Classification of Adversarial Attacks Using Ensemble Clustering Approach

Tatongjai, Pongsakorn; Boongoen, Tossapon; Iam-On, Natthakan; Naik, Nitin; Yang, Longzhi

Published in:
Computers, Materials and Continua

DOI:
10.32604/cmc.2023.024858

Publication date:
2022

Citation for published version (APA):
Tatongjai, P., Boongoen, T., Iam-On, N., Naik, N., & Yang, L. (2022). Classification of Adversarial Attacks Using Ensemble Clustering Approach. *Computers, Materials and Continua*, *74*(2), 2479-2498. https://doi.org/10.32604/cmc.2023.024858

Computers, Materials & Continua
DOI: 10.32604/cmc.2023.024858
Article

Tech Science Press

Classification of Adversarial Attacks Using Ensemble Clustering Approach

Pongsakorn Tatongjai[1], Tossapon Boongoen[2,*], Natthakan Iam-On[2], Nitin Naik[3] and Longzhi Yang[4]

[1]Center of Excellence in AI & Emerging Technologies, School of IT, Mae Fah Luang University, Chiang Rai, Thailand
[2]Department of Computer Science, Aberystwyth University, Aberystwyth, United Kingdom
[3]School of Informatics and Digital Engineering, Aston University, Birmingham, United Kingdom
[4]Department of Computer and Information Sciences, Northumbria University, Newcastle, United Kingdom
*Corresponding Author: Tossapon Boongoen. Email: tob45@aber.ac.uk

Received: 03 November 2021; Accepted: 05 May 2022

Abstract: As more business transactions and information services have been implemented via communication networks, both personal and organization assets encounter a higher risk of attacks. To safeguard these, a perimeter defence like NIDS (network-based intrusion detection system) can be effective for known intrusions. There has been a great deal of attention within the joint community of security and data science to improve machine-learning based NIDS such that it becomes more accurate for adversarial attacks, where obfuscation techniques are applied to disguise patterns of intrusive traffics. The current research focuses on non-payload connections at the TCP (transmission control protocol) stack level that is applicable to different network applications. In contrary to the wrapper method introduced with the benchmark dataset, three new filter models are proposed to transform the feature space without knowledge of class labels. These ECT (ensemble clustering based transformation) techniques, i.e., ECT-Subspace, ECT-Noise and ECT-Combined, are developed using the concept of ensemble clustering and three different ensemble generation strategies, i.e., random feature subspace, feature noise injection and their combinations. Based on the empirical study with published dataset and four classification algorithms, new models usually outperform that original wrapper and other filter alternatives found in the literature. This is similarly summarized from the first experiment with basic classification of legitimate and direct attacks, and the second that focuses on recognizing obfuscated intrusions. In addition, analysis of algorithmic parameters, i.e., ensemble size and level of noise, is provided as a guideline for a practical use.

Keywords: Intrusion detection; adversarial attack; machine learning; feature transformation; ensemble clustering

1 Introduction

To catch up with a development made to new communication platforms and applications, the subject of network security has become one of famous issues that are widely studied. Along this line, many attempts exploit a range of defence mechanism, for instance, firewall and IDS (intrusion detection system) modules to protect assets in a cyberspace [1–3]. To be more specific, unpatched services are good examples of targets of an intrusive attack, which is a significant threat to both individuals and institutes [4]. According to reports of [5–8], NIDS can be effective to monitor traffics and timely identify those considered suspicious. In order to fulfil such a duty, NIDS is to adapt to new attack patterns like polymorphism, which disguised intrusions known to the system [9,10]. As a result, many NIDS may be sub-optimal for those mutated signatures and zero-day attack incidents, whilst facing the rise of FPR (false positive rate) [11,12]. As a response, a rich collection of AI (artificial intelligence) techniques, ML (machine learning) and DL (deep learning) in particular, are explored to enhance NIDS instances, especially in the context of big data [13–15]. In contrary to DL that captures features directly from raw data, the current research follows ML, which disclose useful patterns based on expert-directed or experiment-led feature engineering [16].

Providing the taxonomy of [11] regarding attacks to ML-based NIDS, evasions can be grouped into payload and non-payload types. While the former can be highly effective for specific software/data applications, the latter has proven more applicable to various network settings. In fact, it leads to a great number of investigations, e.g., Protocol Scrubbing [17] and AGENT [18]. Following that, the initial work on non-payload-based IDS together with obfuscation-led adversarial intrusion is published by [19,20]. In those, ML models have been assessed against unseen cases simulated by applying various obfuscation methods to known attack samples. Moreover, the technique proposed therein follows previous feature-engineering works [19,21–25] and develops a framework to select a subset of original features. Despite improved predictive performance, this process is a wrapper in nature [26], which is subject to quality of labels as well as the choice of classifier chosen to evaluate subset candidates. Inspired by this gap of research, the current study aims to answer an obvious question whether existing feature transformation methods as members of the filter approach can perform better than the aforementioned without those constraints. Particularly, the use of ensemble clustering for feature transformation that has been accurate for educational data analysis [27] is to be examined in the present context. Moreover, the practice of noise-induced ensemble generation [28,29] will also be included to provide accurate clusterings, hence the transformed feature set. To be precise, assumption, scope and contribution of this work are summarized as follows.

Assumptions and Scope: The research work presented in this paper focuses on analyzing non-payload and exploit-independent data in the context of classification-based NIDS [19]. Besides, connections at the TCP level are explored, not those corresponding packets at lower layers. Even though an attacker may understand the perimeter of target network, it is assumed that mutating traffics is the only to carry out an intrusive act. As mentioned by [20], this can be obtained through the application of obfuscation functions specifically at network and transport levels. Of course, it leads to unknown intrusive connections that may look alike legitimate ones. Note that the current work falls nicely into the branch emphasizing evasions of measurement phase of IDS, with respect to the model of adversarial attacks against IDS [30].

Contributions: Detail of contributions made by this research work are listed next.

- It presents an original extension to the study of [19], with the aim to invent a new and robust classification-based NIDS. It presents a new alternative of exploiting data transformation techniques to improve detection accuracy, while overcome constraints of class label quality and choice of algorithm commonly faced by the wrapper approach. Hence, the resulting framework is generalized to a wider range of non-payload adversarial attacks.

- The paper presents an organic combination of ensemble clustering and noise-induced ensemble generation [28,29] that is employed as a data transformation prior training a classification model [27]. It is the first to make use of this, especially with the problem of intrusion detection. Its performance is compared with the baseline model reported in [19] and several other data transformation methods found in the literature. This provides an original comparison and findings that are useful to the interdisciplinary community between security and data science.
- In addition to the empirical study, parameter analysis is also provided to exhibit the relation between predictive performance and variables of the proposed method. As such, anyone applies it to a future problem would find this guideline useful for tailoring the model to achieve good performance.

The rest of this paper is organized as follows. In Section 2, background, problem definition and detail of related works are given. After that, Section 3 explains the methodology of proposed ensemble clustering based data transformation, including that of the process of creating a noise-induced ensemble. Having provided those, the performance evaluation of this new technique, its baseline and other compared methods are included and discussed in Section 4. At the end, Section 5 presents the conclusion with directions of future research.

2 Related Works

At first, the section kick offs with detail of background and related studies, specific to subjects of classification-based NIDS, TCP connections as well as non-payload-based obfuscation. Following that, it provides a problem definition from which the proposed technique is developed.

2.1 Classification Approach to NIDS & Feature Engineering Methods

In the recent decade, NIDS appears to be one of significant topics that grows in par with new applications of IoT (Internet of things) network and WSN (wireless sensor network) [31]. In fact, it relies either on determining suspicious connections to signatures of known attacks and legal acts [32], or designing a recognition process called AIDS (anomaly detection-based intrusion detection) [33]. In particular, the latter is able to improve its ability to handle new intrusive patterns by learning these from traffic data [34,35]. However, a typical shortfall is observed that such an approach may encounter the problem of a high FPR, i.e., identification of normal activities to be evasive ones [36]. Other NIDSs such as watchdogs and trust models have been previously proposed, but not relevant to this work that focuses on AI based implementations. Specific to this research line, a classification based system has proven effective as a combination of signature-directed and anomaly-based models. As one example [37], different machine learning techniques are exploited with SMOTE (synthetic minority over-sampling technique) [38] to enhance detection rates of intrusion classes, which are smaller than the majority class of legitimate traffics. This is amongst some works that focus on tackling the difficulty of class imbalance, others pay attention to improving predictive quality through ensemble modeling [39,40] or feature engineering [19,24,25]. The later inspires the current research, with the summarization of related works presented in Tab. 1 (please refer to reviews of [41,42] for a boarder scope of NIDS research).

Table 1: Summarization of related works, specific to classification-based NIDS & feature engineering

Proposed work	Exploited techniques	Feature engineering approach
Oversampling PCA for anomaly detection [43]	Common classifiers; Oversampling	Feature transformation
Adaptive ensemble learning model [40]	DT, RF, KNN & DNN	n/a
Handling of imbalance class in IDS [44]	RF & DNN; Over-& Undersampling	n/a
Hybrid data mining approach [22]	Clustering & KNN	Feature selection
Information-Gain based feature selection [21]	RF; Oversampling	Feature selection
Filter-based attribute reduction [45]	K-means & SVM	Feature selection
Handling of imbalance class in IDS [37]	DT, RF, KNN & LDA; Oversampling	n/a
Determining informative features [24]	RF	Feature selection
Recursive feature elimination [25]	SVM, DT & RF	Feature selection
Feature reduced IDS [23]	ANN	Feature selection
Artificial bee colony for improved classifier ensemble [46]	DT & AdaBoost	n/a
Forwarding feature selection [19]	DT, NB, LR & SVM	Feature selection

As shown in Tab. 1, most of these representative investigations illustrate major directions taken to improve the classification performance using different feature-engineering techniques. On one hand, the approach of feature selection where the most informative subset of original features is employed to build a classification model, appears to be popular for the challenge of NIDS [19,21–25,45]. It has been coupled with many conventional algorithms, e.g., ANN (Artificial neural networks), DNN (Deep neural networks), DT (Decision tree), RF (Random forest), LDA (Linear discriminant analysis), LR (Logistic regression), NB (Naïve Bayes), KNN (K-nearest neighbours), and SVM (Support vector machine). Note that the model proposed by [19] concentrates on the case of adversarial attacks, thus becoming the baseline of the current work. Unlike these methods, the other approach to handle the quest of feature engineering is to transform the original feature space to a more class-wise discriminative one. Only a few such as the study of [43] has attempted to make use of existing algorithms like PCA (Principal component analysis) to achieve the aforementioned goal. Other techniques that are often used for this task include LPP (Locality Preserving Projection [47]), NPE (Neighbourhood Preserving Embedding [48]) and IsoP (Isometric Projection [49]). Handling imbalance data also appears to be an additional direction to further improve a classification-based NIDS, especially when known intrusions are disguised to avoid a positive matching. Actually, methods shown in this table may be able to recognize some unseen instances but are prone to obfuscated attacks. In the next section, this is further explained with the focus on non-payload-based obfuscation.

2.2 Non-Payload-Based Obfuscation

In particular to this research, the study examines network traffic data at the level of TCP, i.e., connection instances that exhibit end-to-end exchanges over the networking stack. With this in mind, each connection γ can be defined by several attributes, e.g., timestamps, details of client/server port and address, transmitted packets between the parties. Based on the work of [19], γ is represented as a set of features, which are generated by the following to map the connection to a space Λ of d dimensions.

$$f(\gamma) \to \Lambda,\ \Lambda = (\lambda_1,\ \lambda_2,\ \ldots,\ \lambda_d) \tag{1}$$

Note that $f_i(\gamma)$ extracts the connecttion under question to the i^{th} dimension.

$$f_i(\gamma) \to \lambda_i,\ i = \{1,\ \ldots,\ d\} \tag{2}$$

Based on the original work of [19,20], these dimensions are, numbers of TCP URG (urgent) and FIN (finish) flags, length of TCP header, deviation of packet size, for instance. With these being clarified, it is possible to specify non-payload-based obfuscation that basically is a modification of those connection attributes. To start with, the next equation formally presents an obfuscation-free connection γ_a.

$$f(\gamma_a) \to \Lambda^a,\ \Lambda^a = \left(\lambda_1^a,\ \lambda_2^a,\ \ldots,\ \lambda_d^a\right) \tag{3}$$

Following that, let us define the connection $\gamma_{a'}$ that is an intrusive instance γ_a to which obfuscation techniques are applied. These so-called mutation methods alters packet properties of the initial connection γ_a by either insertion, removal and transformation functions. As a result, the space Λ^a is then changed to $\Lambda^{a'}$.

$$f(\gamma_{a'}) \to \Lambda^{a'},\ \Lambda^{a'} = \left(\lambda_1^{a'},\ \lambda_2^{a'},\ \ldots,\ \lambda_d^{a'}\right) \tag{4}$$

Given this, a classification model developed without awareness of mutated connection instances might not perform as well as expected. In accordance with to the report of [50], various techniques have been invented for the purpose of building an obfuscation tool in the Unix setting. Some examples of these operations $f(\gamma_{a'})$ are spreading out packets along the time domain via a constant delay, loss of some packet content, duplicated packets, modification of packet order, packet fragmentation through specific MTU (maximum transmission unit), and a mix of these functions.

By following past works on the classification approach to NIDS [39,51], training data $X = V \times Y$ specifies the set of labeled network connections, with V representing the space of n instances ($V \in R^{n\times d}$), Y denoting the $n \times 1$ space of class labels, and each $x_i \in V$ can be categorized as $y_i \in Y$. For that, the value of y_i is chosen from the class domain D_X. For a classification model trained on X using the technique α, the resulting classifier CF_X^α determines the class $y_0 \in D_X$ for an unseen sample $x_0 \in R^{1\times d}$, i.e., $CF_X^\alpha(x_0) = y_0$. Provided that the problem under investigation is a binary classification, the class prediction $y_{\gamma a}$ for a connection γ_a that is represented by the feature vector $f(\gamma_a)$, can be specified as follows.

$$y_{\gamma a} = CF_X^\alpha\left(f\left(\gamma_a\right)\right) \tag{5}$$

provided that $y_{\gamma_a} \in \{\text{Intrusion, Legitimate}\}$. For a connection $y_{\gamma_{a'}}$ whose data attributes have been changed using some obfuscation functions, the goodness of class prediction $y_{\gamma_{a'}}$ is worth exploring.

$$y_{\gamma_{a'}} = CF_X^\alpha\left(f\left(\gamma_{a'}\right)\right) \tag{6}$$

In the course of adversarial attacks, a common classifier CF_X^α can be ineffective without information of obfuscation. As a response, the research of [19] resolves this trouble using a feature selection approach, which repeatedly add informative feature to the target subset. This development can improve performance of classifying adversarial attacks, but at the same time, it is not generalized due to constraints of label quality as well as the choice of algorithm used in a wrapper framework. Consequently, a filter method is introduced in this paper to deliver a robust classifier. This is obtained using the methodology of ensemble clustering for data transformation.

3 Proposed Method

The application of ensemble clustering to improve predictive performance of a classification model has been initially introduced by [27,52], for the categorization of student academic achievement. It is extended here by adding the noise-induced ensemble generation [28,29] that may help the transformed data to be more informative for classifying mutated connections. This sections provides details of different stages within the proposed framework, including the creation of ensemble members, the summarization of within-ensemble information as a transformed data matrix, and the use of this resulting matrix for training a classifier, respectively. Specific to the problem of ensemble clustering or cluster ensemble, let $V = \{x_1, x_2, \ldots, x_n\}$ be the matrix in the normalized domain $[0, 1]^{n \times d}$ of n connection instances with respect to d features. Note that the label space Y from a training dataset $X = V \times Y$ will not be used here as a clustering process is an unsupervised model, which develop a data partition (i.e., a set of clusters) without the knowledge of class labels. In addition, each sample $x_i \in V$ is represented as a vector of d feature dimensions or $x_i = (x_{i1}, \ldots, x_{id}), \forall i \in \{1, 2, \ldots, n\}$. Also let $\Pi = \{\pi_1, \pi_2, \ldots, \pi_M\}$ be a cluster ensemble with M base clusterings, i.e., an ensemble member. In particular, the *gth* member delivers a collection of clusters $\pi_g = \left\{C_1^g, C_2^g, \ldots, C_{k_g}^g\right\}$, where $\cup_{t=1}^{kg} C_t^g = X$, $\cap_{t=1}^{kg} C_t^g = \varnothing$ and k_g is the number of clusters in partition π_g. For any instance $x_i \in V$, $C^g(x_i)$ represents the cluster label in the *gth* base clustering to which x_i belongs, i.e., $C^g(x_i) = t$ if $x_i \in C_t^g$. Now, an ensemble clustering method attempts to find a new partition $\pi^* = \left\{C_1^*, \ldots, C_K^*\right\}$, where K denotes the preferred number of clusters in this ultimate result, which summarizes clustering-wise information across members in Π.

Ensemble Generation. Given this terminology, the first stage is to generate a cluster ensemble Π from which the desired data matrix $\Omega \in R^{n \times n}$ of transformed space is derived. In the current study, the following three generation strategies are employed. Note that the homogeneous ensemble is commonly exploited as a basis, where the k-means technique builds ensemble members π_g, $g = 1 \ldots M$ with different initial cluster centroid settings and the number of clusters k_g randomly selected for a range $\left\{2, 3, \ldots, \sqrt{n}\right\}$. Based on the report of [52], the upper bound is limited to 50 if $\sqrt{n}$ is too large to provide a meaningful partition.

(1) Random-subspace method: each base clustering is generated from a random feature subspace $V' \in [0, 1]^{n \times d'}$ of the space V. Each of the data subspaces is created with respect to the following interval d'.

$$d' = d'_{min} + \lfloor \beta \left(d'_{max} - d'_{min}\right) \rfloor \tag{7}$$

provided that $\beta \in [0, 1]$ is a uniform random variable, while d'_{min} and d'_{max} denote the lower and upper bounds of the generated subspace V'. Following the initial work of [53], $d'min$ and $d'max$ are set to $0.75d$ and $0.85d$. With this, one of d features is picked up at a time to form the desired subspace of d' non-duplicated features is obtained. The index of each randomly selected feature is determined by the following.

$$h = \lfloor 1 + \eta d \rfloor \tag{8}$$

where h denotes the *hth* feature in the pool of d attributes and $\eta \in [0, 1]$ is another uniform random variable.

(2) Noise-induced method: it is also possible to generate a base clustering from a noise-induced feature space $V^{ns} \in [0,1]^{n\times d}$, which is acquired by injecting noisy feature values in the original space V. Given the improvement of clustering quality emphasized in [28], a uniform random noise from the unit range [0, 1] is chosen to replace one of the existing feature values, whose position in the matrix V has been arbitrarily selected using the salt-and-pepper concept. Note that the proportion of noise entries in the resulting V^{ns} is determined by the factor of r%, i.e., $\lceil \frac{r}{100} nd \rceil$.

(3) Combined method: the aforementioned strategies can also be integrated to determine a modified feature subspace, from which a base clustering can be generated. Initially, a noisy feature space V^{ns} is created with the specified noise rate r%. Then, a subspace $V^{ns'}$ can be produced for building a base clustering. This organic combination has not been implemented and assessed in the literature thus far.

Ensemble Summarization. Having completed the previous stage, information within a given ensemble Π is to be aggregated and represented as a high-level data matrix $\Omega \in R^{n\times n}$. This represents pairwise relations among n instances, based on the same-cluster occurrence statistics across M clustering results. In particular to a specific ensemble member $\pi_g \in \Pi$, a pairwise similarity matrix S_g, $g = 1 \ldots M$ is formulated, with an entry $S_g\left(x_i, x_j\right) \in \{0,\ 1\}$ denoting a relationship between two instances $x_i, x_j \in V$. This is 1 if both instances occur in the same cluster within π_g, and 0 otherwise.

$$S_g\left(x_i, x_j\right) = \begin{cases} 1 & if\ C^g\left(x_i\right) = C^g\left(x_j\right) \\ 0 & otherwise \end{cases} \tag{9}$$

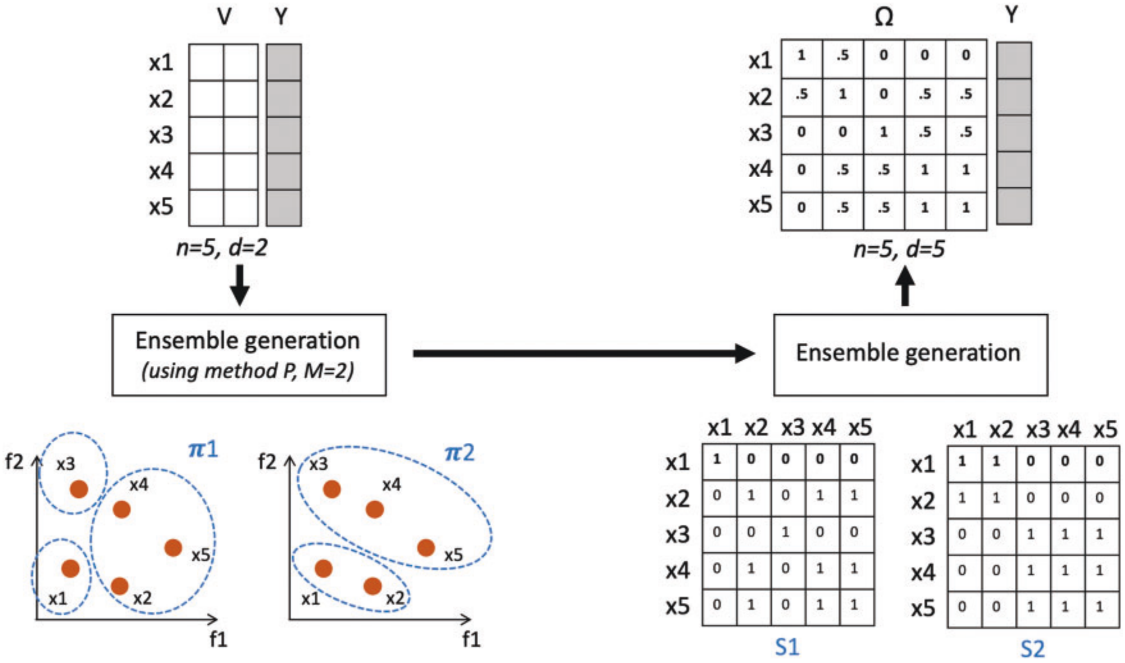
After that, the target Ω matrix is summarized as the average of those M similarity matrices of $S_1, \ldots, S_M$.

$$\Omega\left(x_i, x_j\right) = \frac{1}{M}\sum\nolimits_{g=1}^{M} S_g\left(x_i, x_j\right) \tag{10}$$

Classification Model Development. Having obtained the ensemble-clustering matrix Ω, it can be considered as a new feature space of n dimensions that has been transformed from the original space of d features. Therefore, given the original dataset $X = V \times Y$, the transformed dataset can be achieved as $X^t = \Omega \times \text{Y}$. As a result, a classifier $CF^{\alpha}_{X^t}$ can be trained with the transformed data X^t using the choice of classification algorithm α. As such, the prediction $y_{\gamma_{a'}}$ of a connection instance whose features are altered by different obfuscation techniques is determined by the following definition.

$$y_{\gamma_{a'}} = CF^{\alpha}_{X^t}\left(f\left(\gamma_{a'}\right)\right) \tag{11}$$

It is noteworthy that other filer methods can also be used in this way to generate the transformed data X^t. These will be included in the empirical study reported next. To be more precise, Fig. 1 depicts the processing flow of these stages, with a working example. In particular, this data set contains 5 instances and 2 features, i.e., $V = \{x_1, x_2, \ldots, x_5\}$ and $d = 2$. Using the generation method P that can be one of the three described previously, two clusterings of those instances are generated as $\Pi = \{\pi_1, \pi_2\}$. After that, the transformation matrix Ω can be summarized from both clustering-specific, S_1 and S_2. Lastly, the training stage may kick off using the matrix Ω and the original label vector Y.



x1	1	.5	0	0	0
x2	.5	1	0	.5	.5
x3	0	0	1	.5	.5
x4	0	.5	.5	1	1
x5	0	.5	.5	1	1

	x1	x2	x3	x4	x5
x1	1	0	0	0	0
x2	0	1	0	1	1
x3	0	0	1	0	0
x4	0	1	0	1	1
x5	0	1	0	1	1

	x1	x2	x3	x4	x5
x1	1	1	0	0	0
x2	1	1	0	0	0
x3	0	0	1	1	1
x4	0	0	1	1	1
x5	0	0	1	1	1

Figure 1: Summarization of the proposed method with a working example

4 Performance Evaluation

After defining the problem and proposed method, this paper continues with an experimentation in which the new data transformation model is evaluated against results published in the original work and other filter techniques. Details of dataset, experimental design, results and discussion are emphasized herein.

4.1 Investigated Dataset and Experimental Design

The dataset employed in this research is originally collected for assessing the robustness of machine-learning based NIDS [19]. Both legitimate and intrusion traffics have been generated across vulnerable network services, with obfuscation techniques being applied to mutate appearance of some direct attacks. These connections are then passed to that TCP-level feature extractor, ASNM (advanced security network metrics) [54]. The target dataset $X = V \times Y$ consists of a normalized feature space $V \in [0, 1]^{11,445 \times 194}$, where an instance-specific class $v_i \in V$ is drawn from the domain of 3 possible connect categories, i.e., {Legitimate, Direct attack, Obfuscated attack}. For the paper to be self contained, Tabs. 2 and 3 show details of 11,445 collected connections with respect to network services being exploited, and ASNM feature categories with examples (please consult [54] for a full list). Note that some of ASNM features are highly discriminative between simulated attacks and legitimate connections collected from a real network. This set consists of 10 TTL (time-to-live) based features in the statistical category and all 8 features (e.g., IP addresses, ports and MAC addresses) from the localization group. As a result, these are removed from the feature space, with the final version being reduced to $V \in [0, 1]^{11,445 \times 176}$.

Table 2: Details of connections collected from venerable network services, categorized by types of legitimate and intrusive attacks. This is taken from the original presented in [54]

Network service	Legitimate	Direct attack	Obfuscated attack	Total
Apache tomcat	809	61	163	1,033
DistCC	100	12	23	135
MSSQL	532	31	103	666
PostgreSQL	737	13	45	795
Samba	4,641	19	44	4,704
Server	3,339	26	100	3,465
Other legitimate traffics	647	n/a	n/a	647
All services	10,805	162	478	11,445

Table 3: ASNM feature categories and examples. These are taken from [54] with a full list available therein

Feature type	No. of features	Examples: *Name*; description
Statistical	77	*SumTTLIn*; sum of TTL value for inbound traffic *MedTTLOut*; median of TTL value in outbound traffic *ModTTLOut*; mode of TTL value in outbound traffic *SigTTLOut*; standard deviation of TTL value in outbound traffic
Localization	8	*SrcIP*; the IP address of the source machine (client) *DstIP*; the IP address of the destination machine (server) *SrcPort*; a port of the client machine *DstPort*; a port of the server machine
Distributed	34	*InPkt4s10i*; the same as the previous one, but computed above the first *InPkt8s10i*; the same as the previous one, but computed above the first *OutPktLen4s10i*; the same as the previous one, but computed above the first 4 s. *OutPktLen8s10i*; the same as the previous one, but computed above the first 8 s.
Dynamic	32	*TSesStart*; start time of a connection *TSesEnd*; end time of a connection *MeanTdiff2Pkts*; mean of packet IAT in all traffic *SigTdiff2Pkts*; standard deviation of packet IAT in all traffic

(Continued)

Table 3: Continued

Feature type	No. of features	Examples: *Name*; description
Behavioral	43	*GaussProds1In*; normalized products of inbound packet sizes with 1 Gaussian curve *GaussProds1Out*; normalized products of outbound packet sizes with 1 Gaussian curve *PolyTime5ordIn*; the same as the previous one, but utilizes polynomial of 5th order *PolyTime5ordOut*; the same as the previous one, but utilizes polynomial of 5th order

To achieve a thorough assessment, the collection of compared methods including the proposed one are included in this empirical study. In particular, predictive performance of the new ECT is initially evaluated against its baseline: the data with selected 21 features of FFS (forward feature selection), which are based on the report of [19]. Other compared methods belong to the filter approach, and the implementation is available online (www.cad.zju.edu.cn/home/dengcai/Data/DimensionReduction.html). It is noteworthy that their algorithmic variables are configured to defaults, as suggested by the original publications. These include LPP [47], NPE [48], and IsoP [49]. Other experimental settings are as follows.

- For the proposed method, there are three variations of ECT-Subspace, ECT-Noise and ECT-Combined, given different strategies exploited to generate cluster ensembles. For the noise-induced modification, the ratio of $r = 5\%$ is particularly selected for the overall evaluation, with an in-depth investigation being given later in parameter analysis. In addition, the target ensemble size M is set to 20, and each specific setting of these models is repeated for 20 trials to achieve a reliable conclusion from non-deterministic processes, based on averages of multiple runs.
- The input feature space to FFS of original works [19] is composed of pre-selected 21 features, while the Original and others are fed with same dataset of 176 dimensions.
- For the choice of classification algorithm α, four techniques are included here. These include C4.5 (decision tree) with the maximum depth of 15, NB with the Gaussian kernel function, SVM with the Radial kernel function, and LR, respectively. These are employed with the dataset generated by those filter and wrapper techniques to create a classifier.
- With the focus of this research on robustness of classification-based NIDS to mutated patterns induced by obfuscation, a model will be trained with samples representing normal connections and direct attacks only. By not having access to those obfuscated instances, it is to observe how well different algorithms deal with unfamiliar intrusions. To achieve this, the evaluation framework of stratified 10-fold cross validation is initially exploited for the problem of classifying legitimate traffics and direct attacks, i.e., the data under investigation is the mix of samples belonging only to those two types. The result may illustrate the effectiveness of classifiers to recognize typical intrusive patterns. Building from that, a fold-specific model is used to predict those obfuscated instances, as a legitimate or attack one. This second experiment provides the view of robustness to unseen intrusions. It is noteworthy that a set of assessment metrics include TRP (true positive rate), FPR and F1 (F1 score), respectively.

4.2 Results and Discussion

At first, to provide an overview of experimental results on classifying legitimate and direct attack patterns, F1 scores obtained by different feature-space transformation methods are illustrated in Fig. 2. These are averages across multiple trials of 10-fold cross validation, with four classification algorithms investigated in the current study. In that, variations of the proposed technique, i.e., ECT-Subspace, ECT-Noise and ECT-Combined, usually reach F1 measures that are higher than those of FFS and other three filter methods. Without the application of obfuscation techniques to modify intrusive connections, ECT-Combined has proven the most effective with the highest F1 of 92.30%, with two simpler models of ECT-Subspace and ECT-Noise achieve slightly lower scores of 89.92% and 90.67%, respectively. As such, the new ensemble-clustering data transformation concept is able to produce informative features, thus improving predictive performance from the baseline of 89.23% set by FFS. Besides, they are more generalized without a supervised process of finding a feature subset that yields the optimal classification accuracy. In fact, the set of 21 features disclosed by FFS may not be applicable as future legitimate and direct-attack connections are added to the present dataset. Despite lower F1 measures, other three filter approaches of LPP, NPE and IsoP also enjoy this flexibility as more data becomes available. See Tab. 4 for details of TPR, FPR and F1 statistics, which are categorized by classifiers and feature-transformation competitors. Specific to NB that is the most accurate classification model, predictive performance of ECT-Combined is comparable to that of FFS, while it improves both TPR (from 95.062% to 96.914%) and FPR (from 0.102% to 0.056%) with the second best classifier, i.e., C4.5. For less accurate classifiers of SVM and LR, all the three variations of ECT largely outperform the benchmark set by the supervised FFS wrapper. In addition, other filter models have been comparable to FFS, for these two classifier as well.

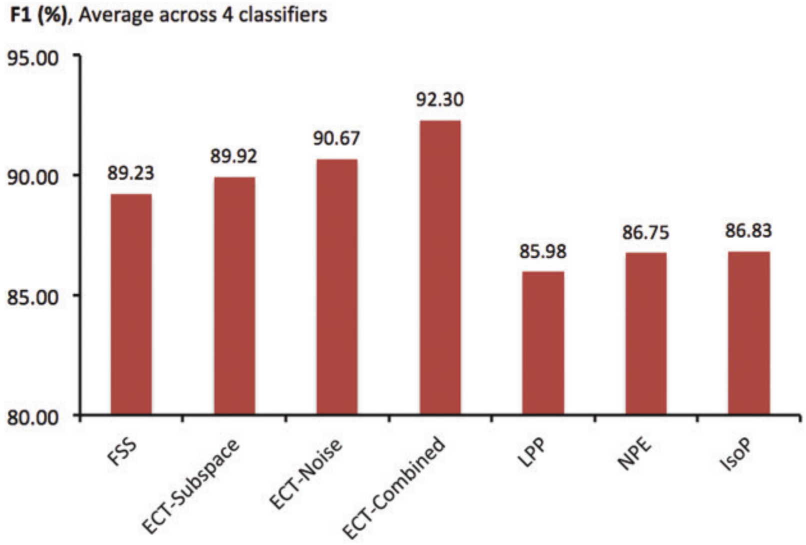


Figure 2: Comparison of F1 scores obtained by different feature-space transformation methods, as averages across classification models and multiple trials of 10-fold cross validation

Table 4: Details of TPR, FPR and F1 scores obtained by examined methods, categorized by four classifiers. Note that corresponding values of standard deviation are given in (brackets)

Classifier	Examined method	TPR (%)	FPR (%)	F1 (%)
NB	FSS	98.148 (2.785)	0.028 (0.018)	98.148 (3.573)
	ECT-subspace	95.679 (3.261)	0.056 (0.022)	95.975 (0.384)
	ECT-noise	96.914 (2.278)	0.019 (0.015)	97.050 (2.801)
	ECT-combined	98.148 (3.102)	0.019 (0.017)	98.452 (2.925)
	LPP	92.593 (4.562)	0.074 (0.073)	93.750 (4.378)
	NPE	91.358 (3.891)	0.093 (0.066)	92.500 (4.006)
	IsoP	93.827 (2.218)	0.056 (0.081)	95.000 (2.673)
C4.5	FSS	95.062 (2.813)	0.102 (0.156)	94.190 (3.014)
	ECT-subspace	94.444 (3.120)	0.074 (0.052)	94.737 (3.271)
	ECT-noise	95.679 (2.712)	0.093 (0.055)	94.801 (3.118)
	ECT-combined	96.914 (2.411)	0.056 (0.401)	96.615 (2.934)
	LPP	90.123 (5.123)	0.120 (0.082)	90.966 (5.181)
	NPE	88.889 (3.416)	0.102 (0.087)	93.705 (4.003)
	IsoP	91.975 (2.799)	0.139 (0.103)	92.315 (3.782)
SVM	FSS	81.481 (2.755)	0.028 (0.041)	88.889 (3.150)
	ECT-subspace	84.568 (4.106)	0.074 (0.067)	89.251 (4.112)
	ECT-noise	85.802 (3.788)	0.093 (0.078)	89.389 (3.904)
	ECT-combined	88.272 (3.152)	0.037 (0.045)	92.557 (3.109)
	LPP	82.099 (4.576)	0.111 (0.961)	86.645 (4.811)
	NPE	79.630 (3.781)	0.046 (0.077)	87.162 (3.998)
	IsoP	80.864 (2.187)	0.065 (0.051)	86.903 (2.352)
LR	FSS	69.136 (2.642)	0.204 (0.103)	75.676 (3.613)
	ECT-subspace	74.074 (3.987)	0.176 (0.118)	79.734 (3.203)
	ECT-noise	75.926 (2.985)	0.157 (0.092)	81.457 (3.543)
	ECT-combined	76.543 (3.177)	0.167 (0.103)	81.579 (3.204)
	LPP	66.049 (4.119)	0.241 (0.142)	72.542 (4.202)
	NPE	67.284 (3.562)	0.231 (0.161)	73.649 (3.618)
	IsoP	64.815 (3.101)	0.185 (0.159)	73.091 (2.998)

Apart from the evaluation of simple patterns, Fig. 3 focuses on the report of TPR scores each of the investigated methods acquires from classifying 478 obfuscated intrusions, presented as averages across classifiers and multiple runs of 10-fold cross validation. It is interesting to see that conventional filter techniques of LPP, NPE and IsoP have become as effective as the carefully formulated FSS, with TPR being around 48–49%. All three new alternatives introduced here in this research possess better statistics than the baseline of FSS, with TPR scores above 50%. Further details are presented in Tab. 5, in which TPR scores have been recorded for each coupling of classifiers and those transformation techniques. According to this, the three variations of ECT usually exhibit predictive performance superior than FSS, and other compared methods. In particular, the best accurate alternative among these combinations is the exploitation of ECT-Combined with NB classifier, which delivers an averaged TPR score of 83.845%. Despite an obvious gap for future improvement, it is clear that the robustness of classifiers to obfuscated intrusions has been notably enhanced here.

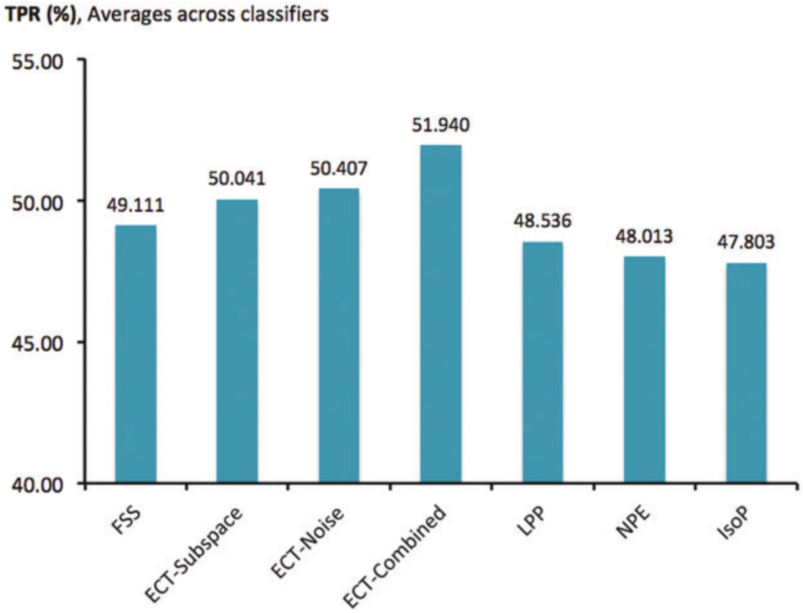


Figure 3: Comparison of TPR scores obtained by different feature-space transformation methods for classifying obfuscated instances, as averages across classifiers and trials of 10-fold cross validation

Table 5: TPR scores as averages across from multiple trials of 10-fold cross validation, categorized by corresponding values of standard deviation are given in (brackets)

Examined method	NB	C4.5	SVM	LR
FSS	81.172 (4.156)	36.402 (2.611)	15.690 (1.984)	63.180 (2.516)
ECT-subspace	81.962 (3.819)	37.238 (3.562)	16.736 (2.226)	64.226 (3.411)
ECT-noise	83.008 (3.773)	37.866 (3.029)	16.318 (3.102)	64.435 (2.893)
ECT-combined	83.845 (4.013)	39.331 (3.151)	17.364 (2.876)	67.200 (4.101)
LPP	79.916 (2.978)	35.983 (4.191)	15.481 (3.177)	62.762 (3.002)
NPE	79.289 (3.115)	35.146 (3.788)	15.063 (3.264)	62.552 (2.847)
IsoP	80.335 (3.787)	34.519 (2.271)	14.644 (3.021)	61.715 (1.993)

Moving away from the comparative scheme previously presented, it is also significant to observe the effects of model parameters to predictive performance. One of these is the ensemble size (M) that has been set to 20 initially. As such, ad additional investigation is conducted on the three variations of ECT with the noise ratio of 5% and different numbers of ensemble members, i.e., $M \in \{20, 30, 40, 50, 60, 70\}$. Specific to the illustration given in Fig. 4 that summarizes the results across four classifiers, increasing M generally leads to improve the prediction quality of those three new methods. According to this figure, both ECT-Noise and ECT-Combined continue to improve as the ensemble size grows up to 60 and 70, while the performance of ECT-Subspace seems to converges around $M = 30$, i.e., adding more members will not yield a higher TPR measure. A similar trend has been witnessed with the NB classifier, based on statistical details in Fig. 5. In particular, the target TPR can be improved from 83.845 to 86.002 after M has been enlarged from 20 to 70. However, a tradeoff between gain in performance and a higher complexity is a concern for resource-constrained applications. Note that the complexity of generating a single base clustering is approximated to $O(n)$ and $O(nM)$ for an ensemble of M members.

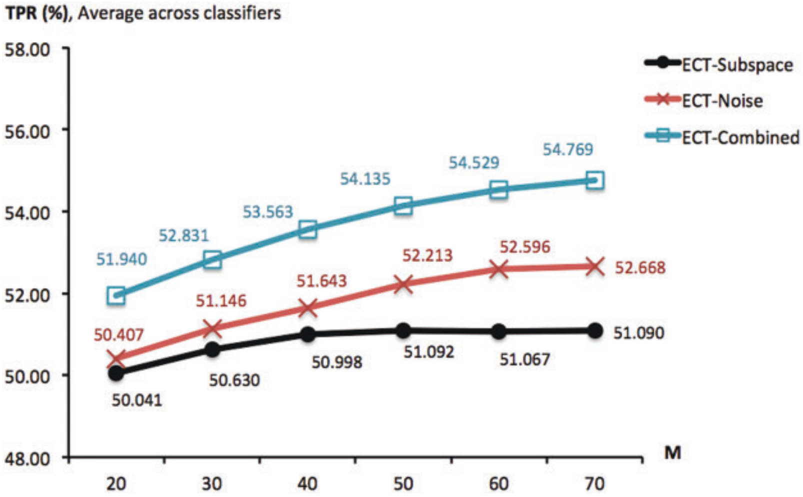


Figure 4: TPR scores obtained by ECT-Subspace, ECT-Noise and ECT-Combined, with the noise ratio of 5% and different ensemble sizes (from 20 to 70). These are summarized across four classifiers and multiple trials of 10-fold cross validation

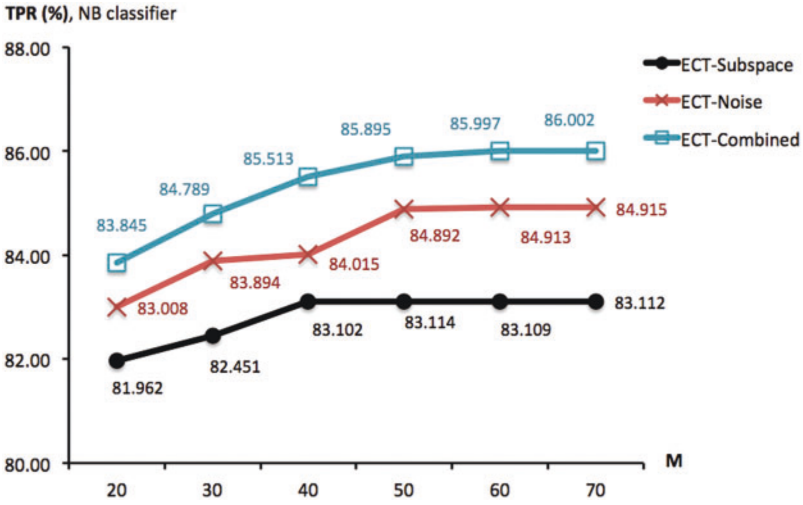


Figure 5: TPR scores obtained by ECT-Subspace, ECT-Noise and ECT-Combined, with the noise ratio of 5% different ensemble sizes (from 20 to 70). These are summarized across NB classifier, multiple trials of 10-fold cross validation

Another important variable is the ratio *r*% of noise injected into the data matrix, which has been set to 5% in previous experiments. Intuitively, adding more noise may lead to a greater diversity that is a factor of effective cluster ensembles. Provided this insight, a new investigation is designed to observe the association between goodness of ECT-Noise and ECT-Combined and different noise lev-els of *r*% ∈ {5, 10, 15, 20, 25, 30}. To focus on this parameter, the ensemble size *M* has been set to 20 and ECT-Subspace is irrelevant and not included. To given an overview of the corresponding result, Fig. 6 reports TPR measures obtained by ECT-Noise and ECT-Combined as averages across four classifiers. In that, an improvement can actually be made by adding more noise, i.e., increasing the ratio from 5% to 20% lift the score of ECT-Combined from 51.940% to 53.824%. This is similarly seen in the case of ECT-Noise whose TPR grows from 50.407% to 51.441%. Moreover, Fig. 7 shows the same result, but only with the NB classifier. It appears that ECT-Noise and ECT-Combined reach their highest TPRs around the noise levels of 15% and 20%, respectively. Despite they promote much higher diversity within an ensemble, noise ratios above 20% may not be effective due to the accuracy of each ensemble member has dropped rapidly, thus the overall quality as a group.

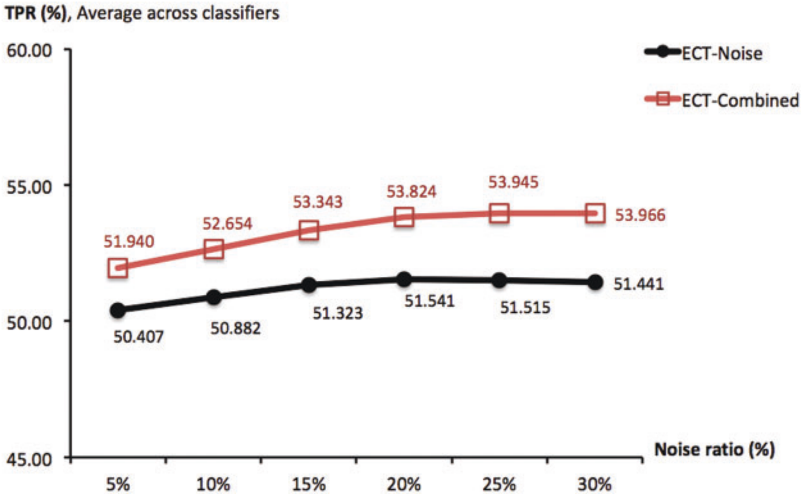


Figure 6: TPR scores obtained by ECT-Noise and ECT-Combined, with the ensemble size of 20 and different noise ratios *r*% ∈ {5, 10, 15, 20, 25, 30}. These are summarized across four classifiers and multiple trials of 10-fold cross validation

Given the aforementioned findings, both ECT-Noise and ECT-Combined are further investigated with respect to optimal ensem-ble size of $M = 50$. Fig. 8 depicts a comparison between two noise ratios of 5% and 20% exploited with these models that have been applied to the two most accurate classifiers of NB and LR. It is shown in this figure that a marginal enhancement to predictive performance can be achieved with the optimal setting of those hyper parameters. Note that the highest TPR scores achieved by ECT-Noise and ECT-Combined with NB are 85.298% and 86.604%, respectively. The proposed methods and results presented thus far can be truly useful for handling adversarial attacks to a machine-learning based NIDS. They are more generalized to different obfuscation techniques than the wrapper model given in original works, thus raising the robustness to unseen and modified patterns.

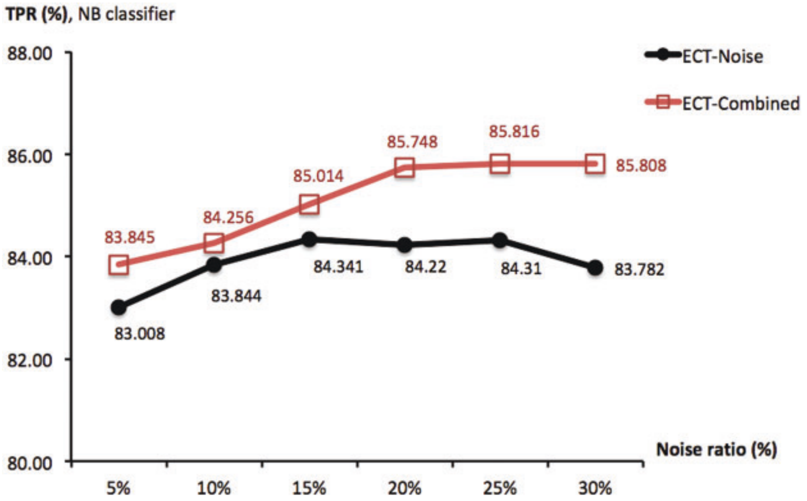


Figure 7: TPR scores obtained by ECT-Noise and ECT-Combined, with the ensemble size of 20 and different noise ratios $r\% \in \{5, 10, 15, 20, 25, 30\}$. These are summarized across NB classifier and multiple trials of 10-fold cross validation

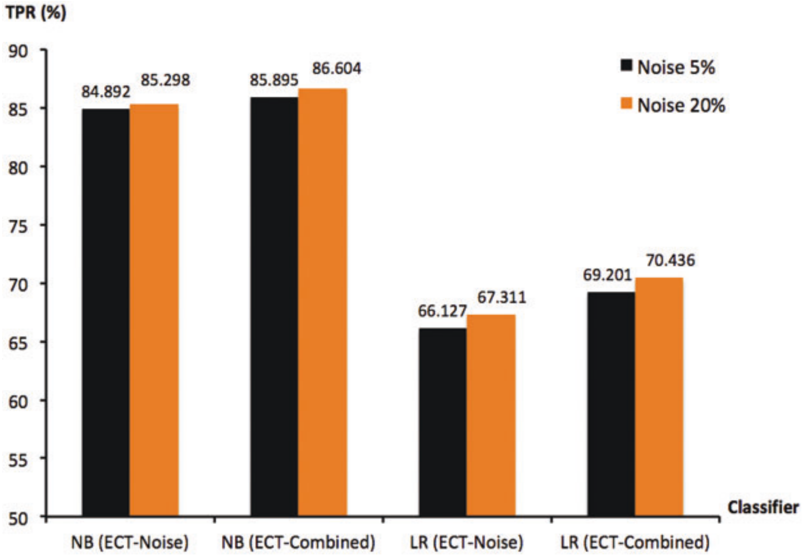


Figure 8: TPR scores of ECT-Noise and ECT-Combined, with ensemble size of 50 and noise ratios $r\%$ $\in \{5, 20\}$. These are summarized for NB and LR, across multiple trials of 10-fold cross validation

5 Conclusion

This paper has presented a novel approach to handle adversarial attacks on machine-learning based NIDS, where legitimate, direct attacks and obfuscated intrusions can be accurately classified. The proposed methods make use of an ensemble-clustering data matrix as the transformed feature space to train a classifier. Unlike the wrapper framework called FFS exploited in the original study, three filter variations of ECT-Subspace, ECT-Noise and ECT-Combined are created without the knoweledge of true classes. in particular, they are formulated using three different strategies of random subspace, injection of attribute noises and the combination of these. In terms of model development, the new alternatives are more generalized to new data compared to FFS, as they are not constrained by the choice of classification evaluator that discriminate significance of feature subsets. In other words, this initial setting may change to data patters and the quality of labels seen with a future collection of traffic connections. Based on experiments with the benchmark dataset and classification algorithms, the proposed techniques usually outperform the original FFS and other filter algorithms found in the literature. In addition, parameter analysis has also been included to visualize relations between predictive performance and hyper parameters of ensemble size (M) and noise ratio (r%).

Despite this achievement, there are several issues leading to a worthwhile future work. At first, it is to assess the proposed techniques with more datasets in order to draw a timely conclusion for practical uses. In particular, they may be applied to other analysis tasks [55–57]. With respect to modeling of base clustering, ensemble clustering, other choices of generation strategies and ensemble summarization schemes can be another good research to conduct [58]. In addition, other aspects of the underlying feature space may well be addressed, for instance, the treatment of missing values [59] and discretization of a feature domain [60]. Finally, an introduction of fuzzy sets and vocabularies is able to support the explainability of reasoning process [61]. This final remark draws a great deal of attention provided the emerging trend of explainable AI for modern applications.

Acknowledgement: This research work is a part of MSc study at Mae Fah Luang University.

Funding Statement: This work is funded by Newton Institutional Link 2020–21 project (NRCT and British Council) and the corresponding author is the project PI. This paper invents and evaluates an ensemble-based data transformation method on network security data (guided by Dr Naik and Dr Yang), then it will be further exploited to classify burnt scar samples in remote sensing images. The authors would like to thank Prof. Qiang Shen and his team at Aberystwyth University for consultation, and Thai partners (GISTDA, DTI, Department of Forestry and RMUTL Chiang Rai) for support.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Tarter, “Importance of cyber security,” in *Community Policing-A European Perspective: Strategies, Best Practices and Guidelines*, vol. 1. Cham, Switzerland: Springer, pp. 213–230, 2017.

[2] L. Nie, Y. Wu, X. Wang, L. Guo, G. Wang *et al.,* “Intrusion detection for secure social internet of things based on collaborative edge computing: A generative adversarial network-based approach,” *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 134–145, 2022.

[3] A. Almomani, A. Al-Nawasrah, W. Alomoush, M. Al-Abweh, A. Alrosan *et al.,* “Information management and IoT technology for safety and security of smart home and farm systems,” *Journal of Global Information Management*, vol. 29, no. 6, pp. 1–23, 2021.

[4] H. Debar, M. Dacier and A. Wespi, “A revised taxonomy for intrusion detection systems,” *Annals of Telecommunications*, vol. 55, no. 7, pp. 361–378, 2000.

[5] J. Li, Y. Qu, F. Chao, H. Shum, E. Ho *et al.,* “Machine learning algorithms for network intrusion detection,” *AI in Cybersecurity*, vol. 151. Cham, Switzerland: Springer, pp. 151–179, 2019.

[6] T. Lunt, “A survey of intrusion detection techniques,” *Computer Security*, vol. 12, no. 4, pp. 405–418, 1993.

[7] Y. Alotaibi, “A new database intrusion detection approach based on hybrid meta-heuristics,” *Computers, Materials & Continua*, vol. 6, no. 2, pp. 1879–1895, 2021.

[8] M. Alauthman, A. Almomani, M. Alweshah, W. Omoushd and K. Alieyane, "Machine learning for phishing detection and mitigation," *Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices*, vol. 1. Florida, USA: CRC Press, pp. 1–27, 2019.

[9] A. Eassa, O. Al-Tarawneh, H. El-Bakry and A. Salama, "NoSQL racket: A testing tool for detecting NoSQL injection attacks in web applications," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 11, pp. 614–622, 2017.

[10] T. Mithal, K. Shah and D. Singh, "Case studies on intelligent approaches for static malware analysis," in *Proc. of Int. Conf. on Emerging Research in Computing, Information, Communication and Applications*, Bangalore, India, pp. 555–567, 2016.

[11] M. Barreno, B. Nelson, A. Joseph and J. Tygar, "The security of machine learning," *Machine Learning*, vol. 81, no. 2, pp. 121–148, 2010.

[12] C. Yin, Y. Zhu, S. Liu, J. Fei and H. Zhang, "Enhancing network intrusion detection classifiers using supervised adversarial training," *The Journal of Supercomputing*, vol. 76, no. 9, pp. 6690–6719, 2020.

[13] R. Prasad and V. Rohokale, "Artificial intelligence and machine learning in cyber security," *Cyber Security: The Lifeline of Information and Communication Technology*, vol. 1. Cham, Switzerland: Springer, pp. 231–247, 2020.

[14] M. Najafabadi, F. Villanustre, T. Khoshgoftaar, N. Seliya, R. Wald *et al.,* "Deep learning applications and challenges in big data analytics," *Journal of Big Data*, vol. 2, no. 1, pp. 1–15, 2015.

[15] S. Huang and K. Lei, "IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks," *Ad Hoc Networks*, vol. 105, pp. 102177, 2020.

[16] C. Dka, J. Papa, C. Lisboa, R. Munoz and A. Dvhc, "Internet of things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[17] D. Watson, M. Smart, G. Malan and F. Jahanian, "Protocol scrubbing: Network security through transparent flow modification," *IEEE/ACM Transactions on Networking*, vol. 12, no. 2, pp. 261–273, 2004.

[18] S. Rubin, S. Jha and B. Miller, "Automatic generation and analysis of NIDS attacks," in *Proc. of Annual Computer Security Applications Conf.*, Tucson, AZ, USA, pp. 28–38, 2004.

[19] I. Homoliak, M. Teknos, M. Ochoa, D. Breitenbacher, S. Hosseini *et al.,* "Improving network intrusion detection classifiers by non-payload-based exploit-independent obfuscations: An adversarial approach," *EAI Endorsed Transactions on Security and Safety*, vol. 5, no. 17, pp. e4, 2018.

[20] I. Homoliak, D. Ovsonka, M. Gregr and P. Hanacek, "NBA of obfuscated network vulnerabilities exploitation hidden into HTTPS traffic," in *Proc. of Int. Conf. for Internet Technology and Secured Transactions*, London, UK, pp. 311–318, 2014.

[21] A. Tesfahun and D. L. Bhaskari, "Intrusion detection using random forests classifier with SMOTE and feature reduction," in *Proc. of Int. Conf. on Cloud Ubiquitous Computing and Emerging Technology*, Pune, India, pp. 127–132, 2013.

[22] M. R. Parsaei, S. M. Rostami and R. Javidan, "A hybrid data mining approach for intrusion detection on imbalanced nsl-kdd dataset," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 6, pp. 20–25, 2016.

[23] A. Akashdeep, I. Manzoor and N. Kumar, "A feature reduced intrusion detection system using ANN classifier," *Expert Systems with Applications*, vol. 88, pp. 249–257, 2017.

[24] N. Farnaaz and M. A. Jabbar, "Random forest modeling for network intrusion detection system," *Procedia Computer Science*, vol. 89, pp. 213–217, 2016.

[25] N. V. Sharma and N. S. Yadav, "An optimal intrusion detection system using recursive feature elimination and ensemble of classifiers," *Microprocessors and Microsystems*, vol. 85, pp. 104293, 2021.

[26] T. Boongoen, C. Shang, N. Iam-On and Q. Shen, "Extending data reliability measure to a filter approach for soft subspace clustering," *IEEE Transactions on Systems, Man and Cybernetics, Part B*, vol. 41, no. 6, pp. 1705–1714, 2011.

[27] N. Iam-On and T. Boongoen, "Improved student dropout prediction in Thai university using ensemble of mixed-type data clusterings," *International Journal of Machine Learning and Cybernetics*, vol. 8, no. 2, pp. 497–510, 2017.

[28] P. Panwong, T. Boongoen and N. Iam-On, "Improving consensus clustering with noise-induced ensemble generation," *Expert Systems with Applications*, vol. 146, pp. 113–138, 2020.

[29] N. Iam-On, "Clustering data with the presence of attribute noise: A study of noise completely at random and ensemble of multiple k-means clusterings," *International Journal of Machine Learning and Cybernetics*, vol. 11, no. 3, pp. 491–509, 2020.

[30] I. Corona, G. Giacinto and F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues," *Information Sciences*, vol. 239, pp. 201–225, 2013.

[31] K. Haseeb, A. Almogren, N. Islam, I. Ud-Din and Z. Jan, "An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN," *Energies*, vol. 12, no. 21, pp. 4174, 2019.

[32] A. Ahmim, M. Derdour and M. Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," *International Journal of Communication Systems*, vol. 31, no. 9, pp. e3547, 2018.

[33] W. Ma, "Analysis of anomaly detection method for internet of things based on deep learning," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, pp. e3893, 2020.

[34] M. Uddin, A. Rahman, N. Uddin, J. Memon, R. Alsaqour *et al.,* "Signature-based multi-layer distributed intrusion detection system using mobile agents," *International Journal of Network Security*, vol. 15, no. 2, pp. 97–105, 2013.

[35] C. Guo, Y. Ping, N. Liu and S. Luo, "A two-level hybrid approach for intrusion detection," *Neurocomputing*, vol. 214, pp. 391–400, 2016.

[36] V. Chandola, A. Banerjee and V. Kumar, "Anomaly detection: A survey," *ACM Comput Survey*, vol. 41, no. 3, pp. 1–58, 2009.

[37] G. Karatas, O. Demir and O. Sahingoz, "Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset," *IEEE Access*, vol. 8, pp. 32150–32162, 2020.

[38] N. Chawla, K. Bowyer, L. Hall and W. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.

[39] Y. Shen, K. Zheng, C. Wu, M. Zhang, X. Niu *et al.,* "An ensemble method based on selection using Bat algorithm for intrusion detection," *The Computer Journal*, vol. 61, no. 4, pp. 526–538, 2018.

[40] X. Gao, C. Shan, C. Hu, Z. Niu and Z. Liu, "An adaptive ensemble machine learning model for intrusion detection," *IEEE Access*, vol. 7, pp. 82512–82521, 2019.

[41] D. P. Kumar, T. Amgoth and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," *Information Fusion*, vol. 49, pp. 1–25, 2019.

[42] B. Molina-Coronado, U. Mori, A. Mendiburu and J. Miguel-Alonso, "Survey of network intrusion detection methods from the perspective of the knowledge discovery in databases process," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2451–2479, 2020.

[43] R. Abdulhammed, M. Faezipour, A. Abuzneid and A. Abumallouh, "Anomaly detection via online oversampling principal component analysis," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 7, pp. 1460–1470, 2013.

[44] R. Abdulhammed, M. Faezipour, A. Abuzneid and A. Abumallouh, "Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic," *IEEE Sensors Letters*, vol. 3, no. 1, pp. 1–4, 2019.

[45] A. Chandra, S. K. Khatri and R. Simon, "Filter-based attribute selection approach for intrusion detection using k-means clustering and sequential minimal optimization technique," in *Proc. of Amity Int. Conf. on Artificial Intelligence*, Dubai, United Arab Emirates, pp. 740–745, 2019.

[46] M. Mazini, B. Shirazi and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and adaboost algorithms," *Journal of King Saud University-Computer and Information Sciences*, vol. 31, no. 4, pp. 541–553, 2019.

[47] X. He, S. Yan, Y. Hu, P. Niyogi and H. J. Zhang, "Face recognition using laplacian faces," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 3, pp. 328–340, 2005.

[48] X. He, D. Cai, S. Yan and H. J. Zhang, "Neighborhood preserving embedding," in *Proc. of Int. Conf. on Computer Vision*, Beijing, China, pp. 1208–1213, 2005.

[49] D. Cai, X. He and J. Han, "Isometric projection," in *Proc. of AAAI Conf. on Artificial Intelligence*, Toronto, Canada, pp. 528–533, 2007.

[50] I. Homoliak, M. Teknos, M. Barabas and P. Hanacek, "Exploitation of netem utility for non-payload-based obfuscation techniques improving network anomaly detection," in *Proc. of Int. Conf. on Security and Privacy in Communication Systems*, Guangzhou, China, pp. 770–773, 2016.

[51] H. Yao, D. Fu, P. Zhang, M. Li and Y. Liu, "MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1949–1959, 2018.

[52] N. Iam-On and T. Boongoen, "Diversity-driven generation of link-based cluster ensemble and application to data classification," *Expert Systems with Applications*, vol. 42, no. 21, pp. 8259–8273, 2015.

[53] N. Iam-On, T. Boongoen, S. Garrett and C. Price, "A Link-based approach to the cluster ensemble problem," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 12, pp. 2396–2409, 2011.

[54] I. Homoliak, M. Barabas, P. Chmelar, M. Drozd and P. Hanacek, "ASNM: Advanced security network metrics for attack vector description," in *Proc. of Conf. on Security and Management*, Las Vegas, USA, pp. 350–358, 2013.

[55] G. Li, F. Liu, A. Sharma, O. I. Khalaf, Y. Alotaibi *et al.,* "Research on the natural language recognition method based on cluster analysis using neural network," *Mathematical Problems in Engineering*, vol. 2021, no. 9982305, pp. 1–13, 2021.

[56] R. Rout, P. Parida, Y. Alotaibi, S. Alghamdi and O. I. Khalaf, "Skin lesion extraction using multiscale morphological local variance reconstruction based watershed transform and fast fuzzy c-means clustering," *Symmetry*, vol. 13, no. 11, pp. 2085, 2021.

[57] A. Alrosan, W. Alomoush, N. Norwawi, M. Alswaitti and S. N. Makhadmeh, "An improved artificial bee colony algorithm based on mean best-guided approach for continuous optimization problems and real brain MRI images segmentation," *Neural Computing and Applications*, vol. 33, no. 5, pp. 1671–1697, 2021.

[58] A. Alrosan, W. Alomoush, M. Alswaitti, K. Alissa, S. Sahran *et al.,* "Automatic data clustering based mean best artificial bee colony algorithm," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 1575–1593, 2021.

[59] M. Pattanodom, N. Iam-On and T. Boongoen, "Hybrid imputation framework for data clustering using ensemble method," in *Proc. of Asian Conf. on Information Systems*, Krabi, Thailand, pp. 86–91, 2016.

[60] K. Sriwanna, T. Boongoen and N. Iam-On, "Graph clustering-based discretization of splitting and merging methods (graphs and graphm)," *Human-centric Computing & Information Sciences*, vol. 7, no. 1, pp. 1–39, 2017.

[61] X. Fu, T. Boongoen and Q. Shen, "Evidence directed generation of plausible crime scenarios with identity resolution," *Applied Artificial Intelligence*, vol. 24, no. 4, pp. 253–276, 2010.