MAC Addresses Blacklist based on the user's behaviour after connecting to the network

Miss. Husna Sabhat
Department of ECE,
4th Semester, Mtech
JSSSTU, Mysuru

B A Sujathakumari
Department of ECE,
Associate Professor
JSSSTU, Mysuru

Abstract-The advent of wireless LANs is a milestone in networking. The use of wireless LANs not only made data transferring or networking easy but also has increased the security threats. However, security is an alarming concern, as everything being transmitted through network where number of systems or devices are connected. Here the data or information is available "in the air". Our work focuses on using existing protocols, standards, tools and technologies to implement security for wireless LAN. However, Security in a network needs to be implemented at multiple levels. Like SSID security, MAC address filtering, encryption and RADIUS based authentication of wireless clients. But our work mainly concentrates on MAC Address filtering, because MAC Address is unique 48 bit Address given by the vendor to every system.

Keywords: wireless LAN, security, RADIUS, MAC.

I. INTRODUCTION

Uniqueness of a device can be predicted by many means such as IP Address, MAC Address. IP Address changes for a device depending upon the network connected. A media access control address (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC) for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi. In this context, MAC addresses are used in the medium access control protocol sublayer.A MAC may be referred to as the burned-in address (BIA). It may also be known as an Ethernet hardware address (EHA), hardware address or physical address (not to be confused with a memory physical address).A network node may have multiple NICs and each NIC must have a unique MAC address. Sophisticated network equipment such as a multilayer switch or router may require one or more permanently assigned MAC addresses.MAC addresses are most often assigned by the manufacturer of a NIC and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. A MAC address may include the manufacturer's organizationally unique identifier (OUI). MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-

64. EUI is an abbreviation for Extended Unique Identifier.

We chose MAC Address for our work because it maintains its uniqueness irrespective of the network the device is connected to. MAC Addresses are bifurcated into Whitelist and Blacklist based on the device behaviour, technically to say the type of data packets exchanged between the device and the network.

II. BACKGROUND

In this section, we briefly discuss the works which is similar techniques as our approach but serve for different purposes

FareehaWaheed, Sadia Muhiuddin and Saqib M Ilyas.[1] This paper presents “Multi-level security for wireless lan” - 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”.

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.

Stephane Onno, Christoph Neumann and Olivier Heen.[2] 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.

S .Raguvaran.[3] This paper discusses about “Spoofing Attack: Preventing in Wireless Networks” - 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.

SnehalPise and Prof.RatnarajKumar[4] - 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.

Thant Zin Oo, Nguyen H. Tran, Duc Ngoc Minh Dang, Zhu Han, Long Bao Le and Choong SeonHon[5] - 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 increase 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.

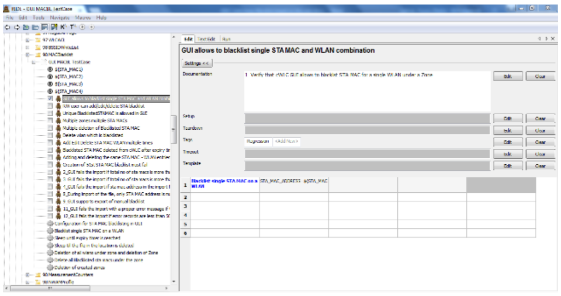
PerumalrajaRengaraju and S. Senthil Kumar[6] – This paper discusses about “Investigation of Security and QoS on SDN

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.

III. PROPOSED WORK

Here, the proposed blacklisting process is described. The proposed scheme includes writing testcases that is "code" in Robot language. In this testcases we have included test scenarios in which MAC Address is blacklisted in multiple manner.

For writing testcases we have used Robot Framework Test Data Editor (RIDE) software. Robot Framework is a generic test automation framework for acceptance testing and acceptance test-driven development (ATDD). It has easy-to-use tabular test data syntax and it utilizes the keyword-driven testing approach. Its testing capabilities can be extended by test libraries implemented either with Python or Java, and users can create new higher-level keywords from existing ones using the same syntax that is used for creating test cases. In our work we have included 17 different scenarios in which MAC Address is Blacklisted using different authentication methods, creation of Zones, Authentication Server, Accounting Server, WLAN with different Authentication method. We tested this testcases in using Graphical user interface. The test results screenshots are included in the paper.


RIDE - GUI MACBL TestCase
File Edit Tools Navigate Macros Help
Edit Text Edit Run
Settings <<

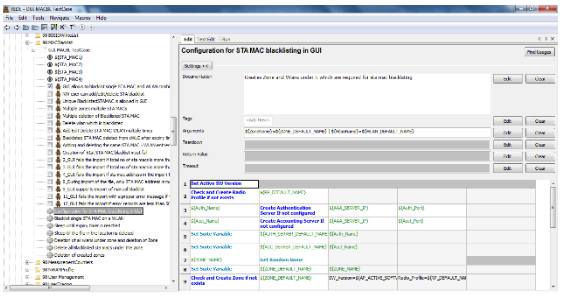
GUI allows to blacklist single STA MAC and WLAN combination

Documentation: 1. Verify that cWLC GUI allows to blacklist STA MAC for a single WLAN under a Zone

Tags: Regression

1	Blacklist single STA MAC on a WLAN	STA_MAC_ADDRESS	${STA_MAC

Fig.1


RIDE - GUI MACBL TestCase
File Edit Tools Navigate Macros Help
Edit Text Edit Run
Find Usages
Settings <<

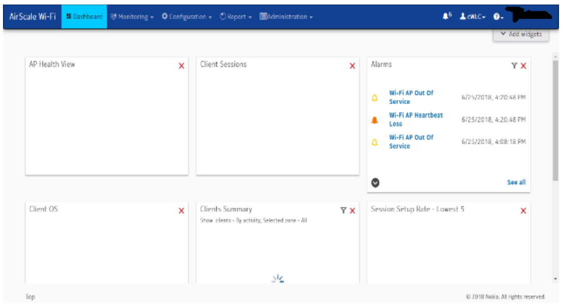
Configuration for STA MAC blacklisting in GUI

Documentation: Creates Zone and Wlans under it which are required for sta mac blacklisting

Arguments: ${zoneName}=${ZONE_DEFAULT_NAME} | ${WlanName}=${WLAN_DEFAULT_NAME}

1	Set Active SW Version			
2	Check and Create Radio Profile if not exists	${RF_DEFAULT_NAME}		
3	${Auth_Name}	Create Authentication Server If not configured	${AAA_SERVER_IP}	${Auth_Port}
4	${Acct_Name}	Create Accounting Server If not configured	${AAA_SERVER_IP}	${Acct_Port}
5	Set Suite Variable	${AUTH_SERVER_DEFAULT_NAME}	${Auth_Name}	
6	Set Suite Variable	${ACC_SERVER_DEFAULT_NAME}	${Acct_Name}	
7	${ZONE_NAME}	Get Random Name		
8	Set Suite Variable	${ZONE_DEFAULT_NAME}	${ZONE_NAME}	
9	Check and Create Zone if not exists	${ZONE_DEFAULT_NAME}	SW_Version=${AP_ACTIVE_SOFTV	Radio_Profile=${RF_DEFAULT_NA

Fig. 2



Show clients - By activity, Selected zone - All

Wi-Fi AP Out Of Service	6/25/2018, 4:20:48 PM
Wi-Fi AP Heartbeat Loss	6/25/2018, 4:20:48 PM
Wi-Fi AP Out Of Service	6/25/2018, 4:08:18 PM

© 2018 Nokia. All rights reserved.

Fig. 3

IV. ALGORITHM

We proposed two effective algorithms for Blacklisting the MAC Address in wireless networks. They are follows as:

A. Manual Process:

Using Graphical User Interface(GUI) we manually navigate to Authentication Server page, Accounting Server page, Zone Page and WLAN Page to create respective objects and then we navigate to MAC Blacklist Page and Manually Blacklist or Whitelist any unauthorized MAC Address.

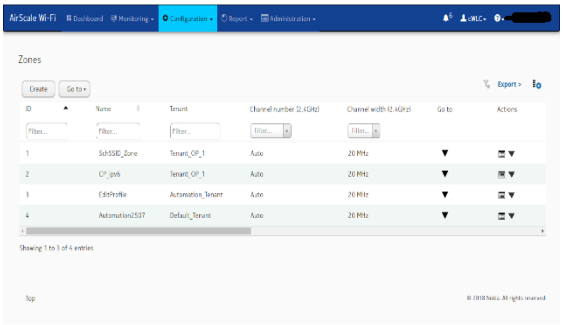
B. Automation Process:

In Automation same scenario as described in manual process is performed but automatically, without any human intervention. GUI is used in the process.

V. IMPLEMENTATION AND RESULTS

Here, we have explained about our 15 test scenario in brief with the results:

1st Test Scenario: “GUI allows to blacklist single STA MAC and WLAN combination.” In this scenario we expected that the GUI should allow to blacklist only one MAC Address with a Authenticated WLAN. The testcase fails when we blacklist another MAC with the same WLAN. Fig.4 shows the result.



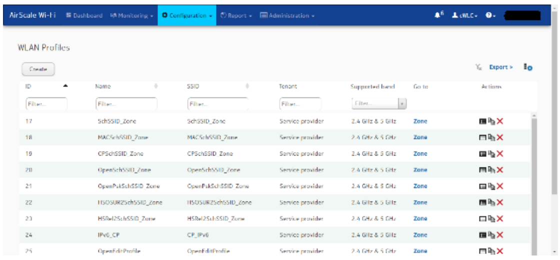
[redacted]

Zones

ID	Name	Tenant	Channel number (2.4GHz)	Channel width (2.4GHz)	Go to	Actions
1	SchSSID_Zone	Tenant_OP_1	Auto	20 MHz	▼	▼
2	CP_ipv6	Tenant_OP_1	Auto	20 MHz	▼	▼
3	EditProfile	Automation_Tenant	Auto	20 MHz	▼	▼
4	Automation2507	Default_Tenant	Auto	20 MHz	▼	▼

Showing 1 to 3 of 4 entries

Fig. 4



[redacted]

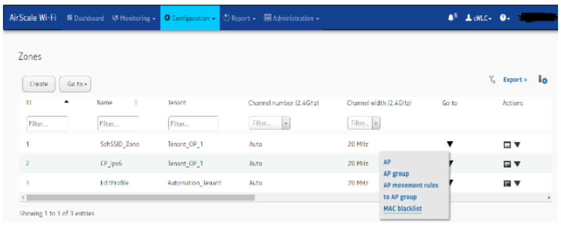
WLAN Profiles

ID	Name	SSID	Tenant	Supported band	Go to	Actions
17	SchSSID_Zone	SchSSID_Zone	Service provider	2.4 GHz & 5 GHz	Zone	✕
18	MACSchSSID_Zone	MACSchSSID_Zone	Service provider	2.4 GHz & 5 GHz	Zone	✕
19	CPSchSSID_Zone	CPSchSSID_Zone	Service provider	2.4 GHz & 5 GHz	Zone	✕
20	OpenSchSSID_Zone	OpenSchSSID_Zone	Service provider	2.4 GHz & 5 GHz	Zone	✕
21	OpenPskSchSSID_Zone	OpenPskSchSSID_Zone	Service provider	2.4 GHz & 5 GHz	Zone	✕
22	HSOSUR2SchSSID_Zone	HSOSUR2SchSSID_Zone	Service provider	2.4 GHz & 5 GHz	Zone	✕
23	HSRel2SchSSID_Zone	HSRel2SchSSID_Zone	Service provider	2.4 GHz & 5 GHz	Zone	✕
24	IPv6_CP	CP_IPv6	Service provider	2.4 GHz & 5 GHz	Zone	✕
25	OpenEditProfile	OpenEditProfile	Service provider	2.4 GHz & 5 GHz	Zone	✕

Fig. 5

2nd Test Scenario: “ReadWrite user can add/edit/delete STA blacklist” Here, only Read write user is allowed to Add, Delete or Edit the Blacklisting of MAC Address. Edit operation is performed to edit the time period of Blacklisting the MAC. The time can vary from 10 seconds to 1800 seconds in our testcases.

3rd Test Scenario: “Unique BlacklistedSTAMAC is allowed in GUI” Here, when we try Blacklist single MAC address twice the testcase fails with GUI throwing error, 'MAC blacklisting object should be unique.' The fig.3 shows the result.



[redacted]

Zones

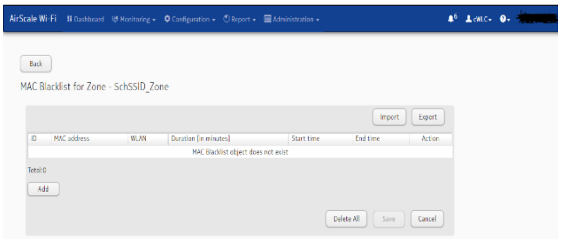
ID	Name	Tenant	Channel number (2.4GHz)	Channel width (2.4GHz)	Go to	Actions
1	SchSSID_Zone	Tenant_OP_1	Auto	20 MHz	▼	▼
2	CP_ipv6	Tenant_OP_1	Auto	20 MHz	▼	▼
3	EditProfile	Automation_Tenant	Auto	20 MHz	▼	▼

Showing 1 to 3 of 3 entries

Fig. 6

4th Test Scenario: “Multiple zones multiple STA MACs” Here, we tested the scenario where we can Blacklist multiple MAC addresses under multiple Zones

5th Test Scenario: “Multiple deletion of Blacklisted STA MAC” In this case we add MAC address to Blacklist in a loop of index 5 and then we delete the MAC Address from the list by randomly picking MAC Address.



[redacted]

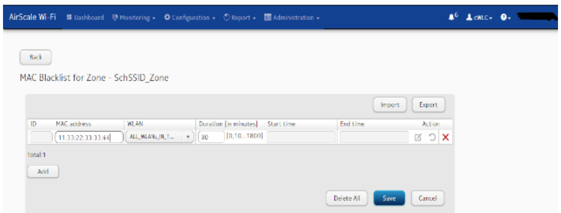
MAC Blacklist for Zone - SchSSID_Zone

ID	MAC address	WLAN	Duration [in minutes]	Start time	End time	Action
MAC Blacklist object does not exist						

Total:0

Fig.7

6th Test Scenario: "Delete wlan which is blacklisted" Here initially a WLAN is created and then the MAC Address is blacklisted in the WLAN. Later the WLAN itself is deleted. So, in return the MAC Address Blacklisted is also deleted.



[redacted]

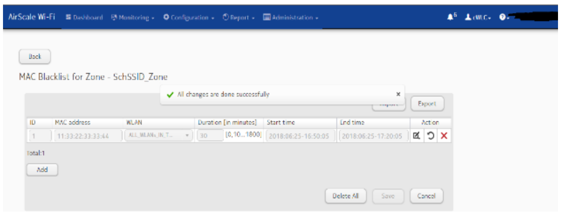
MAC Blacklist for Zone - SchSSID_Zone

ID	MAC address	WLAN	Duration [in minutes]	Start time	End time	Action
	11:33:22:33:33:44	ALL_WLANs_IN_T...	30 [0,10...1800]			

Total:1

Fig. 8

7th Test Scenario: "Add Edit Delete STA MAC WLAN multiple times" Here Add and delete of STA MAC is done spontaneously in GUI. So, that the GUI does not get hung in continues process.



[redacted]

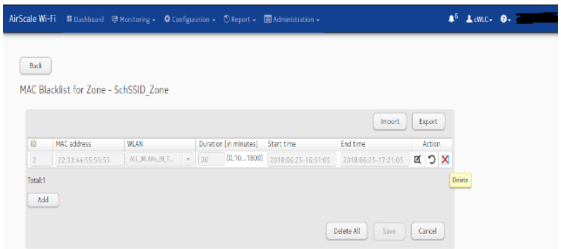
MAC Blacklist for Zone - SchSSID_Zone

✓ All changes are done successfully

ID	MAC address	WLAN	Duration [in minutes]	Start time	End time	Action
1	11:33:22:33:33:44	ALL_WLANs_IN_T...	30 [0,10...1800]	2018:06:25-16:50:05	2018:06:25-17:20:05	

Total:1

Fig. 9



[redacted]

MAC Blacklist for Zone - SchSSID_Zone

ID	MAC address	WLAN	Duration [in minutes]	Start time	End time	Action
2	22:33:44:55:55:55	ALL_WLANs_IN_T...	30 [0,10...1800]	2018:06:25-16:51:05	2018:06:25-17:21:05	

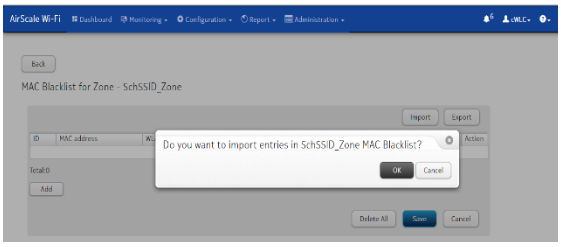
Total:1

Fig. 10

8th Test Scenario: "Blacklisted STA MAC deleted from cWLC after expiry time" Here, the MAC Address is blacklisted for a period of time. After expiry of time the MAC should automatically get deleted from Data base.

9th Test Scenario: "Creation of 51st STA MAC blacklist must fail" In our work we have prefixed that only 50 MAC Addresses can be blacklisted at once, when the GUI tries to blacklist 51st MAC Address GUI should throw error by not allowing to blacklist 51st MAC Address.

10th Test Scenario: "GUI fails the import if total no of sta macs is more than 50 in the import file" In GUI there is provision for importing a file with 50 MAC Address so that it blacklists all 50 MAC Address at once. Now, this testcase will not allow to import a file which has MAC address more that 50.



MAC Blacklist for Zone - SchSSID_Zone

Do you want to import entries in SchSSID_Zone MAC Blacklist?

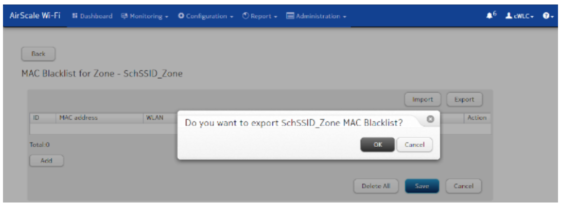
Total:0

Fig. 11

11th Test Scenario: "GUI fails the import if sta mac address in the import file is not according to DM with 50 errors" This testcase is to import file, if the file contains only 50 Errors not more than that from Data Management.

12th Test Scenario: "During import of the file, only STA MAC address is mandatory and also start time and end time, if mentioned, must be ignored." This is a testcase to check that the import file contains only MAC Address. No start time or end time is mentioned.

13th Test Scenario: "GUI supports export of manual blacklist" Similar to import scenario, this testcase allows to export the list of MAC address which are blacklisted.



MAC Blacklist for Zone - SchSSID_Zone

Do you want to export SchSSID_Zone MAC Blacklist?

Total:0

Fig. 12

14th Test Scenario: “GUI fails the import with a proper error message if the file to be uploaded does not have .txt or .tsv as the extension” GUI need to import the import file with extension .txt or .tsv. if in case the import file is of pattern .jpeg or .csv. this testcase will never allow for GUI Import.

15th Test Scenario: “GUI fails the import if total no of sta macs is more than 50 in GUI and import file” This testcase is advance of 10th test case, here the import of file fails if the entries of MAC in GUI as well as imported file exceeds number50.

VI. CONCLUSION

As the usage and need of Wireless LAN is been increased it not only facilitates the transfer of data or any sort of information but also increases the necessity of data security. The necessity of increasing the security of the network is very much required because these networks are oriented to transfer highly confidential data. The survey held as a part of this paper conveys that 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. Our work focused on MAC Address blacklisting because MAC Address have features like predefined, unique and mainly unable to be modified by any individual. Thus, unauthorised user in any network can be blacklisted by the server for a definite period of time. The prominent feature of our work is, the MAC Address is blacklisted in automated way, no human intervention is entertained in the whole system.

ACKNOWLEDEMENT

We hereby would like to thank the Principal of our college and the HOD of the department for all their support in this research work. We would also like to thank the authors of research papers we have referred for their wonderful work. Last but not the least we would like to thank our colleagues, professors and friends for their guidance.

REFERENCES

[1] FareehaWaheed, 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] SnehalPise 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.Wool, “A Quantitative Study of Firewall Configuration Errors”, IEEE Computer Society, pp.62 – 67, 2004

[8] M. Suh, S. Hyong Park, B. Lee, S. Yang. “Building Firewall over the Software-Defined Network Controller”, Proc. ofInt’lConf on Advanced Communications Technology, pp. 744-748,2014.

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

[10] 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.

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

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

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

[14] 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.

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

[16] 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.

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

[18] 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. 16, 2013.

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