Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 1075648, 8 pages
http://dx.doi.org/10.1155/2016/1075648

Research Article

Hybrid Intrusion Detection System for DDoS Attacks

Özge Cepheli,[1] Saliha Büyükçorak,[1,2] and Güneş Karabulut Kurt[1]

[1]*Department of Electronics and Communication Engineering, Istanbul Technical University, 34469 Istanbul, Turkey*
[2]*Gebze Technical University, 41400 Kocaeli, Turkey*

Correspondence should be addressed to Özge Cepheli; irmakoz@itu.edu.tr

Received 6 November 2015; Revised 27 January 2016; Accepted 29 February 2016

Academic Editor: Andrea Ceccarelli

Distributed denial-of-service (DDoS) attacks are one of the major threats and possibly the hardest security problem for today's Internet. In this paper we propose a hybrid detection system, referred to as hybrid intrusion detection system (H-IDS), for detection of DDoS attacks. Our proposed detection system makes use of both anomaly-based and signature-based detection methods separately but in an integrated fashion and combines the outcomes of both detectors to enhance the overall detection accuracy. We apply two distinct datasets to our proposed system in order to test the detection performance of H-IDS and conclude that the proposed hybrid system gives better results than the systems based on nonhybrid detection.

1. Introduction

Distributed denial-of-service (DDoS) attacks stand as a crucial threat to Internet services. A DDoS attack is launched by producing an extremely large amount of traffic to exhaust resources of target systems. As shown in Figure 1, the attack is generally initiated by a single attacker, exploiting and taking control of several devices referred to as zombies. Frequently zombie devices are not aware of the fact that they are being used to perform an attack. The attacker usually makes a sweep operation to determine the devices that are eligible for being used as a zombie, for example, a device with an open port. After this stage, the attack is initiated by the attacker using zombie devices. As the number of zombies can be around hundreds or thousands (and theoretically it is possible to have even more) the detection of the attacker becomes a very hard task.

A number of methods have been proposed to prevent DDoS attacks in the literature, though there is still lack of a methodology addressing all requirements. Therefore, DDoS attacks are still a huge threat to network security. In this paper we propose a novel framework named as hybrid intrusion detection system (H-IDS) to detect DDoS attacks. In this system, in order to achieve more accurate detection we use both anomaly-based and signature-based detection techniques. Anomaly-based detector part of the proposed H-IDS is designed by using multidimensional Gaussian mixture models (GMMs) from a training dataset, while signature-based detector is formed by using SNORT [1]. In addition to this, we design a node referred to as hybrid detection engine (HDE) in order to control and evaluate outputs of these detectors. The proposed H-IDS enhanced the overall performance of DDoS attack detection and shortened the detection delay through using two detectors separately but in an integrated fashion. The proposed H-IDS can be implemented as a module in any IDS solution, as well as being used as a separate DDoS detection system. For the detection performance evaluation of the proposed hybrid detector, we utilize the widely used DARPA 2000 dataset and a dataset provided by a commercial bank in Turkey during a penetration test. With the H-IDS, true positive rate (TPR) is obtained as 92.1% for DARPA and 99.9% for the commercial bank dataset. The TPR is increased by 27.4% with the proposed H-IDS when compared to the signature-based detector for the dataset DARPA.

The remainder of this paper is organized as follows. In Section 2, a detailed overview of the related literature is given. In Section 3, the proposed H-IDS and its components are detailed along with working principles of this hybrid detector. In Section 4, we evaluate experiments by using two distinct datasets to validate our detection model. We conclude this paper in Section 5.

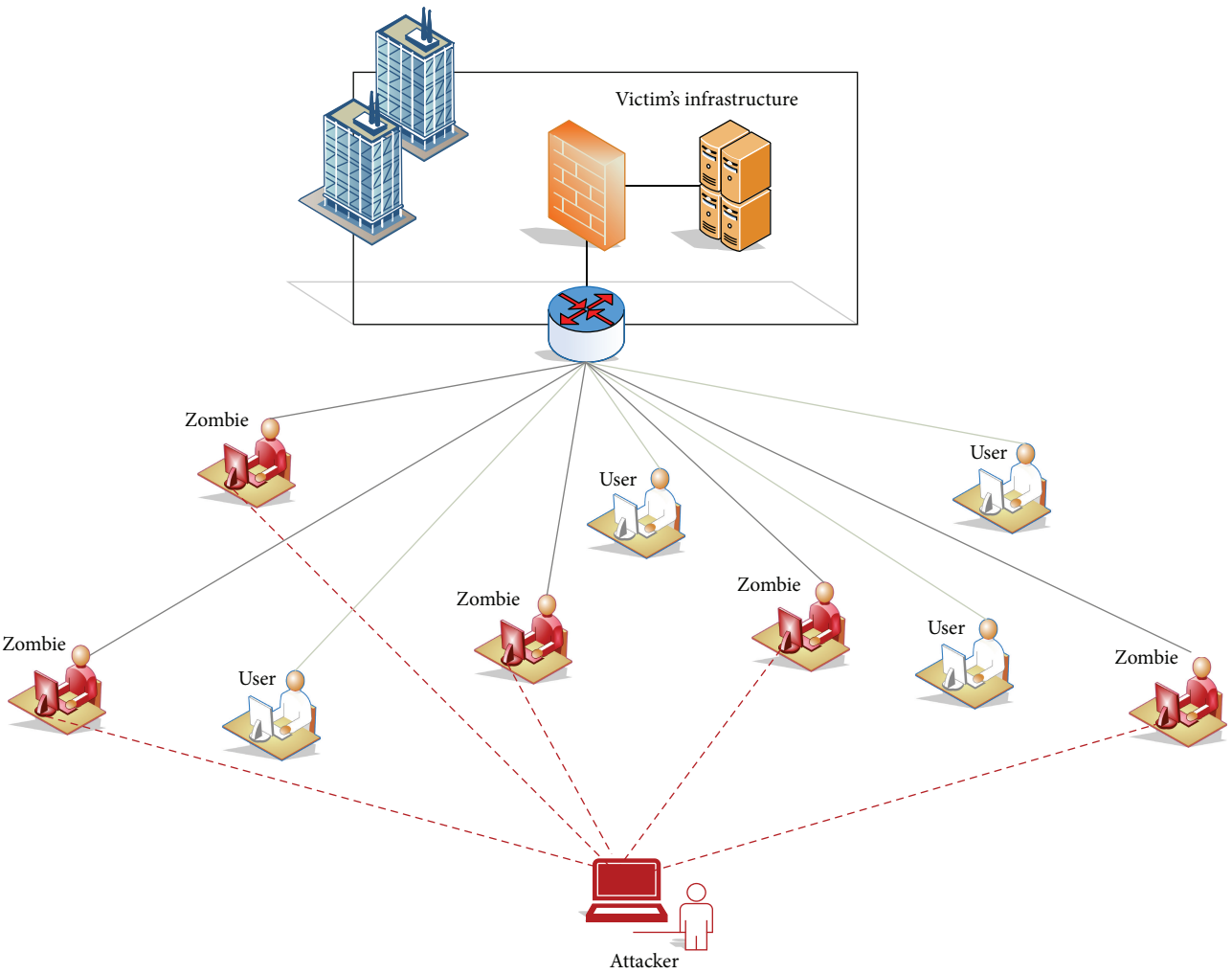

Figure 1: DDoS attack model.

2. Literature Overview

The entropy based DDoS countermeasure methods are independent of the specific attack features. In [2], Tao and Yu proposed a flow entropy based DDoS attack detector. The effectiveness of this method is shown thorough various experiments and simulations. The authors offered a mechanism for IP traceback against DDoS attacks based on entropy variations between normal and attack traffic. This is fundamentally different from commonly used packet marking [3, 4]. Xiang et al. proposed a novel low-rate DDoS attacks detector ground on new information metrics (i.e., the generalized entropy metric and the information distance metric). It is demonstrated that these metrics can expressly reduce the false positive rate by using actual DDoS datasets [5, 6].

DDoS attacks can be detected by examining of the network traffic changes. There are many proposed countermeasure methods based on self-similarity of the network. In [7], the authors introduced a real-time DDoS attack detector based on network self-similarity. It is shown that the attacks can be detected effectively and precisely using the rescaled range algorithm. In the study performed by Chonka et al. [8], by using the property of network self-similarity, a chaotic model is developed to find out DDoS flooding attack traffic. Chen et al. [9] proposed a DDoS intrusion detection algorithm ground on preprocessing network traffic and chaos theory that can detect an anomaly caused either by bursty legitimate traffic or by DDoS flooding attacks. The proposed algorithm's performance is improved by utilizing an exponential smoothing model as forecasting model [10].

Probabilistic methods are also frequently used to detect DDoS attacks. Joshi et al. [11] tested the efficiency of the cloud traceback (CTB) by using a back propagation neural network, named cloud protector, and came to the conclusion that the proposed CTB helps to find out the real sources of attacking packets. Thing et al. [12] proposed a new and high speed nonintrusive traceback technique based on the rationale that packets relating to a particular source-destination flow follow a relatively static path through routers. In [13], the authors introduced a novel anomaly detector ground on hidden semi-Markov model to detect the application layer based DDoS attacks. The effectiveness of this method is demonstrated

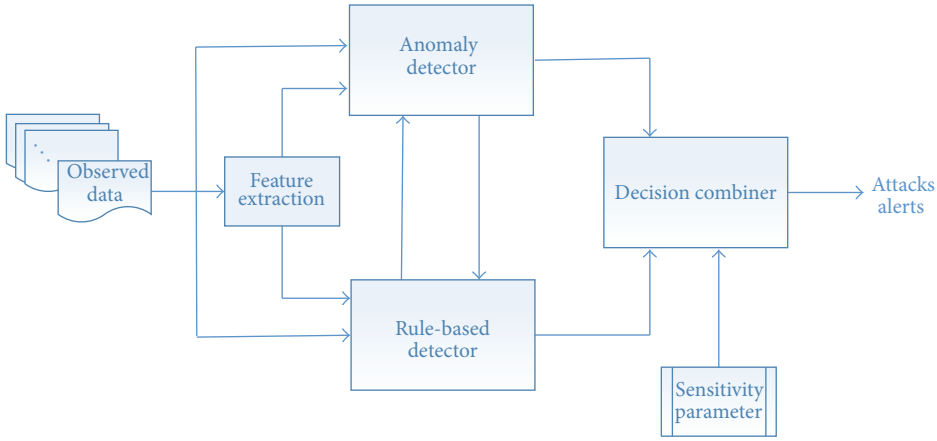

Figure 2: Proposed H-IDS model.

by conducting experiments using real web traffic data. The authors reached the conclusion that identifier/location separation can help to prevent DDoS attacks by investigating numerical results based on the real data [14].

In the study performed by Barati et al. [15], by using a machine learning technique composed of genetic algorithm and artificial neural network, it is shown that the accuracy of DDoS attack detection is improved. Yu et al. [16] guaranteed the quality of service for legitimate users by using a dynamic resource allocation strategy to confront DDoS attacks that target individual cloud customers. Thapngam et al. [17] investigated a detector based on the pattern behavior of traffic sources by observing packet arrivals. It is shown through experiments with several datasets that the proposed detector can discriminate DDoS attack traffic from flash crowd with a quick response.

There are also many hybrid detection algorithms proposed for DDoS attack detection. Hwang et al. [18] proposed a hybrid system that combines a signature-based IDS with an anomaly detection system in a cascade structure, achieving twice the detection accuracy of IDS only system. Gómez et al. [19] extended SNORT by adding an anomaly detection preprocessor. Afterwards, various hybrid systems are proposed following the same aim, to have the strengths of both signature- and anomaly-based detection.

In this paper, we propose a novel hybrid intrusion detection system (H-IDS) to accurately detect DDoS attacks. Our developed system makes use of both anomaly-based and signature-based detection methods in parallel. The decision combiner, which is the core processing unit of the system, combines outputs of the detectors and then generates an attack alarm with a tunable sensitivity parameter. Note that our proposed H-IDS differs from the existing studies in the literature, with its parallel detection methodology, due to its flexible nature with decision combiner and having tunable parameters.

3. Hybrid Intrusion Detection System (H-IDS)

The H-IDS designed within this paper is based on an original approach, where the outputs of an anomaly-based detector and a signature-based detector are collected. The parameters of the detectors are controlled by a centralized node. This node is referred to as hybrid detection engine (HDE). The design goal of this intrusion detection system is to enhance the overall performance of DDoS attack detection, by shortening the detection delay, while increasing the detection accuracy. The block diagram of the proposed H-IDS is shown in Figure 2. As can be seen from this figure, the observed data containing normal traffic and DDoS attacks is processed to extract some features; then processed data is linked to signature-based and anomaly-based detector blocks to detect attacks. Outputs of these detectors are examined by a decision combiner and an alarm gets produced according to sensitivity parameter. The components of the hybrid IDS are explained in detail in the following subsections.

3.1. Feature Extraction and Activity Model Calculation. The first step of the proposed detection process is to analyze the network traffic and to extract some features to build an activity model. In order to give an a priori idea of the detection problem, time analysis of DARPA 2000 dataset is given in Figure 3. From this figure, one can conclude that it is not an easy task to even distinguish between normal and attack periods by solely observing traffic density.

The model of normal network traffic can be achieved by using training data. The training data period can be as short as hours or as long as weeks, similar to the case in DARPA dataset. As the length of the training period affects the model accuracy greatly (but results in a delay), the time required for the training should be optimized in implementation.

In our study, the following features widely used in DDoS studies are selected: packet interarrival times, packet sizes, and protocol frequencies. Note that there are several features that can be used in order to achieve maximum performance.

3.2. Anomaly Detector. In this work, by using multidimensional Gaussian mixture models (GMMs), an anomaly-based detector is designed to distinguish normal and abnormal traffic in the data obtained from the feature extraction step. Expectation maximization (EM) algorithm is used

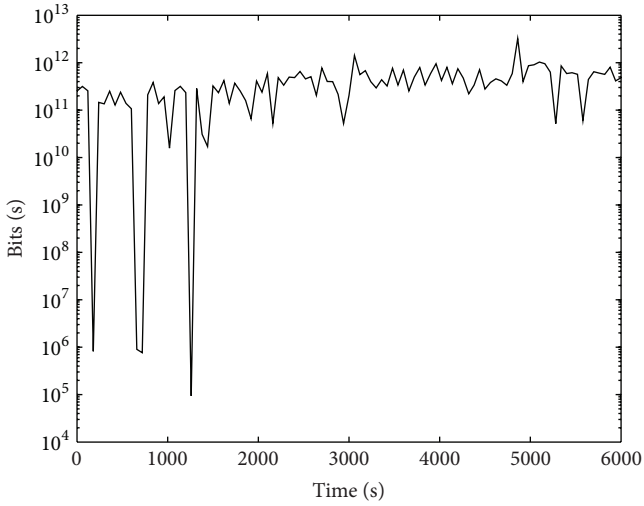

Figure 3: Time domain analysis of DARPA data showing traffic density in bits per second (bps) in logarithmic scale.

to estimate the parameters of the GMMs. Afterwards, the distance between the parameters is investigated and detection is made based upon comparison of this distance with defined thresholds, which constitutes the sensitivity parameter in H-IDS. The output of the anomaly detector is defined as isAlarm_a.

3.2.1. Expectation Maximization Algorithm. EM algorithm is commonly used for simplifying difficult maximum likelihood estimate (MLE) problems that are frequently encountered in mixture models and cannot be analytically solved [18, 20]. This algorithm is a practical parameter estimation technique and named as parametric methods, where the number of mixture components needs to be known a priori.

Let $X = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N\}$ be a given dataset, where $\mathbf{x}_i$ is an M-dimensional vector measurement. In a mixture model, the probability density function (pdf), $p(\mathbf{x})$, can be defined as in the following with a finite K component [20–22]:

$$p(\mathbf{x} \mid \Theta) = \sum_k \omega_k p_k(\mathbf{x} \mid \theta_k), \tag{1}$$

where $p_k(\mathbf{x} \mid \theta_k)$ is defined with parameters θ_k over $p(\mathbf{x})$ and refers to each component of the mixture. $k = 1, 2, \ldots, K$ is the number of mixture components and ω_k is the proportion of kth mixing component in the mixture (which are positive and sum to one). $\Theta = (\omega_1, \omega_2, \ldots, \omega_K, \theta_1, \theta_2, \ldots, \theta_K)$ is the complete set of parameters in a mixture model with K components. The component density $p_k(\cdot)$ is a multidimensional Gaussian distribution defined as

$$p_k(\mathbf{x} \mid \theta_k) = \frac{1}{(2\pi)^{M/2} \det(\Sigma)^{1/2}} \exp\left[-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_k)\Sigma_k^{-1}(\mathbf{x} - \boldsymbol{\mu}_k)\right], \tag{2}$$

where $\theta_k = (\boldsymbol{\mu}_k, \Sigma_k)$ represents parameters of each component in the mixture. $\boldsymbol{\mu}_k$ is the mean vector of length M and Σ_k is the covariance matrix of size $M \times M$. As defined in (1) and (2), Gaussian mixture models assume that all the data points are originated from a mixture of a finite number of Gaussian distributions with unknown parameters.

The EM algorithm begins with some initial estimated Θ values and proceeds by iteratively updating Θ until convergence. Each iteration consists of two steps: the expectation step (E-step) and the maximization step (M-step) [22, 23].

In the E-step, the membership coefficients of data point $\mathbf{x}_i$ in component k are calculated by using the current parameter values Θ as [22]

$$\gamma_{ik} = \frac{\omega_k p_k(\mathbf{x}_i \mid \theta_k)}{\sum_{k=1}^{K} \omega_k p_k(\mathbf{x}_i \mid \theta_k)}, \quad 1 \le k \le K,\ 1 \le i \le N, \tag{3}$$

where $\mathbf{x}_i$ refers to the data in the kth mixture and $\sum_{k=1}^{K} \gamma_{ik} = 1$.

In the M-step, parameter values are updated as mean, covariance, and mixing proportion belonging to each component in the mixture model, by using the membership coefficients obtained in the E-step and the dataset. The new mixture weights are calculated as

$$\widehat{\omega}_k = \frac{1}{N}\sum_{i=1}^{N} \gamma_{ik}, \quad 1 \le k \le K. \tag{4}$$

The updated mean values are obtained as

$$\widehat{\boldsymbol{\mu}}_k = \frac{\sum_{i=1}^{N} \gamma_{ik}\mathbf{x}_i}{\sum_{i=1}^{N} \gamma_{ik}}, \quad 1 \le k \le K. \tag{5}$$

Note that this is a vector equation since $\widehat{\boldsymbol{\mu}}_k$ and $\mathbf{x}_i$ are both M-dimensional vectors. Lastly, the covariance matrices of each component are calculated as

$$\widehat{\Sigma}_k = \frac{\sum_{i=1}^{N} \gamma_{ik}(\mathbf{x}_i - \widehat{\boldsymbol{\mu}}_k)(\mathbf{x}_i - \widehat{\boldsymbol{\mu}}_k)^T}{\sum_{i=1}^{N} \gamma_{ik}}, \quad 1 \le k \le K. \tag{6}$$

The M-step is defined by calculating new whole parameters and then membership weights are recalculated by going back to the E-step. The algorithm iteratively calculates estimation values with maximum likelihood for parameters by applying the E- and M-steps, iteratively.

3.2.2. Information Distance Metrics. The information distance metrics can be described as methods to measure the norm of the similarity between two pdfs. In this work, these metrics are used to quantify the distance between the pdfs of normal and abnormal traffic, and the distance $\mathscr{D}$ is chosen as the output of the anomaly detector.

Let $\mathscr{P} = (p_1, p_2, \ldots, p_{\mathscr{T}})$ and $\mathscr{Q} = (q_1, q_2, \ldots, q_{\mathscr{T}})$ represent two discrete probability distributions. The Kullback-Leibler ($\mathscr{KL}$) distance can be described as [2]

$$\mathscr{D}_{\mathscr{KL}}(\mathscr{P}, \mathscr{Q}) = \sum_t p_t \log_2 \frac{p_t}{q_t}. \tag{7}$$

Here, we note that $\mathscr{KL}$ distance cannot be a perfect metric due to the asymmetry properties, which will result in potential problems. There are a few metrics (i.e., Jeffrey distance,

Sibson distance, and Hellinger distance) that can handle the asymmetric problem of the $\mathcal{KL}$ distance [2, 17].

The Sibson distance can be calculated based on the $\mathcal{KL}$ distance as

$$\mathcal{D}_{\mathcal{S}}(\mathcal{P}, \mathcal{Q}) = \frac{1}{2}\left[\mathcal{D}_{\mathcal{KL}}\left(\mathcal{P}, \frac{1}{2}(\mathcal{P} + \mathcal{Q})\right) + \mathcal{D}_{\mathcal{KL}}\left(\mathcal{Q}, \frac{1}{2}(\mathcal{P} + \mathcal{Q})\right)\right]. \tag{8}$$

In the literature, it is indicated that the Sibson distance is a suitable candidate for DDoS detection in terms of data sensitivity and statistical features [2, 17]. Accordingly, in our numerical experiments, we choose Sibson distance and get a constant value as threshold (α) from HDE and calculated isAlarm_a as

$$\text{isAlarm}_a = \begin{cases} 0, & \mathcal{D}_{\mathcal{S}}(\mathcal{P}, \mathcal{Q}) < \alpha \\ 1, & \mathcal{D}_{\mathcal{S}}(\mathcal{P}, \mathcal{Q}) \geq \alpha. \end{cases} \tag{9}$$

3.3. Signature-Based Detector. Signature-based detector is a type of attack detectors that uses predefined signature sets in order to detect an alarm. The main principle is to extract some features from the traffic data and compare the values of these features with the predefined rules. This process usually does not depend on the application specific cases; however it is usually easier to implement and manage.

The first approach to detect network attacks is to use rule sets. This is the basis of all current IDS or intrusion prevention systems (IPSs) that are used in practice. Hence, there are many tools available, developed by various groups/companies. In addition to the proprietary solutions as the IPS feature of Palo Alto Next Generation Firewall and Juniper IDP, there are also open source signature-based solutions as SNORT [1] and Suricata [24]. In the scope of this study, we used SNORT as our signature-based detector. We specifically choose the rules that are commonly applied in the literature.

SNORT is a free and open source intrusion detection and prevention system (IDPS), created by Martin Roesch in 1998. After the acquisition by Cisco Systems on October 7, 2013, it continues to be developed as an open source solution. It is a widely used solution for network intrusion detection both for practical and for research implementation.

SNORT can be configured to run in three modes:

(i) Sniffer mode, which simply reads the packets off the network and displays them in a continuous stream on the console (screen).

(ii) Packet logger mode, which logs the packets to disk.

(iii) Network IDS mode, which performs detection and analysis on network traffic; this is the most complex and configurable mode.

The rule set of SNORT can be modified for special requirements. Note that different rule sets should be chosen for different performance results. However, in general, extensive optimization of all the rules in the rule set is not aimed at during the implementation of a signature-based solution. Instead one can use the periodically updated rule sets and further create additional rules for special requirements [24]. Granularity of the rule set can be changed on the run to control the security level of the detector. Hence, the amount of work that is necessary to configure the rule-based approach is less than that of the anomaly-based one. In our system, the granularity of the rule set is set by the HDE. The output of SNORT is denoted by isAlarm_r and calculated based on the value $\mathcal{A}(k)$, where k is the time frame index and $\mathcal{A}(k)$ is chosen as the number of generated alerts within the kth time frame. Using $\mathcal{A}(k)$, isAlarm_r is calculated as

$$\text{isAlarm}_r = \begin{cases} 0, & \mathcal{A}(k) = 0 \\ 1, & \mathcal{A}(k) \geq 0. \end{cases} \tag{10}$$

3.4. Hybrid Detection Engine. In this paper, we make use of anomaly- and signature-based detectors and combine their output in order to enhance the overall performance. Also, the hybrid detection engine controls the sensitivity levels of the anomaly- and signature-based detectors according to the calculated suspicion value. The functionalities of HDE can be listed as follows:

(i) Collecting the outputs of anomaly-based detector and signature-based detector.

(ii) Calculating the attack probability.

(iii) Controlling the security levels of the detectors.

(iv) Updating anomaly detector's normal network model.

(v) Updating the signature-based detectors rule set.

These functionalities are detailed below.

3.4.1. Collecting the Outputs of Detectors. The collection of outputs can be conducted in two different approaches: hard detection and soft detection. In hard detection, the outputs of the detectors are the isAlarm value, which is a binary number indicating if there is an attack or not. In soft detection, the outputs of the detectors are collected as a value referring to probability of an attack. As stated previously, hard detection is used within this study, for the results given in the next section. However, we propose the framework of HDE enabling the use of soft detection.

3.4.2. Calculation of the Attack Probability. The HDE calculates the final decision on the probability of an attack by using the collected outputs of the anomaly- and signature-based detectors. The calculation is performed according to a weighted correlation of the two detector inputs. For a hard decision we can define the process as a function as shown in Figure 4. The overall performance is highly related to the threshold selection (th_1 and th_2) of this function.

When using more than one detector, there is always a possibility that one of the detectors detects an intrusion while the other does not. In case of such an output (the blue fields in Figure 4), one option is to use "OR" relation, which means to decide on presence of an attack even if only one of the

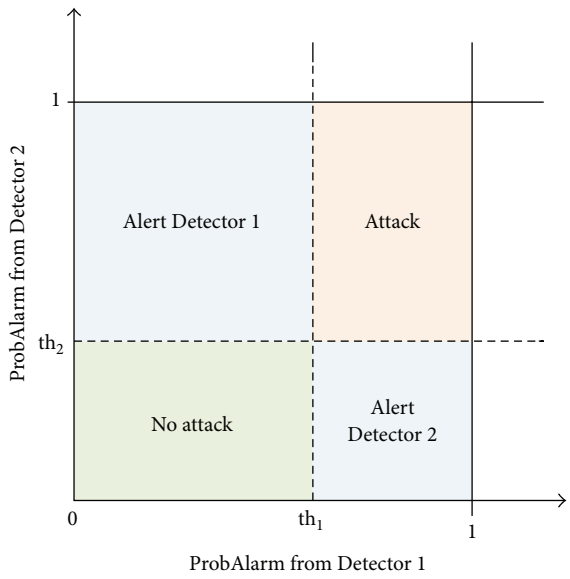

Figure 4: Detection function of HDE.

detectors detects an attack. The other option is to use "AND" relation, where the final decision is presence of the attack if and only if both of the detectors report an intrusion.

For the soft decision, one should provide a probability value for every point in the 2D plane in Figure 4.

3.4.3. Controlling the Security Levels of the Detectors. The security levels of the detectors are controlled by HDE, according to the suspicion level (attack probability). In lower security levels, H-IDS is on a light-working mode; the detector works with a less granular traffic model which has a lower processing power requirement. Hence, it is suitable for systems with high volume of data and lower processing abilities. The security levels can be configured in an adaptive manner according to the production requirements.

The security level of anomaly detector controls the detail level of the traffic modeling. The anomaly detector works with the most detailed model (more Gaussian mixture components) in the highest security level, while it uses a simple network activity model (one or two Gaussian mixture components) for other cases.

The security level of the signature-based detector controls the richness of the applied rule set. For lower security levels, a simple rule set is used while in higher security levels the content of the rule set is extended.

3.4.4. Updating Anomaly Detector's Normal Network Model. One of the most important properties of H-IDS is the feedback feature. If there is an attack that one of the detectors detects and the other does not, it usually means that one of the detectors has missed an attack or the other one gave a false alarm. If the signature-based method detects an alarm with a high probability and the anomaly detector has not detected any anomaly, then we should update the normal network activity model accordingly. This way, we can ensure that the normal network model does not involve an attack situation.

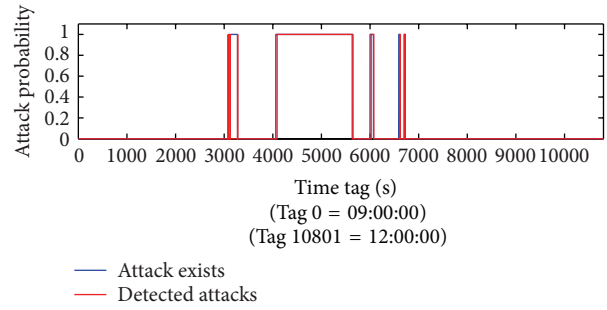

Figure 5: Hard detection results of DARPA dataset.

3.4.5. Updating the Signature-Based Detectors Rule Set. Similar to the update process of the anomaly-based detector's model, HDE also updates the rule set of the signature-based detectors, if it determines that the rule set has missed an attack. The updates of rule parameters are made directly, while rule additions may require a decision support system.

4. Numerical Results

In order to test the performance of our proposed system, the H-IDS is applied to DARPA 2000 dataset and a dataset acquired from a commercial bank in Turkey. The performance indicators are chosen as true positive rate (TPR) and false positive rate (FPR), which are calculated by

$$\begin{aligned} \text{TPR} &= \frac{N_{\text{TD}}}{N_A}, \\ \text{FPR} &= \frac{N_{\text{FD}}}{N_{\text{NA}}}, \end{aligned} \tag{11}$$

where N_{TD} and N_{FD} are the numbers of true detection instances and false detection instances, respectively. N_A represents the number of attack packets, whereas N_{NA} is the number of normal (nonattack) packets.

For the first step in our experiments, a low security level H-IDS using the OR rule is implemented with hard decision and the following results are achieved.

4.1. DARPA 2000 Dataset. We used the dataset DARPA 2000 Lincoln Laboratory Scenario (DDoS) 1.0 which is provided by MIT [25]. This dataset has been used in many studies to test performance of DDoS attack detection.

The attack scenario is carried out over multiple network and audit sessions. These sessions have been grouped into 5 attack phases over the course of which the attacker probes, breaks in, installs Trojan mstream DDoS software, and launches a DDoS attack against an off-site server.

The DARPA dataset is analyzed by using the H-IDS with a hard decision system and by using the OR rule. The obtained results for the first and second weeks of the available data are given in Figure 5. Here, we can see that we have detected the attack with 98.7% TPR and 0.73% FPR by utilizing the proposed H-IDS. Using the AND rule instead of the OR rule, we would have 61.6% TPR and 0.01% FPR.

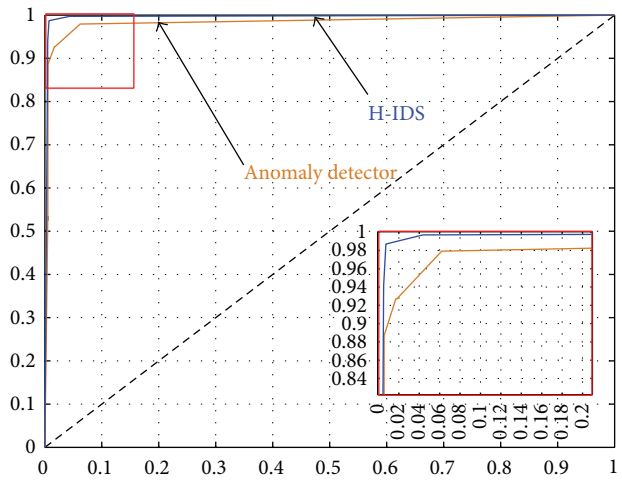

Figure 6: ROC curve for DARPA dataset.

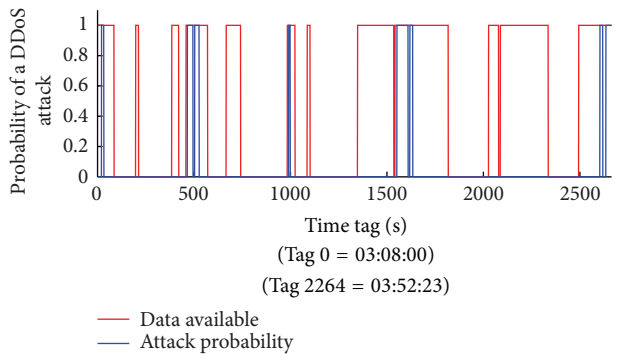

Figure 7: Hard detection results of a commercial bank penetration test dataset.

We also analyzed the sole detection rates of anomaly detector and signature-based detector. With anomaly detector we get a 92.1% TPR and 1.8% FPR, and with signature-based detector we get 64.7% TPR and 13.2% FPR. We can easily see that the attack detection with the H-IDS with OR rule outperforms both systems. This result is similar to the results of [18], as the H-IDS outperforms the single detector systems. Please note that as the authors in [18] have used a different dataset, combining the real-life traffic with the MIT/LL attack dataset, it is not possible to make an exact comparison. However, they reported a 47% detection rate for their system at 1% false alarms and 60% detection rate if the false alarms can be tolerated up to 30%. SNORT has almost a constant 30% detection rate with less than 0.1% false alarm rate.

In Figure 6, the receiver operating characteristic (ROC) curves for both anomaly detector and H-IDS are given for various thresholds (α). The curves show the trade-off between the detection rate and false positive rate under various attacks. Our detection scheme achieves closer to ideal detection performance than the sole use of anomaly detector. This result proves the effectiveness of our H-IDS detection mechanism.

4.2. Dataset of a Commercial Bank from a Penetration Test. The dataset provided by a commercial bank includes banking network data in production and a DDoS attack which is deliberately performed by 400 nodes (zombies) from Amazon.com servers to one web server in the bank's network. There were several ICMP echo attacks within a 45-minute period, each active for 3–7 minutes. The dataset contains 17239 unique IP addresses as destination IP where only one of them is the attack target. The dataset is analyzed and a hard decision system is made on available data. The results are given in Figure 7. Here, our system has a 99.9% TPR and 0.01% FPR, which is very successful. However please note that this particular DDoS attack was easy to detect scenario that is deployed in a penetration test, with very little background traffic and a traceable behavior. The detection performance would probably be lower if more stealthy attacks were performed, especially when attackers try to evade traces that are detectable by the signature-based detector. However even in this case the anomaly detector may detect changes in the network model.

5. Conclusion

In this paper we propose a novel hybrid detection system referred to as H-IDS, which is composed of anomaly-based and signature-based detection techniques for more accurate DDoS attack detection. The proposed detection system can be adopted to networks with varying traffic patterns due to the flexibility provided through the used decision combiner and the associated sensitivity parameter. We test the proposed H-IDS's performance against systems based on nonhybrid detection by using two distinct datasets (i.e., DARPA and a commercial bank penetration test). The results are satisfactory, which shows that the proposed hybrid system can be an efficient solution in the DDoS detection process. We also state that more sophisticated DDoS attacks may evade the signature-based detector rules, which are commonly known, and the system performance may decrease as the detection success solely depends on the anomaly detector. Also the training need of anomaly detector stands as a limitation on the overall system performance. The training data may not reflect the real network model in a practical system or even may be unavailable, which may result in decreased performance. Improvements to the present system, including the enhancement of aforementioned limitations, are left as future work.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported in part by the ITEA2 Project ADAX and the TUBITAK under Grant no. 9130016.

References

[1] Snort, http://www.snort.org/.

[2] Y. Tao and S. Yu, "DDoS attack detection at local area networks using information theoretical metrics," in *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Comm*, pp. 233–240, Melbourne, Australia, July 2013.

[3] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 3, pp. 412–425, 2012.

[4] S. Yu, W. Zhou, and R. Doss, "Information theory based detection against network behavior mimicking DDoS attacks," *IEEE Communications Letters*, vol. 12, no. 4, pp. 318–321, 2008.

[5] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 426–437, 2011.

[6] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Information metrics for low-rate DDoS attack detection: a comparative evaluation," in *Proceedings of the 7th International Conference on Contemporary Computing (IC3 '14)*, pp. 80–84, IEEE, Noida, India, August 2014.

[7] Y. Xiang, Y. Lin, W. L. Lei, and S. J. Huang, "Detecting DDOS attack based on network self-similarity," *IEE Proceedings: Communications*, vol. 151, no. 3, pp. 292–295, 2004.

[8] A. Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," *IEEE Communications Letters*, vol. 13, no. 9, pp. 717–719, 2009.

[9] Y. Chen, X. Ma, and X. Wu, "DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory," *IEEE Communications Letters*, vol. 17, no. 5, pp. 1052–1054, 2013.

[10] X. Wu and Y. Chen, "Validation of chaos hypothesis in NADA and improved DDoS detection algorithm," *IEEE Communications Letters*, vol. 17, no. 12, pp. 2396–2399, 2013.

[11] B. Joshi, A. S. Vijayan, and B. K. Joshi, "Securing cloud computing environment against DDoS attacks," in *Proceedings of the International Conference on Computer Communication and Informatics (ICCCI '12)*, pp. 1–5, IEEE, Coimbatore, India, January 2012.

[12] V. L. Thing, M. Sloman, and N. Dulay, "Locating network domain entry and exit point/path for DDoS attack traffic," *IEEE Transactions on Network and Service Management*, vol. 6, no. 3, pp. 163–174, 2009.

[13] Y. Xie and S.-Z. Yu, "Monitoring the application-layer DDoS sttacks for popular websites," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 15–25, 2009.

[14] H. Luo, Y. Lin, H. Zhang, and M. Zukerman, "Preventing DDoS attacks by identifier/locator separation," *IEEE Network*, vol. 27, no. 6, pp. 60–65, 2013.

[15] M. Barati, A. Abdullah, N. I. Udzir, R. Mahmod, and N. Mustapha, "Distributed Denial of Service detection using hybrid machine learning technique," in *Proceedings of the 4th International Symposium on Biometrics and Security Technologies (ISBAST '14)*, pp. 268–273, Kuala Lumpur, Malaysia, August 2014.

[16] S. Yu, Y. Tian, S. Guo, and D. O. Wu, "Can we beat DDoS attacks in clouds?" *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2245–2254, 2014.

[17] T. Thapngam, S. Yu, W. Zhou, and G. Beliakov, "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS '11)*, pp. 952–957, Shanghai, China, April 2011.

[18] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid intrusion detection with weighted signature generation over anomalous internet episodes," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 1, pp. 41–55, 2007.

[19] J. Gómez, C. Gil, N. Padilla, R. Baños, and C. Jiménez, "Design of a snort-based hybrid intrusion detection system," in *Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living*, pp. 515–522, Springer, Berlin, Germany, 2009.

[20] R. A. Redner and H. F. Walker, "Mixture densities, maximum likelihood and the EM algorithm," *SIAM Review*, vol. 26, no. 2, pp. 195–239, 1984.

[21] G. J. McLachlan and T. Krishnanl, *The EM Algorithm and Extensions*, Wiley Series in Probability and Statistics, 2nd edition, 2008.

[22] J. Bilmes, "A gentle tutorial of the EM algorithm and its application to parameter estimation for Gaussian mixture and hidden Markov models," Tech. Rep. TR-97-021, International Computer Science Institute (ICSI), 1997.

[23] J. Rennie, "A short tutorial on using expectation-maximization with mixture models," 2004, http://people.csail.mit.edu/jrennie/writing/mixtureEM.pdf.

[24] E. Albin and N. C. Rowe, "A realistic experimental comparison of the Suricata and Snort intrusion-detection systems," in *Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA '12)*, pp. 122–127, Fukuoka, Japan, March 2012.

[25] MIT Lincoln Laboratory, Information Systems Technology, 2015, http://www.ll.mit.edu/ideval/data/2000data.html.