Microprocessors and Microsystems 80 (2021) 103637

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Service Attack Improvement in Wireless Sensor Network Based on Machine Learning

Dongxian Yu [1,*], Jiatao Kang [2], Junlei Dong [1]

[1] College of Information and Engineering, Henan Polytechnic, Zhengzhou, Henan, 450046, China
[2] Department of Architectural Engineering, Henan College of Transportation, Zhengzhou, Henan, 450015, China

ARTICLE INFO

Keywords:
Wireless sensor networks
security services
refuse neural network
support vector machine

ABSTRACT

A plurality of sensors in a wireless sensor network (W.S.N.) is a physical parameter node that allows detection sensor nodes to interact. Security is an essential issue in wireless sensor networks of many practical applications. Our goal is to launch denial of service attacks and respond to wireless sensor networks to enhance security by detecting the enemy. Different kinds of different layers in the occurrence WSN. These two types of machine learning techniques, neural network (NN), detect a Support Vector Machine (SVM), a media access control (MAC.) layer attacks. I have to compare the two methods. It has an access channel wireless sensor node, MAC. Protective layer is essential. Use scenario probability WSN. Wireless network simulator, Vanderbilt plow error simulation.

1. Introduction

A sensor is a physical article or an assortment of data about a function that happened, sending most sensors for gathering the information remotely to a preparing station. When these sensors are hugely composed of observing the physical climate, they structure a W.S.N. Remote sensor networks speak to a wide assortment of security issues that must be tended. We should consider one of a kind of difficulties. For instance, energy is the primary consideration related to W.S.N. W.S.N. Hubs sensor by a battery or sun oriented force. These are restricted in the information stockpiling asset, processing force and correspondence transfer speed terms.

Subsequently, asset obliged sensor hubs must be determined, the correspondence produced capacity prerequisites, and upgraded security procedures to meet. Those sensors' middle purpose control network limitations and assets of the organization elements it is unfeasible in. To do this, to locate a conveyed security arrangement. Numerous remote sensor networks are left unattended because they are far off and removed work. It is hard to persistently screen and forestalls assault sensor hubs.

Remote sensor networks in an assortment of utilizations, including debacle alleviation activities, biodiversity planning, hardware observing, accuracy agribusiness, industry, apparatus and clinical use. They are defenseless against other assaults. Guarantee application security, for example, remote sensor networks, is fundamental. This article utilizes two A.I. strategies to recognize and counter the foe to dispatch DoS assaults, improving remote sensor organizations' security: NN. and SVM. NN. is an incredible asset for information investigation. When the significant boundary is reflected in the security level of the W.S.N. is gotten, which is given as the informational information collection to the multilayer perceptron.

Back-proliferation (BP) is utilizing the MLP. Preparing calculation. B. P. calculation to limit the yield determined by the all-out square blunder NN. Preparing and the utilization, which is acquired by executing the option to make a foreordained load on every hub. To give a protected elective technique is improved, trade upholds vector machines and neural organizations. SVM depends on the factual learning hypothesis. It is utilized due to its capacity to deal with high dimensional exactness and information, discover more data in the second from last quarter to reinforce NN. and SVM's security. The reproduction results show that the two strategies and execution investigation WSN. security upgrades showed in the final quarter. At last, ends and future work by the fifth part.

With the advancement of the improvement of remote interchanges, portrayed in that the intelligent miniature electrical frameworks, microelectronics, signal preparing, organizations and different advances,

Conflict of interest statementWe declare that we have no conflict of interest.

* Corresponding author: Dongxian Yu
E-mail address: henan_ydx12062@126.com (D. Yu).

https://doi.org/10.1016/j.micpro.2020.103637
Received 8 November 2020; Received in revised form 3 December 2020; Accepted 8 December 2020
Available online 11 December 2020

remote sensor organization will show up, remote sensor networks are generally circulated in the field of aviation, guard, military, nature observing, medical care, modern offices. The way into the remote sensor network applications is a nominal size, conveyance observing, and asset obliged sensor hubs to powerfully change the directing and exchanging data of the screen, on the best way to tackle the stream issue in the security or viability of the door of the sensor organization.

An assortment of protective methodologies challenge model, encryption calculation, essential administration, security design and organization interruption identification and reaction model: Here, in a sensor network security research fundamental core interest. It zeroed in on the accompanying viewpoints. A diverse security guard and location strategies can be utilized for various organization layers, and they are reciprocal to one another. This paper considers the remote sensor network interruption discovery framework.

There are numerous new assaults in a remote sensor network is not the same as an ordinary organization. This is to improve the discovery of obscure assaults interruption location framework, and the capacity to choose the proper calculation should be tended. Some great calculations to recognize known assaults, while others are acceptable at identifying obscure assaults. A few calculations appropriate to the organization structure's plane, and various calculations reasonable for progressive organization structure. To choose or plan the proper calculation dependent on network necessities.

2. Related Work

WSN identifies different types of attacks, and Sort by H. K. and A. Wireless sensor networks are susceptible to damage enemy to launch the service they provide DoS attacks. Such attacks can be performed in a different layer of the wireless sensor network. Anthony D Wood [1]. Stankovich investigated occurred in a typical sensor network layer DoS attacks. They provide encryption and authentication mechanism in wireless sensor networks against DoS attacks, causing severe complications due to its resource constraints.

As a fixed sensor network self-organization of the main issues, consider the prevention of DoS attacks recommendations to overcome node recognition errors. Based on the fuzzy logic system [2], M.A.C. Protocols have been proposed to detect DoS attacks. The system uses a method based on neural networks to learn to make decisions and attack definitions of fuzzy interference [3]. This hybrid system to identify some of the attacks solve this problem.

SVM using the radiation basis function neural network for detecting the DoS attack two machine learning techniques. Experiments being carried out to compare the profitability of the two technologies. SVM is considered to be more accurate than the RBF neural network. General neurons (G.N.) as the basis for [4] has been proposed by constantly monitoring reflect the possibility of more attacks will be launched to enhance the security parameters enemy DoS attacks media protocol. PSO training for GN. [5]. The simulation results show the trade-off between the network and a specific selectivity affects the suspicious threshold parameter's life.

Machine learning techniques to detect and initiate an anti-DoS attack by the enemy on the M.A.C. Layer of the wireless sensor network [6]. The sensor nodes detect an attack's definition so that it does not come from where they close. They stop moving until the enemy attack. The first defines the technical specifications and the following monitoring activities within the network, following these specifications.

Propose conveyance dependent on predefined rules. The framework is separated into three phases: performing information assortment rules and interruption discovery. Some framework design observing hub [7]. Those in crossover mode, where the bundle gathers them and identify known assault qualities, perform interruption discovery tasks. High selectivity and appropriation rules watch hubs influence the calculation's presentation, just as watch hub asset utilization [8]. Proposed new group based remote sensor network interruption identification. This technique has been created for the early identification and avoidance of interruption by following a legitimate MAC. Address-based framework to follow the interloper.

The interruption location framework's engineering depends on the sensor, the sensor hubs sent, the interruption discovery framework is planned based bunch head, and the group head conveyed in the plan of an organization level interruption identification framework, the focal arrangement on the worker [9]: use-based cycle, every one of the three sorts of interruption discovery frameworks to recognize an irregularity.

Misuse identification framework to distinguish interruption designs dependent on known assault. Guard strategies might be utilized in a remote sensor organization, contingent upon the accepted [10] spread qualities of remote correspondence hubs are thickly disseminated. Rome. [11] Design of a system for I.D.S. They are applied to small sensor organizations. The design incorporates nearby and worldwide operators. Home specialist dwells on every hub, check the neighborhood information traffic.

A worldwide specialist is available on a portion of the organization's hubs and checks the adjoining hub's information stream. In various leveled network geography [12], bunch head, contact the worldwide operator. The planar geography, design, innovation called unconstrained guard dog, and the base number of worldwide specialists, to guarantee that spread the whole organization [13] are utilized to choose a worldwide operator. This methodology has two downsides. Won't have the option to ensure that the entirety of the hubs being observed because of the worldwide intermediary determination's rough idea. The second is that it doesn't consider the impact of the bundle.

Oddity recognition decides if the created by learning the ordinary activity of the interruption sensor hubs. Irregularity recognition is simpler to use than the identification and detail based discovery of abuse [14]. Consequently, the greater part of the analysts, as interruption identification, and the essential methods for innovation, utilize this technique.

Propose to assault interruption location framework asset exhaustion. Every hub screens parcels' normal appearance pace from the neigh exhausting hubs, so the normal gathering rate and the measurable model [15]. The main closest neighbor's hubs n bundles are utilized for factual investigation. In the event thaIfdinates the accompanying factual model of the neighbours'. Meaneighborsdels are generally basic. It can't specifically distinguish a forward assault, worm assault width [16]. The investigation determined expenses and asset utilization.

Interruption discovery technique for learning automata. This strategy is utilized to test the organization's information parcels to decide if the hub dependent on input from a decent climate is vindictive [17]. They settled on concurrence with a basic low-energy complex recognition. The convention consolidates the idea of learning automata and irregular instrument for executing the example energy touchy interruption location framework.

Rajasegarar, a class that upholds vector machine, is utilized to distinguish unusual organization. Propose dependent on help vector machines, in particular, running hyperelliptic help vector machine, and quarterly ball uphold vector machine in two different ways [18]. Adaptability and the benefit of computational unpredictability boundary determination. Be that as it may, the appropriated remote sensor networks face a few restrictions, since it utilizes an incorporated methodology. Functions admirably in a conveyed climate.

Gunasegaram and Periakaruppan proposed an interruption recognition model dependent on hereditary calculations to comprehend rest disavowal assaults in remote sensor organizations [19]. The model actualizes an adjusted R.S.A. calculation in a base station to produce and disseminate key sets between sensor hubs. Before sending/getting bundles, sensor hubs decide the ideal directing through impromptu on-request separation vector steering and afterward use wellness count to guarantee transfer hubs' dependability. Cross and change activities identify and dissect the techniques which are utilized by aggressors.

The assailant in deciding the hub an impeded message to the base

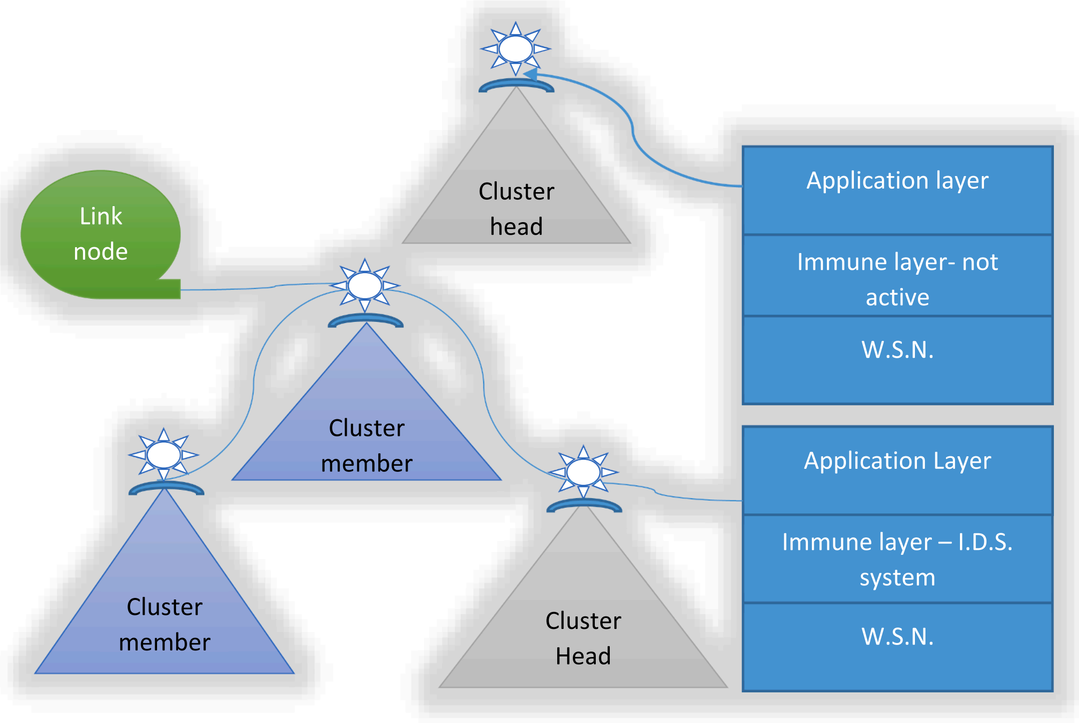


Figure 1. Wireless sensor network General architecture

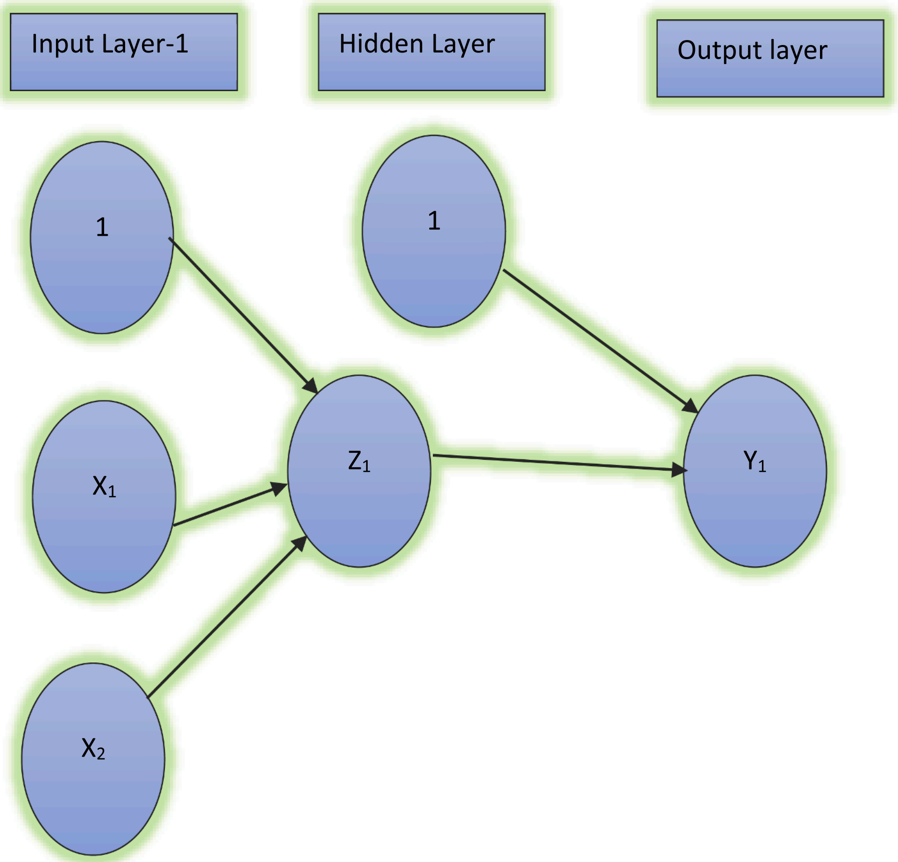


Figure 2. Structure of MLP.

station broadcast organization. Continuous time dependent on Markov chain (CTMC), proposed a state progress model to consider inside assault under the sensor, and spot the assault. The model an inspected epidemiological model and interior assault recognition model the connection and the organizational capacity and security of the equalization of W.S.N. Present status, feasibility, accessibility, and energy utilization. There is a need to evaluate the four components referenced previously.

Chen [24] proposed a distinction between the game mode assailant Intrusion Detection System and the remote sensor organization [20]. The Nash harmony model and accomplish the best insurance and figure the equalization of danger and cost of security arrangements. As it may, models for remote sensor organizations, energy utilization, expenses and correspondence costs application have not yet been given in a re-enactment. Increment in the size of the sensor network when the exhibition debasement of the model.

3. Proposed Methodology

DoS attacks are enemies trying to reduce network services. In a DoS attack, an uncompromising service node malicious node can be provided by request to distract them. The wireless sensor network is a carrier-based collision avoidance mechanism sensitive to multiple access. The source hub has information to communicate on the off chance that it begins the cycle by sending a bundle. This occurred in various layers of the convention stack, various sorts of DoS assaults. Three kinds of M.A.C. Layer DoS assaults incorporate fatigue assaults in crash assaults and caricaturing assaults.

3.1. Collision attack

Sending RTS/CTS bundles, each detecting hub senses the channel to decide if it is occupied or inactive. They convey information just when the channel is inert. There is no contention when sending parcels. In this state, since the adversary assault sensor network bundle crash convergence.

3.2. Unfairness attack

All nodes have the same priority to obtain the same channel. Channel assigned to, based on the first node of the first attempt to provide a way to get the first channel policy. If the waiting time is short or the enemy is not waiting for many data packets to be transmitted in this state. This protects the node from the legitimate use of public channels.

3.3. Exhaustion attack

When the sensor node identification and control packets received control packet control. Since the attacker common node, which node is the node possible legitimate R.T.S., distinguish between a conventional transmissions packets by the attacker, send large amounts of data packets enemy health node identification packet.

Table 1
Critical Parameter Averaged

Probability of Attack	R_r	R_c
0.1	393.9	110.2857
0.2	506.2	124.44
0.3	535.74	135.12
0.4	652.4	163.34
0.5	717.4	177.34
0.6	921.74	220.44
0.7	991.74	239.74
0.8	1056.48	260.64
0.9	1131.34	280.66
1	1190	301.66

3.4. NN Based Approach

M.L.P. is a sort of neural organization utilized. In M.L.P., the feed-forward Nearest Neighbour (NN). Neurons of the multilayer. It implies the last info and yield layers of the primary unit. All different units are called concealed units; they have a shrouded layer. Every neuron is a correspondence interface associated with another neuron. Weight of each communication link with its associated weight. Weight information, rather than a neural network. This function is mathematically equivalent to (1) and is shown in the Figure 1.

$$y = f(x) = \tanh(x) \tag{1}$$

The activation function applied to the output layer is a linear function. This is illustrated in Figure 2. This function is mathematical, equivalent to (2).

$$y = f(x) = x \tag{2}$$

Preparing Algorithm: MLP is prepared to utilize BP calculation. It includes three phases: It includes three phases:

- Feed forward of the information design.
- Calculation and backpropagation of related blunder.
- Adjustment of loads.

During feedforward, each input unit Xi,(i = 1, 2) receives input signal xi and broadcasts it to the remote unit Z1. Z1 aggregates its weighted input signals, as expressed in (3).

$$Z_{in} = v_{01} + \sum_{i=1}^{2} x_i v_{i1} \tag{3}$$

Z_1 applies its activation function to compute its output signal as expressed in (4) and sends this signal to output unit Y_1.

$$z_1 = f(z_{in}) \tag{4}$$

The output unit Y1 sums its weighted input signals, as expressed in (5).

$$y_{in1} w_{01} + z_1 w_{11} \tag{5}$$

Y1 applies its activation function to compute its output signal, as expressed in (6).

$$y_1 = f(y_{in}) \tag{6}$$

During training, the target value of T1 output Y1 and Y1 is determined by their activation close correlation errors. According to this error, the coefficient δ1 is calculated. y_1 Output means for concealing the error backpropagation. Update the weight ratio between the Output and the weight of the intermediate layer. Similarly, the weight between the input layer and the hidden layer is updated by weight. Many times the need to train the neural network to B.P. B.P. is the mathematical basis of the gradient descent algorithm.

4. Result and Discussion

Node to exchange data, important parameters used to observe the scene through the billing W.S.N. 25 is shown in 4 and 1 from the sensor node unique. 25 through the RTS / CTS control method. If two nodes transmit simultaneously, contention occurs, the probability of trials of each node in the received node number per minute is measured as RTS. Packet receiver P. request rate Rr for transmitting packets 0.25 per second. The average number of collisions of the unit of a minute of the R. C. of the collision rate is measured.

By accounting for the W.S.N. 25 to exchange data through the node, view a scene important parameters, shown in Figure. 4 and a unique I.D. of sensor nodes in the graph. 25 via the RTS / CTS control scheme, try each node is transmission collision probability P every 25 seconds at the

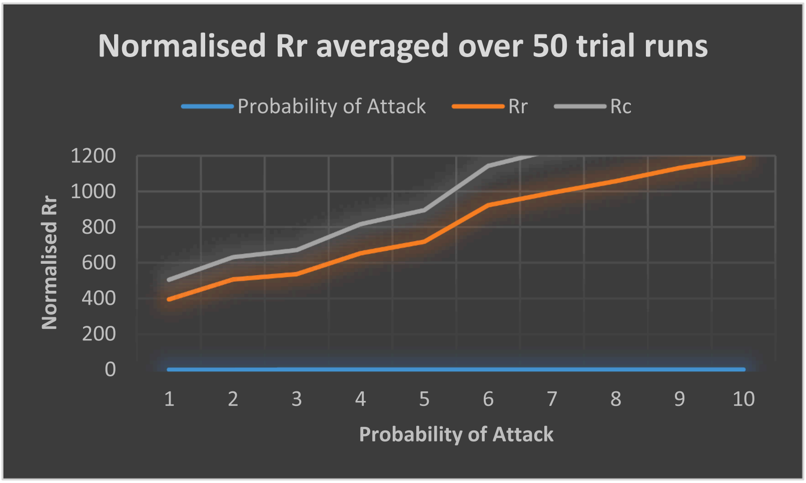


Figure 3. Normalised Rr averaged over 50 trial runs.

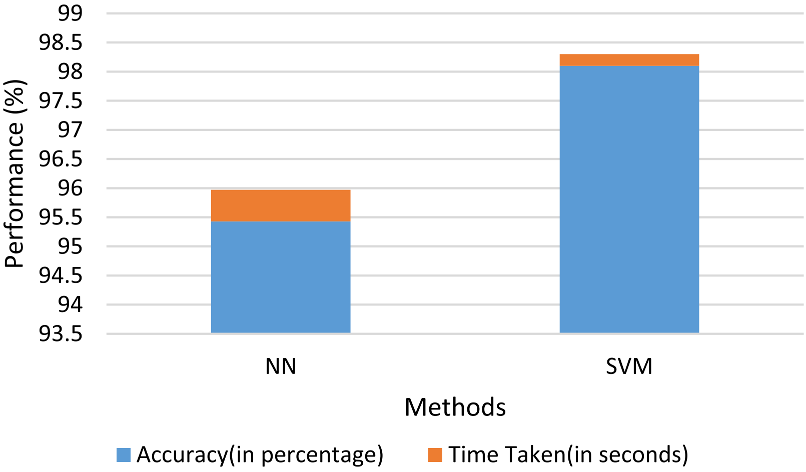


Figure 4. N.N. and SVM based approach for DoS attack detection based on their accuracy and time

TABLE 2
Performance Analysis of N.N. and SVM

Performance Metric	NN	SVM
Accuracy(in percentage)	95.43	98.1
Time Taken(in seconds)	0.54	0.20

receiver if the two nodes send packets simultaneously. The number of nodes per minute is measured as a received request rate Rr is the R.T.S. Packet.

A method of using the neural network-based DoS attacks security. The key parameters in Figures 4 depict the normalized values corresponding to the attack target input probability. The B.P. algorithm trains the M.L.P. M.L.P. to obtain the required target output value matches, which is the possibility of an attack as show you in table 1.

4.1. Security against DoS attack using SVM

High attack, low probability: There are two important parameters normalized. NN method provides training on these values. Every minute, the key parameters' value in two classes, a train NN method program each node. If it detects a possible attack, it will stop working. All nodes detect an attack. This Figure 3 has stopped working. These nodes represent on by a red led. These are marked with circles. If the node does not detect any attacks after the attacks, they are activated and data transmission.

4.2. Performance Analysis

Table 2 shows the DoS attack detection based on SVM-NN and methods, the accuracy and time to produce an output compare. N.N. is accurate 95.43 percent while achieving an SVM 98.1% accuracy rate.

NN0.54 second probability to determine the desired attack, but requires only 0.20 seconds SVM to determine whether the calculated attack sensitive parameters from the sensor node likelihood.

5. Conclusion

Both SVM and neural network machine learning techniques are used to detect DoS attacks. These are just examples, without re-programming. They are based on supervised learning. Using these methods, malicious nodes can prolong the life of the network to save power. NN. is a distributed parallel systems; a linear program can solve the problem can not be solved. SVM training method using kernel-based to find the global minimum. An analysis of the performance between the two techniques can be found SVM DoS attacks can be detected, accuracy 97%, while the N.N. may reach 91% if SVM is more accurate than NN. It will take a longer time than N.N.; the SVM-based method is more like N.N. Rather than detecting DoS attacks.

Declaration of Competing Interest

None.

Acknowledgements

This work was supported by the engineering technology research center of web application software in Zhengzhou.

References

[1] W. Dargie, C. Poellabauer, Fundamentals of Wireless Sensor Networks, Wiley, 2010.

[2] H.K. Kalita, A. Kar, Wireless sensor network security analysis, International Journal of Next-Generation Networks 1 (1) (December 2009).

[3] A. D. Wood & J. A. Stankovic, "Denial of service in sensor networks," IEE JNL, pp. 54–62, October 2002.

[4] F. Hu, N.K. Sharma, Security considerations in ad hoc sensor networks, Ad Hoc Networks 3 (2005) (September 2003) 69–89.

[5] Q. Ren, Q. Liang, Fuzzy logic-optimized secure media access control protocol for wireless sensor networks, in: Proc. IEEE IntemationaI Conference on Computational Intelligence for Homeland Security and Personal Safety, 2005, pp. 37–43.

[6] D.-R. Tsai, W.-P. Tai, C.-F. Chang, A hybrid intelligent intrusion detection system to recognize novel attacks, in: Proc. IEEE 13th Annual International Carnahan Conference on Security Technology, 2003, pp. 428–434.

[7] G.C.Y. Sang, P.P.K. Chan, D.S. Yeung, E.C. Tsang, Denial of service detection by support vector machines and radial-basis function neural network, in: Proc. International Conference on Machine Learning and Cybernetics 7, 2004, pp. 4256–4263.

[8] R.V. Kulkarni, G.K. Venayagamoorthy, A.V. Thakur, S.K. Madria, Generalized neuron based secure media access control protocol for wireless sensor networks, in: Proc. IEEE symposium on Computational intelligence in multi-criteria decision-making, 2009, pp. 16–22.

[9] Q. Ren & Q. Liang, "Secure media access control in wireless sensor networks: intrusion detections and countermeasures," in Proc. 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 4, pp. 3025–3029, 2004.

[10] R.V. Kulkarni, G.K. Venayagamoorthy, Neural network-based secure media access control protocol for wireless sensor networks, in: Proc. International Joint Conference on Neural Networks, June 2009, pp. 13–16.

[11] L. Fausett & Fundamentals of Neural Networks. Prentice-Hall.

[12] K. Soman & R. Loganathan, and V. Ajay, Support Vector Machines and Other Kernel Methods.

[13] T Hemalatha, S. Mithila.T, K.P. Soman, Comparative study of linear and quadratic programming versions of SVM on various real-life data sets, International Journal of Recent Trends in Engineering 1 (2) (May 2009) 23–25.

[14] I. Talzi & S. Schönborn, & C. Tschudin, "Providing data integrity in intermittently connected wireless sensor networks," in 5th International Conference on Networked Sensing Systems, 2008, IEEE, pp. 11–18.

[15] K. Pelechrinis, M. Iliofotou, S.V. Krishnamurthy, Denial of service attacks in wireless networks: The case of jammers, in: Communications Surveys & Tutorials, 13, IEEE, 2011, pp. 245–257.

[16] J. Wheat, R. Hiser, J. Tucker, A. Neely, A. McCullough, Designing a wireless network. Syngress Publishing, 2001.

[17] A.-S. K. Pathan and "Denial of service in wireless sensor networks: issues and challenges, 2010.

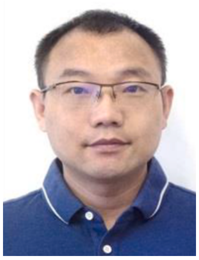
[18] D.R. Raymond, S.F. Midkiff, Denial-of-service in wireless sensor networks: Attacks and defenses, Pervasive Computing, IEEE 7 (1) (2008) 74–81.

[19] P.T. Kalaivaani, Raja Krishnamoorthi, Design and implementation of low power biosignal sensors for wireless body sensing network applications, Microprocessors and Microsystems 79 (2020) 69–79. ISSN 0141-9331.

[20] M. Premkumar, T.V.P. Sundararajan, DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks, Microprocessors and Microsystems 79 (2020), 103278, ISSN 0141-9331.

Dongxian Yu was born in Nanyang, Henan.P.R. China, in 1982. She received her Master degree from Capital Normal University (China). Now, she works in College of Information and Engineering, Henan Polytechnic. Her research interest including computational intelligence, information security and big data analysis.

Jiatao Kang was born in Henan (China), on August, 1984. He received the Master Degree in geotechnical engineering from the Central South University of China in Changsha (China). Now, he works in Henan College of Transportation. His research interests include intelligent building, Virtual reality.



Junlei Dong was born in Zhumadian, Henan.P.R. China, in 1979.He received the Master Degree from Huazhong University of Science and Technology. Now he works in College of Information and Engineering, Henan Polytechnic. His research interest including computational intelligence, information security and big data analysis.