Enhanced Simulating Annealing and SVM for Intrusion Detection System in Wireless Sensor Networks

D Prabakar
Vignan's Foundation for Science Technology and Research
s Gomathi (gomathisam4@gmail.com)
Kongu Engineering College
S Sasikala
Kongu Engineering College
TR Saravanan
SRMIST: SRM Institute of Science and Technology
s Ramesh
Vignan's Foundation for Science Technology and Research

Research Article

Keywords: SA, SVM, WSN, IDS, intrusion detection

Posted Date: March 23rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-193449/v1

Enhanced Simulating Annealing and SVM for Intrusion Detection System in Wireless Sensor Networks

[1]D.Prabakar, [2*]S.Gomathi, [3]S.Sasikala, [4]T R Saravanan, [5]S.Ramesh

Abstract Wireless Sensor Networking (WSN) is among the most recent technologies with uses ranging from medicine to the military. Nevertheless, WSNs are impervious to numerous types of cyber-attacks that could compromise the performance of the entire network, which could lead to fatal problems such as a routing attacks, denial-of-service attack, probe, etc. Key management protocols, secure routing, and authentication protocols cannot offer WSN protections for such kinds of attacks. The intrusion detection scheme is the way to solve the issue. This paper proposes an Enhanced simulated annealing based support vector machine algorithm for intrusion detection. Traditional features selection algorithm simulating annealing takes much time to run. So, to avoid this problem, we have introduced Enhanced simulated annealing. From the performance results, it can be seen that our proposed feature selection method provides better performance results than the existing method.

Keywords: SA, SVM, WSN, IDS, intrusion detection.

D.Prabakar,

Assistant Professor, Department of ECE, Vignan's Foundation for Science, Technology and Research,Andhra Pradesh, India.

Email: prabakarece325@gmail.com

S.Gomathi,

Assistant Professor(SrG), Department of ECE, Kongu Engineering College, Perundurai, Erode, TamilNadu.

Email: gomathisam4@gmail.com

S.Sasikala,

Associate Professor, Department of ECE, Kongu Engineering College, Perundurai, Erode, TamilNadu,

Email: sasikalasece@gmail.com

T R Saravanan,

Assistant Professor,Department of CSE,SRM institute of science and technology ,Kattankulathur ,60320

S.Ramesh,

Associate Professor, Department of ECE,Vignan's Foundation for Science, Technology and Research,Andhra Pradesh, India,

Email: rameshbe9023@gmail.com

1. Introduction

The WSN is a group of simple and cheap sensing devices that are configured with environmental sensors and interact with each other over a wireless radio system.Many WSN applications need a vast number of sensor nodes to run unmonitored.It creates significant utilization and administration issues.Worse still, it is often difficult to reach the deployment region at all, for example in military applications and dangerous areas.Therefore, sensor networks have to become fully independent and show responsiveness and adaptability in live time, without indirect user or admin action, to alterations in evolution[1].

In terms of security risks, this need is much more imperative. An intrusion could be described as a collection of behavior that can contribute to a device being unauthorized to enter or change it. Intrusion detection schemes are entrusted with tracking computer networks, identifying potential network intrusions and notifying consumers to the presence of intrusions, and reorganizing the network if it is[2] possible.

DARPA 1999[3] and KDD CUP 99[4]database records are used for various researches. In this paper NSL KDD 99[5]database used for Intrusion detection system. The overall work flow of suggested work is given in figure 1.Initially features selection is done by proposed enhanced simulated annealing method. In figure 2 the prosed features selection flow was given. After features selection we split the features as train set and test set. Finally, classification is done by Support vector machine (SVM) algorithm.

1.1. Features Selection

Various optimization methods are utilized for the feature selection purposes, such as the genetic algorithm[6][7][8], PSO[9][10][11], GWO[12][13]. For feature selection[14][15], a certain hybrid version of the optimization algorithm was used.

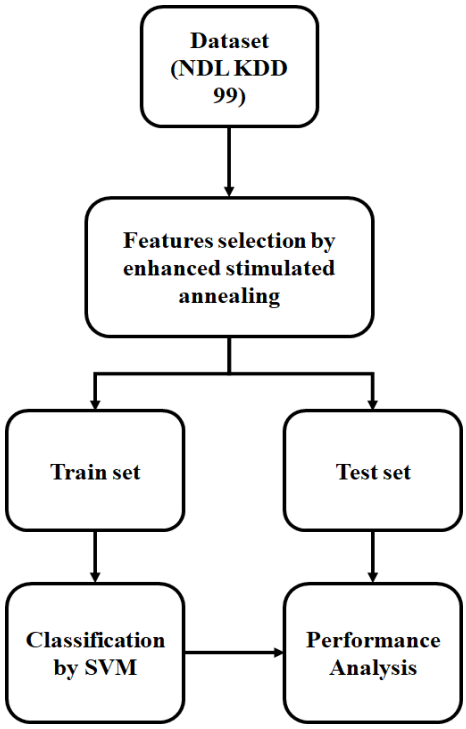

Fig. 1 Overall process of proposed work

In this paper simulated annealing was adopted for feature selection purposes. However traditional simulated annealing very slow to find out the optimal solution. So, it may cause to take much time consumption and less performance. The selection of the initial temperature value affects the performance and

time consumption. So initial temperature value is computed by grey wolf optimization. The best cost value of grey wolf optimization is considered as the initial temperature value of simulated annealing.

1.1.1. Simulated Annealing

Simulated annealing is an efficient and common method for optimization purposes. It helps analyze global optima in the presence of local optima. "Annealing" relates to an analogy of thermodynamics, especially when metals are cold and anneal. It uses the fitness function of the problem of optimization instead of the energy of the object.

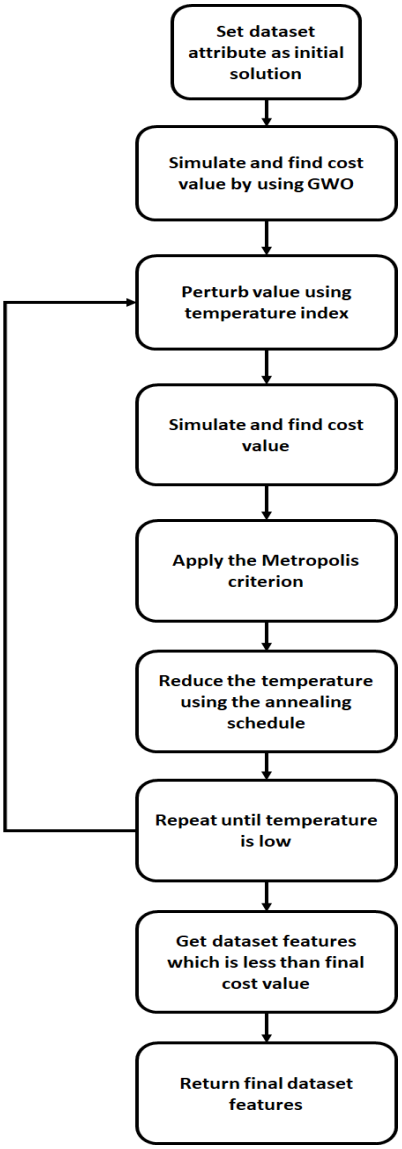

Fig. 2 Proposed Enhanced simulated annealing work flow

Simulated annealing enhances this strategy by introducing two components.The first one is the Metropolis Algorithm[16], which is adopted when serving states to permit the solver to discover the potential locations of solutions that have not been improved.Of that kind "bad" conditions are allowed by the Boltzmann criterion:

$$e^{-\frac{\Delta C}{T_e}} > rand\ [0,1] \quad (1)$$

Where ΔC is the energy change,C represents the cost function, and T_e is the temperature. If T_e is large, several “bad” conditions are recognized, and most of the optimal solution is accessible.The second, by analogy to the annealing of material, is to reduce the temperature again.Afterward visiting several situations and noticing that the fitness function is gradually decreasing, the temperature is lowered and the size of permitted "bad" states is thus limited.Later decreasing the temperature to a minimal rate several times, the process can then be "quench" by embracing only "good" situations to determine a local minimum fitness function.

1.2. Classification

The procedure of grouping things on the basis of features is classification. Here, nodes are categorized as normal and abnormal nodes based on the enhanced simulated annealing features. Numerous machine learning methods is suggested for intrusion detection [17][18][19].Various proposed methods used SVM for classification[20][21][22].

1.2.1. Support vector machine

An SVM is a supervised model of machine learning that utilizes classification techniques for problems with binary classification[23]. They categorize fresh feature after providing an SVM system set of labeled training data with each class.

For several practical issues, it can resolve linear and non-linear issues and perform well.The SVM method's vision is to develop the best decision boundary or line that can differentiate n-dimensional area into class labels so that in the future we can conveniently apply the new feature in the right category. This boundary of the best decision is named a hyperplane.

The extraordinary vectors which help to develop the hyperplane are chosen by SVM. Such extraordinary cases are referred to as support vectors, and the method is therefore referred to as the Support Vector Machine. SVM is classified as two type one is linear SVM and another one is nonlinear SVM.

Linear SVM:

Linear SVM generally handle the two set of features which means group 1 and group 2.Since it is two-dimensional space, we can differentiate these 2 classes conveniently by using a horizontal line. There could be several lines, however, that can differentiate these classes.The SVM method finds the nearest point in both groups of lines. The space between the hyperplane and the vectors is named the margin. And SVM's objective of maximizing this margin.The maximum-margin hyperplane is known as optimal hyperplane[24].

Nonlinear SVM:

If the data is set in a linear manner, it can be segregated using a line, but we could not draw a one line for non-linear data.Two-dimension data are used for linear SVM but in nonlinear SVM need to insert one more dimension to segregate these points[25].

This paper is structured as follows: the related work is described in Section 2; the proposed methodology is provided in Section 3; the experimental results and discussion are presented in Section 4 and the conclusion is reported in Section 5.

2. Related works

Numerous different works has been done on the classification and feature selection for the establishment of Intrusion detection systems by different investigators[26, 27][28][29][30].The PSO based Intrusion detection system algorithm is implemented along with the main component study to determine an intrusion in the WSN [9].The suggested methodology has achieved significant results in terms of false alarm rate and the count of features selected, and besides requires further improvement in terms of accuracy and detection rate. Also, when suggesting this method, the execution time necessary to analyze all threats is completely ignored. Besides,[31] developed a hybrid Intrusion detection system method in the WSN. It gives better accuracy and detection rate, but somehow it neglects the execution time and false alarm rate.To handle the IDS, [32][33][34][35]other optimization techniques can also be reviewed.

Apart from this various improved version of feature selection method were suggested[36][29]. In this paper author proposed an improved binary gray wolf optimizer for feature selection. Three wolves, five wolves and seven wolves were used to identify the best number of wolves. This method significantly increases the processing time compared to [9]. However, that paper, they did not concert on drawback of traditional GWO algorithm. So that work will suffer from slow convergence, low solving precision, and bad local searching skill. So, it will take more time for convergence and also its lead to increase more processing time.

Various machine learning[37][38][39][40], cluster based[29, 41, 42]and deep learning[43][44][45][46]methods were suggested for classification.

3. Proposed Methodology

The keyobjective of this paper is to classify normal and abnormal nodes from given database records. We have utilized NSL-KDD99[5]database for intrusion detection. NSL-KDD 99 database is an freedatabase available online. It has 4,898,431 records, out of which 3,925,650 records are affected records, and the remaining 972,781 records are normal. NSL-KDD 99 database is an enhancedform of the KDD-Cup 99[4]database. Table 1 indicates the attack details of the database.

Denial of service:A DoS attack is a kind of intrusion intended to shut down a network or machine, trying to make it unavailable to its authorized parties[47]**.**

Remote to local: R2L thread has been commonly recognized to be initiated by a hacker to gain illegal admission to a target computer across the network[48]**.**

Probe: It is an attack[49] that is intentionally generated so that in the report its target detects and reports it with an identifiable "fingerprint."

User to root: U2r attack is usually initiated while legitimately accessing a local computer to unlawfully gain the root privileges[48].

3.1 Enhanced Simulated Annealing:

One of the most common heuristic techniques to solve the optimization problem is the SA algorithm [50]. Traditional simulating annealing is very slow to determine the best optimal solution. It leads to taking much time to run. So, to avoid this problem, we have introduced Enhanced simulating annealing.

Algorithm 1: Enhanced simulated annealing

1. Initializing the solution S_{init}[51]

Define the initial T_{init} and final T_{final}temperature

$T \rightarrow T_{init}$ // T_{init} is computed by GWO

2. Creating S_j fromS_{init}

$d_{diff} \rightarrow C(S_j) - C(S_{init})$

3. if $d_{diff} < 0$ then

$S_{init} = S_j$

else if $e^{-\frac{d_{diff}}{T}} > rand\ [0,1]$

$S_{init} = S_j$

end

4. If thermal equilibrium is reached
   Go to step 5

   Else

   Go to step 3
5. If the T_{final} is reached
   End

   Else

   Update T and go to step 2.

6. $Final_{fea} \rightarrow dataset > T$

Table.1 Different type of attacks details of NSL-KDD 99 database

Attack class	Type of attack
Denial-of-Service (DoS)	Back, land, Neptune, Pod, Smurf, Teardrop, Apache2, Udpstorm, Processtable, Worm (10)
Remote to local (R2L)	Guess_password, Ftp_write, Imap, Phf, Multihop, Warezelient, Warezmaster, Spy, Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named (16)
Probe	Satan, Ipsweep, Nmap, Portsweep, Mscan
user to root attack (U2R)	Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps (7)

We have used traditional simulated annealing as per [51]. Instead of fixing the random temperature value, we have calculated the Initial temperature value by using the grey wolf optimization algorithm. The best cost of grey wolf optimizer used as the initial temperature of simulated annealing. The performance results were discussed in section4.

Finally, a support vector machine is utilized for classification purposes.

4. Experimental results and discussion

MATLAB is used for simulation purposes. We have analyzed our proposed algorithm performance results in terms of execution time, false alarm rate, detection rate, and accuracy.

4.1. Accuracy

It is the percentage of exactly categorized data that is a true positive (i.e., TP) and true negative (i.e., TN). Figure 1 signifies the accuracy comparison of the proposed technique with currently existing methods. Our proposed mechanism offers 6.39 % higher accuracy and 9.95 % higher accuracy while comparing with GWO-SVM[18] and PSO-SVM[9].

$$Accuracy_{val} \rightarrow \frac{T_{pos}+T_{neg}}{T_{pos}+F_{neg}+F_{pos}+T_{neg}} \tag{2}$$

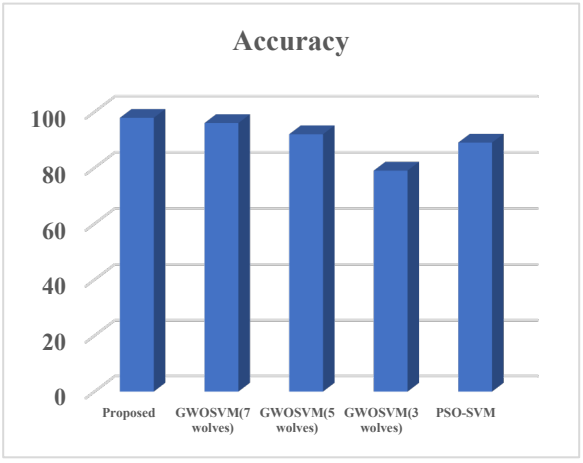

Fig. 3 Accuracy comparison of the proposed technique with existing approaches

4.2. False alarm rate

It is the false-positive ratio between true negative and false positive. Figure 2 represents the false alarm rate comparison of the proposed technique with currently existing approaches. Compared to GWO-SVM[18] and PSO-SVM[9], our proposed mechanism provides a false alarm reduction of 73.95 % and a false alarm reduction of 89.54 %.

$$F_{alarm} \rightarrow \frac{F_{pos}}{T_{neg}+F_{pos}} \tag{3}$$

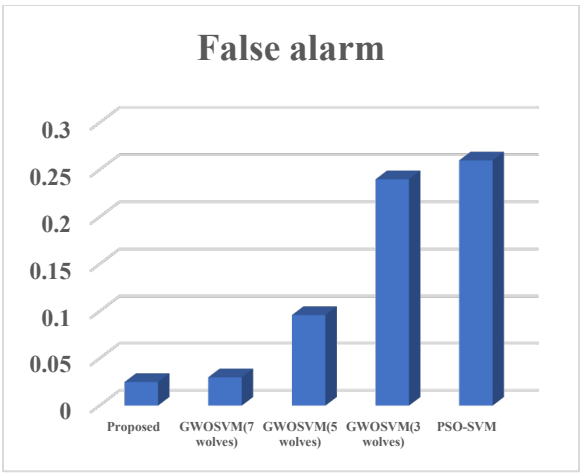

Fig.4.False alarm comparison of the proposed technique with existing approaches

Detection rate:

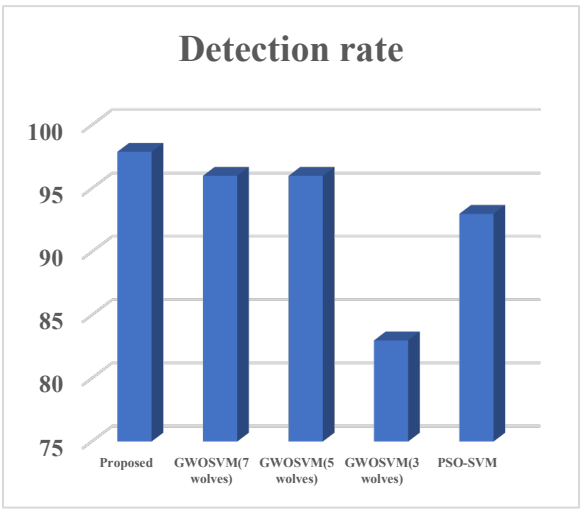

Fig. 5 Detection Rate comparison of the proposed technique with existing approaches

It is the true-positive ratio between true positive and false negative. Figure 3 represents the detection rate comparison of the proposed technique with currently existing approaches. Compared to GWO-SVM[18] and PSO-SVM[9], our proposed mechanism promises a detection rate increase of 2.59% and a detection rate increase of 5.25 %.

$$D_{rate} \rightarrow \frac{T_{pos}}{T_{pos}+F_{neg}} \tag{4}$$

Execution time:

Fig. 6 Execution time comparison of the proposed technique with existing approaches

Indicates the time it takes to complete the normality and abnormality classification. Figure 3 represents the execution time comparison of the proposed technique with currently existing approaches. Compared to GWO-SVM[18] and PSO-SVM[9], our proposed mechanism offers an execution time reduction of 28.44% and execution time reduction of 58.85 %.

5. Conclusion

The intrusion of wireless sensor networks is intended to weaken or eliminate these networks' ability to perform their functions. So, it is necessary to effectively perform intrusion detection. Feature selection methodology plays a major role in intrusion detection because it directly affects the performance of the classifier. So, in this work, we have proposed enhanced simulating annealing for feature selection. For classification purposes, we used the SVM algorithm. Our proposed feature selection methods offer better performance while comparing with currently existing methods. Compared to GWO-SVM and PSO-SVM, our proposed mechanism offers 8.71% higher accuracy, 81.74% lower false alarm rate, 3.92% higher detection rate, and 43.64% lower execution time. We are going to use a deep learning method for classification purposes in our future work.

Reference

1. Ioannis, K., Dimitriou, T., & Freiling, F. C. (2007, April). Towards intrusion detection in wireless sensor networks. In *Proc. of the 13th European Wireless Conference* 1-10.
2. Bace, R. G. (2000). *Intrusion detection*. Sams Publishing.
3. Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (2000). The 1999 DARPA off-line intrusion detection evaluation. *Computer networks*, *34*(4), 579-595.
4. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE symposium on computational intelligence for security and defense applications* (pp. 1-6). IEEE.
5. Haque, S. A., Rahman, M., & Aziz, S. M. (2015). Sensor anomaly detection in wireless sensor networks for healthcare. *Sensors*, *15*(4), 8764-8786.

6. Vijayanand, R., Devaraj, D., & Kannapiran, B. (2018). Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Computers & Security*, *77*, 304-314.
7. Ferriyan, A., Thamrin, A. H., Takeda, K., & Murai, J. (2017, September). Feature selection using genetic algorithm to improve classification in network intrusion detection system. In *2017 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC)* (pp. 46-49). IEEE.
8. Desale, K. S., & Ade, R. (2015, January). Genetic algorithm based feature selection approach for effective intrusion detection system. In *2015 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.
9. Ahmad, I. (2015). Feature selection using particle swarm optimization in intrusion detection. *International Journal of Distributed Sensor Networks*, *11*(10), 806954.
10. Kunhare, N., Tiwari, R., & Dhar, J. (2020). Particle swarm optimization and feature selection for intrusion detection system. *Sādhanā*, *45*, 1-14.
11. Saxena, H., & Richariya, V. (2014). Intrusion detection in KDD99 dataset using SVM-PSO and feature reduction with information gain. *International Journal of Computer Applications*, *98*(6).
12. Seth, J. K., & Chandra, S. (2016, March). Intrusion detection based on key feature selection using binary GWO. In *2016 3rd international conference on computing for sustainable global development (INDIACom)* (pp. 3735-3740). IEEE.
13. Alamiedy, T. A., Anbar, M., Alqattan, Z. N., & Alzubi, Q. M. (2019). Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 1-22.
14. Çavuşoğlu, Ü. (2019). A new hybrid approach for intrusion detection using machine learning methods. *Applied Intelligence*, *49*(7), 2735-2761.
15. Almomani, O. (2020). A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms. *Symmetry*, *12*(6), 1046.
16. Metropolis, N., Rosenbluth, A. W., Rosenbluth, M. N., Teller, A. H., & Teller, E. (1953). Equation of state calculations by fast computing machines. *The journal of chemical physics*, *21*(6), 1087-1092.
17. Borkar, G. M., Patil, L. H., Dalgade, D., & Hutke, A. (2019). A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. *Sustainable Computing: Informatics and Systems*, *23*, 120-135.
18. Safaldin, M., Otair, M., & Abualigah, L. (2020). Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. *Journal of ambient intelligence and humanized computing*, 1-18.

19. Belavagi, M. C., & Muniyal, B. (2016). Performance evaluation of supervised machine learning algorithms for intrusion detection. *Procedia Computer Science*, *89*, 117-123.
20. Kaplantzis, S., Shilton, A., Mani, N., & Sekercioglu, Y. A. (2007, December). Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information* (pp. 335-340). IEEE.
21. Soliman, H. H., Hikal, N. A., & Sakr, N. A. (2012). A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks. *Egyptian Informatics Journal*, *13*(3), 225-238.
22. Jianjian, D., Yang, T., & Feiyue, Y. (2018). A novel intrusion detection system based on IABRBFSVM for wireless sensor networks. *Procedia computer science*, *131*, 1113-1121.
23. Zidi, S., Moulahi, T., & Alaya, B. (2017). Fault detection in wireless sensor networks through SVM classifier. *IEEE Sensors Journal*, *18*(1), 340-347.
24. Vincent, P., & Bengio, Y. (2001, June). K-local hyperplane and convex distance nearest neighbor algorithms. In *NIPS* (Vol. 14, pp. 985-992).
25. Sebald, D. J., & Bucklew, J. A. (2000). Support vector machine techniques for nonlinear equalization. *IEEE transactions on signal processing*, *48*(11), 3217-3226.
26. Rajendran, R., Kumar, S. S., Palanichamy, Y., & Arputharaj, K. (2019). Detection of DoS attacks in cloud networks using intelligent rule based classification system. *Cluster Computing*, *22*(1), 423-434.
27. Zhang, H., Lu, G., Qassrawi, M. T., Zhang, Y., & Yu, X. (2012). Feature selection for optimizing traffic classification. *Computer Communications*, *35*(12), 1457-1471.
28. Selvakumar, K., Karuppiah, M., SaiRamesh, L., Islam, S. H., Hassan, M. M., Fortino, G., & Choo, K. K. R. (2019). Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs. *Information Sciences*, *497*, 77-90.
29. Yan, K. Q., Wang, S. C., Wang, S. S., & Liu, C. W. (2010, July). Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network. In *2010 3rd international conference on computer science and information technology* (Vol. 1, pp. 114-118). IEEE.
30. Abdullah, M., Alshannaq, A., Balamash, A., & Almabdy, S. (2018). Enhanced intrusion detection system using feature selection method and ensemble learning algorithms. *International Journal of Computer Science and Information Security (IJCSIS)*, *16*(2), 48-55.
31. Sedjelmaci, H., & Feham, M. (2011). Novel hybrid intrusion detection system for clustered wireless sensor network. *arXiv preprint arXiv:1108.2656*.

32. Abualigah, L. M., & Khader, A. T. (2017). Unsupervised text feature selection technique based on hybrid particle swarm optimization algorithm with genetic operators for the text clustering. *The Journal of Supercomputing*, *73*(11), 4773-4795.
33. Abualigah, L. M., Khader, A. T., & Hanandeh, E. S. (2018). Hybrid clustering analysis using improved krill herd algorithm. *Applied Intelligence*, *48*(11), 4047-4071.
34. Abualigah, L., Shehab, M., Alshinwan, M., Mirjalili, S., & Abd Elaziz, M. (2020). Ant lion optimizer: a comprehensive survey of its variants and applications. *Archives of Computational Methods in Engineering*, 1-20.
35. Abualigah, L., & Diabat, A. (2020). A novel hybrid antlion optimization algorithm for multi-objective task scheduling problems in cloud computing environments. *Cluster Computing*, 1-19.
36. Osanaiye, O., Cai, H., Choo, K. K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking*, *2016*(1), 1-10.
37. Dwivedi, R. K., Pandey, S., & Kumar, R. (2018, January). A study on machine learning approaches for outlier detection in wireless sensor network. In *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 189-192). IEEE.
38. Alsheikh, M. A., Lin, S., Niyato, D., & Tan, H. P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications. *IEEE Communications Surveys & Tutorials*, *16*(4), 1996-2018.
39. Xiao, Z., Liu, C., & Chen, C. (2009, December). An anomaly detection scheme based on machine learning for WSN. In *2009 First International Conference on Information Science and Engineering* (pp. 3959-3962). IEEE.
40. Jhanjhi, N. Z., Brohi, S. N., & Malik, N. A. (2019, December). Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning. In *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)* (pp. 1-9). IEEE.
41. Yan, K. Q., Wang, S. C., & Liu, C. W. (2009, March). A hybrid intrusion detection system of cluster-based wireless sensor networks. In *Proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 1, pp. 18-20).
42. Mehmood, A., Khanan, A., Umar, M. M., Abdullah, S., Ariffin, K. A. Z., & Song, H. (2017). Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. *IEEE Access*, *6*, 5688-5694.
43. Premkumar, M., & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocessors and Microsystems*, *79*, 103278.

44. Yavuz, F. Y., Devrim, Ü. N. A. L., & Ensar, G. Ü. L. (2018). Deep learning for detection of routing attacks in the internet of things. *International Journal of Computational Intelligence Systems*, *12*(1), 39-58.
45. Yahyaoui, A., Abdellatif, T., & Attia, R. (2019, June). Hierarchical anomaly based intrusion detection and localization in IoT. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 108-113). IEEE.
46. Alshinina, R. A., & Elleithy, K. M. (2018). A highly accurate deep learning based approach for developing wireless sensor network middleware. *IEEE Access*, *6*, 29885-29898.
47. Liu, W. (2009, November). Research on DoS attack and detection programming. In *2009 Third International Symposium on Intelligent Information Technology Application* (Vol. 1, pp. 207-210). IEEE.
48. Hassan, D. (2017). Cost-sensitive access control for detecting Remote to Local (R2L) and User to Root (U2R) attacks. *International Journal of Computer Trends and Technology*, *43*(2), 124-129.
49. Khamphakdee, N., Benjamas, N., & Saiyod, S. (2014, May). Improving intrusion detection system based on snort rules for network probe attack detection. In *2014 2nd International Conference on Information and Communication Technology (ICoICT)* (pp. 69-74). IEEE.
50. Geem, Z. W., Kim, J. H., & Loganathan, G. V. (2001). A new heuristic optimization algorithm: harmony search. *simulation*, *76*(2), 60-68.
51. Martinez-Rios, F., & Frausto-Solis, J. (2012). A simulated annealing algorithm for the satisfiability problem using dynamic Markov chains with linear regression equilibrium. *Simulated Annealing: Advances, Applications and Hybridizations*, 21.

Figures

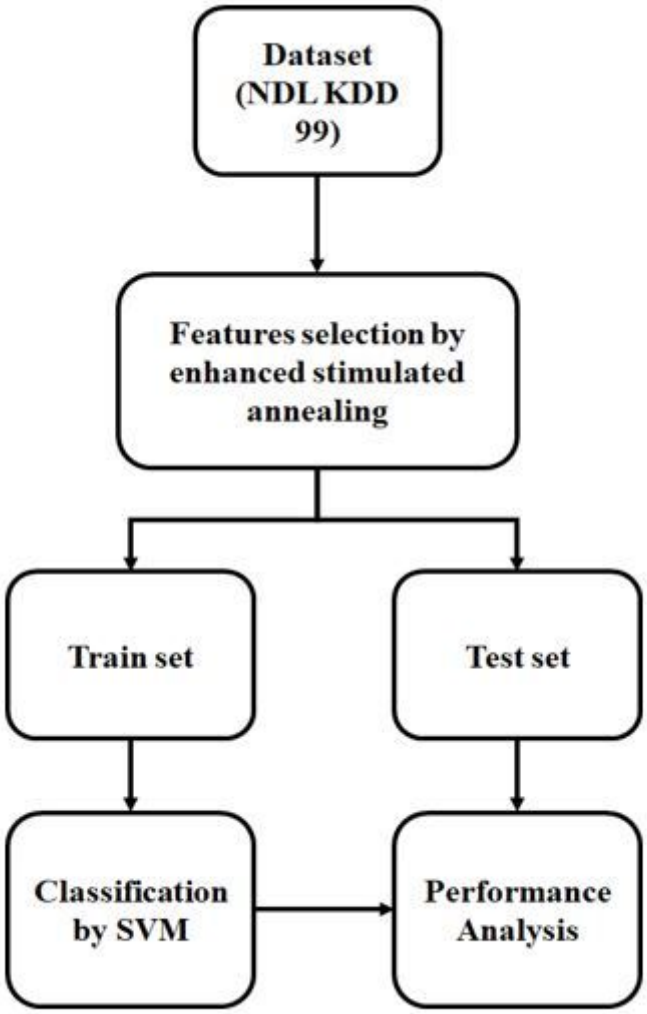

Figure 1

Overall process of proposed work

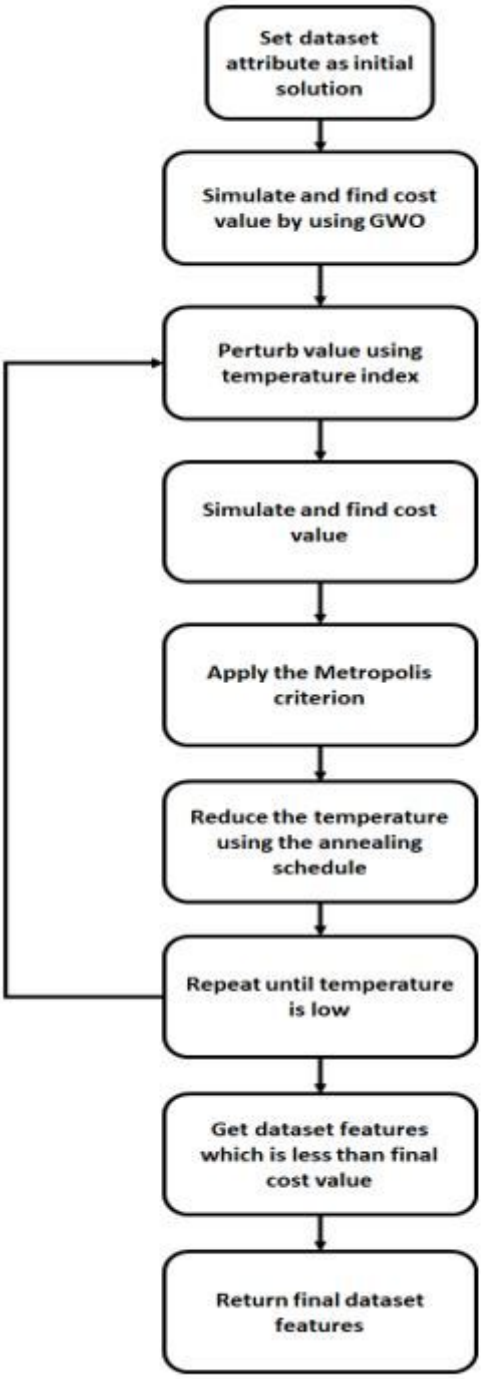

Figure 2

Proposed Enhanced simulated annealing work flow

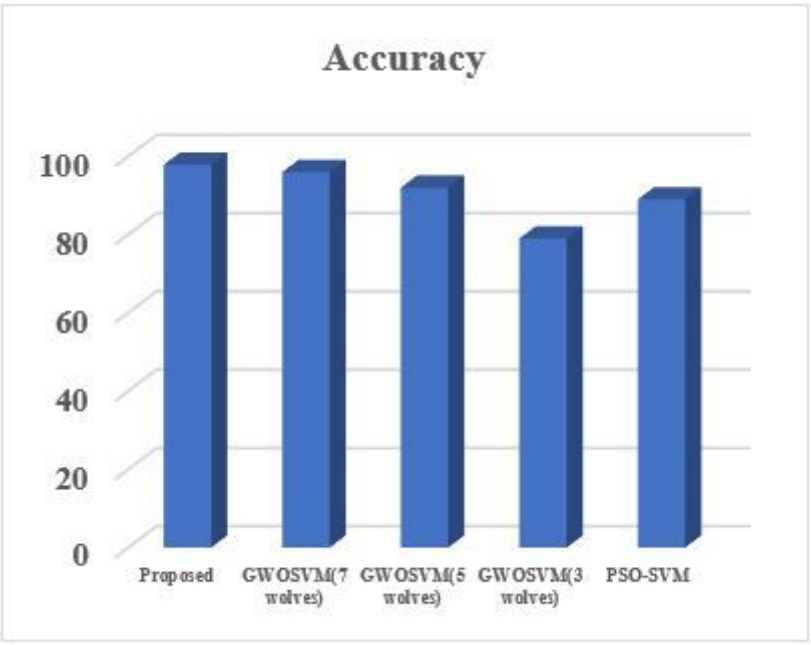

Figure 3

Accuracy comparison of the proposed technique with existing approaches

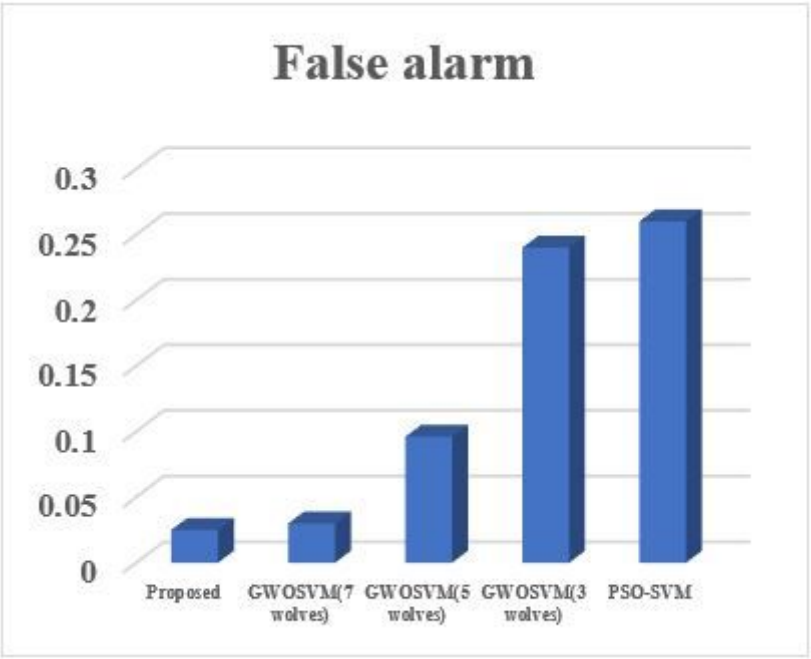

Figure 4

False alarm comparison of the proposed technique with existing approaches

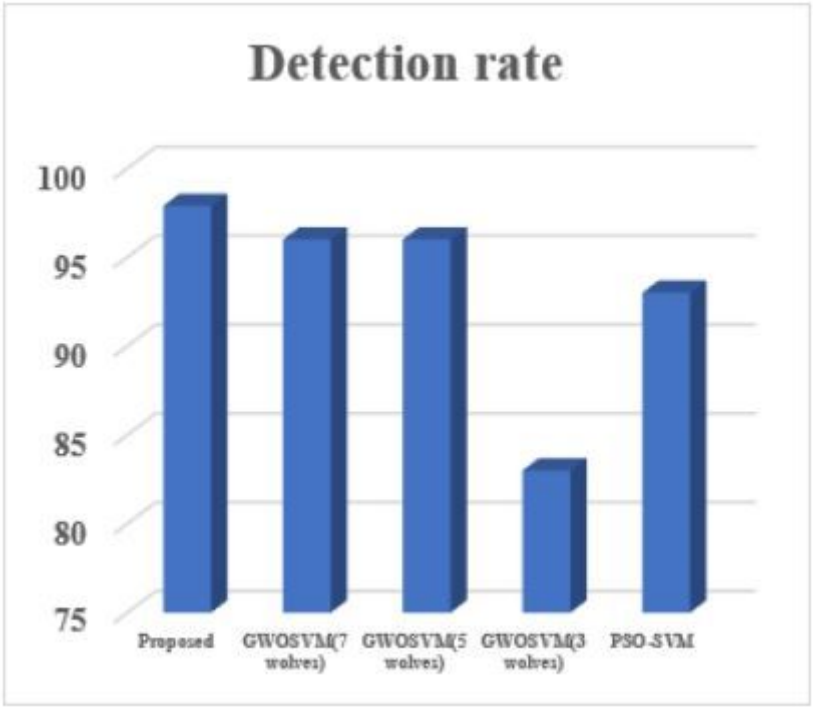

Figure 5

Detection Rate comparison of the proposed technique with existing approaches

Figure 6

Execution time comparison of the proposed technique with existing approaches