Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC200200

Design Secure WSN with Advancement in Finding Rouge Access Point with Soft Computing Tools

Abhijit S.Bodhe[a,1], Pravin Dhanrao[b], Abhimanyu Sangle[c], Jagdisha N.[d]

[a]*Departmentof CSE ,Sanjivani College of Engineering, Kopargaon 423603,*
[b]*Savitribai Phule Pune University, Pune, Maharashtra, India*
[c]*KBP Polytechnic, Kopargaon*
[d]*Canara College of Engineering, Manglore*

Abstract. Now a days wireless communication is become very vast, important and easy to access with multiple wireless sensor network in existence as it having very less cost associated and easily available via multiple mobile devices with sensors to create a hotspots, It creates a potential threat for community using wireless media for communicating some secure information like banking passwords, military information, biometric data etc. on unsecured network. This proposed paper will expose one of such potential threat Rouge Access Point (RAP) detection by making the use of soft computing prediction tool in our case fusion of neural network with fuzzy logic known as neuron-fuzzy method and design a fuzzy controller (FLC) to find such RAP & secure the existing wireless network where multiple sensors are actively working in real time to provide the real time data.

Keywords. Unsecured Network, Rouge Access Point (RAP), Neural Network, neuron-fuzzy method Fuzzy Logic, FLC, WSN

1. Introduction

1.1 Why and what is RAP:-

Rogue Access Point (RAP) is an access point connects wireless devices which are setup on a secure and safe network without having external permission from a network admin [1] it may be added by any managed worker or a attacker which does not matter. It is very much easy technically also practically for a good company or organization worker or any owner or employee to installs a Soft Access Points (SAP), a less cost wireless router's or access points which make access network or entire data from remote devices which become simpler. Perhaps, it is possible that these will manipulate and configure like it is not closed for security or with having less security that generally can allow access to not authorized user or malicious hacker for data to be accessible in the network. If any malicious attacker or employee installing access point in the secure network they can easily able to execute multiple types of vulnerability scanners, and without having physical existence into the nearby location

[1] Abhijit S.Bodhe, Sanjivani College of Engineering, Kopargaon ,
Email id:bodhe.abhijit@gmail.com

they can attack remotely on wireless network from any reception area, building located nearby, side car parking area or even with any high gain antenna, located several miles away from the location as set trap.To prevent such types of possible unauthorized installations of rogue access points, network admin has must be an install wireless intrusion prevention systems which regularly monitored and detects available radio bandwidths for not authorized access point exists in the network under-monitored.

Generally, a presence of multiple wireless APs can be detected in real time environment nearby of any general enterprise network , now days is a very common phenomenon, which includes manage access points in the totally secured wireless network with available access point or points in the nearby possible area. A Wireless Intrusion Prevention System (WIPS) will dose the work of checking or rechecking and monitoring such multiple APs on a frequent basis for learning and checking the existence of Rogue Access Points (RAP) among them are present or not present.In order to detect that RAP existence in network two conditions has to test and well verified:

1. The AP under observation is present in the list of the APs which is maintained by the network administrator for a secure network.

2. The access point device connected to the secure network and will not cause any harm in the present and possibly future to the network because of its existence in a secured network managed by the network admin.

The first condition is much easier to resolve and test, only compare MAC address of wireless device known as BSSID of AP with the maintained or sometimes managed APs SSID from list available backend. It gives the list of AP in the network without the authority of network admin.

However, the second criteria to be tested will become more challenging or complex in the consideration of the following factors:

1. It Needs covering all possible types of AP devices in WSN, Example bridging the networks or nodes, NAT also known as routers, encrypted or unencrypted wireless links, various types of possible relations in wireless MAC and well as wired address for multiple APs with SAP also has been checked.

2. Required to determine all possible access points' connection with Acceptable Response Time (ART) for entire networks monitored under network admin.

3. The necessity to sometimes avoid or remove both possibilities of False Positives (FP) and False Negatives (FN) are illustrated in detail with three possible conditions [2]. A). FP generally occurs when the WIPS monitors or finds an APs are not actually connected to the secured networks and working like the wired RAPs for the network. Frequently as FP result in max utilization of admin s bandwidth utilised to finding these rouge AP or devices. Possibility of these FP's will also create some resistance which enables auto-blocking of wireless or sometimes wired rogue devices because of danger of blocking or closing nearby APs exists in the network

b) FN usually occurs when WIPS unable to identify an AP which is part of secure network like a rogue device with wired connection where FN results in security loopholes [10]. This issue must need to be traced and close in time for the betterment of secure network by network admin itself.

c) Generally, unauthorized APs are found to be connected to the secure networks; these are the RAPs of the first kind traditionally known as the rogue access point with wired connection. On the verge side of this, if the not authorized AP is find not connected to the secure networks, it is external APs which not cause any harm to the network. Among the external possible APs, if any is identified to be mischievous in network or creates any risks like sometimes settings can be attracted or sometimes had already was part of secure network wireless clients, it's labelled as a RAP of type two, which is known an evil twin type of attack [2].

1.2 Fuzzy Logic a Concept

Fuzzy logic is a collection of logical variables, includes the truthiness of variables which includes fractional numbers lies in the large range of zero (0) and One (1) including both. Fuzzy logic is traditionally used to handle the basic concept of truth sometime partial having some numerical values in real world, where the value of truthiness having the boundary of total true or sometimes total false values inclusivity [3], with this core concept, Boolean logic as discussed the truth values of variables are sometimes only are the integer values either 0 or 1 also called as crisp values of truthiness.The term fuzzy logic was introduced in the year 1965, the naive method of fuzzy-set theory by scientist Lotfi Zadeh[4]. Fuzzy logic had been in existence from 1920s, known as infinite-valued logic noted by super minds Lukasiewicz and Tarski.[5].

1.3 Applying truth values

In any application, we might have to decide various possible sub-range or ranges of measured or defined continuous variables for the proposed systems [10]. For simple understanding consider a simple and basic example, a temperature measurement system for anti-lock brakes (ABS) are having multiple separate and unique membership functions. While defining a particular temperature ranges on a real-time scale we needed to control the brakes properly in proper proportion. Generally during this process of mapping the functions each time same temperature value or values map to a truth value in the partial truth range of 0 to 1 as proposed by truth table for ABS inference system. These truth values proposed after certain observations can easily be use to identify how the parameters are controlled to control another output parameter of ABS [7].

2. Proposed System architecture

We use fuzzy logic tool [29] to find the rouge access point exists in environment for this we use traditional algorithm proposed, in which 5 parameters we extract from network and analyze the existence of rouge AP in network. The algorithm will work simply based on rules proposed in given table for different parameters in any wireless network [9].

In proposed system we think about different parameters as detection engine Preemption engine and threshold values as authorized or not authorized in each phase we check about total 5 parameters initially we check for two parameters and then update to 2 parameters as set and then total 3 parameters are compared to find actual access point is rouge or not which shoes improvement on traditional methods as it gives good results from actual CCM protocols [11].

The partial truth table is shared based on which the prediction is made to make the possible conclusion for access point whether it will be having rouge or not. The Mamdani's inference method will use to find the conclusion of the system and check the RAP existence in the network.[12]

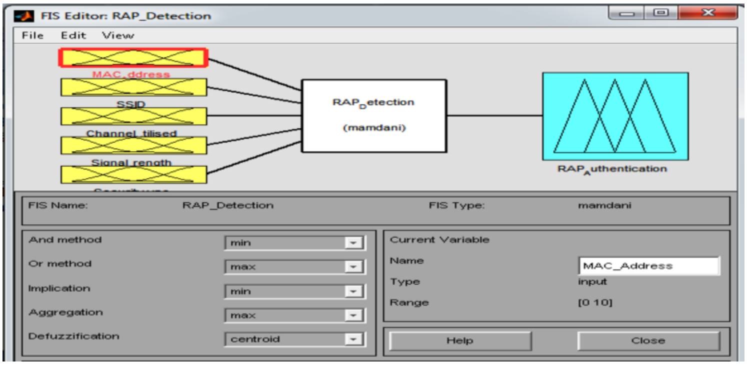
Table 1. Proposed Method Parameters Selection

MAC	**SSID**	**Channel ID**	**Secur**	**Signal Strength**	**Type**
DETECTION-Phase I		**PREEMPTION-Phase II**			**Decision**
Registered	Unregistered	Know	Known	Correct	Authorize
Unregistered	Register	Know	Known	Correct	Authorize
Registered	**Registered**	**Unknown**	**Unknown**	**Incorrect**	**Authorized**
Unregistered	Registered	Unknown	Unknown	Incorrect	Unauthorized
Unregistered	**Unregistered**	**Unknown**	**Unknown**	**Incorrect**	**Unauthorized**
Registered	Registered	Unknown	Known	Correct	Unauthorized
Unregistered	Registered	Unknown	Known	Correct	Unauthorized
Unregistered	Unregistered	Unknown	Unknown	Incorrect	Authorize
Registered	Registered	Unknown	Unknown	Incorrect	Authorize
Unregistered	Registered	Unknown	Known	Correct	Authorized
Unregistered	Registered	Unknown	Known	Correct	Unauthorized

3. Proposed Prototype

The proposed method is explained with following diagram with working flow and shows the results in partial Fuzzification process and Diffuzification using centric method. As per figure1 the proposed system is shared with all five possible partial parameters and its possible outcomes as per table1

Figure 2 indicated rule based designed as per need of the proposed system architecture. Figure 3 shows membership function mapping with different rules to give desire output. Figure 4 analyze how to parameters plays vital role while selecting the proper access point for detection of RAP

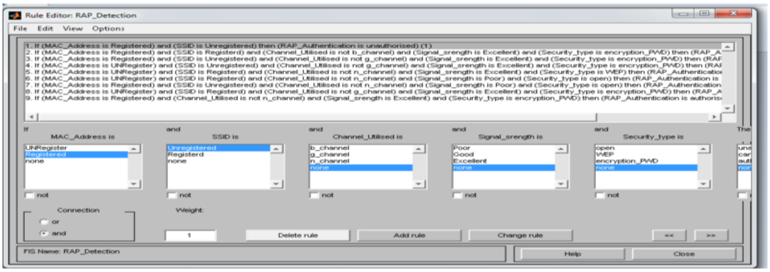


FIS Name: RAP_Detection
FIS Type: mamdani

And method: min
Or method: max
Implication: min
Aggregation: max
Defuzzification: centroid

Current Variable
Name: MAC_Address
Type: input
Range: [0 10]

Figure 1. Proposed System



```
1. If (MAC_Address is Registered) and (SSID is Unregistered) then (RAP_Authentication is unauthorised) (1)
2. If (MAC_Address is Registered) and (SSID is Registerd) and (Channel_Utilised is not b_channel) and (Signal_srength is Excellent) and (Security_type is encryption_PWD) then (RAP_A
3. If (MAC_Address is Registered) and (SSID is Unregistered) and (Channel_Utilised is not g_channel) and (Signal_srength is Excellent) and (Security_type is encryption_PWD) then (RAF
4. If (MAC_Address is UNRegister) and (SSID is Unregistered) and (Channel_Utilised is not g_channel) and (Signal_srength is Excellent) and (Security_type is encryption_PWD) then (RAI
5. If (MAC_Address is UNRegister) and (SSID is Registerd) and (Channel_Utilised is not n_channel) and (Signal_srength is Excellent) and (Security_type is WEP) then (RAP_Authenticatio
6. If (MAC_Address is UNRegister) and (SSID is Registerd) and (Channel_Utilised is not n_channel) and (Signal_srength is Poor) and (Security_type is open) then (RAP_Authentication is
7. If (MAC_Address is Registered) and (SSID is Unregistered) and (Channel_Utilised is not n_channel) and (Signal_srength is Poor) and (Security_type is open) then (RAP_Authentication
8. If (MAC_Address is UNRegister) and (SSID is Registerd) and (Channel_Utilised is not g_channel) and (Signal_srength is Excellent) and (Security_type is encryption_PWD) then (RAP_A
9. If (MAC_Address is Registered) and (Channel_Utilised is not n_channel) and (Signal_srength is Excellent) and (Security_type is encryption_PWD) then (RAP_Authentication is authoris
```

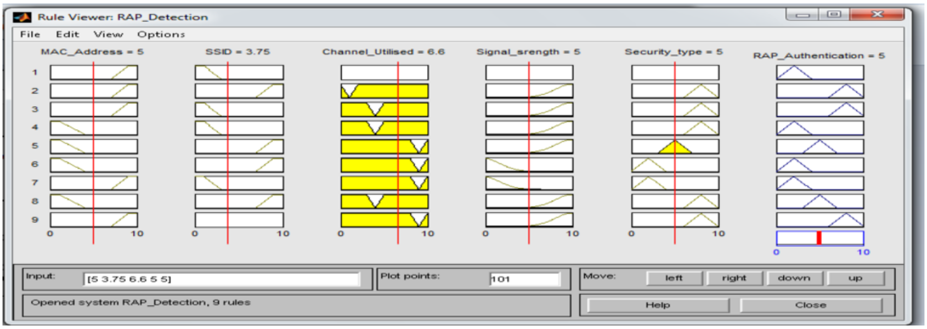
Weight: 1

FIS Name: RAP_Detection

Figure 2. Proposed Rules

In figure 1, it describes about what the proposed method capable of and how RAP detection will be done in fuzzy neural system. as five parameters are input as discussed in tale 1 all given as input which will fuzzify and defuzzify to check the actual output of the system, as ANDing method is done to min and ORing will done at maximum the rule base has prepare with implication setting to min value. The range is selected for each input in triangular function to understand the simple use of system one can use other function for more ambiguous and complex systems.

Figure 2 describes about all the possibilities of rules formation and with three times and operation in phase 2 and twice in phase 1 as final phase will be resultant it forms around 9 rules in rule base per parameter which actually can increases up to 35 rules to create robust system, but as aggregation in fuzzy-neuron system it work well with only 9 parameters with good time complexity and make the systems performance better which discussed in table 2.



MAC_Address = 5 SSID = 3.75 Channel_Utilised = 6.6 Signal_srength = 5 Security_type = 5 RAP_Authentication = 5

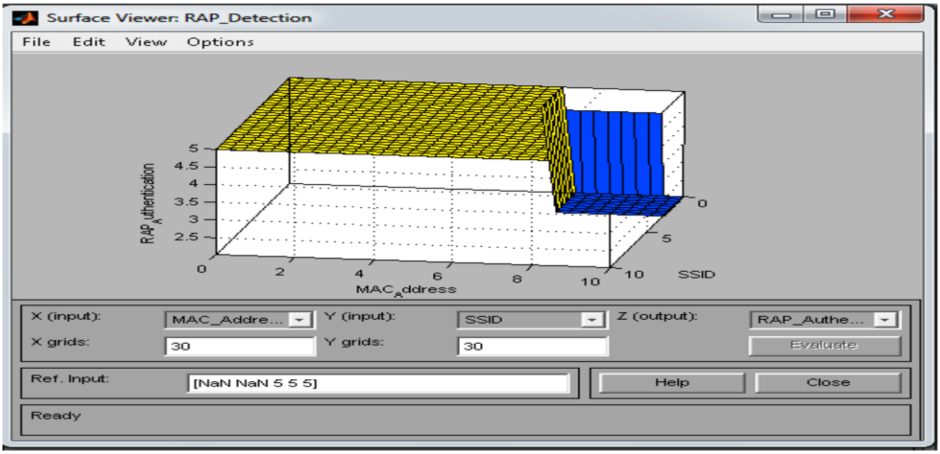
Input: [5 3.75 6.6 5 5]

Plot points: 101

Opened system RAP_Detection, 9 rules

Figure 3. Membership function mapping

Figure 4 is simple pictorial format for RAP detection engine as it shows the analysis with output against the available parameters for the yellow range it describes membership value ranging 0 to 5 for MAC address and blue region it represents SSID as these two are initial phase for detection. Thus the system is robust and performs the proper detection with good accuracy also as it pictorial view understanding of navie user is also simple and faster as these is multidimensional graphs.



X (input): MAC_Addre...

Y (input): SSID

Z (output): RAP_Authe...

X grids: 30

Y grids: 30

Ref. Input: [NaN NaN 5 5 5]

Ready

Figure 4. Analysis of RAP detection method.

AS per paper[8] ,we studied multiple methods to detect RAP in network the comparison is shared in following table with testing on 6 AP exists in network with created 2 RAP so total on 8 Access points the method is tested, Which clearly shows the for all 5 parameters of comparisons this method of WSN [30] security will proves upper hand with no possible limitation over other with having less time for detection and higher end accuracy with simple understanding in its own nature so this proposed method have good proven results over mostly used hybrid frame work and clock skew method to detect and find the existence of rouge access point to damage and manipulate the good wireless sensor networks and make the WSN more secure.

Table 2. Results and comparison with other exixtanting methods

Method Name	**Detection Time (ms)**	**Accuracy (100 %)**	**Limitation**	**Advantage**	**Understandability by naive user**
Proposed method-Fuzzy Logic Method	28	93	Nil (not found)	Faster	Moderate
RTT-Round Trip Time Method	45	85	Propagation Delay	Traditional	Simple
RSS-Received Signal Strength and Seq. Hypothesis Method.	15	84	Signal Strength	Invisible to user	Difficult
Temporal characteristics Method	65	80	Time varying network	Single point of contact	Simple
HMM-Hidden Markov Model Method	55	92	Token system for each	dynamic Bayesian network	Moderate
Clock Skew Method	15	80	Variance due to physical composition temperature	periodic signals	Simple
Hybrid Framework Method	123	82	costly as well as time consuming	Depend on user need can modify	Difficult
Multi Agent Sourcing Method	152	91	multiple interacting intelligent agents	agent-based model	Difficult
Covert Channel method	NA	NA	hard to install	ultra-high-assurance secure OS	Moderate

4. Conclusion & Future Scope

In paper we proposed a naive approach to detect existence of Rouge device which can manipulate sensors in the wireless environment by using fuzzy controller basically designed using madmani’s approach with fuzzy-neuron method introduced in this paper. Also its architecture and implementations details with working model snapshot are discussed in results section. Proposed method is compare with existence methods and shows performance with other methods in real time with working model in real time environment of organization. The method can be more secure as number of parameters from network can increases with more study required as 15 parameters can be implemented but the time complexity and rule base can take more time in evaluation also the system has more ambiguous rules to evaluate which makes access point more secure and ultimately it performs good computation to provide the faster and good solution also as future work some data mining algorithm also can be added to make the parameters characterized and proper shape output. In India very less work done on wireless communication, this is potential filed for researchers to work with and give more inputs and contribution for society.

We also filled a patent on such method to make wireless communication more secure with each node existence in network called RAPD method detection dated 17^{Th} Jan 2020 application id 202021001126 which is published under IPR.

So it concludes that, fuzzy controller or fuzzy-neuron systems can predict the RAP with more accuracy and also can help to detect wireless zone and possible nodes available in the entire network to make it possible more and more advancement in finding proper communication security in any number of access points exists in real time organization. This requires no external hardware or other support so can easily be implemented real time.

References

[1] "Identifying Rogue Access Points"wi-fiplanet.com. Retrieved 2008-02-06.

[2] https://en.wikipedia.org/wiki/Rogue_access_point.

[3] Novák, V.; Perfilieva, I.; Močkoř, J. (1999). Mathematical principles of fuzzy logic. Dordrecht: Kluwer Academic. ISBN 978-0-7923-8595-0.

[4] Zadeh, L.A. (1965). "Fuzzy sets". Information and Control. 8 (3): 338–353. doi:10.1016/s0019-9958(65)90241-x

[5] Pelletier, Francis Jeffry (2000). "Review of Metamathematics of fuzzy logics"(PDF). The Bulletin of Symbolic Logic. 6 (3): 342–346. doi:10.2307/421060. JSTOR 421060. Archived (PDF) from the original on 2016-03-03.

[6] Asli, Kaveh Hariri; Aliyev, Soltan Ali Ogli; Thomas, Sabu; Gopakumar, Deepu A. (2017-11-23). Handbook of Research for Fluid and Solid Mechanics: Theory, Simulation, and Experiment. CRC Press. ISBN 9781315341507

[7] Chaudhuri, Arindam; Mandaviya, Krupa; Badelia, Pratixa; Ghosh, Soumya K. (2016-12-23). Optical Character Recognition Systems for Different Languages with Soft Computing. Springer. ISBN 9783319502526

[8] Prof. Abhijit S. Bodhe1 Dr.A.S.Umesh," Rouge Access Point: A Threat To Wireless Society"15-Jaras-333-December.Pdf

[9] Abhijit Bodhe, SR Deshmukh, SP Patil, International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, ISO 9001:2008 Certified Journal., July 2013.

[10] Bodhe, Abhijit, Mayur Masuti, and A. S. Umesh. "Wireless LAN security attacks and CCM protocol with some best practices in deployment of services." International Research Journal of Engineering and Technology (IRJET) 3.1 (2016): 429-436.

[11] Mr. Abhimanyu D. Sangale , "Drug Reviews using Data Mining Model: A Survey Paper.", published in International Journal of Advance Research and Innovative Ideas in Education(IJARIIE) , Vol. 2, Issue 6, 2016, ISSN : 2395-4396.

[12] Abhijit Bodhe, Dr. Thakur, Sanjay, "RAPD algorithm: detection of rogue access point in wireless network." Int. J. Emerging Technology and Advanced Engineering 3, no. 6 (2013): 85-89.

[13] Mr. Abhijit S.Bodhe Dr.A.S.Umesh," Attacks on Wireless Network and Basic Tips for Securing Wi-Fi Zone.", IJIRMPS 4 no.3(June 2013): 117-115

[14] Dr. Bhagwan Shree Ram, Mr. Abhijit S. Bodhe .A Conceptual Study on Evaluating Network Transit Features in Concern to RAP Detection. International Journal for Research in Engineering Application & Management (IJREAM) 4. No.7 (2018):270-278.

[15] White Paper.Rogue Access Point Detection: Automatically Detect and Manage Wireless Threats To Your Networks. Proxims Corporation, Dec-2004, PP1-8,

[16] https://www.arubanetworks.com/pdf/products/AB_AW_RAPIDS.pdf.

[17] Beetle and Bruce Potter, "Rogue AP 101-Threat Detection & Defense", Dec-12, http://www.airsnort/access_detection/rogue/ap101.pdf.

[18] Bandal Ganesh B., Dhamdhere Vidya S.,and Pardeshi Siddharth A., "Rogue Access Point Detection System in Wireless LAN", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2 Issue5, Oct-2012, PP6-11.

[19] Technical Whitepaper, "Air Magnet: Best Practices for Rogue Detection and Annihilation", Nov–2004, http://airmagnet.flukenetworks.com/assets/whitepaper/ Rogue_Detection_White_Paper.pdf.

[20] Beetle and Potter Bruce, “Rogue Squadron: Evil Twins, 802.11intel, Radical Radious and Wireless Weaponry for Windows”, Black Hat USA, Nov-2005,

[21] Han Hao, Sheng Bo, Tan Chiu C., Li Qun and Lu Sanglu, “A Measurement Based Rogue AP Detection Scheme”, Infocom, Nov-2008, https://www.cs.wm.edu /~hhan/papers/info09_rogue.pdf

[22] Technical White Paper,Cloud Controller Product Manual for Wireless Systems.Meraki Production Product Manual St. San Francisco California, Dec-2011, https://www.meraki.com.

[23] Behede Snehel S., and Wanajale S.B., ”Providing Data Security in WLAN by Detecting Unauthorized AP & Attacks”, International Journal On Engineering & Technology (IJEST), ISSN 0975-5462, May-11, PP 3783-3791

[24] Technical White Paper, A Practical Approach to Identifying and Tracking Unauthorized 802.11 Cards and Access Points.Interlink Networks, Oct-2002, PP1-25, http://www.interlinknetworks.com

[25] Reference Manual, “16 AP Wireless Management System WMS5316” Net Gear Pro Safe, 202-10601-02, San Jose, CA 95134 US, July-10, https://www.netgear.com/upload/product/wms5316/wms5316_ds_01apr10.pdf.

[26] Karygiannis Tom, Owens Les, “Wireless Network Security 802.11, Bluetooth and Handheld Devices”, NIST Special Publication, Nov-12, http://csrc.nist.gov/publications/ nistpubs/800-97/SP800-97.pdf.

[27] Ma Liran, Teymorian Amin Y and Cheng Xiuzhen, ”A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks”, IEEE INFOCOM proceedings 978-1-4244-2026-1, Dec-2008.

[28] Technical White Paper, “A Wireless Networks”, HP Procurve Networking’s, June-2006, http://www.procurve.com

[29] V.D.Ambeth Kumar and M.Ramakrishan (2013) “A Comparative Study of Fuzzy Evolutionary Techniques for Footprint Recognition and Performance Improvement using Wavelet based Fuzzy Neural Network” for the International Journal of Computer Applications in Technology (IJCAT-Inderscience), Vol.48, No.2,pp.95 – 105.

[30] V.D.Ambeth Kumar (2017), “Efficient Routing for Low Rate Wireless Network a Novel Approach”, International Journal of Image Mining, Vol. 2, Nos. 3/4, 2017, 2017