SENTIMENTAL ANALYSIS OF FIRMWARE ATTACKS IN WIRELESS SENSOR NETWORKS USING ADAPTIVE ROUTING IN COMPARISON WITH THE NOVEL DISTRIBUTION ALGORITHM TO IMPROVE PRECISION

B. Pavan Kumar[1],V. Karthick[2*]

Article History: Received: 12.12.2022 **Revised:** 29.01.2023 **Accepted:** 15.03.2023

Abstract

Aim: The Aim of this Research paper is Analysing the security over the Firmware attacks in Wireless Sensor Network by using the Novel Distribution algorithm and Adaptive Routing algorithm(AR) classification Algorithms.
Materials and Methods: The study contains the survey among the Different operating systems such as FreeRTOS, POSIX or WIN32.And there are nearly 10 simulators to take a survey among these. Here the number of groups is 2 and group1 is Distribution algorithm (79.50%) and group2 is Adaptive Routing(81.25%) and the sample output size is 32.
Result: The performance has been improved in terms of accuracy for the novel Distribution algorithm with 79.50% while the Adaptive Routing Algorithm has shown accuracy of 81.25%. The mean 85.49, mean accuracy detection is ±1SD and significant value is .0424 ($p < 0.05$) from an independent sample T test with gpower value of 80.
Conclusion: The final outcome of the Distribution algorithm is found to be more significantly more accurate than the Adaptive routing algorithm.

Keywords: Wireless Sensor Network, Attack Simulation, Power Consumption, Distribution Algorithm, Adaptive Routing Algorithm.

[1]Research Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu,India. Pincode: 602105.
[2*]Project Guide, Department of Computer Science and Engineering, Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu, India. Pincode: 601205.

1. Introduction

The facilities of sensor deployment and the cost reduction have raised the use of wireless sensor networks. These days we find networks in industrial monitoring, environmental data, home automation, fire detection, medical or even in the military. Most of the applications are deployed to monitor an area and to have a reaction when they record the critical factor. Attacks over these different aspects are Sinkhole attacks that should be caused by malicious nodes attacking directly the data, which roam near the sink, because sink is the point which catches the maximum data on the entire network. To make this attack happen the malicious node should offer the quickest route to reach the sink by using a powerful connection (Bhola et al. 2021).

The other specified attack amongst these is a kind of attack based on the kind of sensor. An attacker will turn by physical means the response of the sensor. For example, it is like a light as flame on before the therma; sensor or light a lamp in front of a brightness sensor (Ghous et al. 2021). The Sybil attack is also malicious which is divided into multiple sensors. If the routing table is wrong, it is used to modify which is wrong. A malicious node which is divided into multiple nodes has an important advantage for electing a cluster head with getting a higher number of votes to a particular node, it compromises the neighbour nodes to be a cluster head.

To detect these attacks, malicious attacks on wireless sensor networks researchers are finding several ways to overcome this particular scenario (Pineda et al. 2015). Radio jamming is the type of attack that sends the radio waves to the same frequency that is used for the wireless sensor networks if the node is in a transport medium which is flooded by the radio interfaces (Fang et al. 2016). In order to overcome these attacks over the wireless sensor networks the distributive algorithm is an efficient algorithm that gives the passive results but here on this particular attacks routing algorithm is much more efficient than the distributive algorithm, adaptive shows a little bit more accuracy than the distributive algorithm (Gabsi et al. 2021).Our team has extensive knowledge and research experience that has translated into high quality publications(Pandiyan et al. 2022; Yaashikaa, Devi, and Kumar 2022; Venu et al. 2022; Kumar et al. 2022; Nagaraju et al. 2022; Karpagam et al. 2022; Baraneedharan et al. 2022; Whangchai et al. 2022; Nagarajan et al. 2022; Deena et al. 2022)

A mechanism used to detect the malicious nodes (Ghous et al. 2021).The main Aim is to detect and giving the measures to avoid the firmware attacks amongst the wireless sensor networks (Royer and Perkins, n.d.).This sometimes leads to restricting to finding the solutions for the firmware attacks.The main Aim is to detect and give the measures to avoid the firmware attacks amongst the wireless sensor networks.

2. Materials and Methods

This research paper was carried out in the Department of Networking Laboratory of Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences. This study involves 2 groups and group 1 is the novel Distribution algorithm (79.50%) and group 2 is Adaptive Routing algorithm(81.25%). The total number of groups for this are two groups (Liu, Peng, and Zhong 2021). Group one refers to the existing system, and Group two refers to the proposed system. The total number of samples are 32 , out of which 16 are the samples for the first group and the remaining 16 are used as samples for the second group. Size was calculated using previous study results (Holt and Huang 2010).The number of samples that are taken are from the previous study by setting confidence interval as 85% and along with g power as 80%.

In addition, it is important to notice that the virtual platform provides estimations that are useful plane for no-attack cases. The total energy consumption of the linear topology is lower than for the other topologies. The interpretation of the node Power Consumption moreover enables the interpretation of the node shower life that is an essential parameter of WSN. The time of all simulations is similar and it is less than 1 min depending on the traffic network. simulation times of the experiments included in this section which are performed in core i5-3470 3.20 GHz with 4 Gb RAM in a Fedora 32 bits. This is a very low simulation time when taking into worth that the simulated time is 1 h

Adaptive Routing

Adaptive routing, also called dynamic routing, is a process of determining the optimal path that a data packet should follow through a network to reach a specific destination. Adaptive routing can be compared to a commuter taking a different route to work after learning that traffic on their usual route will be supported. Adaptive routing uses routing algorithms and protocols that read and respond to changes in network topology. Besides Open Shortest Path First (OSPF), other routing protocols that facilitate adaptive routing include Intermediate System to Intermediate System (ISIS) Protocol for large networks such as the Internet and Routing Information Protocol (RIP) for local traffic.

The most related theory of Adaptive routing protocols was brought up by Perkins(Royer and

Perkins, n.d.) DSDV (Dynamic Destination-Sequenced Distance-Vector Routing Protocol). This is a table-driven routing protocol. The memory of every sensor node has a forwarding table and a ventilated one. Forwarding table is a routing table, which contains destination-node field, next node field, hop-number field, sequence-number field Attack Simulation and time-adjustment field(Holt and Huang 2010). The value of sequence-number will multiply and its main function is to indicate the new and old condition. Thus the value stored in the sensor is unchangingly the largest, which ensures the routing path is the newest. Advertised table sustains the records of links(Kim et al. 2020). As long as the status changes, the documents inside the advertised table will vary.Various routing protocols have various methods to update the routing table.

In this table the the destination should be started at 1 and carried upto 7 and the next value should be swing between the 3 and 5. Sequence should be started at the ID50-1 and its time is T01-3 and ends up at the sequence ID62-7 and its time is T02-3(Chabalala, Muddenahalli, and Takawira 2011)**.**

Adaptive routing, also called dynamic routing, is a process of determining the optimal path that a data packet should follow through a network to reach a specific destination. Adaptive routing can be compared to a commuter taking a different route to work after learning that traffic on their usual route will be supported. Adaptive routing uses routing algorithms and protocols that read and respond to changes in network topology. Besides Open Shortest Path First (OSPF), other routing protocols that facilitate adaptive routing include Intermediate System to Intermediate System (ISIS) Protocol for large networks such as the Internet and Routing Information Protocol (RIP) for local traffic.

Thus the value stored in the sensor is unchangingly the largest, which ensures the routing path is the newest. Advertised table sustains the records of links(Kim et al. 2020). As long as the status changes, the documents inside the advertised table will vary.Various routing protocols have various methods to update the routing table.

In this table the the destination should be started at 1 and carried upto 7 and the next value should be swing between the 3 and 5. Sequence should be started at the ID50-1 and its time is T01-3 and ends up at the sequence ID62-7 and its time is T02-3 (Chabalala, Muddenahalli, and Takawira 2011).

Adaptive Routing Algorithm Steps

Step 1: Begin the program with a loop of if to check the actual values of D as well as A.

Step 2: Further step forward to mod P-L(j) is minimum for D or A which are equal.

Step 3: If the above steps are not accurate then we start the else to bring the packets

Step 4: Let assume that the X and Y are shl of D and A as well R(x) and R(y) both are not equal

Step 5: In case of X and Y are equal then the R(x) and R(y) are forwarded to Minimum other Step 6 : Case is to X is greater than Y then only R(x) is not equal to null or else forward to R(y)

Step 6: On to the last case that is to be forwarded to Z then it will be maximum of x and y.

Step 8: Here the Z belongs to buckets of Z with respect to the First and Second.

Step 9: This is the Steps for initialising the base algorithm for Novel attack simulation.

Distribution Algorithm

Distribution algorithm is designed to run in computer hardware to build interconnected processors. Due to the interconnections with the computer hardware its impact should be but little than the Adaptive routing algorithm. The attacks over the wireless sensor attacks should be a problem and by this algorithm there should be a very little impact among the Sensors because it's a matter for out of the system. On coming to the parallel algorithm which is part of overriding a bit of solution finder for these types of attacks in the Distribution algorithm.

The function of the subtype parallel algorithm which comes under the Distribution algorithm is to first find the distance of ipp and nipp and reserve it to send the packets. And checks the neighbour list and sends the hello packets to test the conditions and check that the network is attack free or not. Calculates the weights using the equation and analyses the best weight and current weight and sends the RREQ packets to show the algorithm whether it is flexible or not. And also to calculate the amount of risk that should be for a device from the firmware attacks. And sends the RREQ packets to all the neighbours in the list and broadcasts all the packets to the neighbours. Now the RREQ packets are there at their destinations to do the optimal forwarding path and generate the RREP packets back at source to tell the attacks over the network should be cleared.

Steps for Distribution Algorithm

Step 1: Initialise the for loop for the neighbour list and if the n ipp is equal to distance ipp then
send the packet and ipp of n.

Step 2: End the module. And initialise the for loop again for all the neighbour list for n send the
hello packets and again end the for loop.

Step 3: For all n in neighbour list do the calculation for weight using the equation.End for

Step 4: Select the best weight from the neighbour list and calculate the current weight again
using the same equation 1. If the current weight is less than or equal to the best weight

then insert the best weight into the RREQ packet.

Step 5: Then the Distribution algorithm with neighbour list and best weight are equal to the

nexthop then send the packets and nexthop.

Step 6: Else insert the current weight into RREQ packets and broadcast RREQ packets to all

neighbours and if it should end for sure.

Step 7: For all RREQ packets to be in destination do the optimal forwarding path and end the for

Loop and generate RREP packets and send it back to the source.

Statistical Analysis

The data for Security analysis of wireless network sensors were collected from the url website that contains over 60 participants in testing this system. The statistical software used for implementation in IBM SPSS version 21. The independent variables of the data are accuracy, Standard deviation and standard mean error and dependent variables in the data are Eye aspect ratio of x and y axis as parameters that is considered in the task. The independent sample T test analysis is carried out in this research work.

3. Results

Additionally, the virtual platform estimations are quite accurate. In this example, the estimated error of the virtual platform is only 8%. In terms of power consumption and execution time,the verism of the results is similar to other native-simulation based approaches. Thus,the proposed virtual platform can be used to evaluate the WSN network policies plane when the WSN is not deployed and it is not possible to perform real measurements by using the Distribution algorithm it gives the accuracy of 79.50%.

Table 1 shows the Adaptive routing algorithm forwarding table which shows the destination Sequence and Time. The time starts at the T01-3 and ends at T02-3

Table 2 shows the For getting the precision value we have to compare the data description between the proposed and the existing algorithm.

Table 3 shows the comparative study between the Distribution algorithm and the Adaptive Routing algorithm with precision rate 81.25%.

Table 4 indicates the Group statistics T-Test for existing algorithm Mean (81.2540) and Distribution algorithm (79.5050) with the sample size 10. There is a statistically slight difference in the SD accuracy of the two algorithms. The Adaptive Algorithm had the highest accuracy and the (5.04543) Distribution Algorithm(4.49504).

4. Discussion

From the result, The Adaptive algorithm (81.25%) appears to be better than the Distribution algorithm (79.50%). The values of the Effective precision are analysed statistically and the difference is found out by plotting the graph against the algorithms.

Similar results related to the Distribution algorithm are significantly more efficient in security analysis on the wireless sensor network of the user compared to the existing algorithm(Mao and Fidan 2009), that is the Adaptive routing algorithm (Rachamalla and Kancherla 2016). The dataset containing a large number of images is given as input into both the algorithms, and the accuracy rate (Shaikh and Wismuller 2017) of prediction is obtained for the existing and the proposed algorithms. These values obtained are used for analysis and comparison for precision.

The similar findings are implemented by the security analysis on the networking based technologies.If the device or node can be going to effect by the any security issue the Distribution algorithm will be divide that node information into several nodes and it should be depend on the path distance(Parsapoor and Bilstrup 2013).So easily the attack will be founded between the nodes and eventually the problem will be solved in a very less time. On coming to the adaptive routing it is only based on the shortest path it would not divide into nodes(Luo et al. 2018).So comparing with adaptive routing Distribution algorithms shows more precision.

On going to the further research among the Security analysis of the wireless network sensor this divide and detection of the attacks make a crucial role which is named as the Distribution algorithm(Sohraby, Minoli, and Znati 2007). By this the detection distributed algorithm computes the least path cost from source to destination and it changes iteratively with size. On talking the size of the sensor as a main aspect it fails at analysing the attack on sensor size as well what if the small sensor had a big attack.

5. Conclusion

The research study found that the proposed Distribution algorithm shows more precision than the given adaptive routing algorithm.The precision of the proposed Distribution Algorithm is significantly 79.50%. Hence, Using the Adaptive Algorithm gives better results than the existing algorithm means the Distribution algorithm gives the precision of 81.25%.

Declarations

Conflict of Interest

No conflict of interest in this manuscript

Author Contribution

Author BPK is involved in data collection, data analysis and manuscript writing. Author VK was involved in conceptualization, data validation and critical review of the manuscript.

Acknowledgements

The authors would like to express their gratitude towards Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Formerly known as Saveetha University) for providing the necessary infrastructure to carry out this work successfully.

Funding

Thankful for the following organisations for providing financial support that enabled us to complete the study.

1. Vee Eee Technologies Solution Pvt.Ltd., Chennai.
2. Saveetha University
3. Saveetha Institute of Medical and Technical Sciences
4. Saveetha School of Engineering.

6. References

Baraneedharan, P., Sethumathavan Vadivel, C. A. Anil, S. Beer Mohamed, and Saravanan Rajendran. 2022. “Advances in Preparation, Mechanism and Applications of Various Carbon Materials in Environmental Applications: A Review.” *Chemosphere*. https://doi.org/10.1016/j.chemosphere.2022.134596.

Bhola, Jyoti, Mohammad Shabaz, Gaurav Dhiman, S. Vimal, P. Subbulakshmi, and Sunil Kumar Soni. 2021. “Performance Evaluation of Multilayer Clustering Network Using Distributed Energy Efficient Clustering with Enhanced Threshold Protocol.” *Wireless Personal Communications*, August, 1–15.

Chabalala, S. C., T. N. Muddenahalli, and F. Takawira. 2011. “Cross-Layer Adaptive Routing Protocol for Wireless Sensor Networks.” *IEEE Africon ’11*. https://doi.org/10.1109/afrcon.2011.6072005.

Deena, Santhana Raj, A. S. Vickram, S. Manikandan, R. Subbaiya, N. Karmegam, Balasubramani Ravindran, Soon Woong Chang, and Mukesh Kumar Awasthi. 2022. “Enhanced Biogas Production from Food Waste and Activated Sludge Using Advanced Techniques – A Review.” *Bioresource Technology*. https://doi.org/10.1016/j.biortech.2022.127234.

Fang, Qing-Po, Yong-Jun Hu, Si-Han Wang, and Wen Gu. 2016. “A Security Analysis of Wireless Network.” *Wireless Communication and Network*. https://doi.org/10.1142/9789814733663_0045.

Gabsi, Souhir, Vincent Beroulle, Yann Kieffer, Hiep Manh Dao, Yassin Kortli, and Belgacem Hamdi. 2021. “Survey: Vulnerability Analysis of Low-Cost ECC-Based RFID Protocols against Wireless and Side-Channel Attacks.” *Sensors* 21 (17). https://doi.org/10.3390/s21175824.

Ghous, Mujtaba, Ziaul Haq Abbas, Ahmad Kamal Hassan, Ghulam Abbas, Thar Baker, and Dhiya Al-Jumeily. 2021. “Performance Analysis and Beamforming Design of a Secure Cooperative MISO-NOMA Network.” *Sensors* 21 (12). https://doi.org/10.3390/s21124180.

Holt, Alan, and Chi-Yu Huang. 2010. *802.11 Wireless Networks: Security and Analysis*. Springer Science & Business Media.

Karpagam, M., R. Beaulah Jeyavathana, Sathiya Kumar Chinnappan, K. V. Kanimozhi, and M. Sambath. 2022. “A Novel Face Recognition Model for Fighting against Human Trafficking in Surveillance Videos and Rescuing Victims.” *Soft Computing*. https://doi.org/10.1007/s00500-022-06931-1.

Kim, Beom-Su, Sangdae Kim, Kyong Hoon Kim, Tae-Eung Sung, Babar Shah, and Ki-Il Kim. 2020. “Adaptive Real-Time Routing Protocol for (,)-Firm in Industrial Wireless Multimedia Sensor Networks.” *Sensors* 20 (6). https://doi.org/10.3390/s20061633.

Kumar, P. Ganesh, P. Ganesh Kumar, Rajendran Prabakaran, D. Sakthivadivel, P. Somasundaram, V. S. Vigneswaran, and Sung Chul Kim. 2022. “Ultrasonication Time Optimization for Multi-Walled Carbon Nanotube Based Therminol-55 Nanofluid: An Experimental Investigation.” *Journal of Thermal Analysis and Calorimetry*. https://doi.org/10.1007/s10973-022-11298-4.

Liu, Guiyun, Baihao Peng, and Xiaojing Zhong. 2021. “Epidemic Analysis of Wireless Rechargeable Sensor Networks Based on an Attack-Defense Game Model.” *Sensors* 21 (2). https://doi.org/10.3390/s21020594.

Luo, Chuanwen, Wenping Chen, Jiguo Yu, Yongcai Wang, and Deying Li. 2018. “A Novel Centralized Algorithm for Constructing Virtual Backbones in Wireless Sensor Networks.” *EURASIP Journal on Wireless Communications and Networking*. https://doi.org/10.1186/s13638-018-1068-7.

Mao, Guoqiang, and Baris Fidan. 2009. *Localization Algorithms and Strategies for Wireless Sensor Networks: Monitoring and Surveillance Techniques for Target*

Tracking: Monitoring and Surveillance Techniques for Target Tracking. IGI Global.

Nagarajan, Karthik, Arul Rajagopalan, S. Angalaeswari, L. Natrayan, and Wubishet Degife Mammo. 2022. "Combined Economic Emission Dispatch of Microgrid with the Incorporation of Renewable Energy Sources Using Improved Mayfly Optimization Algorithm." *Computational Intelligence and Neuroscience* 2022 (April): 6461690.

Nagaraju, V., B. R. Tapas Bapu, P. Bhuvaneswari, R. Anita, P. G. Kuppusamy, and S. Usha. 2022. "Role of Silicon Carbide Nanoparticle on Electromagnetic Interference Shielding Behavior of Carbon Fibre Epoxy Nanocomposites in 3-18GHz Frequency Bands." *Silicon*. https://doi.org/10.1007/s12633-022-01825-1.

Pandiyan, P., R. Sitharthan, S. Saravanan, Natarajan Prabaharan, M. Ramji Tiwari, T. Chinnadurai, T. Yuvaraj, and K. R. Devabalaji. 2022. "A Comprehensive Review of the Prospects for Rural Electrification Using Stand-Alone and Hybrid Energy Technologies." *Sustainable Energy Technologies and Assessments*. https://doi.org/10.1016/j.seta.2022.102155.

Parsapoor, Mahboobeh, and Urban Bilstrup. 2013. "A Centralized Channel Assignment Algorithm for Clustered Ad Hoc Networks." *2013 IEEE Conference on Wireless Sensor (ICWISE)*. https://doi.org/10.1109/icwise.2013.6728784.

Pineda, Miguel Garcia, Jaime Lloret, Symeon Papavassiliou, Stefan Ruehrup, and Carlos Becker Westphall. 2015. *Ad-Hoc Networks and Wireless: ADHOC-NOW 2014 International Workshops, ETSD, MARSS, MWaoN, SecAN, SSPA, and WiSARN, Benidorm, Spain, June 22--27, 2014, Revised Selected Papers*. Springer.

Rachamalla, Sandhya, and Anitha Sheela Kancherla. 2016. "A Two-Hop Based Adaptive Routing Protocol for Real-Time Wireless Sensor Networks." *SpringerPlus*. https://doi.org/10.1186/s40064-016-2791-3.

Royer, E. M., and C. E. Perkins. n.d. "An Implementation Study of the AODV Routing Protocol." *2000 IEEE Wireless Communications and Networking Conference. Conference Record (Cat. No.00TH8540)*. https://doi.org/10.1109/wcnc.2000.904764.

Shaikh, Farrukh Salim, and Roland Wismuller. 2017. "Centralized Adaptive Routing in Multihop Cellular D2D Communications." *2017 2nd International Conference on Computer and Communication Systems (ICCCS)*. https://doi.org/10.1109/ccoms.2017.8075287.

Sohraby, Kazem, Daniel Minoli, and Taieb Znati. 2007. *Wireless Sensor Networks: Technology, Protocols, and Applications*. John Wiley & Sons.

Venu, Harish, Ibham Veza, Lokesh Selvam, Prabhu Appavu, V. Dhana Raju, Lingesan Subramani, and Jayashri N. Nair. 2022. "Analysis of Particle Size Diameter (PSD), Mass Fraction Burnt (MFB) and Particulate Number (PN) Emissions in a Diesel Engine Powered by Diesel/biodiesel/n-Amyl Alcohol Blends." *Energy*. https://doi.org/10.1016/j.energy.2022.123806.

Whangchai, Niwooti, Daovieng Yaibouathong, Pattranan Junluthin, Deepanraj Balakrishnan, Yuwalee Unpaprom, Rameshprabu Ramaraj, and Tipsukhon Pimpimol. 2022. "Effect of Biogas Sludge Meal Supplement in Feed on Growth Performance Molting Period and Production Cost of Giant Freshwater Prawn Culture." *Chemosphere* 301 (August): 134638.

Yaashikaa, P. R., M. Keerthana Devi, and P. Senthil Kumar. 2022. "Advances in the Application of Immobilized Enzyme for the Remediation of Hazardous Pollutant: A Review." *Chemosphere* 299 (July): 134390.

TABLES AND FIGURES

Table 1. This is the forwarding table for the Adaptive Routing Algorithm.

Destination	**Next**	**Hop**	**Sequence**	**Time**
1	3	1	ID50-1	T01-3
2	5	4	ID36-2	T01-3
3	3	0	ID28-3	T01-3

4	5	1	ID46-4	T01-3
5	5	3	ID15-5	T01-3
6	5	2	ID70-6	T02-3

Table 2. For getting the precision value we have to compare the data description between the proposed and the existing algorithm.

S.No	**Attribute**	**Value**	**Description**
1.	No. of observation	Integer	The number of data used in the system.
2.	Co-ordinates	Integer	The x and y axis coordinates of the eye.

Table 3. Comparative study between the Distribution Algorithm and the Adaptive Routing algorithm with precision rate 81.25%

S.No	Distribution Algorithm	AdaptiveRouting
1.	72.36	76.72
2.	73.69	77.21
3.	75.69	79.35
4.	76.88	76.42
5.	78.33	78.32
6.	79.78	80.55
7.	81.65	83.73
8.	83.64	84.27
9.	85.69	86.76
10.	87.34	89.21

Table 4. Group statistics T-Test for existing algorithm Mean (81.2540) and Distribution algorithm (79.5050) with the sample size 10. There is a statistically slight difference in the SD accuracy of the two algorithms. The Adaptive Algorithm had the highest accuracy and the (5.04543) Distribution Algorithm(4.49504).

Pair 1	**N**	**Mean**	**Std. deviation**	**Std.Error Mean**
Distribution Algorithm	10	79.5050	4.49504	1.42146
Adaptive Routing	10	81.2540	5.04543	1.59550

Table 4. An Independent sample T-test is performed for the two groups for significance and standard error determination. The two-Tailed Significance value is 0.001 ($p<0.05$) and it is statistically significant.

		Levene's Test for Equality of Variance		T-test for Equality of Means						
	Equal Variance	F	Sig	t	df	Sig(2-tailed)	Mean Difference	Std.Er ror Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Efficiency	**Assumed**	.097	.760	.818	18	.0424	1.749	2.136	-2.740	6.238
	Not Assumed			.818	17.765	.0424	1.749	2.136	-2.744	6.242

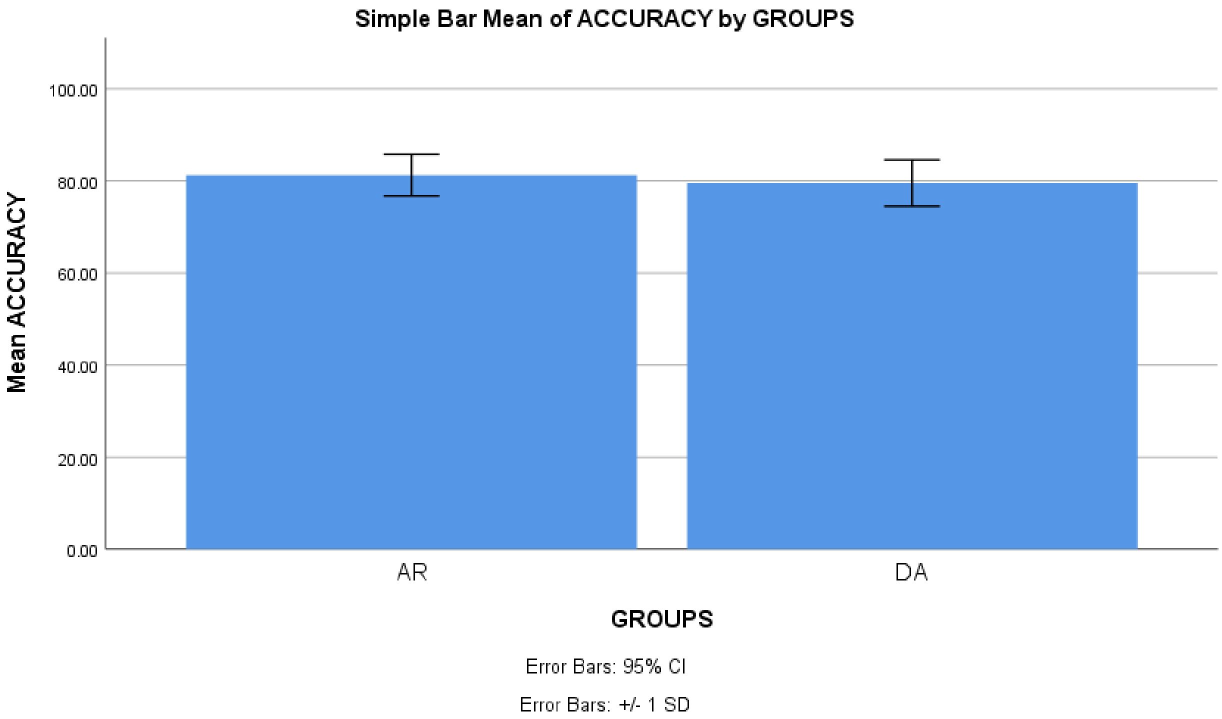

Fig.1. Bar chart representation of the comparison of mean accuracy of the proposed and the existing algorithm. The accuracy of the prediction of the proposed algorithm is found to be 79.50% and the proposed algorithm gives better results compared to the existing algorithm that has accuracy of 81.29% the mean accuracy detection is ±1 SD.