IoT INTRUSION DETECTION SYSTEM LEVERAGING PSO AND SEQUENTIAL FORWARD FEATURE SELECTION

Van-Thinh Pham, Huu-Cam Nguyen, Hai-Chau Le and Chien-Trinh Nguyen
Posts and Telecommunications Institute of Technology, Hanoi, Vietnam

Abstract: The Internet of Things (IoT) plays an important role with wide application in various fields. However, the sustainability of IoT is limited by several challenges and security-related problems are the most dangerous. Therefore, in this work, the ability of two distinct feature selection methods including Particle Swarm Optimization-based and sequential forward-based approaches are leveraged and compared to find the most appropriate feature extraction technique and the most valuable feature set of the IoT-23 dataset to construct an efficient Intrusion Detection System validated by multiple Machine Learning algorithms. The prospect of solving problems in practical environments is demonstrated through the achieved results.

Keywords: Intrusion Detection System, Machine Learning, Particle Swarm Optimization, Sequential forward feature selection.

I. INTRODUCTION

The Internet of Things (IoT) is a pioneering technology that has found applications in various real-world domains. For instance, it enhances agricultural practices by optimizing crop yields and enabling automated farming. In the healthcare sector, IoT devices are being used to create advanced medical equipment that aids in patient treatment. It also contributes to the development of smart cities equipped with intelligent solutions like smart transportation, smart buildings, and smart education systems. The range of IoT applications is very vast, making our everyday life smarter and more efficient than ever before. Moreover, with the rapid advancement of IoT technology, there has been a rapid proliferation of connected devices, reaching an estimated 29 billion IoT devices by the year 2030 [1].

However, although IoT is a revolutionary technology that offers numerous benefits, it also presents a multitude of challenges. These challenges extend beyond security issues and include interoperability, scalability, power consumption, data overload, and legal and regulatory issues. Despite these challenges, IoT continues to evolve. However, security remains a critical concern. Most IoT systems are equipped with numerous sensors that monitor their surroundings, gather data, and relay it to the system's data processing components. These sensors, due to their small size and limited resources, often struggle to implement traditional, complex security measures like intricate deep learning models, making them prime targets for attacks. Furthermore, the data shared among IoT devices or stored on cloud platforms may not be adequately encrypted, leaving them vulnerable to attackers. This data, which can be sensitive, could potentially expose users' privacy or crucial information, enabling unauthorized access to the IoT systems. Additionally, the communication protocols used in IoT systems are diverse and heterogeneous, complicating the implementation and maintenance of security measures. Therefore, given these factors, it is more critical than ever to devise new and effective strategies to address these concerns in IoT.

Intrusions can take various forms. For example, an intruder might gain unauthorized access to a user's account by stealing their password, impersonating them, intercepting their communications, or injecting harmful code. The system can also be compromised by insiders who exploit software application vulnerabilities or server weaknesses. Numerous tools and services, such as firewalls, password encryption, access control, and intrusion prevention systems, are used to safeguard the network against these threats. Intrusion Detection System (IDS) stands out as one of the most effective. The IDS is a potent tool for identifying and categorizing various types of attacks in both computer networks and IoT networks. Typically, IDS is divided into two categories: 1) Signature-based IDS, which is highly efficient in dealing with known attacks, and 2) Anomaly-based IDS, which is adept at handling unknown intrusions [2]. The popularity of this security method stems from its compatibility with machine learning (ML) and deep learning (DL), which can be effectively employed for intrusion detection. In [3], authors introduced a method called stacked dilated convolutional

Contact author: Chien -Trinh Nguyen,
Email: *trinhnc@ptit.edu.vn*
Manuscript received: 18/4/2024, revised: 18/6/2024, accepted: 28/6/2024.

autoencoder (DCAE), which is capable of autonomously learning crucial features from a substantial volume of raw network traffic. The DCAE model has a smaller number of parameters compared to fully connected neural networks like SAE. However, a notable drawback of the DCAE model is its relatively lengthy training process. To address this issue, the authors plan to utilize GPU parallelization technology in future work. It's important to note that their models use a private dataset to train and test, which means a direct comparison with other models isn't possible. The Random Forest Regressor method was implemented to extract significant features from the CICDDoS2019 dataset for building their DDoS Network Intrusion Detection System. This system was constructed using a combination of multiple machine learning classifiers, including BayesNet, Bagging (BG), k Nearest Neighbors (KNN), Sequential minimal optimization, and Simple Logistic, along with the application of 5-fold cross-validation (CV) techniques. Furthermore, the author utilized oversampling and undersampling strategies to enhance the DDoS detection rate of their model. While the average performance achieved was relatively satisfactory, there were instances of lower results for some subsets of the CICDDoS2019 dataset with the mentioned classifiers.

The feature selection method is characterized as the process of extracting a subset of features from the existing set of features, which plays an important role in constructing IDS effectively because valuable information can be achieved through this stage. According to [5], the feature selection method is categorized into 3 different approaches including filter, wrapper, and embedded. Although this method is very popular for building efficient IDS such as authors in [6] suggest an effective IDS that utilizes ML, with feature selection guided by a metaheuristic optimization algorithm and a voting classifier or an improved feature selection method based on the Genetic Algorithm, referred to as GA-based Feature Selection (GbFS), is proposed to boost the accuracy of classifiers in [7]. These methods are very powerful and can enhance the

Figure 1. Block diagram of proposed method

outcome considerably, which helps IDS deal with well in practical environments.

However, not too much previous research has been done to find the most outstanding feature selection method for constructing IDS better. Therefore, in this paper, two popular feature selection methods namely PSO-based and sequential forward leveraging Random Forest (RF) feature importance approaches are leveraged to extract the most informative feature of the IoT-23 dataset, a novel data collected from the IoT environment and they are compared to find the most suitable one for IDS construction. Multiple ML classifiers such as RF, AdaBoost (AB), BG, and XGBoost (XGB) are utilized to validate these selected features and find the optimal set that can enhance the classification performance. Moreover, to increase the reliability of the proposed method, a 5-fold CV procedure is made use of for training and validating all chosen classifiers.

II. METHODOLOGY

This approach consists of three main phases, as depicted in Figure 1. Firstly, the IoT-23 dataset undergoes cleaning and quality improvement, as described in the previous section. Secondly, two feature selection methods including PSO-based and sequential forward-based are employed to extract significant features from the cleaned data, enhancing classification performance and reducing the complexity of the proposed methods. Subsequently, various ML classifier techniques are used to build the IDS. Both processes are validated using 5-fold cross-validation to prevent overfitting. Furthermore, to identify the most effective feature selection method for the IoT-23 dataset, the performance of the optimal feature set from each method is compared. Finally, the classification results of the proposed method are evaluated against other previous research to provide an overview of its effectiveness.

A. Data preprocessing

The IoT-23 dataset used in this research is directly extracted from IoT environments, consisting of 20 malware and 3 benign records [8]. This dataset provides a variety of contemporary attack types essential for building an effective IDS [9].

First, features with excessive missing values are removed. Next, features that specify particular IDs, sources, and destinations of IP addresses and ports are excluded, as these are specific to the data collection environment and could affect classifier performance in different environments. The 'history' feature is also removed as it only provides connection history.

Based on the correlation graph in [10], two pairs of correlated features were identified, and only one feature from each pair was retained. Additionally, the 'missed-bytes' feature was discarded because most of its values are zero.

TABLE I. DESCRIPION OF REMAINED LABELS

Attack Class	Number of samples
DDoS	1643225
Benign	115399
PartOfAHorizontalPortScan	69198
Okiru	14942
Attack	9363
C&C	9363
Total	**187130**

Since ensemble ML classifiers require numerical inputs, categorical features such as 'proto', 'service', and 'duration' are converted to numerical form using a probability density algorithm, which replaces characters with the ratio of their frequency to the total number of samples. To reduce value range differences among features, logarithmic normalization is applied to 'duration', 'orig-bytes', 'resp-bytes', 'orig-pkts', and 'resp-pkts'. Duplicate values are removed (keeping only the first occurrence), and minority classes are eliminated to address data imbalance. Finally, Min-Max normalization is applied within the range [0, 1].

After preprocessing, 8 features include 'proto', 'service', 'conn-state', 'duration', 'orig-bytes', 'resp-bytes', 'orig-pkts', and 'resp-pkts'—are extracted from the original dataset. The remaining labels and their corresponding sample counts after preprocessing are shown in Table I.

B. Detection algorithm

In this project, four machine learning algorithms namely BG, RF, AB, and XG are chosen for classification purposes. These algorithms are selected due to their categorization into two distinct methodologies. The first approach, which includes BG and RF, utilizes the bagging method for training, while the second approach employs boosting techniques. This division enables a comprehensive exploration of both bagging and boosting methodologies within the classification process.

BG [11]: A well-known ensemble machine learning algorithm commonly used to address overfitting issues. It involves selecting portions of the original training data to create multiple bootstrap samples, which are then used to train and validate individual classifiers in parallel. Each model generates its own output, offering unique advantages and disadvantages. In classification tasks, a majority voting procedure is employed to combine these outputs, resulting in the overall model performance.

RF [11]: An advanced version of BG, this algorithm trains multiple Decision Trees (DTs) in parallel. Data subsets are created from the original training data for each base classifier. Additionally, different feature subsets are randomly selected from the entire set for each tree during its construction. The final classification results are obtained through a majority voting or averaging approach.

AB [11]: A classification algorithm based on Boosting, consisting of a series of weak learners, typically DTs, arranged sequentially. Unlike BG and RF, AB uses the original training set to train all base classifiers in sequence. The algorithm focuses on samples misclassified by previous models by assigning higher weights to these data points before training the next weak learner. This adaptive weighting scheme aims to enhance overall classification performance over iterations.

XG [11]: Similar to AB, this algorithm is based on the Boosting principle, using a sequential model of multiple weak classifiers. However, instead of increasing the weight of misclassified samples like AB, XG improves overall classification performance by minimizing the loss of the previous base classifier.

C. Feature Selection

1) PSO-based Feature Selection

Particle Swarm Optimization (PSO), proposed in [12], is inspired by the foraging behavior of bird swarms. In this algorithm, particles simulate birds, each acting as a search entity within an N-dimensional search space. The current position of a particle represents a potential solution to the problem, and each particle is characterized by its velocity and position. The velocity indicates the movement step size, while the position indicates the direction of movement. The best solution found by each particle is considered its personal best, and the best solution found by the swarm is regarded as the global best. Through multiple iterations, particles update their velocities and positions, and the process continues until termination conditions are satisfied. The process of PSO can be outlined as follows. Firstly, randomly initialize the velocities and positions of particles within the search space. Secondly, each particle identifies its own personal best solution, and the global best solution is determined from these individual bests. The current global best is then compared with the historical global best, and based on this comparison, the global best is updated if a better solution is found. Finally, the objective of these particles is to locate and converge at the global minimum position. The particles' velocities and positions are updated based on the following equations.

$$v_i^{t+1} = w v_i^t + \phi_b r_b (x_{ib} - x_i) + \phi_g r_g (g_b - x_i) \quad (1)$$

$$x_i^{t+1} = x_i^t + v_i^t \quad (2)$$

with v_i representing the random velocity of each particle, ϕ_b and ϕ_g as scaling parameters for local and global components respectively, and both r_b and r_g being random values.

TABLE II. THE PERFORMANCE COMPARISON BETWEEN TWO FEATURE SELECTION METHOD

Classifier	PSO-based Feature Selection				Sequential Forward Feature Selection			
	Acc (%)	Pre (%)	Rec (%)	F1 (%)	Acc (%)	Pre (%)	Rec (%)	F1 (%)
AB	98.10	99.43	98.51	98.97	97.25	86.93	97.66	91.44
BG	98.13	99.42	98.55	98.98	97.24	86.96	97.59	91.43
XG	98.08	99.65	98.27	98.95	97.22	86.86	97.46	91.33
RF	**99.94**	**99.53**	**99.99**	**99.76**	97.81	89.12	98.6	93.02

To apply PSO for feature selection, subsets of features are randomly selected from the original set to form a population. The corresponding fitness values, calculated using Root Mean Square Error (RMSE), are then computed. With the initial velocities, the particles' positions are updated to balance exploration and exploitation. If a feature set reduces the fitness value, the associated indices are stored to identify an effective subset.

2) Sequential Forward Feature Selection

The paper employs a sequential forward-based method as the second feature selection approach. Initially, after preprocessing, the importance score of each feature is calculated using RF importance score. These scores are then sorted in descending order. Subsequently, the optimal feature set is determined by setting a threshold. A feature is considered optimal if its importance score surpasses this threshold. The threshold value is determined iteratively based on the RF scores, which evaluate each feature from the most to the least essential. At each iteration, a feature is added to the optimal set, and the threshold is adjusted until the process halts. If a feature exhibits a significant disparity in importance compared to the subsequent one, such as being over two times more important, the iteration stops, and the threshold is set to the importance score of that feature.

D. Evaluation

The optimal feature sets obtained from two distinct feature selection methods are validated using four different classifiers: BG, RF, AB, and XG, in conjunction with the 5-fold CV procedures. Two binary classifications between "Normal" created by extracting the "Benign" class and "Intrusion" generated by combining all attack classes in the preprocessed data. This validation process is essential before comparing the performance of each feature selection method with each other to determine the most effective approach for IoT-23 feature selection.

In the 5-fold CV technique, the dataset is divided into five similar segments, with each segment used as a testing set while the remaining data serves as the training set. This process is repeated five times, with each segment taking a turn as the testing set. By employing this approach, the results obtained are more reliable because it helps mitigate overfitting issues. Overfitting occurs when a model performs exceptionally well on the training data but fails to generalize effectively to unseen data. The 5-fold CV technique aids in addressing this concern by ensuring that the model's performance is evaluated on multiple subsets of the data, thus providing a more comprehensive assessment of its capabilities.

III. SIMULATION RESULTS AND DISCUSSION

A. Performance Evaluation Metrics

To assess the effectiveness of the proposed method, four common metrics are employed: Accuracy (Acc), Precision (Pre), Recall (Rec), and F1-score (F1). Acc quantifies the proportion of correctly classified samples out of the total. Pre measures the accuracy of identifying attack samples among those classified as such, while Rec denotes the proportion of correctly classified attack samples out of all actual attack instances. F1 is a balanced metric that combines Precision and Recall. Therefore, in this study, Acc and F1 are the primary evaluation metrics. The equations for calculating these metrics are provided in (3), (4), (5), and (6).

$$Acc = \frac{TP+TN}{TP+FP+TN+FN} \quad (3)$$

$$Rec = \frac{TP}{TP+FN} \quad (4)$$

$$Pre = \frac{TP}{TP+FP} \quad (5)$$

$$F1 = \frac{TP}{TP+\frac{1}{2}(FP+FN)} \quad (6)$$

with True Positive (TP) occurs when the IDS correctly identifies instances of attacks as attacks, thus effectively detecting malicious activities. True Negative (TN) signifies

the system's accurate identification of non-attacks as non-attacks, ensuring that normal activities are not flagged as suspicious. False Positives (FP) arise when the IDS erroneously identifies non-attacks as attacks, resulting in false alarms that can lead to unnecessary investigation or resource allocation. On the other hand, False Negatives (FN) represent instances where the IDS fails to detect actual attacks, potentially allowing malicious activities to go unnoticed.

B. Feature Selection

1) PSO-based Feature Selection

As previously discussed, PSO Feature Selection is employed to identify a subset of features that enhances both classification accuracy and reduces training costs. The technique involves generating multiple particles, each with its own velocity, to explore local and global optimal solutions. In the feature selection process, candidate feature subsets are randomly extracted, and their respective RMSE values are calculated. The optimal feature subset is determined by observing a reduction in the RMSE value, indicating a higher-quality subset with improved performance.

The calculation of the RMSE fitness value for each feature subset following 100 iterations is depicted in Figure 2. Following each iteration loop, updates are made to the position and velocity. Additionally, the index and size of each selected feature set are retained as the result of this feature selection phase. Consequently, the top 5 features exhibiting the highest quality for the initial layer of the proposed IDS are identified, comprising: 'conn_state', 'orig_bytes', 'resp_bytes', 'orig_pkts', and 'orig_pkts'.

TABLE III: THE PERFORMANCE COMPARISON BETWEEN OTHER PREVIOUS RESEARCH

Reference	**Acc (%)**	**Pre (%)**	**Rec (%)**	**F1 (%)**
[13]	98.89	99.47	98.37	98.92
[14]	97.25	99.83	97.19	98.49
[15]	NA	100	95	98
This paper	**99.94**	99.53	**99.99**	**99.76**

2) Sequential Forward Feature Selection

In the second approach to feature selection, the importance scores of each feature are calculated using Random Forest (RF) and arranged in descending order, as illustrated in Figure 3. As explained earlier, a threshold is established to determine the optimal feature set. Consequently, the computed scores are as follows: [0.291717, 0.273589, 0.211896, 0.100063, 0.058742, 0.031966, 0.020948, 0.011079] for the features 'duration', 'conn_state', 'orig_pkts', 'orig_bytes', 'resp_pkts', 'proto', 'resp_bytes', and 'service'. Following the method described, the threshold value is set at 0.100063, which equals one-third of the highest score. The subsequent score is only about one-sixth of the highest, which is considered too low so the rest starts from this feature to the last is eliminated. Therefore, the optimal feature set is determined to include 'duration', 'conn_state', 'orig_pkts', and 'orig_bytes'.

Figure 2. PSO-based feature selection results

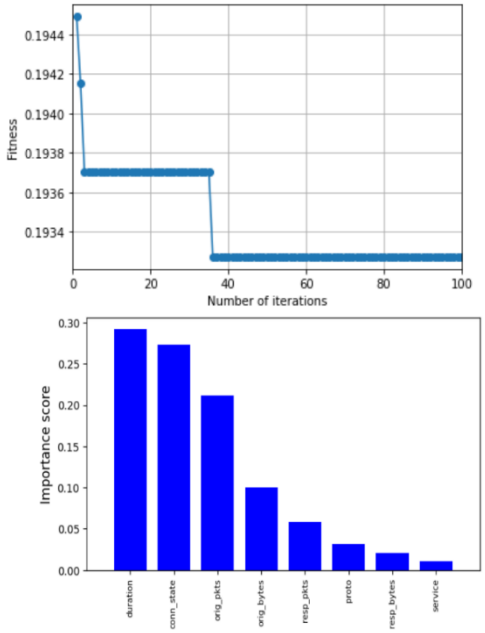

Figure 3. RF importance scores-based ranking results

C. Evaluation

In this paper, two feature selection methods including PSO-based and sequential forward feature selection are conducted to achieve the optimal set, and these evaluations are compared with each other. Both optimal feature sets received from the two methods are validated with 4 ML algorithms with 5-fold CV procedures. The outcome comparison of both sets is represented in Table II to find the most valuable feature set of the IoT-23 dataset. Moreover, to evaluate the performance of the best set in the general view, the best outcome of the proposed IDS is compared with other previous classes in Table III. The achieved results are impressive with the best feature set received from the PSO-based feature selection approach, which can peak at extremely high evaluation metrics with 99.94% Acc, 99.53% Pre, 99.99% Rec, and 99.76% F1 utilizing RF classifiers. Moreover, this outcome is also very outstanding in comparison to other published research.

D. Discussion

In this work, two distinct feature selection methods are leveraged to find the optimal feature set for the IoT-23 dataset to construct a power IDS that can detect intrusions efficiently in IoT environments. According to Table II, the best performance utilizing PSO-based feature selection outperforms the highest one using sequential forward with

RF importance score approaches, both thanks to the ability of the RF classifier. While Acc and Pre of the PSO-based method are larger than these metrics of sequential forward technique at 2.13% and 0.13% respectively, the difference between values of Pre and F1 is up to over 6%. Additionally, the effectiveness of the initial optimal set extends to other classifiers, yielding accuracy rates of over 98% and F1 scores approaching 99%. Besides that, the performance of other classifiers when using the PSO-based method is also better than with about 13% larger in Pre metric in AB, XG, and BG. This result indicates that the PSO-based method is more appropriate and effective for developing IDS based on the IoT-23 dataset for practical IoT environments.

In addition, for a comprehensive assessment of this layer's performance, we compare the best results achieved with previous studies focusing on binary classifications. Consequently, results of the optimal feature set received from the PSO-based method of the proposed IDS maintain superior performance, surpassing previous research by over 1% in both accuracy and F1 scores in identifying network attacks.

IV. CONCLUSION

In this paper, this study presents a systematic approach for enhancing the performance of IDS on the IoT-23 dataset. Two feature selection methods, namely PSO-based and sequential forward-based, are utilized to extract important features, thereby improving classification accuracy while reducing model complexity. The effectiveness of these methods is validated through the implementation of various ML classifiers and 5-fold CV to mitigate overfitting. Additionally, a comparative analysis of the performance of optimal feature sets derived from each selection method aids in identifying the most suitable approach for the IoT-23 dataset. As a result, the PSO-based approach is demonstrated as the most appropriate method for feature selection method. The achieved results prove the prospect of tackling security problems in practical IoT environments.

REFERENCES

[1] Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. Available at:
https://www.statista.com/statistics/1183457/iotconnected-devicesworldwide/

[2] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti and T. -H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," IEEE Access, vol. 10, pp. 121173-121192, 2022, doi: 10.1109/ACCESS.2022.3220622.

[3] Y. Yu, J. Long, and Z. Cai, "Network intrusion detection through
stacking dilated convolutional autoencoders," Security and Communication Networks, vol. 2017, pp. 1–10, 2017, doi: 10.1155/2017/4184196.

[4] Yasar Shahid Hussain, "Network Intrusion Detection for Distributed Denial-of-Service (DDoS) Attacks using Machine Learning Classification Techniques," (2020).

[5] Ankit Thakkar, and Ritika Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," Artificial Intelligence Review 55.1 (2022): 453-563.

[6] Zhou, Yuyang, et al. "Building an efficient intrusion detection system based on feature selection and ensemble classifier," Computer networks 174 (2020): 107247.

[7] Halim, Zahid, et al. "An effective genetic algorithm-based feature selection method for intrusion detection systems." Computers & Security 110 (2021): 102448.

[8] Sebastian Garcia, Agustin Parmisano, and Maria Jose Erquiaga, "IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0)." [Data set]. Zenodo. http://doi.org/10.5281/zenodo.4743746

[9] Pham, Van Thinh, Hoang Long Nguyen, Hai-Chau Le, and Minh Tuan Nguyen. "Machine Learning-based Intrusion Detection System for DDoS Attack in the Internet of Things." 2023 International Conference on System Science and Engineering (ICSSE). IEEE, 2023.

[10] Sajun N. Abdalgawad, Y. Kaddoura, I. A. Zualkernan, and F. Aloul, "Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset." IEEE Access, 10, pp. 6430-6441, 2022, doi: 10.1109/ACCESS.2021.3140015.

[11] Cha Zhang, and Yunqian Ma, eds, "Ensemble machine learning: methods and applications," Springer Science & Business Media, 2012.

[12] Federico Marini, and Beata Walczak, "Particle swarm optimization (PSO). A tutorial," Chemometrics and Intelligent Laboratory Systems 149 (2015): 153-165.

[13] Van Thinh Pham, H. L. Nguyen, Hai-Chau Le, and M.T. Nguyen, "Machine Learning-based Intrusion Detection System for DDoS Attack in the Internet of Things," 2023 International Conference on System Science and Engineering (ICSSE), Ho Chi Minh, Vietnam, 2023, pp. 375-380, doi: 10.1109/ICSSE58758.2023.10227227.

[14] Vibekananda Dutta, Michał Choraś, Marek Pawlicki, and Rafał Kozik, "A deep learning ensemble for network anomaly and cyber-attack detection," Sensors 20.16 (2020): p. 4583.

[15] Imtiaz Ullah, and Qusay H. Mahmoud, "Design and development of RNN anomaly detection model for IoT networks," IEEE Access 10 (2022): 62722-62750.

HỆ THỐNG PHÁT HIỆN XÂM NHẬP IoT TẬN DỤNG LỰA CHỌN ĐẶC TRƯNG CHUYỂN TIẾP TUẦN TỰ VÀ DỰA TRÊN PSO

Tóm tắt: Công nghệ Internet of Things (IoT) đóng vai trò quan trọng với ứng dụng rộng rãi trong nhiều lĩnh vực khác nhau. Tuy nhiên, tính bền vững của IoT bị hạn chế bởi một số thách thức và các vấn đề liên quan đến bảo mật là nguy hiểm nhất. Do đó, trong công việc này, khả năng của hai phương pháp lựa chọn đặc tính riêng biệt bao gồm các phương pháp dựa trên Tối ưu hóa bầy đàn và dựa trên tuần tự được tận dụng và so sánh để tìm ra kỹ thuật trích xuất tính năng phù hợp nhất và bộ đặc tính có giá trị nhất của IoT -23 tập dữ liệu để xây dựng hệ thống phát hiện xâm nhập hiệu quả được xác thực bằng nhiều thuật toán học

máy. Triển vọng giải quyết vấn đề trong môi trường thực tế được thể hiện qua kết quả đạt được.

Từ khoá: Internet vạn vật, hệ thống phát hiện xâm nhập, học máy, tối ưu hóa bầy đàn, lựa chọn đặc trưng chuyển tiếp tuần tự.

Van Thinh Pham is currently a B.E. student in Electronics and Telecommunications Engineering of Posts and Telecommunications Institute of Technology (PTIT) of Vietnam. His research interests include machine learning, deep learning and network security.

Huu Cam Nguyen received the B.E degree from Hanoi University in 2013, and the M.E of Information System Design of University of Central Lancashire, United Kingdom in 2016. He joined the Research Institute of Posts and Telecommunications in Vietnam. He is currently a lecturer in Telecommunications Faculty at PTIT. His research interests include Machine Learning, Bioinformatics and Information System Design.

Hai-Chau Le received the B.E. degree in Electronics and Telecommunications Engineering from Posts and Telecommunications Institute of Technology (PTIT) of Vietnam in 2003, and the M.Eng. and D.Eng. degrees in Electrical Engineering and Computer Science from Nagoya University of Japan in 2009 and 2012, respectively. From 2012 to 2015, he was a researcher in Nagoya University of Japan and in University of California, Davis, USA. He is currently a lecturer in Telecommunications Faculty at PTIT. His research interests include optical technologies, network design and optimization, and future network technologies. He is an IEEE member.

Chien Trinh Nguyen received the B.E degree from the University of Electro-Communications, Odessa, Ukraine in 1989, and the M.E. and Ph.D. degrees in 1999 and 2005 from the University of Electrical and Information Engineering, Tokyo, Japan. He joined the Research Institute of Posts and Telecommunications in Vietnam in 1990. He is currently Vice Dean of the Faculty of Telecommunications, Posts and Telecommunications Institute of Technology. Fields of interest include Next Generation Networks, QoS Assurance, QoS routing, traffic engineering, SDN, and Wireless Sensor Networks.