings of the ACM/IEEE 8th International Conference Cyber-Physical Systems (ICCPS), Pittsburgh, PA, USA, 18–20 April 2017; pp. 207–216.
24. Bulck, J.V.; Mühlberg, J.T.; Piessens, F. VulCAN: Efficient component authentication and software isolation for automotive control networks. In Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, Florida, USA, 4–8 December 2017; pp. 225–237.
25. Macher, G.; Sporer, H.; Brenner, E.; Kreiner, C. An automotive signal-layer security and trust-boundary identification approach. *Procedia Comput. Sci.* **2017**, *109*, 490–497. [CrossRef]
26. Macher, G.; Sporer, H.; Brenner, E.; Kreiner, C. Signal-layer security and trust-boundary identification based on hardware-software interface definition. *J. Ubiquitous Syst. Pervasive Netw.* **2018**, *10*, 1–9. [CrossRef]
27. Wang, Q.; Lu, Z.; Qu, G. An entropy analysis based intrusion detection system for controller area network in vehicles. In Proceedings of the 2018 31st IEEE International System-on-Chip Conference (SOCC), Washington, DC, USA, 4–7 September 2018; pp. 90–95.
28. Kim, Y.-S. Low Complexity Estimation Method of Rényi Entropy for Ergodic Sources. *Entropy* **2018**, *20*, 657. [CrossRef]
29. Rényi, A. On measures of entropy and information. In Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Berkeley, CA, USA, 20 June–30 July 1960; pp. 547–561.
30. CAN Dataset for Intrusion Detection (OTIDS). Available online: http://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset (accessed on 24 January 2020).
31. Debar, H.; Dacier, M.; Wespi, A. Towards a taxonomy of intrusion-detection systems. *Comput. Netw.* **1999**, *31*, 805–822. [CrossRef]
32. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; Wiley-Interscience: Hoboken, NJ, USA, 2006.