INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

REVIEW: COVERT CHANNELS IN 802.11e WIRELESS NETWORKS

Mr. Shreyas Shinde, Prof. Dhanshri Patil,

Nutan Maharashtra Institute of Engineering Technology
Talegaon-Dabhade, Pune - 415 507

Abstract: - Now a day’s WLANs (Wireless Local Area Networks) have been mostly used in offices, colleges and public areas. This network may or may not be secure for secrete data transfer. The newly adopted 802.11e protocol gives many QoS in WLANs. However there are some lacks of security in it. In this looking on the 802.11e protocol for QoS provide in WLANs and two new covert channels are proposed. These new covert channel methods use signaling technique to provide suitable communication. This type of covert channels have no effect on traffic, thus it may not be detected by continuously monitoring on traffic.

Index Terms— Network Steganography, information hiding, 802.11e WLAN, covert channel

I. INTRODUCTION

Wireless communication has been used in lot of places because of its reliability to provide tremendous benefits in the world. Wireless technology can help us to make connection between any type of situations where it is very costly, impossible to construct and dangerous to use cables. So, wired LANs (Local Area Network) could extend or substitute by wireless technology. By constructing wireless LAN customers and employees are getting the freedom of mobility in the area of an organization or outside of an organization. The standard 802.11 was introduced by IEEE organization and makes it specified by a set of all technologies using wireless Ethernet communication between user devices and wireless APs (Access Points) connected to that of wired network from 1999. The 802.11 is the set of all standards which are 802.11a, 802.11b, and 802.11g for implementing Wireless LAN (WLAN) communications in the 2.4, 3.6, and 5GHz frequency bands. The IEEE 802.11b (Wi-Fi) standard is use in most of companies and organizations for making wireless LANs. Mobility and accessibility of wireless communication are very interesting characteristics to the client, though there is additional problem security. In WLANs, radio waves carried frames which can be propagated far distances behind the buildings which are containing the wireless base stations and its hosts. It is very hard to do control mechanism in which computers or devices are managed by the wireless radio signal. So there is vulnerability for covert channels. To keep safe WLANs from any exploited attacks, we need to continuously count their vulnerabilities and devise techniques to less down them. So finding possible covert channels which are presents an ongoing challenge with the potential uses of these covert channels range from well intentioned authentication mechanisms to malware propagation, or command and control [1].

Covert channels are mainly manipulate for certain characteristics of the communication medium in which an unexpected, unconventional and unforeseen way to transmit the information through any medium without being detected by any rather entities which are operating the covert channel [2]. The covert channels have been classified into storage and its timing channels [4]. Covert storage channel has been described as the writing of any hidden data through storage location which is not specifically use for communication by

The any other communicating entities. In contrast, the communication between covert timing channels happens whenever the communication signal information used by manipulating its resources which is affected by response time observed. Covert channels have been using considerable in the network security methods.

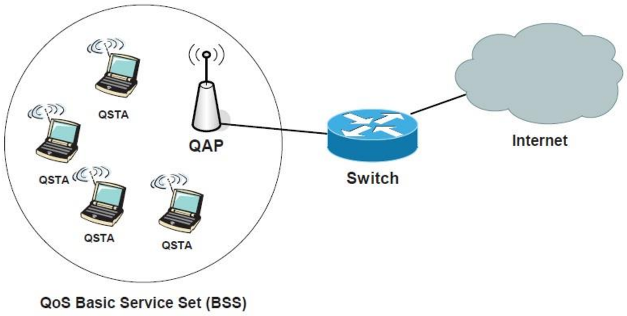
Some of header fields in wireless protocols are likely for covert channels because of the introduced by the protocol for some security reason. The wireless networks have some factors like mobility, RF interference and collision avoidance algorithms which are contributing for no-determination in which can cause covert channels [6]. Now a day's researchers have began to investigate 802.11 WLANs to identify covert channels in the MAC (Medium Access Control) layer. Some covert channels change a MAC header fields to send covert message [8] [10]. The IV (Initialization Vector) field of WEP (Wired Equivalent Privacy) was used to carry the covert message [10]. Wang *et al. is* used a MAC splitting tree algorithm for possible covert communication. The tree-splitting algorithm was introduced to solve collisions between active channels. Colliding nodes are divided into two subsets by randomly selecting the left or right subsets. By using this type of feature a 0 can be encoded to join left side and 1 can be encoded to join the right side. A splitting tree is produced where the tree nodes are collision resolution periods and the tree edges have left or right subsets, and then a secret message is also transmitted. In this type of case the station encodes a covert message as a sequence of subset selection. 802.11 rate switching algorithm could also be used to create a covert channel. As 802.11b rate switching algorithm was used to encode secret information between a mobile station and it's an access point [6]. There are mainly 4 possible data rates: 1.0Mbps, 2.0Mbps, 5.5Mbps and 11Mbps in 802.11b with 2.4Mhz frequency band and each data rate can encode 2−bit information.802.11e is an extension of 802.11, which is designed for providing QoS support in WLAN. To our best knowledge that data hiding in

802.11e has not been studied yet. In this, QoS provision in 802.11e will be studied. Here the two new covert channels are proposed. The flow of this paper is as follows. Section II describes briefly reviews of 802.11e protocol and its possible places to hide information. In Section III, shows different possibilities of data hiding in 802.11e. The proposed covert channel design is conducted in Section IV; performance analysis is presented in Section V; finally, conclusions are given in Section VI.

II. 802.11E ARCHITECTURE

IEEE 802.11 WLAN is to be considered as a wireless Ethernet, in which it supports best-effort services. There are two MACs specified in 802.11: a) the mandatory Distributed Coordination Function (DCF) and b) the optional Point Coordination Function (PCF) [3]. This DCF uses the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) method for listen-before-talk scheme. CSMA/CA can support best-effort services, but not any QoS guarantees. And the PCF can enable stations which have priority access to that medium, coordinated by a station called Point Coordinator (PC). Access Point (AP) often used as PC with PCF function and it polls each station for data manages, one by one; these stations are waiting for their turn for transmitting data and no stations are allowed to transmit up to it is polled. The PCF appears have capability potential to provide QoS but there are a number of limitations. Now a today's most of 802.11 devices don't support PCF and it's operating only in the DCF mode, which is just providing best-effort services.

As in multimedia applications which are more and more popular over WLANs, in which quality of service support must be considered in wireless networks. Wherever, the lack of a built-in mechanism for providing real time services in DCF as well as PCF makes it very difficult to support QoS for multimedia applications over WLANs. To provide real time applications over WLAN, 802.11e was proposed in 2005 for defining a set of QoS. The newly introduced Hybrid Coordination Function (HCF) is installed in stations in QoS Basic Service Set (QBSS) as shown in Fig. 1.



.

Fig. 1. IEEE 802.11e EDCA channel access

The HCF can provide QoS by introducing QoS for traffic classes, the frame subtypes and allowing Transmit Opportunity (TXOP) to stations. With these type of QoS specific mechanisms, a uniform set of frame exchanging sequences can be done for QoS data transfers while both the Contention-Free Period (CFP) and Contention Period (CP). HCF has two access mechanisms: 1) Contention based, Enhanced Distributed Channel Access (EDCA) and controlled channel access, HCF Controlled Channel Access (HCCA). HCF can use both EDCA and HCCA at a time for QoS data transfer. The QoS support in EDCA which realized four Access Categories (ACs) is containing background, best effort, voice and video traffics, and 8 User Priority (UP) for ACs. The traffic of higher UP will be transmitted first in one AC. Fig. 2 shows different ACs contending for channel access in EDCA.

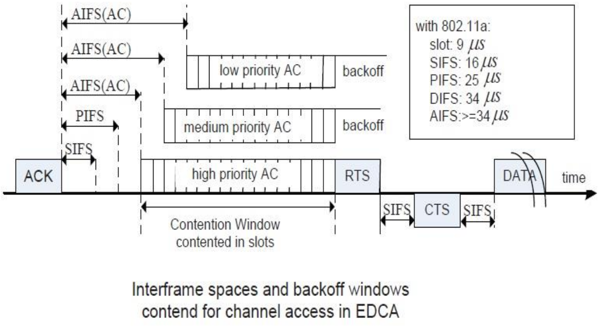


Fig. 2. IEEE 802.11e EDCA channel access

Here EDCA can provide high-priority traffic with a higher chance than low-priority traffic. A station with high priority traffic may wait a little less before it sends its packet than a station with low priority traffic statistically. In addition, contention-free access in EDCA is also provided for a period called a Transmit Opportunity (TXOP). A TXOP is a time period in which a station can send as many frames as possible (as long as the duration of the transmission does not extend beyond the maximum duration of the TXOP). HCCA extends to EDCA access rules. It uses polling scheme (by sending QoS CF poll frame) under both CP and CFP. During CP, each TXOP begins either when the medium is determined to be available under the EDCA rules or when the station receives a special poll frame from HC (Hybrid Coordinator): the QoS CF-Poll [12]. The QoS CF-Poll from the HC can be sent after a PIFS idle period without any backoff. Therefore the HC can issue polled TXOPs in the CP using its prioritized medium access. During the CFP, the starting time and maximum duration of each TXOP are specified by the HC, again using QoS CF-Poll frames. Stations will not attempt to get any type medium access on its own during CFP, so only the HC can grant TXOPs by sending QoS CF-Poll frames. The CFP ends after the the time announced in the beacon frame or by a CF-End frame from the HC. An example of 802.11e superframe is shown in the Fig. 3.

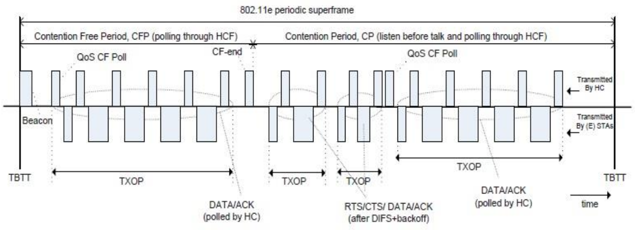
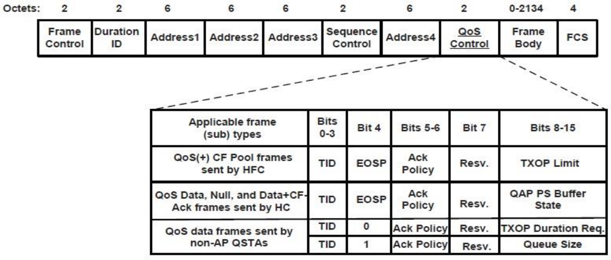


Fig. 3. IEEE 802.11e periodic superframe

III. 802.11E FRAME FORMAT

The WLAN MAC frame format consists of a set of fields that occur in a fixed order in all frames as shown in Fig.4.The field *QoS Control* was added in 802.11e for QoS service. To allow the possibility of hiding data in an 802.11e frame let us consider QoS related fields. In this *Frame Control* field, there are 6 bits to show frame type and its subtype. The function of a frame is determined by both the type and subtype fields. There are three frame types which are control frame, data frame, and management frames. Each of the frame types has several subtypes already defined. For data frames, the Most Significant Bit (MSB) of the subtype field is defined as the QoS subfield. With all QoS related data frames, this field is set to 1. The *QoS Control field* is a 16-bit field that identifies the TC (Traffic Category) or TS (Traffic Stream) to which the frame belongs and various other QoS related information about the frame that varies by frame type and subtype. The *QoS Control* filed is present in all data frames in which the QoS subfield is set to 1. There are five subfields in *QoS Control* field as shown in Fig. 4. The usage of these fields is described as

A. Following [12]:



Octets:	2	2	6	6	6	2	6	2	0-2134	4
	Frame Control	Duration ID	Address1	Address2	Address3	Sequence Control	Address4	QoS Control	Frame Body	FCS

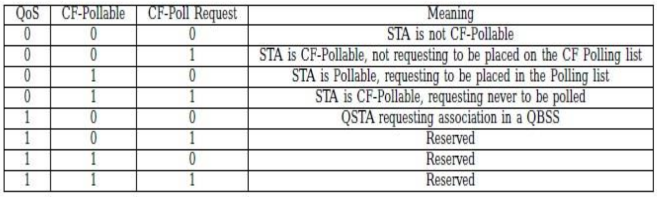
Applicable frame (sub) types	Bits 0-3	Bit 4	Bits 5-6	Bit 7	Bits 8-15
QoS(+) CF Pool frames sent by HFC	TID	EOSP	Ack Policy	Resv.	TXOP Limit
QoS Data, Null, and Data+CF-Ack frames sent by HC	TID	EOSP	Ack Policy	Resv.	QAP PS Buffer State
QoS data frames sent by non-AP QSTAs	TID	0	Ack Policy	Resv.	TXOP Duration Req.
	TID	1	Ack Policy	Resv.	Queue Size

Fig. 4. IEEE 802.11e frame format

- TID–The TID subfield identifies the TC or TS to which the corresponding MSDU (MAC service data unit) belongs. It also identifies the TC or TS traffic for which a TXOP is being requested, through the setting of TXOP duration requested or queue size.
- EOSP–End of Service Period (1-bit) is used by the HC to indicate the end of the current SP (Service Period). The EOSP is set to 1 to indicate the transmission of the SP's final frame and is set to 0 otherwise.
- ACK Policy—This subfield (2-bit) identifies the acknowledgement policy followed upon the delivery of the MPDU. Four choices are available: Normal Ack, No Ack, No explicit Ack, and Block Ack.
- TXOP Limit—This 8-bit subfield is present in QoS data frames including CF-Poll. It specifies the time limit on a TXOP granted by a QoS (+)CF-Poll frame from a HC in a QBSS. The addressed QSTA is granted a TXOP that begins a SIFS period after CF-Poll frame and lasts no longer than the number of 32µs periods specified by the TXOP limit value.
- QAP PS Buffer State–This 8-bit subfield indicates the PS buffer state at the QAP (QoS Access Point) for a non-AP QSTA.
- Queue Size–It is an 8-bit subfield that indicates the amount of traffic for a given TC or TS at the non-AP QSTA sending this frame. The Queue size subfield is present in QoS data frames sent by STAs associated in a QBSS with Bit 4 of the *QoS control* field set to 1. The QAP may use information contained in the Queue Size subfield to determine the TXOP duration assigned to non-AP QSTA.
- TXOP Duration Requested–This 8-bit subfield indicates the duration, in units of 32µ, that the sending STA desires for its next TXOP for the specified TID. This subfield is present in QoS data frames sent by non-AP QSTAs associated in a QBSS with bit 4 of the QoS control field set to 0. Quality of Service is provided through these QoS control fields.

IV. THE PROPOSED COVERT CHANNELS

In an 802.11e QBSS as in Fig. 1, QoS enhancements are in QoS stations, which are associated with a QAP. To increase QoS, include two mechanisms as EDCA which makes to deliver traffic based on UP, and HCCA makes the TXOP reservation with HC located in QAP available. TXOP could be allocated over both CP and CFP, which alternate continuously over time. The EDCA is used in CP only while HCCA can be used in both phases. The Fig. 3 shows an example of a super frame. Two important parameters: TID and TXOP, which are used to provide QoS. Let us see at the following communication example:
1) A new QSTA learns the AP's information from Beacon frames sent from APs, and decides which AP to associate with. Then the QSTA sends Association Request to the selected AP. This Association Request frame body contains 2-byte capability information field and 1-byte QoS Information field.
2) The AP sends Association Response frame to indicate that the association is either successful or failure through status code. The EDCA Parameter Set is also included which provides information needed by non-AP QSTA for proper operation of the QoS facility during the CP.
3) The QSTA is able to send/receive MSDU during CP and CFP to/from other QSTAs. STAs set the *QoS CF Pollable* and *CF Poll Request* of *QoS Capability* field in Association Request frame according to the following Table I [12]



QoS	CF-Pollable	CF-Poll Request	Meaning
0	0	0	STA is not CF-Pollable
0	0	1	STA is CF-Pollable, not requesting to be placed on the CF Polling list
0	1	0	STA is Pollable, requesting to be placed in the Polling list
0	1	1	STA is CF-Pollable, requesting never to be polled
1	0	0	QSTA requesting association in a QBSS
1	0	1	Reserved
1	1	0	Reserved
1	1	1	Reserved

TABLE I. STA USAGE OF QOS, CF-POLLABLE, AND CF-POLL REQUEST

As QSTAs turn on, turn off, come off range, and go out of range, the association between a QSTA and a QBSS is dynamic. In this proposed covert channel, Association or Re-association Request can be used for signaling. In 802.11e management frames such as Association or Re-association request frames, the frame body consists of the fixed fields followed by the information elements defined for each management frame subtype [12]. The frame body of a management frame of subtype of Association Request contains the information in the order of: *Capability, listen interval, extended support rates, Power capability, SSID, Supported channels, Support rates, RSN, QoS Capability, Vender specific*. *QoS Capability* field which appears as the order 9 is used to embed signal information in our proposed covert channel. Fig. 6 depicts the 2- byte *QoS Capability* filed. Each *QoS Capability* information subfield is interpreted according to the management frame subtype. The combination of three fields: *QoS*, *CF-Pollable* and *CF-Poll Request* will indicate if QSTA is pollable and could be placed on the CF polling list. QSTAs set these fields according to Table I. Among the 8 different combinations of these three fields, the combinations 101, 110, and 111 are reserved. So here, the 101 and 110 are selected in covert channel for signaling to start and to make end of a covert communication. As all fixed fields of management frames are appeared in the specified and relative order. QSTAs that encounter an element ID that they do not recognize in the frame body of a received management frame ignore that element and continue to parse the remainder management body to make additional information elements with recognizable element ID [12]. Thus this will not have any type of impact on the association process, but QoS won't be provided to the requesting station. Once the QAP received the association request, it will send the Association Response frame which contains *EDCA Parameter Set*, providing information needed by QSTAs for proper operation of the QoS facility during the CP. To receive QoS, the QSTA sends another re-association request with *QoS*, *CF-Pollable* and *CF-Poll Request* set as 010, and TXOP and TID will be used in transmitting secret information. The following shows the scenario of covert communications in a QBSS shown in Fig. 5.

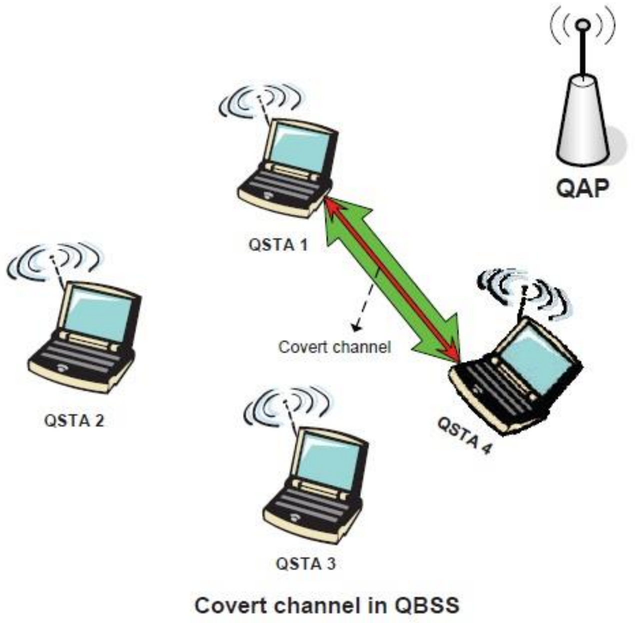


Fig. 5. The proposed covert channel in a QBSS

• QSTA1 sends Association Request with *QoS*, *CFPollable* and *CF-Poll Request* set as 101. This informs the intended receiver QSTA4 the start of a covert communication.

- The intended receiver QSTA4 listens the channel for 101 sent from QSTA1 in its Association Request frame and be ready for receiving secret data.
- As QSTA1 needs to conduct normal communication and secret data will be inserted in its normal data frames, QSTA1 sends Association Request again with these three fields set as 010. So the QSTA1 is CF\ pollable, requesting to be placed on the CF-Polling list.
- When it is the turn for QSTA1 to send data, secret data is transmitted through TXOP and TID of *QoS control* field in a frame or the frame body of data frames.
- QSTA4 receives secret data sent from QSTA1; Once the transmission is finished, QSTA1 or QSTA4 sends Reassociation Request with 110, informing the end of secret communication

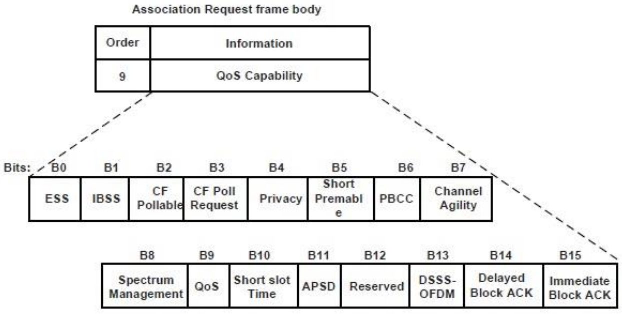


Fig. 6. IEEE 802.11e Association request frame

V. PERFORMANCE ANALYSIS

The proposed covert channel provides more reliable and more secure covert communication because it uses signaling to synchronize both the sender and the receiver. Association/Re-association frames are used to establish the secret communication. The association frame looks like normal frame and the signaling information (101, 110) contained in the three fields as *QoS*, *CF-Pollable* and

CF-Poll Request of an association request frame will not be recognized by AP, because these two are reserved. AP just ignores it and continues to parse the rest of the association frame body. So there will be no error message sent from AP. The QSTA may or may not be associated with the AP depending on the implementation of 802.11e protocol. The intended receiver monitors these codes as the start or the end of the secret communication and be ready for it. To get required QoS, the QSTA makes one more association request. The secret message is then transmitted through *QoS control* field or the frame body. The proposed signaling for covert communication increased the number of association/re-association frames. In a QBSS, QSTAs are frequently turned on/off, or moved in/out, the number of Association/Re-association frames is dynamic. It is hard to identify covert channels by observing the number of Association/Re-association frames. There are also some non- QSTAs in a QBSS, so it is reasonable for some association frames without QoS setting. The association frame used for signaling will not raise any attention to abnormal case. The secret data is transmitted through TXOP (8 bit) in *QoS Control* field of data frame. The Bit 7 in *QoS control* field is reserved and used in the proposed covert channel as the indication of previous data received. Thus signaling is provided to the covert channel. Another way to provide reliable communication is through normal data communication as each frame is acknowledged in WLAN 802.11e. The bandwidth of the covert channel is 8 bits/frame. The bandwidth is low, however there is no additional traffic introduced. To increase the bandwidth, embedding data in frame body is also proposed. By doing this, the whole data frame is used for secret message, the bandwidth is increased greatly. The reliability is realized by acknowledgement provided in WLAN. There is no abnormal traffic pattern as the secret data is transmitted as normal packets.

VI. CONCLUSION

In this paper we had studied the 802.11e protocol and its mechanism for QoS support. To our best knowledge 802.11e has not been studied for covert communications. By analyzing the 802.11e protocol and its structure for providing QoS, two new covert channels are proposed to hide information through 802.11e frames. The proposed channels provide signaling to their secret communications, and thus they provide reliable secret communications. Most existing covert channels have lack of signaling method. So in this the proposed covert channels do not change traffic pattern, they cannot be detected by monitoring traffic pattern. The secret data is embedded in QoS control field; there will be no impact on the existing traffic.

REFERENCES

[1] R. Goncalves, M. Tummala and J. McEachen "A MAC Layer Covert Channel in 802.11 Networks", The Third International Conference on Emerging Network Intelligence (EMERGING 2011), pp. 88-99.

[2] H. Zhao and X. Zhang, "SIP Steganalysis Using Chaos Theory", CMCSN 2012 (The First International Conference on Computing, Measurement, Control and Sensor Network) , Taiyuan, China, July 7-9, 2012.

[3] H. Zhao and N. Ansari, "Cross-Layer Design for Multimedia Streaming over 802.11e Networks", IEEE WTS 2011(Wireless Telecommunication Symposium), New York City, Apr.13-15, 2011.

[4] S. Attallah, "Trusted Computer System Evaluation Criteria," Tech. Rep. DOD 5200. 28-STD, 1985.

[5] H. Zhao and Y. Q. Shi, "Detecting Covert Channels in Computer Networks based on Chaos Theory", IEEE Transaction on Information Forensics and Security, vol. 8, No. 2, pp. 273-282, February, 2013.

[6] T. E. Calhoun, X. Yingshu, and R. Beyah, "An 802.11 MAC Layer Covert Channel", Wireless Communications and Mobile Computing, 2010.

[7] C. G. Girling, "Covert Channels in LAN's," IEEE Transactions on Software Engineering, vol. SE-13, No. 2, pp. 292-296, February 1987.

[8] C. Kratzel, D. Jana, L. Andreas, K. Tobias,"WLAN Steganography: A First Pratical review", 8th Workshop on Multimedia and Security 2006.

[9] M. Wolf, "Covert Channels in LAN Protocols," LNCS 396, pp. 91-101, 1989.

[10] L. Frikha, Z. Trabelsi and W. Ei-Hajj, "Implementation of a Covert Channel in the 802.11 Header", Wireless Communication amd Mobile Computing Conference 2008, pp. 594-599.

[11] D. Martins and H. Guyennet, "Steganography in MAC Layers of 802.15.4 Protocol for securing Wireless Sensor Networks", 2010 International Conference on Multimedia Information Networking and Security, pp. 824-828.

[12] IEEE standard 802.11e, 2005.

[13] IEEE standard 802.11, 2007

[14] Hong Zhao Fairleigh Dickinson University 1000 River Road T-MU1-01, Teaneck, NJ 07670, USA "Covert Channels in 802.11e Wireless Networks", 978-1-4799-1297-1/14/ $31.00 c2014 IEEE