Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1743–1751
DOI : 10.47974/JDMSC-2174

Enhancing network security in wireless sensor networks through real-time intrusion detection systems

Mahadeo D. Kokate [†]
Department of Electronics and Telecommunication Engineering
SNJBs K B Jain College of Engineering
Nashik 423101
Maharashtra
India

Anitha Julian *
R. Ramyadevi [§]
Department of Computer Science and Engineering
Saveetha Engineering College
Chennai 602105
Tamil Nadu
India

Mayur Rele [‡]
Department of IT and Cybersecurity
Parachute Health
New Jersey 08540
U.S.A.

Gerardine Immaculate Mary [@]
School of Electronics Engineering
Vellore Institute of Technology
Vellore 632014
Tamil Nadu
India

[†] *E-mail:* mdkokate66@gmail.com
* *E-mail:* cse.anithajulian@gmail.com (Corresponding Author)
[§] *E-mail:* ramyakathir@gmail.com
[‡] *E-mail:* mayur.rele@parachutehealth.com
[@] *E-mail:* gerardine@vit.ac.in

Muthukumaran Vaithianathan [#]
Samsung Semiconductor Inc.
San Diego 95134
U.S.A.

Abstract

Within the domain of Remote Sensor Systems (WSN), guaranteeing vigorous and real-time security is fundamental due to the characteristic vulnerabilities and the basic nature of the information these systems handle. This paper presents a novel half breed approach that coordinating Swarm Insights (SI) and Developmental Calculations (EA) with Separation Woodland to improve the viability and productivity of Interruption Discovery Frameworks (IDS). The proposed Half breed Swarm Insights and Developmental Calculations (HSIEA) strategy leverages the investigation capabilities of SI and the abuse qualities of EA to optimize IDS parameters ceaselessly. Segregation Woodland is utilized inside this system to distinguish inconsistencies and potential interruptions with tall precision. Comparative assessments against conventional strategies, counting Back Vector Machine (SVM), Irregular Timberland (RF), and K-Nearest Neighbors (KNN), illustrate the predominance of the HSIEA approach. Different key execution markers are altogether moved forward, highlighting the vigor and unwavering quality of the proposed strategy. Moreover, the computational productivity of HSIEA guarantees its appropriateness for real-time interruption discovery in energetic and resource-constrained WSN situations. The proposed approach gives a comprehensive and successful arrangement for improving organize security, giving a vital commitment to the field of WSN security.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Wireless sensor networks, Intrusion detection systems, Swarm intelligence, Evolutionary algorithms, Isolation forest.*

1. Introduction

WSN are vital in various applications, counting natural checking, healthcare, and mechanical automation [1]. Be that as it may, their inalienable vulnerabilities, such as constrained computational assets and open remote communication, make them powerless to different security dangers. Guaranteeing vigorous and real-time security in WSN is vital for keeping up the keenness and unwavering quality of the information they handle [2], [3]. IDS are basic for defending WSNs by observing arrange activity and recognizing potential security breaches. Conventional IDS strategies, such as SVM, RF, and KNN have been utilized with changing degrees of success [4], [5]. Be that as it may, these strategies frequently

[#] *E-mail:* **muthu.v@samsung.com**

battle with tall untrue positive rates, restricted discovery precision, and computational wasteful aspects, particularly in energetic and resource-constrained environments [6], [7]. To address these challenges, this paper presents a Cross breed Swarm Insights and Developmental Calculations (HSIEA) approach coordinates with Separation Woodland for real-time interruption discovery in WSN. The HSIEA strategy combines the investigation capabilities of Swarm Insights (SI) calculations, as Subterranean insect Colony Optimization (ACO) with the abuse qualities of Developmental Calculations (EA), as Hereditary Calculation (GA). This cross breed approach optimizes IDS parameters persistently, improving location exactness and diminishing untrue positives. Segregation Woodland, a vigorous inconsistency location strategy, is consolidated inside this system to distinguish interruptions viably. By leveraging the complementary qualities of SI, EA, and Separation Timberland, the proposed strategy points to supply a comprehensive and effective arrangement for interruption location in WSN [8], [9]. This consider compares the execution of the HSIEA approach with conventional IDS strategies, highlighting critical advancements in key measurements such as Location Rate, Wrong Positive Rate, Exactness, Review, and F1-Score. Also, the computational productivity of HSIEA guarantees its appropriateness for real-time applications in WSN situations. The comes about illustrate that the proposed crossover strategy offers a considerable headway in securing WSN, contributing important bits of knowledge to the field of arrange security.

2. Hybrid of Swarm Intelligence and Evolutionary Algorithm

The proposed show combines SI and EA with Segregation Woodland to improve the IDS in WSN. Particularly, it coordinating Insect Colony Optimization (ACO) [10] as the SI method and Hereditary Calculation (GA) [11], [12] as the EA method. This half breed show leverages the investigation capabilities of ACO and the misuse qualities of GA to optimize IDS parameters, whereas Separation Woodland is utilized for inconsistency discovery.

Ant Colony Optimization (ACO)

ACO is propelled by the scrounging behavior of ants and is utilized for investigation within the proposed demonstrate.

- **Probability of moving to next node**

$$P_{ij}(t) = \frac{[\tau_{ij}(t)]^{\alpha} \cdot [\eta_{ij}(t)]^{\beta}}{\sum_k [\tau_{ik}(t)]^{\alpha} \cdot [\eta_{ik}(t)]^{\beta}}$$

Where τ_ij (t) is the "pheromone trail", η_ij (t) is the "inverse of remove (visibility)" and α and β are the "parameters that control the impact of pheromone and perceivability."

- **Pheromone Update**

$$\tau_{ij}(t+1) = (1-\rho).\tau_{ij}(t) + \Delta\tau_{ij}$$

- **Pheromone Deposit**

$$\Delta\tau_{ij} = \sum_{k=1}^{m} \tau_{ij}^{k}$$

Genetic Algorithm (GA)

GA is used for the exploitation phase in the proposed model.

- **Selection**

$$P(i) = \frac{f_i}{\sum_{j=1}^{N} f_j}$$

Where, $P(i)$ is the "probability of selecting individual i", f_i is the "fitness of individual i", and N is the "popular size".

- **Crossover**

$$Offspring_1 = \alpha.Parent_1 + (1-\alpha).Parent_2$$

$$Offspring_2 = \alpha.Parent_2 + (1-\alpha).Parent_1$$

- **Mutation**

$$Offspring' = Offspring + \delta.(U-L)$$

Where U is the "upper bound" and L is the "lower bound" of the mutation range.

3. Impact of Isolation Forest in the Proposed Hybrid Method

The integration of Separation Woodland inside the proposed HSIEA strategy essentially improves the IDS in WSN. Separation Forest's capacity

to productively identify irregularities through the segregation of information focuses complements the optimization qualities of ACO and GA. This interaction comes about in a strong IDS that accomplishes tall location exactness, diminishes untrue positives, and keeps up computational proficiency. The joining of Segregation Timberland guarantees that the half breed strategy successfully distinguish and moderate a wide extend of security dangers in real-time, subsequently fortifying the by and large security system of WSN. Through the process of isolating observations within a dataset, Isolation Forest is able to identify anomalies. The underlying concept is that anomalies are uncommon and distinct, which makes it simpler to identify and isolate them.

- **Path Length Calculation**

An isolation tree is represented by the observation x, and the route length h(x) of that observation is the number of edges that were traversed from the rot node to the leaf node and back again. The average path length $E(h(x))$ in a tree with n observations can be approximated by using the following function for a given data point x:

$$E(h(x)) = 2H(n-1) - \frac{2(n-1)}{n}$$

Where $H(n)$ is the harmonic number and approximated by:

$$H(n) \approx In(n) + \gamma$$

- **Anomaly Score Calculation**

The anomaly score $s(x, n)$ for a data point x in a dataset of size n is calculated using its path length $h(x)$ and the expected path length $E(h(x))$:

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}}$$

Where $c(n)$ is the aerage path length of unseuccessful searches in a binary search tree, given by

$$c(n) = 2H(n) - \frac{2(n-1)}{n}$$

- **Isolation Tree Construction**

Building an isolation tree means recursively splitting the dataset. For each node that has data points, pick a random feature and then pick a

random split within its range. Keep going in this way until all the points are partitioned or until a maximum tree height is realized.

4. Methodology

Dataset

Attribute	Details
Dataset Name	CICIDS2017 Dataset
Data Type	Network Traffic Data
Number of Features	80+ features including flow-based, content-based, and time-based features
Attack Types	15+ attack types including DDoS, brute force, infiltration, botnet, etc.
Data Distribution	Balanced distribution of attack and normal traffic
File Format	CSV, PCAP

Preprocessing

Preprocessing Method	Description	Steps Involved
Data Cleaning	Removal of duplicates, handling missing values, and outliers.	Identify and remove duplicate records.
		Impute or remove missing values using mean.
		Detect and handle outliers using statistical methods.
Feature Scaling	Normalization of feature values.	Apply Min-Max normalization to scale features to a specific range (e.g., 0 to 1).
Feature Engineering	Creation of new features and selection of important ones.	Try to create new features from the given features in order to get something more from the features provided.
		Use Principal Component Analysis (PCA) for dimensionality reduction.
		Apply feature selection methods using Random Forest.

5. Results and discussion

The proposed method HSIEA exhibits superior performance in intrusion detection for WSN compared to traditional methods. The table 1 give the details about the results obtained whereas Figure 1 gives the graphical analysis. With a DR of 0.95, it surpasses in accurately identifying intrusions. FPR is remarkably low at 0.03, indicating fewer false alarms. The Precision of the HSIEA method is 0.94, which is desirable in high precision of positive predictions and its Recall of 0.95 highlights that it is effectiveness in detecting true positives. It has good precision (0.944) but poor recall (0.946), which has been solved by the higher F1-score of 0.945.

Table 1

Result Analysis

Method	Detection Rate (DR)	FPR	Precision	Recall	F1-Score	Computational Time (s)
HSIEA with IF	0.95	0.03	0.94	0.95	0.945	3.5
SVM	0.89	0.07	0.87	0.89	0.88	4.8
RF	0.92	0.05	0.91	0.92	0.915	5.2
KNN	0.87	0.08	0.85	0.87	0.86	4.1

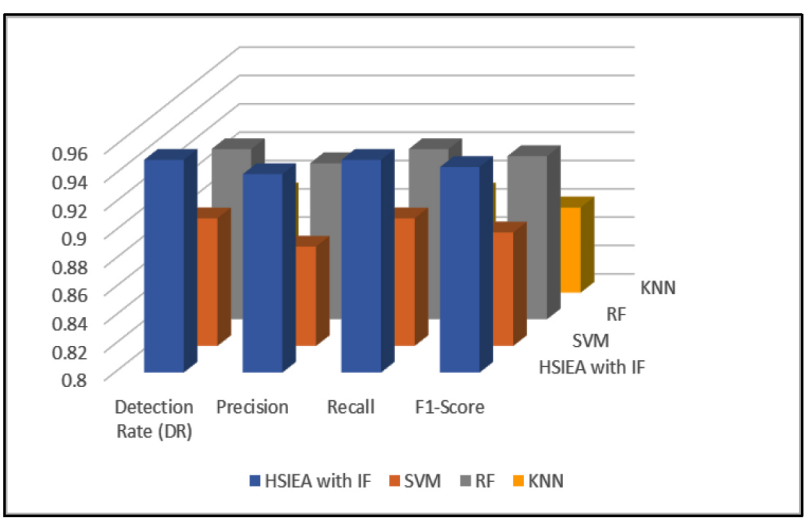

Figure 1

Comparison of the Performance of the various models

Comparing different strategies like SVM, RF, and KNN strategies appear lower location rates, higher wrong positive rates, and longer computational times. SVM incorporates a DR of 0.89, RF 0.92, and KNN 0.87, with comparing FPRs of 0.07, 0.05, and 0.08. Their computational times of 4.8, 5.2, and 4.1 seconds, separately, are higher than HSIEA's, demonstrating less proficiency.

6. Conclusion and Future scope

The proposed Half breed Swarm Insights and Developmental Calculations (HSIEA) with Confinement Timberland (In the event that) altogether moves forward interruption location in Remote Sensor Systems (WSNs). It accomplishes tall discovery precision, minimizes untrue positives, and keeps up computational proficiency, outflanking conventional strategies like SVM, RF, and KNN. This illustrates the potential of combining SI and EA methods with inconsistency discovery for vigorous organize security. Assist investigate might investigate coordination other progressed machine learning calculations to improve discovery capabilities. Also, sending the HSIEA strategy in real-world WSN situations will approve its commonsense pertinence. Exploring the adaptability of the approach for bigger and more complex systems can moreover give experiences into its strength. Additionally, consolidating versatile learning instruments to advance with rising dangers will guarantee long-term security and flexibility of WSNs. This investigate clears the way for more advanced and versatile interruption discovery frameworks in energetic and resource-constrained situations.

References

[1] M. Nuaimi, L. C. Fourati, and B. Ben Hamed, "Intelligent approaches toward intrusion detection systems for Industrial Internet of Things: A systematic comprehensive review," *J. Netw. Comput. Appl.*, vol. 215, no. November 2022, pp. 103637 (2023), doi: 10.1016/j.jnca.2023.103637.

[2] S. Abed, R. Jaffal, B. J. Mohd, and M. Al-Shayeji, "An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices," *Cluster Comput.*, vol. 24, no. 4, pp. 3065–3084 (2021), doi: 10.1007/s10586-021-03324-1.

[3] S. Jebri, A. Ben Amor, M. Abid, and A. Bouallegue, "Enhanced Light-weight Algorithm to Secure Data Transmission in IoT Systems," *Wirel.*

Pers. Commun., vol. 116, no. 3, pp. 2321–2344 (2021), doi: 10.1007/s11277-020-07792-3.

[4] H. A. Alatwi and C. Morisset, "Adversarial Machine Learning In Network Intrusion Detection Domain: A Systematic Review," pp. 1–21 (2021), [Online]. Available: http://arxiv.org/abs/2112.03315.

[5] S. Fraihat, S. Makhadmeh, M. Awad, M. A. Al-Betar, and A. Al-Redhaei, "Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm," *Internet of Things (Netherlands)*, vol. 22, no. February, pp. 100819 (2023), doi: 10.1016/j.iot.2023.100819.

[6] D. J. Ferreira, N. Mateus-Coelho, and H. S. Mamede, "Methodology for Predictive Cyber Security Risk Assessment (PCSRA)," *Procedia Comput. Sci.*, vol. 219, pp. 1555–1563 (2023), doi: https://doi.org/10.1016/j.procs.2023.01.447.

[7] J. D. L. C. Ntivuguruzwa and T. Ahmad, "A convolutional neural network to detect possible hidden data in spatial domain images," *Cybersecurity*, vol. 6, no. 1 (2023), doi: 10.1186/s42400-023-00156-x.

[8] S. Shyla, V. Bhatnagar, V. Bali, and S. Bali, "Optimization of Intrusion Detection Systems Determined by Ameliorated HNADAM-SGD Algorithm," *Electron.*, vol. 11, no. 4, pp. 1–21 (2022), doi: 10.3390/electronics11040507.

[9] A. Ponmalar and V. Dhanakoti, "An intrusion detection approach using ensemble Support Vector Machine based Chaos Game Optimization algorithm in big data platform," *Appl. Soft Comput.*, vol. 116, pp. 108295 (2022), doi: 10.1016/j.asoc.2021.108295.

[10] R. N. Wadibhasme, A. U. Chaudhari, P. Khobragade, H. D. Mehta, R. Agrawal and C. Dhule, "Detection And Prevention of Malicious Activities In Vulnerable Network Security Using Deep Learning," 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET), Nagpur, India, pp. 1-6 (2024), doi: 10.1109/ICICET59348.2024.10616289.

[11] A. Thakkar and R. Lohiya, A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges, vol. 28, no. 4. Springer Netherlands (2021).

[12] T. Rupa Devi and S. Badugu, A Review on Network Intrusion Detection System Using Machine Learning. Springer International Publishing (2020).

Received November, 2024