A secured MAC address based Login System

Tanuj Tiwari, Tanya Tiwari, and Sanjay Tiwari

Abstract—Wi-Fi an acronym for wireless fidelity is a wireless networking technology that allows computers and other devices to communicate over a wireless high speed Internet and utilizes one of the IEEE 802.11 wireless standards to achieve a wireless connection to a network. Every device has a unique MAC Address used for identifying devices connected over Wi-Fi. Since virtually every device now in the market is Wi-Fi capable, MAC address can be considered as a universal identifier. This paper proposes innovative approach to use the MAC Address as an authentication method.

Index Terms— MAC address; Wi-Fi; Bluetooth.

I. INTRODUCTION

Mobile and wireless communications applications are fastest growing most vibrant technological areas in the communication field and there is a clear impact on improving the quality of life of mankind. The telecom sector has now transformed almost all applications from cell phones to wireless internet to home and office devices, from wired into wireless communication. The Internet of things and other advanced wireless communication environments represent the future technology and evolutionary development step in homes, airports, hospitals, industrial, vehicular and transportation systems. An emerging research area in these environments has been the wireless ad hoc, sensor and mesh networks. The major advantage of Wireless communication is freedom of mobility and eliminates the need for cabling, but is inherently less secure and have to follow heavy regulation of the radio frequency spectrum. In addition to act as preferred means for connecting to the internet - at home, in the office, in hotels and at airports, Wi-Fi also provides internet access for remote communities where it is deployed by volunteers in community-based networks, by operators in 'hotspots' and by municipalities in 'hotzones' [1]-[4].

Recently there has been growing demand to have networks that permit access by wireless stations so that restriction of physical connectivity of the station to the transmission media is overcome. Wireless local area network as the name reflects is a local area network that uses wireless transmission medium and extends flexibility of mobility of the stations and find applications where cabling is not feasible or practical. Configuration of a wireless local area network is defined in terms of Basic Service Set,

Extended Service Set, Access Point and Distribution System and the most widely accepted WLAN standard is the IEEE 802.11. The WLAN standards and Several basic services sets can be interconnected through a distribution system as depicted in Fig. 1.

WLAN standard	Pros	Cons
802.11a	<ul style="list-style-type: none"> Faster data transfer rates (up to 54Mbps) Supports more simultaneous connections Less susceptible to interference 	<ul style="list-style-type: none"> Short range (60-100 feet) Less able to penetrate physical barriers
802.11b	<ul style="list-style-type: none"> Better at penetrating physical barriers Longest range (70-150 feet) Hardware is usually less expensive 	<ul style="list-style-type: none"> Slower data transfer rates (up to 11Mbps) Doesn't support as many simultaneous connections More susceptible to interference
802.11g	<ul style="list-style-type: none"> Faster data transfer rates (up to 54Mbps) Better range than 802.11b (65-120 feet) 	<ul style="list-style-type: none"> More susceptible to interference
802.11n	<p>The 802.11n standard was recently ratified by the Institute of Electrical and Electronics Engineers (IEEE), as compared to the previous three standards. Though specifications may change, it is expected to allow data transfer rates up to 600Mbps, and may offer larger ranges.</p>	

ESS: Extended service set
BSS: Basic service set
AP: Access point

Fig. 1. WLAN standards and Extended service set in WLAN configuration

An IEEE 802.11 wireless local area network can support both the modes of communication, Distribution coordination function (DCF) and Point coordination function (PCF) simultaneously on time sharing basis. DCF mode can be implemented for applications that are not time sensitive and PCF is used for high priority and time sensitive data. Recently Wireless sensor networks (WSN) has emerged as a high and new technology consists of spatially distributed autonomous sensors to monitor physical or environmental conditions. With the development of computer and communication, wireless sensor network has been a research hot point. The applications of Wireless sensor networks (WSN) have become manifold due to its proficiency to monitor observations and report them to a central unit. Therefore, WSNs have been adopted by several applications, as Industrial process & monitoring. Machine monitoring. Monitoring the environment. Healthcare. Home

Published on February 16, 2018.

Tanuj Tiwari is with the University of Texas at Dallas, Richardson TX 75080, USA (e-mail: Tanuj98@gmail.com)

Tanya Tiwari is with R & D Division of Samsung India Electronics Pvt.Ltd., Noida, Uttar Pradesh 201305 India. (e-mail: Tt14ryp@gmail.com)

Sanjay Tiwari is with the Photonics Res. lab., S.O.S. in Electronics & Photonics, Pt. Ravishankar Shukla University, Raipur(CG), India. (e-mail: drsanjaytiwari@gmail.com)

automation. Traffic control. and military surveillance [5]-[7].

Wireless local area networks have become popular because they can be easily deployed, portable devices are easily available and doesn't rely on wired Ethernet connections. A WLAN can be either an extension to a current wired network or an alternative to it. . In WLANs, malicious attacks have increased enormously because of the shared medium that wireless networks use to serve wireless devices [8]-[11]. The network of a LAN consists of a physical transmission medium which interconnects various stations of the network. The common transmission medium is shared by the stations connected to it. A discipline is followed by the stations so that every station gets fair opportunity to transmit its data and collisions i.e. two stations simultaneously accessing the media do not take place. Procedures for accessing the medium for signal transmission are called media access control methods. Media access control and addressing functions are implemented in the data link layer of the stations. These functions are in addition to the error and flow control functions of the data link layer. A discipline is built up among the stations of the LAN so that fair opportunity is given to each station to transmit its data frames. The MAC address exists in the data link layer as shown in Fig. 2. For the media access control, the data link layer is divided into two sublayers. The media access control mechanisms are implemented in the media access control sublayer of the data link layer. The media access control (MAC) address identifies wireless devices in wireless networks and MAC based application has been discussed [12]-[15].

Fig. 2. Datalink layer where the MAC address exists

Reuse, Reduce and Recycle are the three R's of waste management. But we seldom apply these concepts in case of the technologies we produce. The best way to fully optimize our technologies is their re use. The most popular re use of technology will be of our phone lines. The phone lines were re used to provide Internet connectivity. In recent years new technologies are being produced every day, but usually they are only used for achieving one or two ends. This creates what we may call a huge amount of technological waste. A single technology if properly analyzed, can present itself as usable in different fields. This paper describes a novel use of a preexisting popular technology of login using unique MAC address.

II. WI-FI BASED LOGIN SYSTEM

In an Ethernet network the MAC address is used to uniquely identify each node (computer etc) on the network. Every packet broadcast over the network must contain the MAC address of the intended receiver to ensure packets get

where they need to go. MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers – Logical Link Control(LLC) Sublayer and Media Access Control(MAC) Sublayer. MAC address is used by Media Access Control (MAC) sublayer of Data-Link Layer. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each. MAC addresses are generally assigned by the vendor/manufacturer of every network interface card (NIC) developed. They are implemented in most network types, but unlike IP address, MAC addresses are permanent and can't be changed. A MAC address is created using the specifications provided by IEEE. MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation as shown in Fig. 3. First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (Organizational Unique Identifier). IEEE Registration Authority Committee assign these MAC prefixes to its registered vendors.

3A-34-52-C4-69-B8

Fig. 3. A unique 48-bit MAC address

Therefore, using a packet sniffing tool it is quite easy to extract valid MAC addresses "off the wire". Once you have the MAC address, as you already know, spoofing the MAC address is even easier.

III. AUTHENTICATION

Every device has a unique MAC Address used for identifying devices connected over Wi-Fi. Since virtually every device now in the market is Wi-Fi capable, MAC address can be considered as a universal identifier. Now this presents a huge plethora of opportunities. This MAC Address can be used as an authentication method.

Fig. 4. MAC authentication process

Authentication is the important component of wireless security. Network authentication is essentially client access control. Before a client can communicate with a wireless access point, it must authenticate with the network. There are two basic forms of authentication: server-based and preshared key (PSK)-based.

Most enterprise networks have at least one authentication server, usually running a Remote Authentication Dial-In User Service (RADIUS). WPA2 Enterprise network security makes use of the IEEE 802.1X port-based authentication standard and consists (a) Supplicant which is the client wireless devices accessing the network, (b) Authenticator – the wireless access point that controls what a supplicant can access and (c) Authentication server – the server that provides an authentication service (usually RADIUS) to the authenticator.

Fig. 5. The IEEE 802.1X authentication process involves a layered exchange between the supplicant, authenticator, and authentication server.

IV. APPLICATION

A simple scenario can be recreated to represent the usefulness of this concept. Consider a person wants his computer to be locked automatically as he leaves his house with his mobile phone or tablet. A program can be designed to check the presence of the MAC Address of a specified device after every short interval. The computer can act as a Wi-Fi hotspot, and check the presence every say 10 minutes. A typical Wi-Fi device has a range of 32 m; this would ensure that the device is not locked even when present in the same house.

V. BENEFITS

The major benefits of Wi-Fi based login authentication are

1. *No external equipment* - The foremost advantage of this concept is that this authentication method uses the most general equipment and there is no need for any external equipment. Usually authentication methods like fingerprint require the purchase of external equipment whose compatibility and platform independence is often tricky.
2. *Margin of error*- The other advantage is low margin of error. The major drawback with modern authentication methods like face recognition is their

low accuracy. The face recognition method also requires recreating the same conditions as the pre fed image, which is not always possible. With the mac address method, the computer just has to match the MAC addresses available to the MAC addresses authorized, which is highly free of errors.

3. *Number of devices*- This method can also be used as a single authentication method for many devices. For example a single smartphone can be used to lock all the computers in the home.
4. *Universal Nature*- Since this method requires no installation of software on the authenticating device, it is virtually universal. Any Wi-Fi Capable device can be used as the authenticating device.
5. *Multiple Authenticating devices*- Unlike most authenticating methods, this method can have multiple authenticating devices. For a single setup a lot of authenticating devices can be used.

Recently Bluetooth was also pushed forward as an authenticating method, but this Wi-Fi method has various advantages over the former-

1. *Popularity*- Wi-Fi is now a more universal certification found in all devices, whereas Bluetooth is somewhat obsolete. This allows a greater number of devices to be used as authenticators in case of Wi-Fi.
2. *Range*- The range of Bluetooth is typically up to 10 m whereas of Wi-Fi is 32m. This range factor is useful if devices to be authenticated are placed apart in a house.
3. *Power Saving*- Wi-Fi is constantly being already used by devices usually in a home to access the Internet. So there is usually no need of separately switching on Wi-Fi, whereas in case of Bluetooth it is rarely used and to keep connected constantly through Bluetooth will be a huge power drain.

This authentication method is not revolutionary, but its beauty lies in the fact it uses the most common profiles already present on majority of devices. Though not feasible for industry or large-scale applications, it can be used for small-scale home uses. Every programmer can use it in a different way for different authentication purposes. Though it still has some challenges we need to overcome

VI. MAJOR CHALLENGES

The major challenge is the MAC Address duplication. Since MAC Address is sent unencrypted over Wi-Fi networks, anyone can access the MAC Address of all the devices in the network. These addresses can be easily broadcasted from a different device. This security flaw makes it unsuitable for high-level security

VII. AT LAST

Due to relatively less security of the MAC Address, this method is not very suitable for high-level encryption. But it is apt for small home computers security as an alternative security method. This authentication system has high level of opportunities if they are suitably harnessed.

REFERENCES

- [1] W. Lemstra, V. Hayes, J. Groenewegen The Innovation Journey of Wi-Fi: The Road to Global Success, Cambridge University Press, 2010
- [2] B. Ballmann "Wifi Fun." In: Understanding Network Hacks. Springer, Berlin, Heidelberg, 2015
- [3] B. Alotaibi, K. Elleithy "A New MAC Address Spoofing Detection Technique Based on Random Forests". Reindl LM, ed. Sensors (Basel, Switzerland). :16(3):281, 2016. doi:10.3390/s16030281.
- [4] A.Holt.,C.Y.Huang,"802.11 Wireless Networks: Security and Analysis" Springer; 2010
- [5] S.S. Ahammed ,B.C. Pillai, Design of Wi-Fi Based Mobile Electrocardiogram Monitoring System on Concerto Platform Engineering, Volume, Pages 65-73, 2013
- [6] Bin Yu., Lisheng Xu., Yongxu Li, 2012"Bluetooth Low Energy (BLE) Based Mobile Electrocardiogram Monitoring System", Proceeding of the IEEE International Conference on Information and Automation Shenyang, China.
- [7] Rolf Nilsson and Bill Saltzstein, "Wireless Low Energy Technology Makes New Medical applications Possible", 2011
- [8] Kolias, C.; Kambourakis, G.; Stavrou, A.; Gritzalis, S. Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset. IEEE Commun. Surveys Tutor., 99, 184–208, 2015.
- [9] B. Bloessl, C. Sommer, F. Dressler and D. Eckho The scrambler attack: A robust physical layer attack on location privacy in vehicular networks. In ICNC, 2015.
- [10] V.Brik., S. Banerjee, M. S. Gruteser, S. Oh "Wireless device identification with radiometric signatures. In MobiCom" 2008,.
- [11] P.O. Carlos, J. Bernardos, J. Carlos and Z.U. Niga, "Wi-Fi internet connectivity and privacy: hiding your tracks on the wireless internet". In IEEE CSCN 2015.
- [12] Mohammed Abbas Fadhil Al-Husainy MAC Address as a Key for Data Encryption International Journal of Computer Science and Information Security, Vol. XXX, No. XXX, 2013
- [13] P.M. Jonker, W. Preface, "Special issue on secure data management," Journal of Computer Security, 17(1), pp.1-3, 2009.
- [14] M. Lei, Z. Qi, X. Hong, and S. V. Vrbsky, "Protecting Location Privacy with Dynamic Mac Address Exchanging in Wireless Networks," in Proc. of the 2007 Intelligence and Security Informatics (ISI'07), New Brunswick, New Jersey, USA. IEEE, May 2007,
- [15] B. Danev, D. Zanetti, S. Capkun. On physical-layer identification of wireless devices. ACM Computing Surveys (CSUR), 45(1):6, 2012

Tanuj Tiwari born in Jan 1998 in India is at Department of Computer Science University of Texas at Dallas. Worked at the Face Perception Lab under IARPA project to train algorithms to better recognize the human face.

Used Matlab and R for large scale data handling and visualization. He has developed many social and scientific websites to assist patients and scientists and founded a firm specializing in Affiliate Marketing and Search Engine Optimization. He is active

member of Association for Computing Machinery and IEEE Computer Society.

Tanya Tiwari born in India completed her BE from prestigious BITS-PILANI and joined Samsung India Electronics Pvt.Ltd Noida as System Software Engineer Software Engineer and Designated Team Leader with through hands on experience in all levels of testing, including performance, functional, integration, system, regression and user acceptance testing. Have experience of system implementation including initial implementation, migrations, solving complex technical problems and business

requirement gatherings.

Dr. Sanjay Tiwari born in India is Professor with the School of Studies in Electronics & Photonics, Pt. Ravishankar Shukla University, Raipur India. He has been US Fulbright Fellow, Visiting Academic of renowned Cavendish Lab, University of Cambridge, U.K and SAARC Fellow. And ICTP Senior Associate.