COGNITIVE MACHINE LEARNING APPROACHES TO IDENTIFY UNAUTHORIZED ACCESS POINTS

Ms. Botlagunta Hemalatha #1, Ms. Maram Uma Maheswari #1,
Ms. Mannam Sravani #1, Ms. Aravapalli Sandhya Rani #1, Mr. B Nagaraju #2
#1 Student, Dept Of IT, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#1 Student, Dept Of IT, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#1 Student, Dept Of IT, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#1 Student, Dept Of IT, Qis College of Engineering and Technology, Ongole, Prakasam (Dt)
#2 Assistant professor, Dept Of CSE, Qis College of Engineering and Technology, Ongole, Prakasam

Abstract

With the successive utilization of Wi-Fi and hotspots that give a remote Internet condition, mindfulness and dangers to remote AP (Access Point) security are relentlessly expanding. Particularly when utilizing unapproved APs in organization, government and military offices, there is a high probability of being exposed to different infections and hacking assaults. It is important to distinguish unapproved Aps for insurance of data. In this paper, we use RTT (Round Trip Time) esteem informational collection to distinguish approved and unapproved APs in wired/remote incorporated condition, break down them utilizing AI calculations including SVM (Support Vector Machine), C4.5, KNN (K Nearest Neighbors), and MLP (Multilayer Perceptron). By and large, KNN demonstrates the most noteworthy exactness.

Keywords: *Machine Learning, Data Mining.*

I. INTRODUCTION

Because of the fast improvement of gadgets utilizing remote systems, it is elusive spots without WiFi in our lives. WiFi is promptly accessible in organizations, bistros, military offices, schools and open foundations. WiFi is utilized by numerous unspecified clients, making it hard to check each one. What's more, regardless of whether you are tying like a hotspot utilizing approved WiFi, distinguishing proof is troublesome except if you take a gander at the AP (Access Point) rundown and take a gander at the settings intently. In a remote neighborhood (WLAN), a passageway is a station that transmits and gets information (now and then alluded to as a handset). A passage interfaces clients to different clients inside the system and can likewise fill in as the purpose of interconnection between the WLAN and a fixed wire arrange. Be that as it may, because of different shrewd gadgets, the presence of unapproved AP has turned out to be unavoidable. Use is additionally insignificant, in light of the fact that there are no guidelines or arrangements identifying with unapproved APs, for example, hotspots, just as open spots. This gives an exceptionally frail point to remote systems. The system can be hurt by taking or shining data of different clients who approach unapproved APs, and in light of the fact that PCs can likewise be hacked . Research to recognize log AP and its dangers have been effectively contemplated as of not long ago. Different techniques for research are as of now in advancement, tending to different parts of the issue In request to avert such harm, it is important to discover which AP is an unlawful AP. Tests on different calculations are expected to distinguish this with high accuracy]. In this paper, a dataset was made utilizing RTT (Round Trip Time) values. The informational collection along these lines built is connected to the AI calculation to get the outcome, and after that the outcomes acquired are looked at, to indicate which calculation is progressively exact.

II LITERATURE SURVEY

Various algorithms are applied for classification of rogue APs even in unplanned situations.[9] [10] As a method of selecting feature points for RTT values, the difference, mean, variance, and standard deviation of delay times of each authorized and unauthorized AP are used [11]. In further studies, differentiating connection types is based on active measurements or certain assumptions about wireless links (such as very low bandwidth and high loss rates), which are not applicable to our scenario. Detection is difficult for users because the access point to which a user’s device binds does not identify itself in a fashion that can be verified reliably by the user.

[1] “Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology”, V. S. Shankar Sriram1, G. Sahoo, Krishna Kant Agrawal

It proposes a totally machine-driven idea (without any manual intervention) of detection and eliminating RAPs by applying the mobile Multi-Agents onto the network. We tend to are utilizing two completely different levels of mobile agents- Master and Slave Mobile Agents. For attaining the multi-agent sourcing methodology we extend the System design as mentioned. Firstly a master agent is generated on the DHCP-M server that is liable for control all the procedures of the authorization in Wireless Network. This Master Agent generates slave agents depends upon the quantity of active Access Points Connected to the Server at that moment of your time. These slave agents are then sent on the individual APs connected. Currently these slave agents are cloned on each Access Points are being sent to the each connect consumer system to the APs. Once the cloned salve agent at the consumer system detects any new Access purpose, it mechanically builds and sends data packet information of the Unauthorized AP to Clone Agent to the connected AP such as (SSID, MAC-Address, Vendors Name, and Channel Used). The Slave Agent at AP dispatches this data to its Master Agent on the Server. At the server the small print of the suspected AP is detected and matched therewith of the data kept into the repository regarding all the access points. If the data is matched and therefore the AP is found approved then a replacement slave agent is generated and send to it AP, rather if it’s detected as a consumer MAC address, a disassociation frame is send to any or all APs to tell them to not connect with it, else if the main points doesn’t match with the either of it then the MAC-Address of the AP is fetched from the data, the port at that the MAC-Address is connected is searched and so be blocked for any local area network traffic. This multi agent based mostly design proved to not only establish however additionally eliminate the rogue access points fully. Our projected technique is extremely reliable and value effective, because it deals with multiple level of detection and doesn’t need any specialised hardware device; implementation performed also supports our belief and results in a really effective methodology of complete removal of RAPs.

[2] "Rogue-Access-Point Detection Challenges, Solutions, and Future Directions” Raheem Beyah Georgia Tech, Aravind Venkataraman Cigital

RAPs are on around 20 % of all enterprise networks.1 Since APs have reached goods valuation, the appeal of deploying them in an unauthorized fashion has fully grown. Also, as a result of APs became significantly smaller, network administrators have difficulty visually detection them. This can be significantly true if an attacker uses a portable computer as an AP. unlike traditional attacks that initiate outside the network RAP insertion is most frequently because of within users. This apparently simple misfeasance will have important consequences because these rogue devices produce a back door to the network and threaten network security. This seemingly easy misfeasance will have important consequences; it creates a back door to the network, fully negating the numerous investments in securing the network. Many RAP detection approaches exist, however none are foolproof. Industry, government, and domain got to be aware of this drawback and promote progressive detection ways. It creates a back door to the network, fully negating many investments in securing the network. Many RAP detection approaches exist, however none are foolproof. Industry, government, and domain have to be compelled to be aware of this drawback and promote progressive detection strategies.

[3] “A Novel Approach for Rogue Access Point Detection on the Client-Side”, Somayeh Nikbakhsh, Azizah Bt Abdul Manaf, Mazdak Zamani, Maziar Janbeglou

There is an enormous risk for public Wi-Fi users being tricked into connecting to rogue access points. Rogue access purpose is especially serious threats in local area network, since it exposes a large range of users to MITM and evil twin attack. This paper planned a sensible technique that warns users to avoid connecting to the rogue access points. This technique compares the gateways and therefore the routes that a packet travels to work out whether or not an access purpose is legitimate or not. This technique will simply find Man-In-The-Middle and evil twin attack with none help from the local area network operator. This paper is regarding about one among the security problems in wireless networks that are termed installation of unauthorized access purpose or rogue access purpose. Some researchers outline it as “wireless access point that's installed while not specific authorization from a local network management”. The others define it as “Wi-Fi Access purpose that is setup by an attacker for the aim of sniffing wireless network traffic”. During this paper we tend to use rogue access point we illustrate to the second definition. The projected model may be a quite wireless Intrusion Detection System (Wireless IDS). The main approach during this work is utilizing consumer devices to perform scanning of rogue access point rather than Utilizing dedicated scanning devices. The second approach during this paper is to have one comprehensive resolution for all attainable rogue access points together with Man-In-The-Middle attacks and evil twin attacks. The projected methodology has the subsequent advantages compared to existing solution: Projected methodology will observe each MITM and evil twin attack. A user is often warned of a rogue access point to prevent being exposed to the attacker

[4] “Online Detection of Fake Access Points Utilizing Received Signal Strengths”, Taebeom Kim, Haemin Park, Hyunchul Jung, and Heejo Lee

This paper proposes a unique fake AP detection methodology to resolve the same issues within the client-side. The strategy leverages usual signal strengths (RSSs) and on-line detection algorithmic rule. Our methodology collects

RSSs from close APs and normalizes them for correct measure. They calculate the similarity of normalized RSSs. If the resemblance between normalized RSSs is less than the fixed threshold value, it decides that the RSSs are generated from a pretend device. We will measure the optimum threshold value derived from the consecutive hypothesis testing. In experiment, once the fixed threshold value was two, actuality positive was over than 99 and therefore the false positive was less than 0.1% in 3 observations. Our main contributions are as follows: To ensure the quality of a consumer, we tend to considered developing the pretend AP detection methodology on a restricted platform like a Smartphone. To ensure availableness to the client, our methodology discovers fake APs while not further observation devices or a network manager privilege in WLANs. Moreover, the method doesn't need modification of the AP device, and it will notice the fake APs even if their traffic is encrypted. For the light-weight methodology, we offer fixed threshold values for detecting the fake APs utilizing• consecutive hypothesis testing to enable us to notice malicious APs while not learning tasks. There are two constraints to the client-side methods: cumbersome processes and limited resources. Once the strategies plan to collect information, hard interval time incurs long processes to detect fake characteristics within the client-side. Moreover, the operational systems in smart phones offer restricted resources that may hardly be adopted within the client-side.

[5] “Active User-side Evil Twin Access Point Detection Utilizing Statistical Techniques”, Chao Yang, Yimin Song, and Goofier Gu, Member, IEEE

It proposes to exploit fundamental communication structures and properties of evil twin attacks in wireless networks and to design new active, statistical and anomaly detection algorithms. Their preliminary evaluation in real-world widely deployed 802.11b and 802.11gwireless networks shows very promising results. It can identify evil twins with a very high detection rate while maintaining a very low false positive rate.

EXISTING SYSTEM

In a wireless local area network (WLAN), an access point is a station that transmits and receives data (sometimes referred to as a transceiver). An access point connects users to other users within the network and can also serve as the point of interconnection between the WLAN and a fixed wire network. Research to detect log AP and its risks have been actively studied until recently. Various methods of research are currently in progress, addressing various aspects of the issue. In order to prevent such damage, it is necessary to ascertain which AP is an illegal AP.

Disadvantages:

However, due to various smart devices, the existence of unauthorized AP has become unavoidable. Usage is also irrelevant, because there are no regulations or provisions relating to unauthorized APs, such as hotspots, as well as public places. This provides a very weak point to wireless networks. The network can be harmed by stealing or gleaming information of other users who have access to unauthorized APs, and because PCs can also be hacked.

III PROPOSED SYSTEM

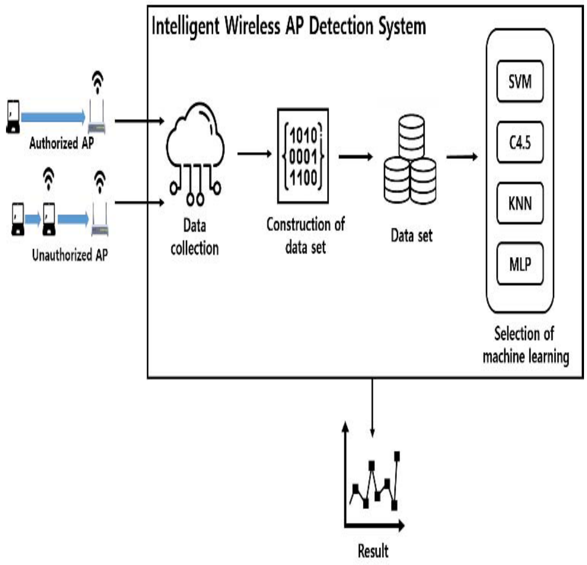
In this, a dataset was created using RTT (Round Trip Time) values. The data set thus constructed is applied to the machine learning algorithm to obtain the result, and then the results obtained are compared, to show which algorithm is more accurate. For detection of unauthorized AP, we developed the “Intelligent Wireless AP Detection System” as shown in Architecture. Data are collected from the authorized APs and unauthorized Aps and constructed as data sets. Data sets are analyzed by applying machine-learning algorithms including SVM (Support Vector Machine), C4.5, KNN (K Nearest Neighbors), and MLP (Multilayer Perceptron). The unauthorized AP has built a new AP using the LG XNOTE P210-GE30P and the iptime N500 connected to it.

Advantages:

The protocol used in network experiments can affect the results depending on which one is used. There may be a big difference in the communication protocol for each protocol, and the bandwidth and channel can also cause errors in the experiment. 802.11n is used for wireless communication protocol that is the most widely used in real world.

IV METHODOLOGY

The architecture of the proposed system and its components are given by



Components:

SVM(support vector machine) : Based on a given set of data, we create a non-probabilistic binary linear classification model that determines which classifications of new data should be broken down and used to represent boundaries in the space in which data is mapped. The SVM algorithm is the algorithm that finds the boundary with the largest width.

C4.5 : It is one of the algorithms for classifying and predicting data by making a decision tree. It is an algorithm that complements the limit of the existing ID3 (Iterative Dichotomizer 3) algorithm. The C4.5 algorithm uses the concept of information entropy to create a decision criterion and uses it to classify the sample set most

effectively.

KNN(k-nearest neighbors algorithm) : As a type of map learning, the input consists of the k closest training data in the feature space, and if used for classification purposes, the object is the object assigned to the most common item among the k nearest neighbors and classified by majority vote.

MLP(multilayer perceptron) : The hidden layer is added between the input layer and the output layer, and supervisory learning is performed using the back propagation algorithm, so that data that cannot be linearly separated can be classified.

V CONCLUSION

In this paper, we showed that the difference between authorized and unauthorized APs can be classified by machine learning algorithms. If we detect the attacks from an unauthorized AP, we can disconnect it for protection of the system. The methods in this paper will be applied to the protection of information,, including personal lifelong data. As a future research, we will design the protection scheme of personal lifelong data which are collected from smart devices analyzed using intelligent algorithms.

VI REFERENCES

[1] S. Jana and S.K. Kasera. "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Transactions on Mobile Computing*, Vol. 9, No. 3, pp. 449-462, 2010.

[2] H.Han, et al. "A timing-based scheme for rogue AP detection," *IEEE Transactions on parallel and distributed Systems*, Vol. 22, No.11, pp. 1912-1925, 2011.

[3] F. Awad, M. Al-Refai, and A. Al-Qerem. "Rogue access point localization using particle swarm optimization," in *8th International Conference on Information and Communication Systems (ICICS)*, Irbid, Jordan. May 2017. doi: 10.1109/IACS.2017.7921985

[4] S. Liu, Y. Liu, and Z. Jin. "Attack behavioural analysis and secure access for wireless Access Point (AP) in open system authentication," in *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, Spain, June 2017. doi: 10.1109/IWCMC.2017.7986377

[5] F. Awad, et al. "Access point localization using autonomous mobile robot," in *2017 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, Aqaba, Jordan, July 2017. doi: 10.1109/IWCMC.2017.7986377

[6] M. Agarwal, S. Biswas, and S. Nandi. "An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks," *International Journal of Wireless Information Networks*, Vol 25. No. 3, pp 120-135, 2018.

[7] V. Modi, and C. Parekh. "Detection & Analysis of Evil Twin Attack in Wireless Network," *International Journal of Advanced Research in Computer Science* Vol. 8, No. 5, pp. 774-777, 2017.

[8] B. Pradeepkumar, et al. "Predicting external rogue access point in IEEE 802.11 b/g WLAN using RF signal strength," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, India, Sept. 2017. Doi: 10.1109/ICACCI.2017.8126135

[9] A. Este, F. Gringoli, and L. Salgarelli. "On the stability of the information carried by traffic flow features at the packet level," *ACM SIGCOMM Computer Communication Review* Vol. 39. No. 3, pp. 13-18, 2009.

[10] L. Watkins, R. Beyah, and C. Corbett. "A passive approach to rogue access point detection," in *IEEE Global Telecommunications Conference 2007*, Washington, DC, USA, Nov. 2007, pp. 355 - 360.

[11] Peng, Lizhi, et al. "Early Stage Internet Traffic Identification Using Data Gravitation Based Classification," In *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech*, Auckland, New Zealand, Aug. 2016. doi: https://doi.org/10.1109/DASC-PICom- DataCom-CyberSciTec.2016.98

[12] C. Yang, Y. Song, and G. Gu. "Active user-side evil twin access point detection using statistical techniques," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No.5, pp. 1638-1651, 2012.

[13] V. Vapnik, “Support Vector Machine,” in *The nature of statistical learning theory*, Springer science & business media, 2013.

[14] J. R. Quinlan, *C4. 5: Programs for Machine Learning*,Morgan Kaufmann Publishers Inc., 1993.

[15] N. S.Altman, "An introduction to kernel and nearest-neighbor nonparametric regression," *The American Statistician*, Vol. 46, No. 3, pp. 175-185, 1992.

[16] D.E. Rumelhart, G. E. Hinton, and R. J. Williams. “Learning internal representations by error propagation,” in *Parallel distributed processing: explorations in the microstructure of cognition*, vol. 1, pp. 218-362, MIT Press, 1986.

Authors Profile

Ms. **Botlagunta Hemalatha** pursuing B Tech in Information Technology from Qis college of Engineering and Technology (Autonomous & NAAC ‘A’ Grade), Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affliated to Jawaharlal Nehru Technological University, Kakinada in 2015-19 respectively.

Ms. **Maram Uma Maheswari** pursuing B Tech in Information Technology from Qis college of Engineering and Technology (Autonomous & NAAC ‘A’ Grade), Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affliated to Jawaharlal Nehru Technological University, Kakinada in 2015-19 respectively.

Ms. **Mannam Sravani** pursuing B Tech in Information Technology from Qis college of Engineering and Technology (Autonomous & NAAC ‘A’ Grade), Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affliated to Jawaharlal Nehru Technological University, Kakinada in 2015-19 respectively.

Ms. **Aravapalli Sandhya Rani** pursuing B Tech in Information Technology from Qis college of Engineering and Technology (Autonomous & NAAC ‘A’ Grade), Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affliated to Jawaharlal Nehru Technological University, Kakinada in 2015-19 respectively.

Mr **B NAGARAJU** working as a Assistant professor in Qis College Of Engineering andTechnology(Autonomous & NAAC ‘A’ Grade), specialization in computer science and engineering Ponduru Road, vengamukkapalem, Ongole, Prakasam Dist, Affliated to Jawaharlal Nehru Technological University, Kakinada respectively.