Jestr

Journal of Engineering Science and Technology Review 9 (5) (2016) 93- 96

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

A MAC-centric Approach to Detect and Mitigate EDCA Misbehavior Attacks

A. C. Politis[1,*], P. Kyramaridis[2] and C. S. Hilas[1]

[1]*Department of Informatics Engineering, Technological and Educational Institute of Central Macedonia, Serres, Greece.*
[2]*AT&T, Global Network Services, Brno, Czech Republic.*

Received 30 June 2015; Accepted 25 January 2016

Abstract

The Medium Access Control (MAC) layer of modern Wireless Local Area Networks (WLANs) is known to be susceptible to a number of misbehaving actions. Malicious users are able to alter MAC-layer parameters or alter packet markings to fraudulently gain better service levels from the network to the disadvantage of well-behaved users. If a user is able to successfully perform such acts then the Quality of Service (QoS) functionality of the WLAN can be dramatically altered. In this paper we consider altering the QoS markings on frames as the topic of investigation. This is a type of misbehavior that is harder to detect. Existing research work exploits game theory to discourage such abusive behaviors. Unlike these proposals we follow a deterministic approach to detect and confront this type of anomaly.

Keywords: Quality of Service, EDCA, WLANs, misbehavior.

1. Introduction

QoS provisioning in modern WLANs relies on properly marking frames that belong to different traffic classes (i.e., applications). Packet marking is typically performed at layer-3 (i.e., network layer) of the protocol stack and this information is passed on to the MAC-layer of a wireless station. In the MAC-layer the arriving frames are classified according to their markings and they receive different access priorities. This differentiation-priority duplet is called Enhanced Distributed Channel Access (EDCA). It was initially defined in the IEEE 802.11e amendment [1] in 2005 and is now an integral part of the IEEE 802.11 standard [2].

A large number of misbehavior attacks can be realized in an EDCA WLAN. A well studied abuse is the backoff misbehavior which refers to the act of deliberately altering the Contention Window (CW) values of a node in order to gain an unfairly large portion of the network throughput. This type of misbehavior seems to have drawn the attention of the scientific community and a significant number of research proposals are available in the literature [3], [4].

Another, less studied, type of misbehavior is produced when a user intentionally alters the QoS marking of the produced frames. Intuitively, the one and only strategy that the misbehaving user will follow is to apply the highest priority marking available. This will cause the EDCA function to treat the masqueraded frame with the highest priority. This type of behavior is known as *Class Hijacking* [5] or *EDCA Remapping* [6]. Since the former seems to be a more accurate naming of this type of misbehavior we will use it throughout the rest of this paper.

Performing class hijacking is nowadays a trivial task. Modern operating systems allow marking capabilities to users through APIs and administration tools. For example the iptables administration tool can be used to set the desired markings to outbound traffic in stations running the Linux OS.

The benefits of class hijacking are straightforward: the user performing this type of attack will assign to his/her transmitted frames the highest priority possible and gain the highest service levels available in an unfair manner. On the other hand, the consequences of this anomaly to conforming nodes can be devastating. To our knowledge only a few papers put this misbehaving technique under investigation. The authors of these research papers follow a game theoretic approach to provide counter-incentives to misbehaving nodes [6], [7].

In this paper, we follow a deterministic approach to detect and confront class hijacking in QoS-enabled WLANs. The proposed mechanism resides at the MAC-layer of each STA and performs a series of tests on outgoing packets in order to detect a possible marking misbehavior on each frame. The tests aim at mapping these frames (and the flows they belong to) to well-known traffic types (i.e., multimedia and non-multimedia). Once a flow is characterized as misbehaving the mechanism attempts to re-instate the proper QoS markings on the packets belonging to that flow. Thus, a corrective action is applied at a level that is not accessible by the misbehaving user, rendering the act of class hijacking completely harmless. The mechanism is evaluated by means of network simulation.

2. Background

QoS in IEEE 802.11e is achieved in two stages: per packet differentiation and priority provisioning. Towards this direction, EDCA implements four access categories (ACs) in a QoS-aware wireless station (QSTA). Each AC is a priority transmission queue which runs an instance of the EDCA access function. The access parameters for every priority queue are preset to a specific configuration in order to statistically prioritize real-time over non real-time traffic.

* E-mail address: anpol@teicm.gr

This unequal service provisioning is feasible by manipulating Inter-Frame Spaces (IFS) and Minimum and Maximum Contention Windows (CW_{min} and CW_{max}).

In order to exploit the EDCA benefits, a higher layer data frame must be marked with a specific user priority (UP). This may be achieved by utilizing the IP Type of Service (ToS) or the Differentiated Services Code Point (DSCP) field included in the IP header of the frame. When the marked frame arrives at the MAC-layer it is classified to an AC according to its UP information. The mappings of the UPs to ACs are application specific and are summarized in Table 1.

Table 1. UP to AC mapping and relative priorities.

Priority	UP	AC	Designation
Lowest	1 and 2	AC_BK	Background
Low	0 and 3	AC_BE	Best Effort
High	4 and 5	AC_VO	Video
Highest	6 and 7	AC_VI	Voice

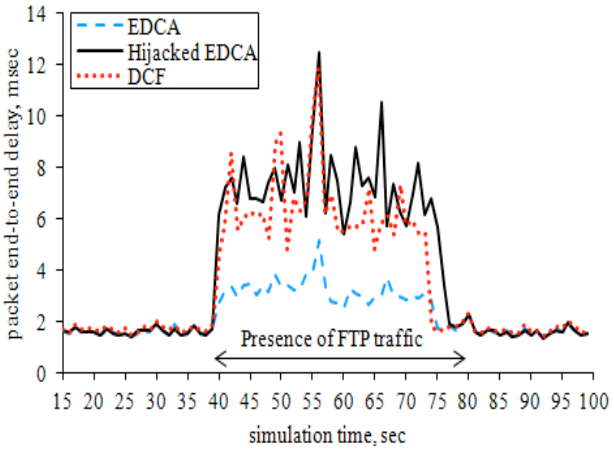

Fig. 1.B. Video packet end-to-end delay for the standard EDCA, hijacked EDCA and DCF functionality.

3. Impact of Class Hijacking

Design principles can be applied to confront class hijacking. Indeed, in a well administrated network, properly defined and controlled trust boundaries may provide protection against this fraud. These boundaries can be maintained with the appropriate Service Level Agreements (SLAs) between the network administration and the users, together with the deployment of traffic policers, shapers and rate limiters to ensure conformance to the SLAs.

On the other hand, ad-hoc WLANs lack central administration. In such self-organized networks it is impossible to define and maintain trust boundaries. Moreover, and according to the IEEE 802.11e standard, if a QSTA acts as a traffic source, then marking, classification and priority provisioning are all provided by the same node but performed by different levels of the protocol stack. Marking, which is typically a layer-3 process, can be easily achieved by exploiting operating system functions. Class hijacking, in this case, can be accomplished without any protection.

In order to highlight the effects of class hijacking a simple simulation scenario was developed in the OPNET network simulation tool. The scenario included an ad-hoc IEEE 802.11e WLAN with three application sources, each producing a different type of traffic. More specifically, background (i.e. FTP), streaming video and voice over internet protocol applications were enabled. To simulate video traffic a real video trace taken from [8] was used. Voice traffic was produced by using the G.729 codec. Each traffic class had a different starting point during the simulation run. The simulation time itself was set to 100 sec.

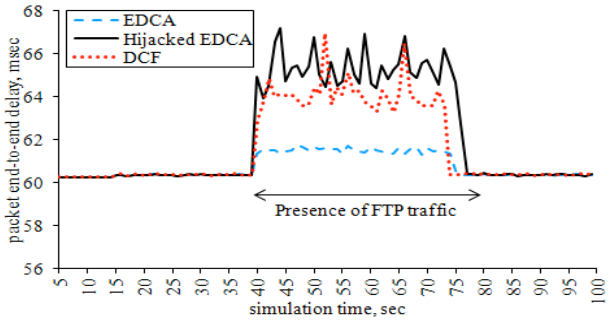

Fig. 1.A. Voice packet end-to-end delay for the standard EDCA, hijacked EDCA and DCF functionality.

The duration of applications were manipulated so that all applications coexisted from the 40th to the 80th second of simulation time. Voice traffic starts at the 5th second of simulation time while video and FTP commence at the 15th and 40th second, respectively.

Each time a QSTA wins the contention for medium access, it has also the benefit of transmitting multiple frames (if available) due to the contention-free burst transmission technique (TXOP) enabled by default in EDCA. The IEEE 802.11b physical layer (PHY) was used at the rate of 11 Mbps. The rationale of selecting IEEE 802.11b (and not one of the newer PHYs) was entirely based on simulation ease. The simulation statistics used to evaluate the impact of class hijacking on multimedia traffic performance are video and voice application-level end-to-end delay.

Fig. 1.A and 1.B depict the impact of improperly marking low priority FTP and video frames as frames with the highest priority (i.e., UP=6). When only voice and video traffic are present (15th-40th and 80th-100th second) the impact of video frames on the end-to-end delay of voice packets (and vice-versa) is imperceptive. This is expected due to the fact that both applications inject frames into the network with high inter-arrival times (20ms for voice and 33ms for video) resulting in a low traffic load.

However, when FTP commences operation both voice and video applications are negatively affected with increased packet end-to-end delays. FTP uses TCP as its transport-layer protocol which transmits multiple packets at irregular intervals. Hence, multiple FTP frames accumulate at the high priority AC_VO of the hijacked QSTA. These frames take advantage of the significantly lower minimum and maximum contention window, inter-frame spaces and the available TXOP values assigned to that AC. Thus, background traffic contents equally with high priority voice and video traffic.

For comparison reasons, Fig. 1 displays the simulation results obtained when the same scenario was implemented with DCF as the standard access mechanism. It is clear that when class hijacking is performed the EDCA functionality is reduced to the legacy DCF behaviour and all QoS aspects are eliminated.

4. Proposed Mechanism

The goal of the proposed mechanism is to detect signs of possible hijacking actions in a QSTA that acts as a traffic source and ultimately reinstate the standard EDCA functionality. This task has do be achieved at the MAC-layer of the QSTA, outside the vicinity of possible user intervention.

Our solution resides at the MAC-layer of a QSTA but uses information from the network and the transport layer headers as well. Two broad classes of (internally) incoming frames are created, i.e., multimedia and non-multimedia frames. In order to categorize a frame in one of the two classes an IP header check must be performed. This check aims at discovering the transport-layer protocol. Typically, multimedia packets use UDP as their transport protocol while non-multimedia frames use the TCP protocol. A frame that holds an UP that is mapped in one of the two multimedia ACs (AC_VI or AC_VO) but its transport protocol is indicated to be TCP is a hijacked non-multimedia packet and is automatically placed at the lowest priority AC (i.e., AC_BK).

It must be noted that a frame that is classified as a multimedia packet may be also non-conforming (e.g., a video frame that has been marked with the highest UP). The identification of such cases is based on the fact that VoIP applications typically produce equally-sized frames while video traffic usually consists of packets with variable length. To this direction, the algorithm periodically samples and buffers a number of incoming frames classified as multimedia frames having the same source port number and keeps track of their size. If their sizes are found to be equal then every other frame originating from the same port is classified as a voice frame. On the other hand, if the sizes are found to be unequal then every packet containing the same source port number is classified as a video frame and is assigned with the UP value of 4.

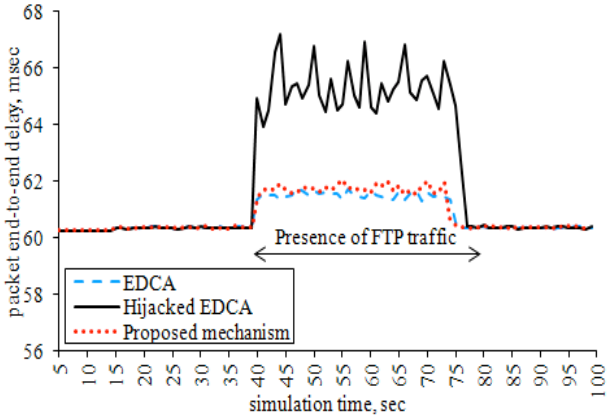

Fig. 2.A. Voice packet end-to-end delay for the standard EDCA, hijacked EDCA and the proposed mechanism.

The aforementioned algorithm was implemented and tested in the OPNET network simulation tool. The simulation scenario is the one described in the preceding Section. The impact of the proposed mechanism is compared to the standard EDCA functionality which is taken as a reference. Figures 2A and 2B reveal the effectiveness of the proposed scheme. The proposed mechanism takes all the corrective countermeasures and the QoS levels on both voice and video applications are restored to levels that correspond to those of the standard EDCA procedure.

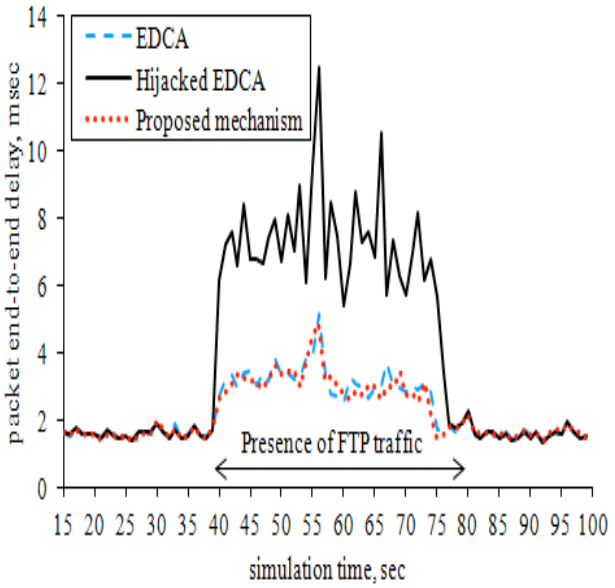

Fig. 2.B. Voice packet end-to-end delay for the standard EDCA, hijacked EDCA and the proposed mechanism.

5. Conclusions

In this paper a possible fraud which can take place in QoS ad-hoc WLANs was investigated. This phenomenon is called class hijacking and is accomplished when packets that belong to low priority applications (such as FTP) are marked as frames with higher precedence and thus receive privileged treatment by the priority queuing system. A mechanism was developed to confront this abuse which resides at the MAC-layer of a QSTA that acts as a traffic source. Simulation results confirm the effectiveness of the proposed mechanism which restores the QoS levels that the EDCA functionality is designed to provide.

This paper was presented at Pan-Hellenic Conference on Electronics and Telecommunications - PACET, that took place May 8-9 2015, at Ioannina Greece.

Acknowledgment

The authors wish to acknowledge financial support provided by the Research Committee of the Technological Educational Institute of Central Macedonia, Greece, under grant 54/6/29-04-2015.

References

1. IEEE Std 802.11e, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, 2005.
2. 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, IEEE Standard 802.11, 2012.

3. Y. Rong, S. Lee and H. Choi, "Detecting stations cheating on backoff rules in 802.11 networks using sequential analysis," *in Proc. IEEE INFOCOM*, pp. 1–13, 2006.
4. A. Toledo and X. Wang, "A robust Kolmogorov-Smirnov detector for misbehavior in IEEE 802.11 DCF," *in Proc. IEEE ICC*, pp. 1564–1569, 2007.
5. Haywood R. , Mukherjee S., Peng X.-H., 'Investigation of H.264 video streaming over an IEEE 802.11e EDCA wireless testbed', IEEE Intl Conf on Commun, Dresden, Germany, pp. 1-5, 2009.
6. S. Szott and J. Konorski, "A Game-Theoretic Approach to EDCA Remapping Attacks," *in Proc. Int. Conf. Wireless Commun. Networking and Mob. Comp.*, pp. 1–4, 2012.
7. J. Konorski and S. Szott, "EDCA remapping in ad hoc IEEE 802.11 WLANs: An incentive compatible discouragement scheme," *in Proc. IFIP Wireless Days*, pp. 1–8, 2012.
8. Video Traces Research Group, http://trace.eas.asu.edu/, accessed January 2015.