Evolving Neural Network Intrusion Detection System for MCPS

Nishat Mowla*, Inshil Doh**, KiJoon Chae*

*Department of Computer Science and Engineering

**Department of Cyber Security

Ewha Womans University, 52, Ewhayeodae-gil, Seodaemun-gu, Seoul, 120750, Korea

nishat.i.mowla@gmail.com, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

***Abstract*— Medical Cyber Physical Systems (MCPS) are some of the most promising next generation technologies so far. Like many other systems connected to a wider network such as internet, MCPS are also vulnerable to various forms of network attacks. For detecting such diverse forms of attack, we need smart and efficient mechanisms. Human intelligence is good enough to track such attacks but when it is a huge number of traffic it is no more a feasible process to detect them manually as it is time consuming and computationally intensive. Machine learning techniques embracing artificial intelligence are emerging as powerful tools to detect abnormalities in the network data. Supervised Neural Networks are some of the most efficient techniques to perform such classification. In this paper, we propose an evolving neural network technique that evolves based on classification, elimination and prioritization while focusing on time, space and accuracy to efficiently classify the four major types of network attack traffic found in an effectively pruned KDD dataset. We also show a leap of performance with hyper-parameter optimization which highly enhances the benefit of our proposed mechanism. Finally, the new performance gain is compared with a boosted Decision Tree. We believe our proposed mechanism can be adopted to new forms of attack categories and sub-categories.**

***Keyword*— MCPS, Machine Learning, Neural Networks, Intrusion Detection System**

I. INTRODUCTION

THIS is an era of various body worn devices that can record multiple physiological signals, such as ECG and heart rate or even more sophisticated devices that measure physiological markers such as body temperature, skin resistance, gait, posture, and EMG. Medical Cyber Physical Systems are the much-promised technologies which aim at providing remote healthcare to patients using the sensor information collected from such body worn devices [14]. With great prospect come great responsibilities. The data collected from these devices can be stored in a public or private cloud to be later analysed by the hospital authorities. Therefore, assuring the accessibility of the personal health information during the transmission from the sensory networks to the cloud and from the cloud to doctors' mobile devices will necessitate the design of an intelligent malicious traffic detection system which would prevent normal traffic from getting the proper connection [15].

Machine learning classification techniques are popular when it comes to the issue of classifying normal from abnormal. Among them recently deep learning techniques such as Neural Network are shown to act as powerful tools in order to classify various forms of network attack exploits.

In this paper, we propose an evolving neural network based intrusion detection system for detecting the four key major forms of network attack types by evolving the multi-class data to a 2-class problem following classification based data pruning and class prioritization.

We discuss some of the related works in sections II. In section III we discuss our proposed mechanism. Section IV shows our performance evaluation results followed by a discussion of our proposed mechanism in section V. Finally, section VI concludes our paper.

II. RELATED WORKS

A. Intrusion Detection

Intrusion Detection Expert System was first proposed by Dorothy E. Denning [1]. It had a rule-based expert system to detect known types of intrusions with a statistical anomaly detection component based on profiles of users, host systems and the target systems. Later, a new version called Next-Generation Intrusion Detection Expert System was developed [2].

The idea of using anomaly detection came into mainstream with DARPA Intrusion Detection Evaluation in information security released in 1998 and 1999 in conjunction with the MIT [3]. However, it was shown that the DARPA datasets are not appropriate to simulate real network systems [4] initiating the need for development of new datasets for developing IDS.

Manuscript received on Mar. 21, 2017. This work is sponsored by Basic Science Research Program through the National Research Foundation of Korea(NRF) grant funded by the Korea government (MSIP), and a follow-up of the invited journal to the accepted & presented paper of the 19th International Conference on Advanced Communication Technology (ICACT2017), and Grant ID is 2016R1A2B4015899. Kijoon Chae is the corresponding author.

Chae. Kijoon. Author is with Ewha Womans University, Seoul, 120750 Korea (corresponding author to provide phone: +82-10-3726-6157; e-mail: kjchae@ ewha.ac.kr).

Mowla Nishat. Author, is with Ewha Womans University, Seoul, 120750 Korea. (e-mail: nishat.i.mowla@gmail.com).

Doh Inshil. Author is with Ewha Womans University, Seoul, 120750 Korea. (e-mail: isdoh1@ewha.ac.kr).

B. Machine Learning Techniques for IDS

Various forms of existing machine learning techniques are used for developing IDS. [5] and [6] discusses a survey of these techniques. Among them one of the most promising techniques called the neural network consists of a collection of actions to transform a set of inputs to a set of searched outputs through a set of simple processing units, or nodes and connections between them. There are schemes for both supervised and unsupervised learning techniques such as multi-layer perceptron [7] and self-organizing maps [8] respectively. Neural networks are ideal when we consider all the various forms of network attack traffic that we can experience based on the misuse detection model and the anomaly detection model [9]. Neural networks have also been ideally combined with clustering techniques to achieve promising performance [18]. Different existing dataset are used to evaluate the performance of IDS using neural networks in many research works [10].

C. Modern IDS

Modern IDS have difficulty in dealing with high speed network traffic while attackers can utilize that to hide their exploits by IDS overloading with irrelevant information while executing an attack [11]. A memory efficient multiple character-approaching architecture suited for ASIC implementations was proposed in [12]. The focus mainly went into memory management which could reduce the accuracy. Therefore, to manage higher traffic throughput and increasing link speed hardware accelerators were used to create various forms of NIDS. [13] depicts that while working with a huge number of data, a two-class problem is always more accurate than multi-class problem. In our approach, we try to combine lessons from all the related works and develop a more accurate mechanism that also considers space and time efficiency as will be discussed in the next section.

III. Proposed Mechanism

There is always a trade-off between time, space and accuracy while designing an efficient Intrusion Detection System. When we increase the number of classes to be distinguished, the accuracy of the machine learning model decreases while the IDS becomes slow. Again, when we decrease the number of attributes, the accuracy of the system goes down while the IDS work faster. Reducing the number of attributes is not always a good idea since various forms of attacks can only be classified when we have an abundant number of attributes to distinguish them from others. Considering all these aspects, we try to create a mechanism which is not only accurate but also considers space and time efficiency. Therefore, to overcome the various penalties to the techniques due to huge data handling, we utilize the benefit of a two-class problem since it is time efficient and enhances accuracy as we will also discuss later. As we go down the process, we also try to make it space efficient by a logical elimination process. This step allows us to make our system more space efficient. However, we also make sure all the classes come in the process of classification step by step while we try to maintain a 2-class problem. The approach is to start with the two basic classes namely normal and attack classes. Once the data are identified not to belong to the normal class we eliminate the normal class instances and re-construct a two-class problem from the later class by taking one class of attack as our prioritized attack and the other class as other attack type class. If the data are not identified to be our prioritized attack type, then the instances for this attack class are removed and a new two class problem is constructed by following the same prioritization procedure as shown in Fig. 1

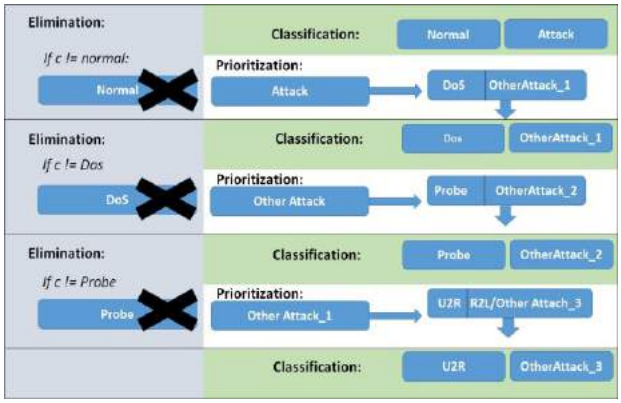

Fig. 1. Evolving ANN based 2-class IDS mechanism.

Fig. 1 shows our evolved ANN mechanism working with these the three major steps of classification, elimination and prioritization. We prioritize the attacks as DoS, Probe, U2R and R2L respectively. Our mechanism in the form of an algorithm for the four major types of network attack traffic in shown in Fig. 2.

Algorithm 1 Evolving ANN Intrusion Detection System

```
class =sum of 2 or more classes;
normal = 1;
attack =0;
run classification test;
i = 1;
if c == 0 && class ==TRUE then
    eliminate normal instances;
    dos = 1;
    other_attack_i = 0;
    if c == 0 && class ==TRUE then
        eliminate DoS instances;
        probe =1;
        other_attack_i+1 =0;
        if c == 0 && class==TRUE then
            eliminate probe instances;
            U2R =1;
            R2L/other_attack_i+2 =0;
            if c == 0 && class ==TRUE then
                traffic is R2L;
            else
                traffic is U2R;
        else
            traffic is probe;
    else
        traffic is DoS;
else
    traffic is normal;
```

Fig. 2. Evolving ANN Intrusion Detection System Algorithm for current four major network attack types.

Neural Networks classify with feature inputs by training a network formed with weights to derive higher level features that can be classified by a non-linear activation function. As shown in the Fig 3, x_i are the feature vectors input to the ANN system. In our case, we used 41 features provided by the KDD dataset [17]. u_j and u_k are the hidden layers which are also

called the intermediary output layers. u_l is the final output layer which helps us to identify the classes. w_{ij}, w_{jk} and w_{kl} are the weight from x_i to u_j, u_j to u_k and u_k to u_l respectively. Finally, a sigmoidal function is used at the outer layer to classify the input to an output class. Fig 3 shows the basic workflow of our ANN (Artificial Neural Network) based 2-class IDS mechanism in general.

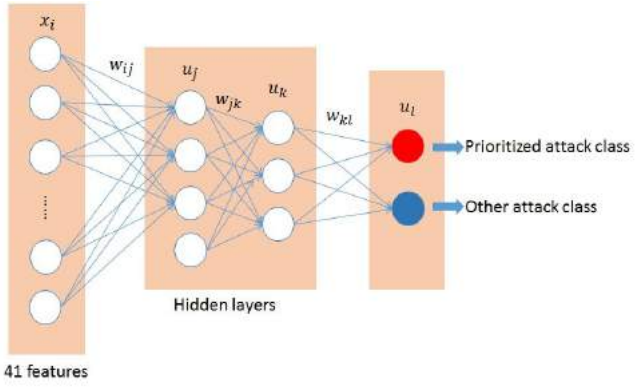

Fig. 3. ANN based 2-class IDS mechanism.

Currently there are 4 major types of network attack traffic namely DoS, Probe, R2L and U2R. Among them DoS refers to all the network traffic flooding attack types. Relevant features include source bytes, packet rates etc. Probe attacks are attacks conducted by sending meaningless packets in order to gain knowledge about the network. They are often detected by features such as duration of connection or source bytes. R2L refers to remote access attacks where the attacker tries to gain access to a remote system. Relevant features include duration of connections, service requested or failed log-in attempts. U2R is the type of attack in which the attacker tries to log-in to a normal account and then gain root administrator access. They are often identified by features such as number of files created or number of shell prompts invoked [16]. On these 4 classes of attack traffic and 1 class of normal traffic, we apply our evolving mechanism which, as discussed before, can be summarized to follow three major steps discussed below.

Classification

Our classification follows the ANN model of Multi-Layer Perceptron (MLP) working on a 2-class problem. Initially a normal class and an attack class are taken as the 2-classes.

Elimination

After a successful classification, the class with the lowest possibility is eliminated to effectively prune the analysed network traffic and a new 2-class problem is constructed from the later class.

Prioritization

In this step, a class with higher priority to be analysed is taken as the first form of class while making the other class as other attack class.

Our proposed mechanism is further optimized with hyper-parameter optimization with learning rate different datasets behave differently in different learning rates. Finally, we compare our performance gain with a highly-optimized Decision Tree algorithm.

IV. Performance Evaluation

We used all 41 features of KDD99 dataset [17] and evaluated the training time and detection accuracy for different attack types. We use a total of 1200 data instances from all the four different kinds of network attack traffic along with normal network traffic. We also took samples from all the subclasses of the 4 major types of network attack traffic. Table 1 shows all the sub-types of the 4-major network attack traffic that we used in our simulation [16]. In our first experiment, we show how the training time decreases as we decrease the number of classes from n to 2. Fig. 4 illustrates that as we decrease the number of classes, the number of training time also decreases significantly.

TABLE I
Network Attack Traffic

Attack Class	Attack Types
DoS	Back, Land, Neptune, Pod, Smurf, Teardrop
Probe	Satan, Ipsweep, Nmap, Portsweep
R2L	Guess_Password, Ftp_write, Imap, Phf, Warezmaster
U2R	Loadmodule

The four network intrusion traffic classes which are further sub-classified by KDD99 to accumulate samples from all the existing attack categories belonging to these four main classes of network attacks.

Fig. 4. Change in training time as the number of classes are decreased.

The above figure also depicts that if we have a huge number of classes reducing the sub-types to higher level types can effectively make the system faster. Next, we show how the time reduces as we use an evolved neural network.

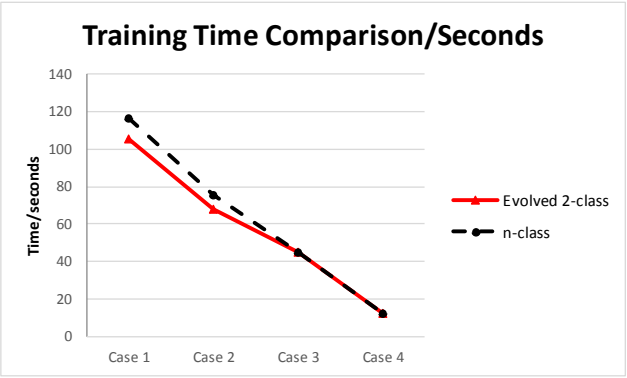

Fig. 5. Training time comparison between n-class and evolved 2-class.

Fig. 5 shows the comparison between the linear class reduction in neural network and an evolved neural network

class reduction performance. Here case 1 is all the 5 classes included (Normal, DoS, Probe, R2L, U2R), case 2 is all the 4 classes included (DoS, Probe, R2L, U2R), case 3 is all the 3 classes included (Probe, R2L, U2R) and class 4 is the 2 classes included (R2L and U2R). In case of our evolved 2-class mechanism case 1 means Normal and Attack class, case 2 means DoS and other attack class, case 3 means Probe and other attack class, case 4 means R2L and U2R class. As can be seen from the following figure our evolved 2-class mechanism is more time efficient than the normal n-class mechanisms and the difference of time efficiency tends to be higher as we increase the initial total number of classes in case 1.

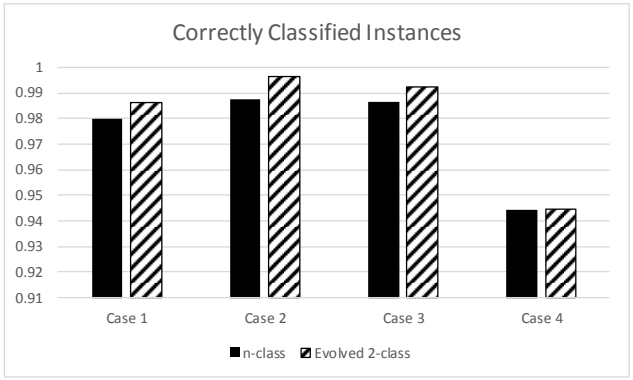

Fig. 6. Correctly classified instances.

Fig. 6 shows the correct classification results of our evolved neural network 2-class model versus the normal n-class neural network classification. As can be seen from the above figure our evolved 2-class model has higher correct classification in all the 4 cases of network attack traffic analysis. Since we have four major network attack traffic categories our model has only 4 cases. We believe our proposed mechanism can scale to other types of attacks with a higher number of classifications.

In the next experiment, we vary the learning rate from 0.1 to 0.0001 and observe the performance gain with a varied learning rate for our evolved neural network. Fig. 7, Fig 8, Fig 9 and Fig 10 shows the performance with varied learning rate for normal vs attack, DoS vs other attack, Probe vs other attack, and R2L vs U2R.

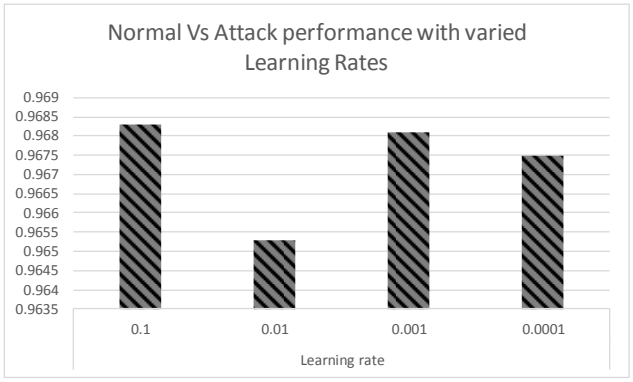

Fig. 7. Performance gain of normal vs attack with varied learning rates.

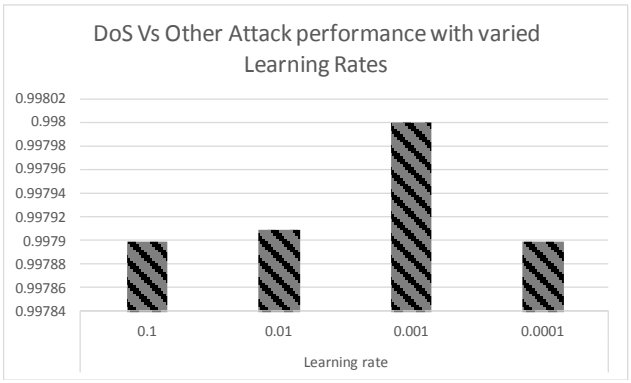

Fig. 8. Performance gain of DoS vs other attack with varied learning

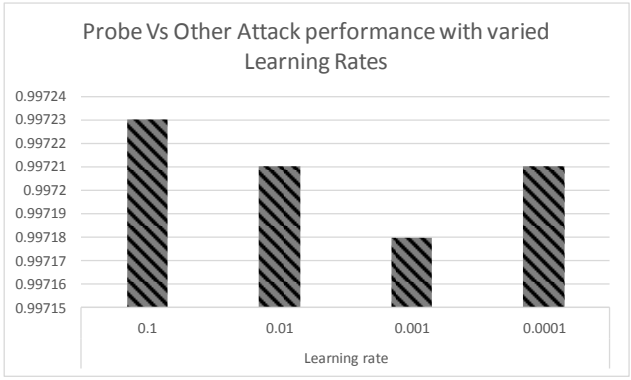

Fig. 9. Performance gain of Probe Vs other attack with varied learning rates.

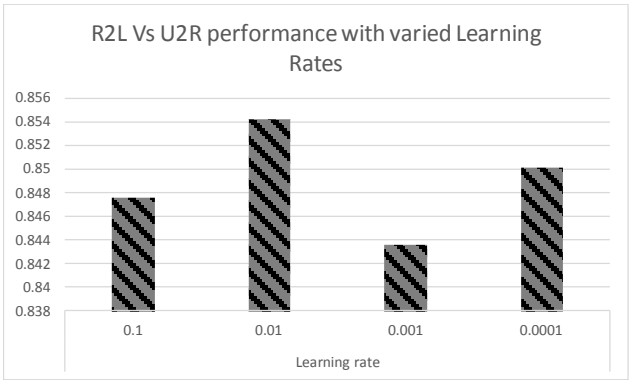

Fig. 10. Performance gain of R2L vs U2R with varied learning rates.

As can be seen from the above figure, the evolved two-class normal vs attack, DoS vs other attack, Probe vs other attack and R2L vs U2R achieves the highest performance with a learning rate of 0.1, 0.001, 0.1, and 0.01 respectively. Therefore, we use these optimized hyper-parameter values and compare the optimized evolving neural networks with a boosted Decision Tree. Fig. 11 shows the performance of the above four cases named case 1, case 2, case 3, and case 4.

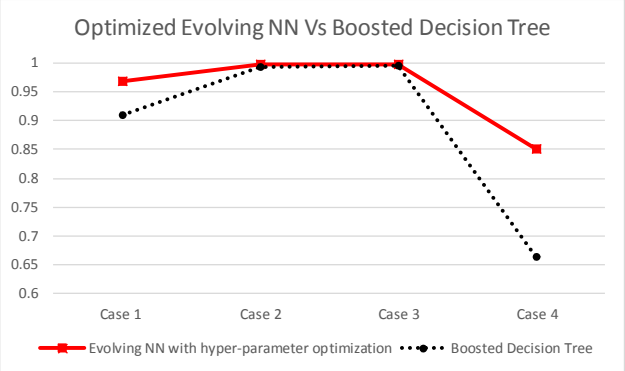

Fig. 11. Performance of hyper-parameter optimized Evolving Neural Network compared with boosted Decision Tree.

The above figure depicts that our evolved neural network with optimized hyper-parameters can outperform the state of the art Boosted Decision Tree. The performance is promising and it depicts that simpler neural networks can be optimized with techniques such as pairwise learning and hyper-parameter optimization to achieve similar and higher performance than more computationally intensive efficient machine learning algorithms.

V. Discussion

The performance gain of this paper is credited to the fact that as we decrease the number of classes in concern we make the classification borderline simpler. Thus, the classifier's complexity is reduced which can be evolved every time to create a two-class problem and solved pairwise to find the specific class in concern. The reduction in complexity is also contributing to the time efficiency of our mechanism. Besides the elimination process to create a new two-class problem allows us to make the problem space smaller and thus saving space.

Finally, the combination of evolved pairwise learning with hyperparameter optimization creates an ultimate leap of performance while reducing the complexity and making the problem space smaller but robust. The idea, thus, achieves a unique combination of high performance, speed with efficient space consumption.

VI. Conclusion

In this paper, we have proposed an Intrusion Detection System inspired by evolving neural network classification technique in order to detect the key 4 different types of attack traffic that can occur in a Medical Cyber Physical System network. We have shown that our proposed mechanism enhances the performance of the traditional supervised multilayer perceptron neural network. With certain hyper-parameter optimization, our mechanism can also achieve promising performance. With optimized hyper-parameters, our mechanism can outperform state-of-the-art algorithms such as boosted Decision Tree. Our mechanism, however, doesn't have a standardized mechanism for attack prioritization yet. Therefore, in future work we hope to identify and develop techniques to prioritize the attack traffic class based on attack prediction mechanisms. Also, we will consider other attack classes and evolving mechanism with clustered neural network.

Acknowledgment

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2016R1A2B4015899). Kijoon Chae is the corresponding author.

References

[1] D. E. Denning, "An Intrusion-Detection Model," *IEEE Symposium on Security and Privacy*, 1986, pp. 118–131.
[2] D. Anderson, T. Frivold, and A. Valdes, "Next generation Intrusion Detection Expert System (NIDES): A summary," *SRI Int.*, no. May 1995, p. 47, 1995.
[3] M. Lincoln Laboratory, "DARPA Intrusion Detection Data Sets." [Online]. Available: https://www.ll.mit.edu/ideval/data/. [Accessed: 07- Apr-2016].
[4] J. McHugh, "Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory," *ACM Trans. Inf. Syst. Security*, vol. 3, no. 4, pp. 262–294, 2000.
[5] J. Singh and M. J. Nene, "A Survey on Machine Learning Techniques for Intrusion Detection Systems," *Int. J. Adv. Res. Computer Communication Eng.*, vol. 2, no. 11, pp. 4349–4355, 2013.
[6] S. K. Wagh, "Survey on Intrusion Detection System using Machine Learning Techniques," *Int. J. Computer Appl.*, vol. 78, no. 16, pp. 30–37, 2013.
[7] C. Qiu, J. Shan, B. Polytechnic, and B. Shandong, "Research on Intrusion Detection Algorithm Based on BP Neural Network," *Int. J. Security and its Applications*, vol. 9, no. 4, pp. 247–258, 2015.
[8] L. Vokorokos, A. Baláž, and M. Chovanec, "Intrusion detection system using self-organizing map," *Informatica*, vol. 6, no. 1, pp. 1–6, 2006.
[9] J.-P. Planquart, "Application of Neural Networks to Intrusion Detection," 2001.
[10] S. K. Sahu, S. Sarangi, and S. K. Jena, "A detail analysis on intrusion detection datasets," Souvenir 2014 IEEE Int. Adv. Computer Conf. IACC 2014, pp. 1348– 1353, 2014.
[11] V. Paxson, "Bro: a system for detecting network intruders in real-time," *Computer Networks*, vol. 31, no. 23–24, pp. 2435–2463, 1999.
[12] H. Lu, K. Zheng, B. Liu, X. Zhang, and Y. Liu, "A memory-efficient parallel string matching architecture for high-speed intrusion detection," *IEEE J. Sel. Areas Communication*, vol. 24, no. 10, pp. 1793–1803, 2006.
[13] L. Dhanabal and S. P. Shantharajah, "A Study on NSLKDD Dataset for Intrusion Detection System Based on Classification Algorithms," *Int. J. Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 446–452, 2015.
[14] M. Alam, S. Abedin, M. Ameen and C. Hong, "Web of Objects Based Ambient Assisted Living Framework for Emergency Psychiatric State Prediction," *Sensors*, Vol. 16, No. 9, September 2016.
[15] O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging Security Mechanisms for Medical Cyber Physical Systems", *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, Vo. 13, No. 3, June 2016.
[16] S. Potluri, C. Diedrich, "Accelerated deep neural networks for enhanced Intrusion Detection System", 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1-8, September 2016.
[17] KDD 99 dataset, http://tunedit.org/repo/KDD_Cup/KDDCup99.arff
[18] W. Gang, H. Jinxing, M. Jian, H. Lihua. "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering." *Expert Systems with Applications*, Vol. 37, No. 9, pp. 6225-6232, 2010.

Nishat Mowla received the B.S degree in Computer Science from Asian University for Women, Chittagong, Bangladesh in 2013, an M.S. degree in Computer Science and Engineering from Ewha Womans University, Seoul, Korea in 2016. She is currently a PhD student at Ewha Womans University, Seoul, Korea. Her research interests include next generation network security, IoT

network security and network traffic analysis.

Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. Her research interests include wireless network, sensor network security, and M2M network security.

Prof. Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984, and a Ph.D. degree in electrical and computer engineering from North Carolina State University in 1990. He is currently a professor in Department of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests include sensor network, smart grid, CDN, SDN and IoT, network protocol design and performance evaluation.