A Novel Machine Learning assisted Hierarchical Clustering approach for Wireless UAV System

Soufiene Ben Othman[1] , Abdullah Ali Bahattab[2]
[1]PRINCE Laboratory Research, ISITcom, Hammam Sousse, University of Sousse, Tunisia
[2]Computer Technology Department, College of Telecomm and Electronics, Jeddah, Saudi Arabia
Ben_oth_soufiene@yahoo.fr, abahattab@gmail.com

Abstract:
The current wireless Unmanned Aerial Vehicle (UAV) approaches based on supervised learning have a high false detection rate, making it difficult to recognise novel types of attack activities, and increasing the cost of collecting labelled network data. The method employs unsupervised learning and does not require human tagging of large amounts of wireless network data. As a result, it can quickly obtain training data sets and discover unknown assault patterns. The multi-view cosine distance method for hierarchical clustering is introduced. This makes clustering results more rational, network behavior assessment more accurate, and intrusion detection false detection rate lowered. The experiment uses the AWID (Aegean WIFI Intrusion Dataset) attack data collection. The principle component analysis approach decreases the dimensionality of the experimental data set, reducing the temporal complexity of the intrusion detection algorithm. The experimental findings reveal that the proposed multi-view hierarchical clustering wireless network intrusion detection algorithm outperforms the classic wireless network intrusion detection method in terms of detection rate, false detection rate, and unknown attack types.

Keywords: ***Multi-View; UAV; Hierarchical Clustering; Wireless Network; Intrusion Detection; Principal Component Analysis***
DOI Number: 10.48047/NQ.2023.21.1.NQ20059 NeuroQuantology 2023; 21(1): 748-762

I. Introduction

The rapid development of wireless local area network technology and mobile communication equipment makes the WiFi network environment gradually popularized and integrated into people's lives, making WiFi a target of network attacks. Wireless network crimes such as "rubbing the Internet" and "wireless phishing" occur from time to time, causing information security risks such as personal data leakage and tampering and even leading to significant economic losses [1]. The continuous evolution and upgrading of network attack behaviors make the network security problems in the wireless network environment more and more severe and become a new dilemma for information security.

As researchers have paid more attention to unsupervised anomaly detection, a number of useful data mining and machine learning methods have been used to find anomalies without any help. Among other things, author [4] came up with a new method for detecting clustering that takes into account the degree of cluster deviation (Deviation Degree) when labelling clusters, and the (Improved Nearest

Neighbor, INN) algorithm is used in clustering. This algorithm improves the quality of clustering. Author [5] came up with an unsupervised way to find out if something is out of the ordinary. This model combines all attribute clustering and feature attribute clustering. Service sets are divided into different groups by the model. Then it does all attribute clustering and part of it for related attribute clustering, and the method with the best training results is used for the service detection model. Using an improved clustering algorithm called "Clustering Using Representative, CURE," the author came up with an unsupervised way to find out when something isn't right. As long as the performance of the original CURE clustering technique remains constant, we may make more perfect clusters by reasonably enhancing it, which also provides us with more pure normal behaviour data for building a normal behaviour model. Author [7] devised a method to reduce false negatives and false positives caused by outliers and normal values interacting with one other. He proposed utilising the reverse K-nearest neighbour approach to filter outliers and using statistical distance as the distinct group data. The measure of how similar they are, the algorithm has a high rate of spotting anomalies and is very stable. At the moment, the clustering or K-nearest neighbor algorithms used by these unsupervised anomaly detection methods are not flexible enough to change the number of clusters when the wireless network environment changes in real time [8]. Besides, most algorithms use Euclidean distance as a measure of how similar two data objects are. For high-dimensional data, it is better to use cosine distance to describe than Euclidean distance [9]. This is how the full-granularity clustering algorithm proposed by author [10] works: It uses cosine distance to show how similar data objects are, and it comes up with a better and more accurate clustering result than Euclidean distance. That is not the case with this algorithm. Instead, it grids the Euclidean space to find the reference points. The cosine distance measurement, on the other hand, has a lot of internal factors that can change how well it works. Gridding in the Cartesian coordinate system, on the other hand, picks a lot of reference points and is more difficult. Authors are proposing various techniques[17-20] in wireless network to identification of users.

This research proposes an unsupervised wireless network intrusion detection technique. Hierarchical clustering and the selection of reference points from various viewpoints are the foundations of this approach [21][22]. In order to deal with today's ever-changing and complicated wireless network environment, it is possible to adjust the distance threshold for hierarchical clustering during the clustering process. It also comes up with a mechanism to quantify distance for hierarchical clustering: the multi-view cosine distance. A number of views are taken into account while assessing the similarity between two data items. As a result, there is a closer connection between the data points [23][24]. Due to the increased reliability and accuracy of the similarity measure, the detection rate of the intrusion detection algorithm and the false detection rate have increased and declined, respectively. This similarity metric is much superior to the usual Euclidean distance measure for comparing outlier data points and data items that are not part of a cluster. The experiment in this paper is based on data from the AWID public wireless network. When there are fewer variables in the dataset, a technique may execute more quickly and efficiently, and Principal Component Analysis (PCA) is utilised to do this. When compared to a more traditional technique, the proposed wireless network intrusion detection algorithm beats the more traditional one in terms of identifying both known and new attack types [25][26].

II. Wireless Network Intrusion Detection Based on Multi-view Hierarchical Clustering

2.1 Wireless Network Intrusion Detection Process

The wireless network intrusion detection process [11] mainly includes the following modules (1) Wi-Fi network data acquisition; (2) data preprocessing; (3) classifier learning; (4) building a classifier; (5) wireless network data detection ; (6) Response mechanism. Among them, modules (1) (2) (3) (4) belong to the intrusion detection learning stage, and modules (5) (6) belong to the detection stage. Wi-Fi wireless network data is generally obtained through wireless network monitoring devices in the actual network environment [27][28][29]. First, the received wireless network data is preprocessed and entered into the classifier learning module. Then, a classifier that can judge the behavior of network data is constructed by training a large amount of wireless network data. Finally, the detection module analyses and evaluates the wireless network real-time traffic to determine its behavior category, and the intrusion detection and response mechanism are activated promptly. The detection process is shown in Figure 1.

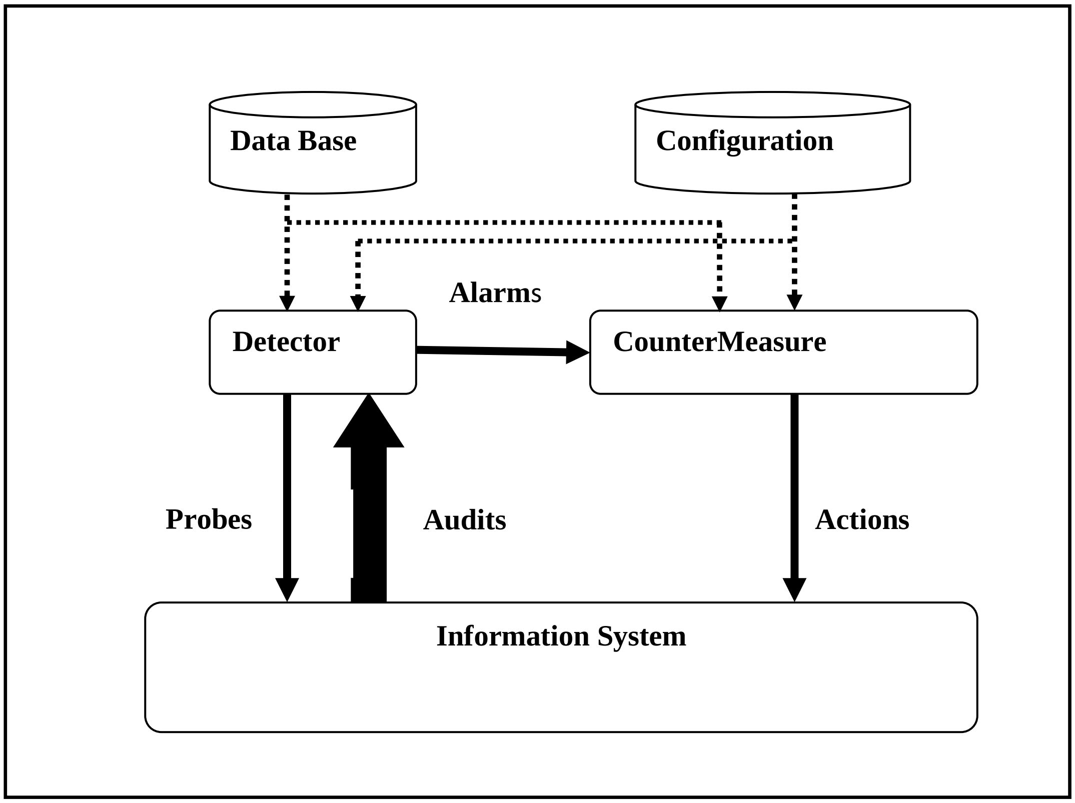

Fig.1 Schematic diagram of wireless network intrusion detection process

Classic classifier-building techniques include the K-means clustering algorithm and the (K-Nearest Neighbor, KNN) classification algorithm. This method classifies and learns data sets based on differences in network data behaviour, extracts network data behaviour features, and creates data classifiers for real-time monitoring. Different detection systems will often set suitable data behaviour assessment thresholds based on various network settings and network states. In the process of intrusion detection, the detection system will output the final judgment result of the data behavior in combination with the classification situation of the classifier and the setting of the threshold. With the continuous diversification and complexity of wireless network intrusion behaviors, K-means and KNN algorithms with a fixed number of classifications can no longer meet the needs of intrusion detection systems. In unknown wireless network environments, intrusion detection systems cannot obtain network data in advance. This phenomenon dramatically reduces the learning ability and classification performance of data classifiers based on K-means and KNN algorithms with a fixed number of classifications. The hierarchical clustering approach is used to design the classifier in this study to minimise the impact of the stated number of classification K on the classifier's performance. In contrast to the K-means and KNN algorithms, the hierarchical clustering method allows for more control over the number of classifications by adjusting the hierarchical clustering distance threshold while building the classifier. As a result, the categorization outcomes are consistent with the present wireless network environment.

2.2 Hierarchical Clustering Algorithms

The main idea of hierarchical clustering [12] is to divide the data set at different levels, which can be divided into two forms: "bottom-up" aggregation strategy and "top-down" splitting strategy. The "bottom-up" approach treats each raw data as a single cluster and continuously aggregates small groups into large groups. The "top-down" process begins by treating all data as a cluster, by dividing extensive collections until every single data is separated. Combined with the data characteristics of the wireless network data set AWID, this paper adopts the "bottom-up" hierarchical clustering aggregation strategy. The clustering termination condition meets the preset distance threshold α or reaches the preset number of clusters k. The key to hierarchical clustering is choosing the distance between clusters and determining the clustering threshold α. In the clustering process, each group is a set of data samples. When calculating the distance between clusters, it is only necessary to calculate a certain distance between the set locations the collections D_i and D_j are given, and the following formula can calculate the distance:

The minimum distance between clusters:

$$e_{\min}\left(D_i, D_j\right) = \min_{x \in D_{i,}, z \in D_j} \operatorname{dist}(x, z)(1)$$

Maximum distance between clusters:

$$e_{\max}\left(D_i, D_j\right) = \max_{x \in D_{i,} z \in D_j} \operatorname{dist}(x, z) \qquad (2)$$

Average distance between clusters:

$$e_{\text{avg}}\left(D_i, D_j\right) = \frac{1}{|D_i||D_{j|}} \sum_{x \in D_i} \sum_{x \in D_i} \operatorname{dist}(x, z) \quad (3)$$

where |·| is the cardinality of the set.

As a measure of the distance between clusters, the average length comprehensively measures the influence of all data objects in the group on the distance between clusters, which is more suitable for the classification of wireless network data sets and increases the robustness of the clustering algorithm. Figure 2 is a schematic diagram of bottom-up hierarchical clustering. The abscissa represents the data objects in the network dataset, numbered p1-p6, and the ordinate is the distance between clusters. The clustering process is shown in Figure 3. The clustering process can be terminated in the hierarchical clustering algorithm according to the preset distance value or the number of clusters, and the corresponding clustering results can be obtained. For example, when the distance threshold is set to 0.118 (as shown by the dotted line in Figure 2), the following clustering results can be obtained:

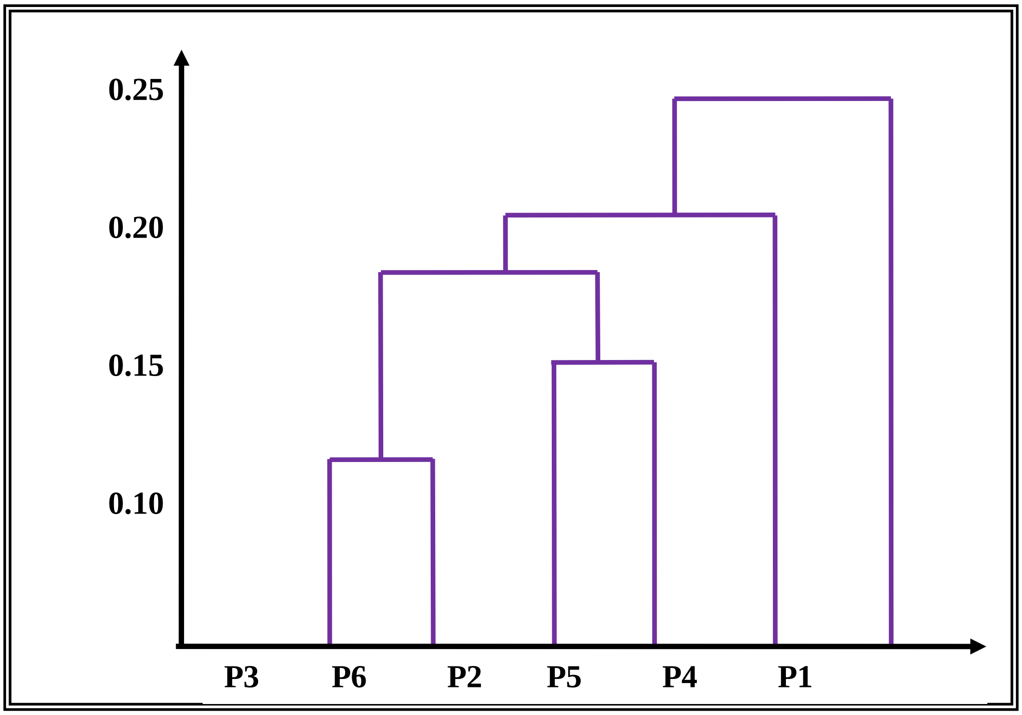

Fig.2 Hierarchical clustering diagram

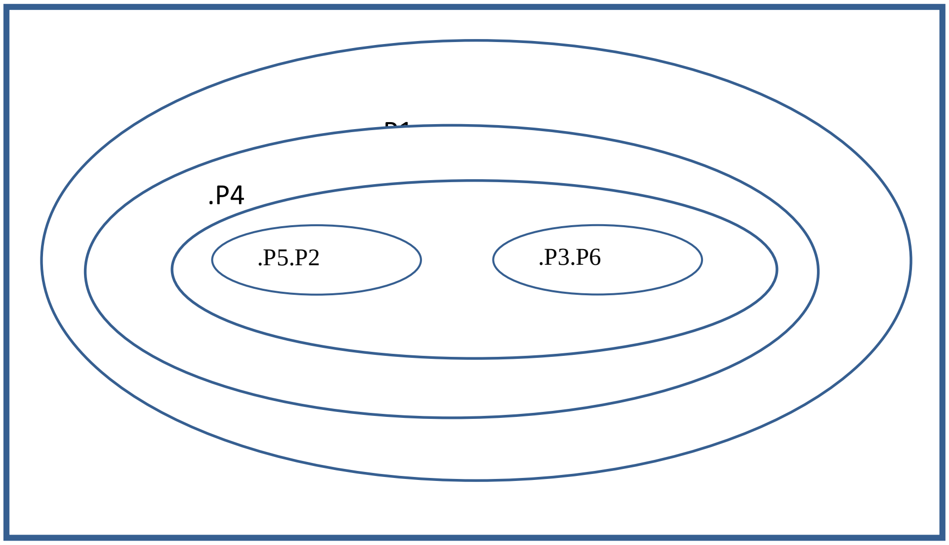

Fig.3 Hierarchical clustering process diagram

2.3 Wireless network intrusion detection algorithm based on multi-view hierarchical clustering

Input: A sample set containing n data objects Y= $\{y_1, y_2, \ldots, y_n\}$ multi-view step size N, hierarchical clustering threshold a, weight vector m = ($m_1,m_2,\cdots,m_p)^T$

Output: Clustering result set D.

- All data objects in the dimensionality reduction dataset Y= {y_1, y_2, …, y_n} through the weight vector m = (m_1,m_2,⋯,m_p)^T
- Consider each data object in the dataset Y= {y_1, y_2, …, y_n} as an initial cluster, that is, construct an initial cluster V= {v_1, v_2, …, v_n}, where V_1= {y_1} , V_2= {y_2}, …, V_n= {y_n} .
- Traverse all the data objects y_i in the initial cluster and calculate$dist(y_i, y_j)(y_i \in V_i, y_j \in V_{j,i\neq j})$.
- When $\exists Mindist(y_i, y_j)(y_i \in V_i, y_j \in V_{j,i\neq j}) < a$, update the cluster set as V= {v_1, v_2, …, v_{n-1}}, where V_1= {y_1} , V_2= {y_2}, V_i= {y_i , y_j} ,…, V_{n-1}= {y_n} . Otherwise, the algorithm ends, and re-enter a reasonable hierarchical clustering distance threshold.
- The reference point set T_h = {e1, e2, .., dh } is determined by the multi-view step N.
- Traverse all the clusters in the cluster V= {v1, v2, …, vn-1}, when $\exists \mathrm{Min}(\mathrm{V_i}, \mathrm{V_j}) < a$, merge the clusters Vi, Vj. Update cluster V= {v1, v2, …, vn-1}.

$$c\ (V_i, Vj\ \ ) = \frac{\sum_{Y_a \in V_i, Y_b \in V_j} dist(Y_a, Y_b)}{|V_i||V_j|} (13)$$

$$dist\ (Y_a, Y_b) = \frac{1}{2|T_h|} \sum_{e_h \in T_h} [dist(Y_a - e_h, Y_b - e_h) + dist(Y_a - 0, Y_b - 0)] = \frac{1}{2|T_h|} \sum_{e_h \in T_h} [\frac{(Y_a - e_h, Y_b - e_h)}{||Y_a - e_h|| * ||Y_b - e_h||} + \frac{(Y_a)^T (Y_b)}{||Y_a|| * ||Y_b||}] \qquad (14)$$

Otherwise, output the clustering result set U.

(1) Repeat step (5) to output the final clustering result set U.

III. Experiment and result analysis

An Intel i5 processor with 8GB of RAM runs the experiment, which uses the Windows 10 operating system. The data used in the experiment comes from the AWID wireless network data collection. Also in python3.7, we ran the following comparative tests:

- A comparison of wireless network intrusion detection techniques based on multi-view cosine distance hierarchical clustering with classical K-means clustering, KNN classification, and Density-Based Spatial Clustering of Applications with Noise (DBSCAN).

- For wireless network intrusion detection, a comparison of the standard Euclidean distance hierarchical clustering technique with the multi-view cosine distance hierarchical clustering algorithm.
- Comparative trials of network intrusion detection techniques based on full-granularity cosine distance hierarchical clustering and multi-view cosine distance hierarchical clustering.
- Studies comparing standard K-means clustering, KNN classification, density clustering DBSCAN and wireless network intrusion detection algorithms based on multi-view cosine distance hierarchical clustering are used to discover unknown attack types in comparison experiments.

Wireless network intrusion detection algorithms are evaluated using the detection rate ACC, the false detection rate FDR, the recall rate Recall, and F1 in this article details are as follows:.

- The detection rate ACC, which is the ratio of the network data of the proper category to the total network data. Intrusion detection algorithms work better if they have a high detection rate.

$$BCC = \frac{UP+UN}{UP+UN+GP+GN} \qquad (16)$$

- FDR is the ratio of the quantity of average behavior data that is incorrectly interpreted as attack behavior to the total of average behavior. As an example, in an intrusion detection method, a lower false detection rate means a greater detection rate.

$$FDR = \frac{UG}{UN+GP} \qquad (17)$$

- Data volume of network attack behaviors in relation to overall attack behaviors, which is known as a recall rate. The intrusion detection algorithm's capacity to recognise attack activity improves with increasing recall rates.

$$Scall = \frac{UP}{UP+GP} \qquad (18)$$

For example, the number of network data behaviors that properly classify normal network data behaviors as nominal is represented by TN (true negative). There are a variety of network data characteristics that may be used to identify an attack type, called TP (true positive). Network data that misidentifies typical data activity as an assault is referred to as FN (false negative) or FP (false positive).

A sample data set from the CLS dataset is provided in Table 1, along with the data sets h1-h9and d1-d9 in Table 6. To avoid evaluating experimental findings obtained by the intrusion detection approach on a single experimental data set, this study randomly selects experimental data sets H1-H10 and D1-D10 from the CLS data set with unique attack behaviour classes. Datasets d1-d10 contain anonymized attack behaviour data from related categories (masked by well-known attack behaviours) and are used in comparative studies to assess the effectiveness of intrusion detection systems to detect unexpected attack behaviours.

Table 1 Test data set of Experiment 1

Data Set	**Data**		**Aggressive Class**
	Normal	Attack	
1	100	100	3
2	200	200	5
3	300	300	6
4	400	400	8
5	500	500	10
6	600	600	11
7	700	700	13
8	800	800	14
9	900	900	15

Table 2 Test data set of Experiment 2

Data Set	**Data**		**Aggressive Class**	**Unknown Attack Class**
	Normal	Attack		
1	100	100	3	1
2	200	200	5	2
3	300	300	6	3
4	400	400	8	4
5	500	500	10	5
6	600	600	11	6
7	700	700	13	7
8	800	800	14	8

9	900	900	15	9

3.1.1 Comparative Experiment One

Clustering methods such as K-means, KNN classification, density clustering DBSCAN, and multi-view cosine distance hierarchical clustering are used in comparison studies. A total of ten trials including test data from the first through tenth places were conducted. Results of the experiment are depicted in Figures 4-7, along with a table of data.

Table 3: Comparison of ACC in Experiment 1

Serial Number	K-means clustering	KNN classification	density clustering DBSCAN	Hierarchical clustering
1	75	90	95	100
2	80	95	98	105
3	60	80	100	95
4	65	82	102	98
5	68	84	104	100
6	70	86	106	105
7	72	88	108	106
8	76	90	110	107
9	78	92	113	108
10	80	95	115	110

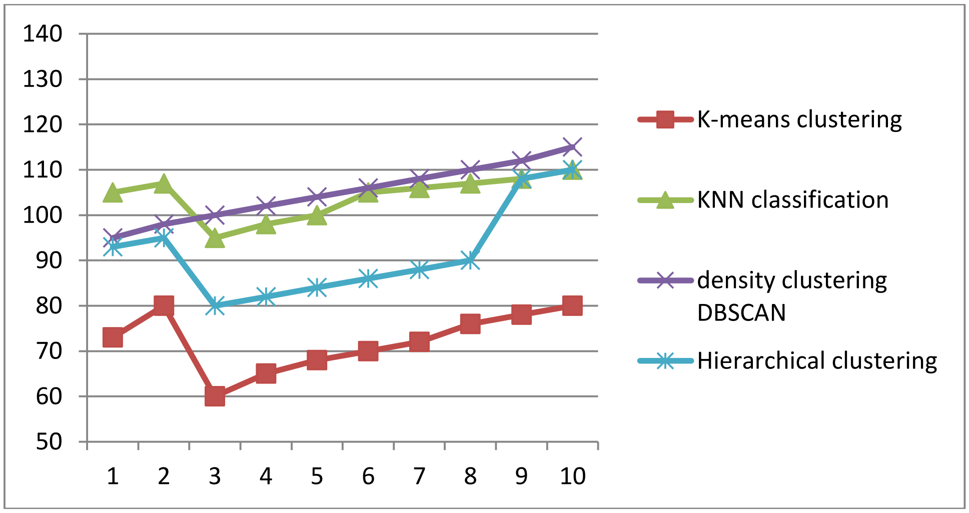

Fig.4 Comparison of ACC in Experiment 1

Table 4: Comparison of false detection rate in Experiment 1

Serial Number	K-means clustering	KNN classification	density clustering DBSCAN	Hierarchical clustering
1	10	8.5	6	3
2	9.8	7.5	6.3	2
3	9.5	5	5.5	3
4	9	6	6.3	1.5

5	9.3	6.3	6	3.5
6	9	6.5	6.3	4
7	9.5	7	6	4.2
8	9.3	7.2	5.8	4.5
9	9.3	7.5	5.5	5
10	9.2	8	5.2	5.5

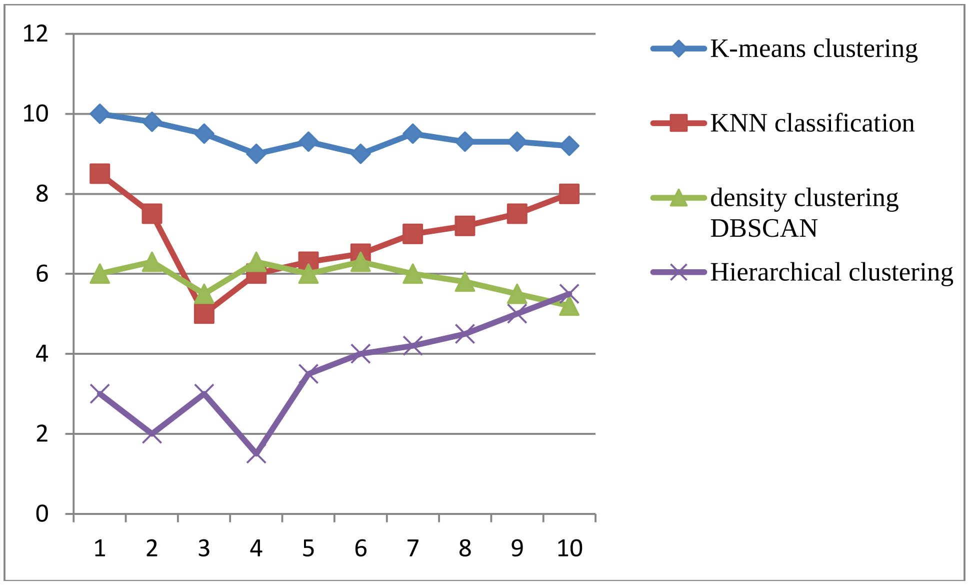

Fig.5 Comparison of false detection rate in Experiment 1

Table 5: Comparison of Recall rate in Experiment 1

Serial Number	K-means clustering	KNN classification	density clustering DBSCAN	Hierarchical clustering
1	95	90	75	100
2	98	95	80	105
3	100	80	60	95
4	102	82	65	98
5	104	84	68	100
6	106	86	70	105
7	108	88	72	106
8	110	90	76	107
9	113	92	78	108
10	115	95	80	110

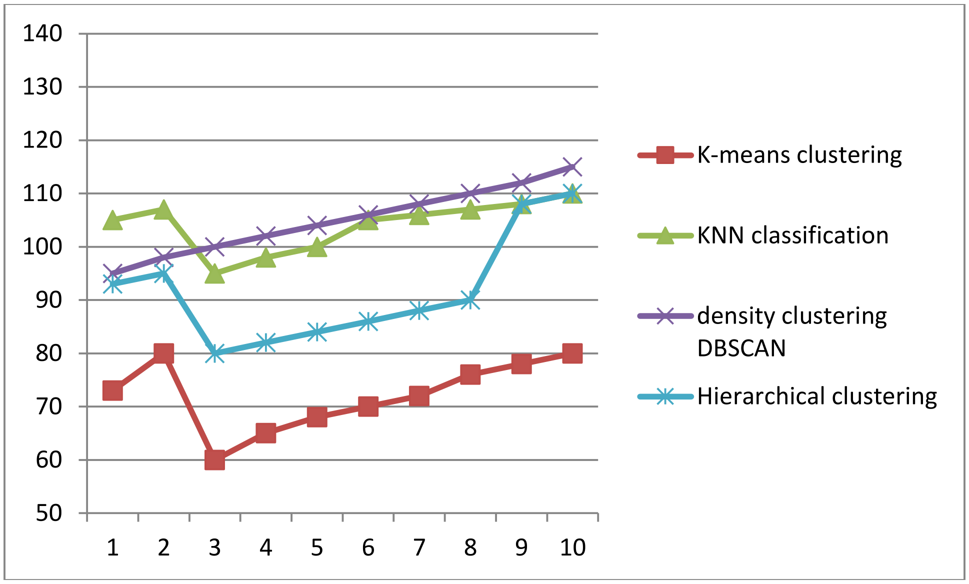

Fig.6 Recall comparison in Experiment 1

Table 6: Comparison of F1 Score in Experiment 1

Serial number	K-means clustering	KNN classification	Density clustering DBSCAN	Hierarchical clustering
1	95	100	75	90
2	98	105	80	95
3	100	95	60	80
4	102	98	65	82
5	104	100	68	84
6	106	105	70	86
7	108	106	72	88
8	110	107	76	90
9	113	108	78	108
10	115	110	80	110

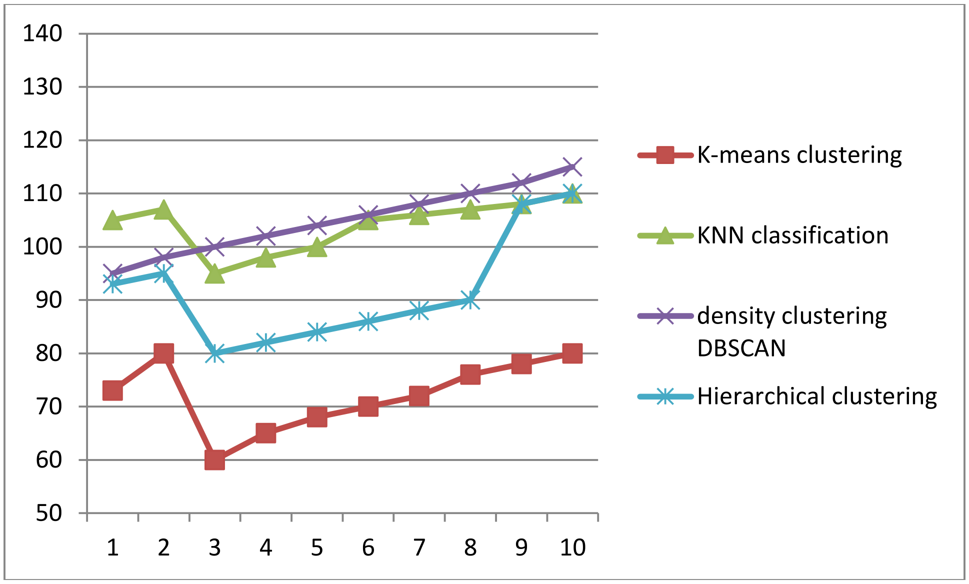

Fig.7 Comparison of F1 Score in Experiment 1

3.1.2 Comparative Experiment 2

This study compares classical K-means clustering, KNN classification, density clustering DBSCAN and wireless network intrusion detection algorithms based on multi-view cosine distance hierarchical clustering to see which is better at finding unknown attack types. It was decided to conduct ten comparison studies on data sets d1, d2, d3, d4, d5, and d6. Figure 8 with table shows the outcomes of the experiment.

Table7: Comparison of ACC in Experiment 2

Serial Number	K-means clustering	KNN classification	density clustering DBSCAN	Hierarchical clustering
1	73	105	95	93
2	80	107	98	95
3	60	95	100	80
4	65	98	102	82
5	68	100	104	84
6	70	105	106	86
7	72	106	108	88
8	76	107	110	90
9	78	108	112	108
10	80	110	115	110

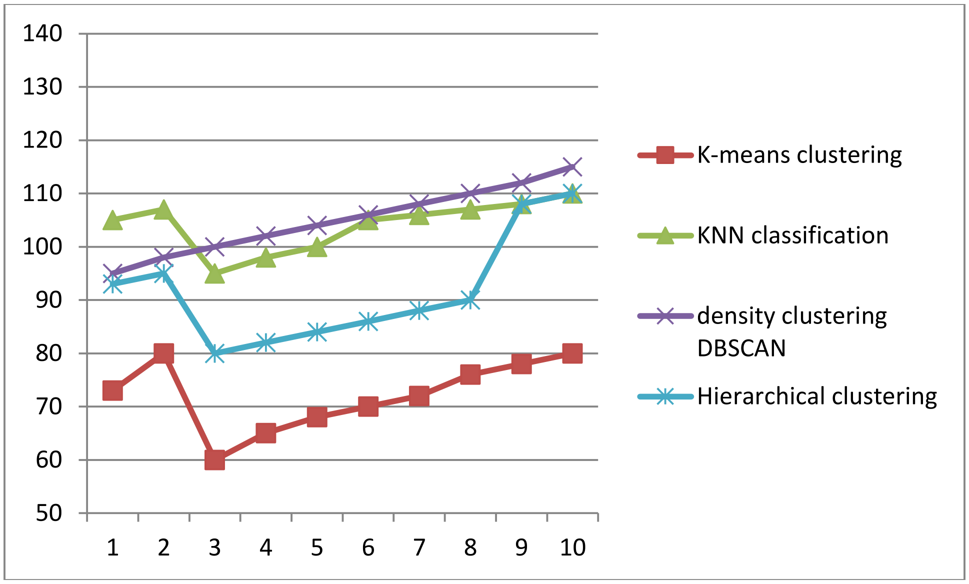

Fig.8 Comparison of ACC in Experiment 2

When compared to typical K-means clustering and KNN classification algorithms, the wireless network intrusion detection method described in this study is more efficient in intrusion detection based on multi-view hierarchical clustering, as demonstrated in the following four trials. The algorithm's detection rate ACC, false detection rate FAR, recall rate Recall, and comprehensive performance F1 have all been dramatically enhanced, as has the identification of new attack types. This new wireless network intrusion detection method has a higher detection rate ACC; a higher recall rate Recall and comprehensive performance F1; and lower false detection rate FAR compared to the old technique based on Euclidean distance hierarchical clustering. A reduction in the dimensionality of the wireless network attack data set AWID through principal component analysis can accurately reflect its initial characteristics. This, in turn, reduces algorithm time complexity and increases algorithm detection efficiency, while also ensuring higher ACC detection rates, recall rate Recall, comprehensive performance F1 and lower false detect rates are maintained. Overall, the time complexity of this work is O(n^2).

IV. Conclusion

This study proposes the use of multi-view cosine distance as a measure of the similarity between data objects in the process of hierarchical clustering, rather than traditional cosine distance, to improve the effectiveness of an unsupervised wireless network intrusion detection method based on clustering. The use of the measuring approach improves the detection rate of the intrusion detection algorithm, while the false detection rate of wireless network data clustering discovers is reduced to a minimum. Even if a more multi-perspective technique to choosing reference points decreases the total reference point set size greatly when compared to a full-grained approach, a bigger reference point set is still required to increase the performance of the intrusion detection algorithm. Afterwards, it's time to devise a more logical and effective approach for selecting reference points and shrinking the quantity of the trial data, in order for the clustering algorithm to run in less time and perform better overall. Further, this paper is extended to other real-life engineering applications such as IoT, Blockchain and metaheuristics.

Data Availability

The data used to support the findings of this study are available from the author upon request (**abahattab@gmail.com**).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors Contributions

Soufiene Ben Othman simulated the methodsand Abdullah Ali Bahattabwrote the paper.

V. References

[1] Q. Wang, S. Wang and Z. Meng, "Applying an Intrusion Detection Algorithm to Wireless Sensor Networks," *2009 Second International Workshop on Knowledge Discovery and Data Mining*, 2009, pp. 284-287, doi: 10.1109/WKDD.2009.92.

[2] J. Tian and M. Gao, "Network Intrusion Detection Method Based on High Speed and Precise Genetic Algorithm Neural Network," *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, 2009, pp. 619-622, doi: 10.1109/NSWCTC.2009.228.

[3] Xiangdong Hu and Runzi Bai, "Research on intrusion detection model of wireless sensor network," *2011 International Conference on Computer Science and Service System (CSSS)*, 2011, pp. 3471-3474, doi: 10.1109/CSSS.2011.5972093.

[4] Q. Duan, X. Wei, J. Fan, L. Yu and Y. Hu, "CNN-based Intrusion Classification for IEEE 802.11 Wireless Networks," *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, 2020, pp. 830-833, doi: 10.1109/ICCC51575.2020.9345293.

[5] J. Tian and M. Gao, "Intelligent community intrusion detection system based on wireless sensor network and fuzzy neural network," *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, 2009, pp. 102-105, doi: 10.1109/CCCM.2009.5268049.

[6] A. Shakil Ahmed and A. Rajeswari, "Intrusion detection in heterogeneous Wireless Sensor Networks with an energy efficient localization algorithm," *2012 International Conference on Recent Trends in Information Technology*, 2012, pp. 389-394, doi: 10.1109/ICRTIT.2012.6206815.

[7] S. Amaran and R. Madhan Mohan, "An Optimal Multilayer Perceptron with Dragonfly Algorithm for Intrusion Detection in Wireless Sensor Networks," *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, 2021, pp. 1-5, doi: 10.1109/ICCMC51019.2021.9418355.

[8] D. Yu, "Research on Anomaly Intrusion Detection Technology in Wireless Network," *2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, 2018, pp. 540-543, doi: 10.1109/ICVRIS.2018.00138.

[9] S. Singh and R. S. Kushwah, "A Study on Intrusion Detection in Wireless Networks by Using Genetic Algorithm Applications," *2014 International Conference on Computational Intelligence and Communication Networks*, 2014, pp. 749-752, doi: 10.1109/CICN.2014.162.

[10] Y. Changguo, Z. Qin, Z. Jingwei, W. Nianzhong, Z. Xiaorong and W. Tailei, "Improvement of Association Rules Mining Algorithm in Wireless Network Intrusion Detection," *2009 International Conference on Computational Intelligence and Natural Computing*, 2009, pp. 413-416, doi: 10.1109/CINC.2009.19.

[11] Y. Mao, "A semantic-based intrusion detection framework for wireless sensor network," *INC2010: 6th International Conference on Networked Computing*, 2010, pp. 1-5.

[12] H. -b. Wang, Z. Yuan and C. -d. Wang, "Intrusion Detection for Wireless Sensor Networks Based on Multi-agent and Refined Clustering," *2009 WRI*

International Conference on Communications and Mobile Computing, 2009, pp. 450-454, doi: 10.1109/CMC.2009.172.

[13] H. Elbahadır and E. Erdem, "Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks," *2021 6th International Conference on Computer Science and Engineering (UBMK)*, 2021, pp. 401-406, doi: 10.1109/UBMK52708.2021.9558928.

[14] S. Tiwari, S. S. Roy, S. Charaborty and A. Kumar, "A novel hybrid model for network intrusion detection," *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, 2013, pp. 685-688, doi: 10.1109/ICGCE.2013.6823522.

[15] L. Li, Y. -h. Li, D. -y. Fu and W. Ming, "Intrusion Detection Model Based on Hierarchical Structure in Wireless Sensor Networks," *2010 International Conference on Electrical and Control Engineering*, 2010, pp. 2816-2819, doi: 10.1109/iCECE.2010.688.

[16] N. K. Mittal, "A survey on Wireless Sensor Network for Community Intrusion Detection Systems," *2016 3rd International Conference on Recent Advances in Information Technology (RAIT)*, 2016, pp. 107-111, doi: 10.1109/RAIT.2016.7507884.

[17] Nayak, N.R., Kumar, S., Gupta, D. et al. Network mining techniques to analyze the risk of the occupational accident via bayesian network. Int J Syst Assur Eng Manag (2022). https://doi.org/10.1007/s13198-021-01574-1

[18] Shobanadevi, A., Tharewal, S., Soni, M. et al. Novel identity management system using smart blockchain technology. Int J Syst Assur Eng Manag (2021). https://doi.org/10.1007/s13198-021-01494-0

[19] Singh, P., Kaur, R., Rashid, J., Juneja, S., Dhiman, G., Kim, J., & Ouaissa, M. (2022). A Fog-Cluster Based Load-Balancing Technique. *Sustainability*, *14*(13), 7961.

[20] Tiwari, P., Pant, B., Elarabawy, M. M., Abd-Elnaby, M., Mohd, N., Dhiman, G., & Sharma, S. (2022). CNN Based Multiclass Brain Tumor Detection Using Medical Imaging. *Computational Intelligence and Neuroscience*, *2022*.

[21] Bhoi, A., Balabantaray, R. C., Sahoo, D., Dhiman, G., Khare, M., Narducci, F., & Kaur, A. (2022). Mining social media text for disaster resource management using a feature selection based on forest optimization. *Computers & Industrial Engineering*, 108280.

[22] Mekala, M. S., Dhiman, G., Srivastava, G., Nain, Z., Zhang, H., Viriyasitavat, W., & Varma, G. P. S. (2022). A DRL-Based Service Offloading Approach Using DAG for Edge Computational Orchestration. *IEEE Transactions on Computational Social Systems*.

[23] Alferaidi, Ali, Kusum Yadav, Yasser Alharbi, Navid Razmjooy, Wattana Viriyasitavat, Kamal Gulati, Sandeep Kautish, and Gaurav Dhiman. "Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles." *Mathematical Problems in Engineering* 2022 (2022).

[24] Gupta, Neha, Kamali Gupta, Deepali Gupta, Sapna Juneja, Hamza Turabieh, Gaurav Dhiman, Sandeep Kautish, and Wattana Viriyasitavat. "Enhanced virtualization-based dynamic bin-packing optimized energy management solution for heterogeneous clouds." *Mathematical Problems in Engineering* 2022 (2022).

[25] Ding, H., Cao, X., Wang, Z., Dhiman, G., Hou, P., Wang, J., ... & Hu, X. (2022). Velocity clamping-assisted adaptive salp swarm algorithm: balance analysis and case studies. *Mathematical Biosciences and Engineering*, *19*(8), 7756-7804.

[26] Mekala, M. S., Srivastava, G., Lin, J. C. W., Dhiman, G., Park, J. H., & Jung, H. Y. (2022). An efficient quantum based D2D computation and communication approach for the Internet of Things. *Optical and Quantum Electronics*, *54*(6), 1-19.

[27] Alferaidi, A., Yadav, K., Alharbi, Y., Viriyasitavat, W., Kautish, S., & Dhiman, G. (2022). Federated Learning Algorithms to Optimize the Client and Cost Selections. *Mathematical Problems in Engineering*, *2022*.

[28] Zeidabadi, F. A., Dehghani, M., Trojovský, P., Hubálovský, Š., Leiva, V., & Dhiman, G. (2022). Archery algorithm: A novel stochastic optimization algorithm for solving optimization problems. *Computers, Materials and Continua*, *72*(1), 399-416.

[29] Yadav, K., Alshudukhi, J. S., Dhiman, G., & Viriyasitavat, W. (2022). iTSA: an improved Tunicate Swarm Algorithm for defensive resource assignment problem. *Soft Computing*, *26*(10), 4929-4937.