A Theoretical Survey on MAC Address Blacklisting

B A Sujathakumari
Associate Professor
Dept. of ECE
SJCE, Mysore

Husna Sabhat
4th Semester M.Tech
Dept. of ECE
SJCE, Mysore

***Abstract*: - The Wireless LAN's are gaining noticeable scope in networking. As, the usage of WLAN's are increasing, it is also facing risk of network security. While accessing the network the user must be authorized user, this can be done by bifurcating the user into blacklists and whitelists. The Security rules can be predefined by using either the IP Address or the MAC [Media Access Control] address filtering. In this paper, we propose a security implementation for WLAN's using MAC Filtering. MAC Filtering is done completely in automated way. No human intervention will be there in Whitelisting or Blacklisting MAC Address.**

Keywords- MAC; WLAN;

I. INTRODUCTION

The vast use of Wireless LAN has increased ease of information transmission as well as possibilities of security treats. Now, as the enhancement in WLAN's increases the focus of security hardening of these WLAN. The security need to be provided for the systems that are connected to WLAN's. In every organization these WLAN's are widely used in which more confidential data are transferred.

To keep this data secured care need to taken that no unauthorized system is connected WLAN. This is done in many ways. Multiple level security can be provided. SSID security, MAC Address filtering, encryption and RADIUS based authentication, IP Address filtering are the prominent method followed for providing security [1]. Mainly, when it comes to wireless LAN there must be good measures of security to be implemented. In this paper we have concentrated mainly towards MAC Address filtering for every system MAC Address filtering or MAC Address blacklisting. This is because for every system MAC Address is very uniquely specified.

MAC Address is 48-bit address assigned to each network-card. This unique assigned address to each card can be used to get network permits or denies network access to specific devices through the use of Blacklists and Whitelists. There are many advantages of MAC Address filtering and IP Address filtering apart from getting access to network. When users are nomadic and want access to the home network. Now, any random system from a distance cannot get accessed to network. Thus, to avoid treats in this scenario MAC Address filtering is used. [2]

The prominent key factor of this paper is the whole process of MAC Blacklisting or MAC filtering is done in automated manner through running test scenarios.

There are many techniques proposed previously to tackle the false information injection, Identity theft attacks and IP spoofing in the wireless networks. In order to overcome the obstacles in the previously proposed methods, implementation of effective algorithm for the authentication process or verification and filtering of the MAC addresses of the Roger wireless devices is done. [3]
Two main implementation parts to address the spoofing attacks. One part is to identify the uniqueness of the client address and other is to make the modification access point control list in each client
Another implementation is Opportunistic spectrum access (OSA) in cognitive radio has been proposed to improve spectrum efficiency in which secondary users (SUs) can access the unused portion of the primary users' (PUs) spectrum temporally or spatially. OSA by multiple SUs is controlled by the medium access control (MAC) protocol. OSA MAC protocols have to avoid or prevent collisions during transmission. In addition, OSA MAC protocols have to deal with the interference between the primary and secondary systems. [5]
Now, coming to Software Defined Networking (SDN) is the latest trend in the networking domain. In SDN, the control plane is decoupled from the data plane in network devices and controlled by the centralized controller using the Open Flow Protocol. As the centralized controller does all the control functions, strong security support is mandatory. Firewall can be an effective means to protect the SDN controller from network security threats. The firewall rules can be predefined by using either the IP address or the MAC address filtering. [6]

II. RELATED WORK

In this column we have discussed about advantages of MAC filtering over other methods of providing security to access WLAN.

A. SSID and MAC Address Filtering:

Multi-Level Security can be provided to access any network. Here, the security level is increased by filtering in multiple levels such as SSID, MAC Address, Encryption and RADIUS based authentication for clients to

connect Wireless network. SSID is defined as a unique name given to the Wireless connection, SSID can also be named as "Network name". Most of the network implementations leave the SSID at its default state, which permits anyone with a wireless interface to join the wireless LAN. Recent versions of Microsoft Windows do allow a user to discover and join wireless LANs with non-default SSIDs as well. However, for other versions and other operating systems, a non-default SSID does place a hurdle in the attacker's path. Also, SSID broadcast means that the access points advertise their SSID to the wireless clients, which would make it easy for an intruder to connect to the wireless LAN.

Another measure that is employed to prevent anyone from joining a wireless LAN is MAC address based filtering. MAC spoofing can be used to bypass this mechanism, however, discusses ways of detecting MAC spoofing in a wireless LAN.[1]

B. Accessing Remote Home Network with MAC Address Filtering:

The Access control module of almost all Virtual private networks will have an advantage of allowing only required MAC Address to get connected to the network. Almost all existing home gateways will allow the MAC Filtering. This can be done in many ways, either predefined MAC Address can be listed to access control so that only those listed MAC Address will only be allowed by the access control to connect to the remote network. This is again Blacklisting and Whitelisting method followed. The connecting process can also be dynamic if any MAC Address need to be connected to network it will undergo authentication by entering Username, password. Only with correct credentials MAC Address will be allowed to connect to the network.[2]

C. Spoofing Attack Prevention by MAC Filtering:

MAC spoofing is a procedure for altering a factory assigned Media Access Control (MAC) address of a structure edges on a system devices. The MAC address is the hardcoded on a system border controller and cannot be changed forever. Though, there are many tools which can create a working scheme consider that the NIC have the MAC tackle of a user's selecting. The procedure of masquerade a MAC address is well-known as MAC spoofing of the wireless devices. Essentially, MAC spoofing requires altering a computer's uniqueness, for any motive, and it is comparatively effortless. [3]

D. Blocking Abusive Users in Anonymizing network:

Website administrator depends on blocking IP address of misbehaving users machines but as these users are coming from anonymizing network, blocking of their IP address is not possible. In such cases, web site admin blocks entire anonymizing network, thereby denying access to good and bad users at the same time. The Reliable Credential system (RCS) comes up with the solution where it blocks abusive users in anonymizing network and has many more improvements compared to base system. In RCS, user's identity is his machine's MAC address and based on this identity, misbehaving users are blacklisted. System is reliable and can handle failure of its credential manager with the backup credential manager. Our system gives better result by giving improved reliability and preventing Sybil attack. Also It mitigates risk of colluding Pseudonym manager and Credential manager, and that is how keeps user's identity more secured. The anonymity of any user is not at all compromised in this solution. [4]

E. OMF-MAC:

Opportunistic spectrum access (OSA) is an effective mechanism to mitigate the scarcity of the radio spectrum. The radio spectrum can be considered as a resource that is diminishing with respect to significant increases in the number of ubiquitous wireless devices. However, some of the spectrums licensed to primary users (PUs) are underutilized for example, TV white spaces. OSA enables the secondary users (SUs) with cognitive capability to dynamically access the idle radio spectrum. Spectrum access, i.e., how and when a user can transmit on the channel, is controlled by a MAC protocol. A MAC protocol performs coordination among users in conventional systems such as IEEE 802.11 wireless local area network (LAN) and IEEE 802.16 wireless metropolitan area network (MAN). A centralized MAC protocol is used for wireless MAN, whereas a distributed MAC protocol, i.e., distributed coordination function (DCF) [4], is implemented in wireless LAN. At present, due to the flexible and scalable nature of DCF, wireless LAN (or Wi-Fi) is one of the most popular wireless technology. As a consequence, the operating spectrum for wireless LAN, i.e., 2.4-GHz industrial–scientific–medical band, is becoming increasingly congested. OSA is one of the viable solutions, and the IEEE 802.11af task group is now currently working on this topic. [5]

F. Investigation of Security and QoS on SDN firewall using MAC Filtering:

These days, enterprises and Internet Service Providers (ISPs) are starting to realize the limitations of their network infrastructure due to a rapid growth of Internet users and multimedia applications. Using the present network architecture, most of the forwarding decisions are determined at the routers, based on packet headers and also predefined policies. Further, vendors must reconfigure multiple routers, switches, firewalls, etc., to change the network flow or hardware devices, which is time consuming and cost inefficient. Simply, almost any change in a network is too much of an effort with the need to configure each hardware entity. Therefore, the current network is inflexible for dynamic traffic engineering requirements. To increase flexibility, Software-Defined Networking (SDN) plays an important role in paving the way for managing and utilizing the network resources effectively in an on demand manner.

In SDN, the firewall can be configured in two ways:

(1) Configuring the firewall in SDN controller
(2) Configuring firewall on every switch of the network.

On the other hand, the firewall implementation can be done either using the IP or the MAC address filtering.

In general, the Access Control List (ACL) in firewall mechanism has hundreds of filtering/admission rules that ensure the given security policies by allowing or denying data packets. Those filtering rules are based on the source and destination IP addresses or the MAC addresses. The ACL in the traditional firewall is fully based on the IP address. However, the nature of mobile networks is dynamic IP environment. As the MAC address is unique and static for all network elements, the MAC address filtering is more convenient for wireless networks. Further, MAC address filtering consumes lower processing time than IP address filtering, because each packet is processed at Layer 2. Therefore, the firewall at SDN switches using the MAC address filtering technique. Also, when packet filtering is handled at SDN switches, the workload of the SDN controller shall be reduced and packets with unknown MAC address will be filtered out within the access network.[6]

III. IMPLEMENTATION

Through the literature survey done a part of this paper we found that there are many methods of implementing security for Wireless networks. Our implementation focuses on Filtering MAC Addresses. MAC [Media Access Card] addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network. These two lists are used to filter the MAC address. All this process can be done manually and in automated way, as described earlier in this paper we focus on filtering MAC by automated way by writing test scenarios. On running these test scenarios we can confirm the MAC Address Blacklisting.

IV. CONCLUSION

In modern days as the use of Wireless LAN is been increased the necessity of increasing the security of the network is also required because these networks are oriented to transfer highly confidential data. The survey held as a part of this paper conveys tht there are many ways of strongly implementing network security SSID, MAC filtering, and a good RADIUS implementation to achieve optimal security in a wireless LAN are prominently used.

V. REFERENCES

[1] Fareeha Waheed, Sadia Muhiuddin, and Saqib M Ilyas "Multi-level security for wireless lan" , Karachi, Pakistan.

[2] Stephane Onno, Christoph Neumann, Olivier Heen, "Conciliating remote home network access and MAC-address control", Technicolor, Security & Content Protection Labs,2012

[3] S .Raguvaran, "Spoofing Attack: Preventing in Wireless Networks", International Conference on Communication and Signal Processing, India April 3-5, 2014

[4] Snehal Pise and Prof. Ratnaraj Kumar, "RCS-Blocking Abusive Users in Anonymizing Networks" , IEEE Global Conference on Wireless Computing and Networking , India , 2014

[5] Thant Zin Oo, Nguyen H. Tran, Duc Ngoc Minh Dang, Zhu Han, Long Bao Le and Choong Seon Hon, "OMF-MAC: An Opportunistic Matched Filter-Based MAC in Cognitive Radio Networks", IEEE transactions on vehicular technology, vol. 65, no. 4, April 2016.

[6] PerumalrajaRengaraju and S. Senthil Kumar "Investigation of Security and QoS on SDN Firewall Using MAC Filtering" , International Conference on Computer Communication and Informatics, India, 2017.

[7] A. Lara, A. Kolasani, and B. Ramamurthy. "Network Innovation Using OpenFlow: A Survey", *IEEE* Communications Surveys & Tutorials, Vol. 16, No. 1, 2014.

[8] A.Wool, "A Quantitative Study of Firewall Configuration Errors", IEEE Computer Society, pp.62 – 67, 2004

[9] M. Suh, S. Hyong Park, B. Lee, S. Yang. "Building Firewall over the Software-Defined Network Controller", Proc. ofInt'l Conf on Advanced Communications Technology, pp. 744-748, 2014.

[10] T. Javith, "A Layer2 Firewall for Software Defined Network", Proc. ofInt'l Conf. on Information Assurance and Cyber Security, pp. 39 – 42, 2014.

[11] J. Jeong, J. Seo, G. Cho, and J. Park, "A Framework for Security Services Based on Software-Defined Networking"Proc. of Int'l Conf on Advanced Info. Networking & Applications Workshops, pp. 150–153, 2015.

[12] J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," Ph.D. dissertation, Roy. Inst. Technol. (KTH), Stockholm, Sweden, 2000.

[13] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," IEEE J. Sel. Areas Commun., vol. 23, no. 2, pp. 201–220, Feb. 2005.

[14] E. Hossain, D. Niyato, and Z. Han, Dynamic Spectrum Access and Management in Cognitive Radio Networks. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[15] IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, pp. 1–2793, 2012.

[16] "IEEE P802.11—TASK GROUP AF." [Online]. Available: http://www. ieee802.org/11/Reports/tgaf_update.html

[17] P. Tsang, A. Kapadia, C. Cornelius, and S. Smith, "Nymble:Blocking misbehaving users in anonymizing networks," IEEE Transcations on dependable and secure computing, vol 8, no. 2, March-April 2011.

[18] R.A. Haraty, B. Zantout, "The TOR data communication system," IEEE communications and networks, vol 16, pp. 415-420, 2014.

[19] S. Malgaonkar, Y.B. Nag, G. Damle, "Implementation of optimized Nymble system to enhance network security," IEEE International Conf. on Computational Intelligence and Computing Research, pp. 1-6, 2013.

[20] R. Dingledine, N. Mathewson "Tor: The second-generation onion router," Proc. Usenix Security Symp., pp. 303-320, Aug. 2004.

[21] P.P. Tsang, A. Kapadia, and Smith, "Blacklistable anonymous credentials: Blocking misbehaving users without TTPs," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 72-81, 2007.

[22] J Yang, Y. Chen, and W. Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments,"Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON),2009.

[23] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks,"Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON),May 2007.

[24] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks,"Proc. ACM Workshop Wireless Security (WiSe),pp. 79-S7, 2003 .
[25] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,"Proc. IEEE Int'l Conf. Comm. (ICC),pp. 4646-4651, June 2007.
[26] Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking,pp. 116-127, 2008
[27] Arunesh Mishra and William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1x Standard," *CS-TR-4328 and UMIACS-TR-2002-10*, February 2002
[28] Nikita Borisov, Ian Goldberg and David Wagner "Intercepting Mobile Communications: The Insecurity of 802.11," *ACM SIGMOBILE*, pp. 180 - 189 July 2001
[29] Nancy Cam-Winget, Russ Housley, David Wagner, Jesse Walker, "Security flaws in 802.11 data link protocols," *Communications of the ACM* Volume 46, Number 5, pp. 35-39, 2003
[30] Stubblefield, A., Ioannidis, J., and Rubin, A. "Using the Fluhrer, Mantin, and Shamir attack to break WEP," in *Proceedings of the 2002 Network and Distributed Systems Security Symposium* pp. 17–22, 2002.
[31] Walker, J. "Unsafe at Any Key Size: An Analysis of the WEP Encapsulation," *IEEE 802.11 doc 00-362*, Oct. 27, 2000
[32] OpenVPN , http://openvpn.net/
[33] Remote Access Architecture:1, UPNP, 2009, www.upnp.org/specs/ra/ UPnP-ra-RAArchitecture-v1.pdf
[34] LogMeIn, Hamachi https://secure.logmein.com/products/hamachi2/
[35] OpenVPN Secure Bridge Implementation, Dave Andrews, 2010, http: //web2.uwindsor.ca/courses/cs/aggarwal/cs60564/Assignment1 /Dave.pdf
[36] OpenVPN Portable Open Source Software , SourceForge, 2011, http://ovpnp.sourceforge.net/
[37] Linux-based bridging firewall, 2011, http://ebtables.sourceforge.net/