Identification & Punishment of Misbehaving Wireless Stations in IEEE 802.11

Heamngi Kothadiya
hemangi1501@gmail.com
M.E(IT) Dept of IT,
Parul Institute of Engineering & Technology,
Vadodara, Gujarat, India

Yask Patel
patelyask@gmail.com
Asst. Prof, Dept of Information Technology
Parul Institute of Engineering & Technology
Vadodara, Gujarat, India

***Abstract*— Contemporary wireless devices should be equipped with functionality for supporting Quality of Service (QoS) & integrity of the data. Unfortunately, most widely used Medium Access Control (MAC) protocols, IEEE 02.11a/b/g, could not satisfy these requirements because they do not provide assurance for fluent QoS. Misbehaving stations are the ones which tend to change the original data. Thus it is necessary to identify such misbehaving wireless stations and punish them to improve QoS of the entire system which assures originality of data.**

Keywords-IEEE 802.11; QOS;cheater detection; MANETs; malicious station

I. INTRODUCTION

As a result of wireless technology, the traditional ways of wired networks have become inadequate in meeting the challenges of present arena posed by our collective lifestyles. Wireless technology provides us with cheap and flexible wireless access. It is also easy to install on campuses, airports, in stock markets, offices, hospitals, and other places. Mobility, ease and speed of installation, flexibility and cost are the core characteristics that place wireless solutions on great demand in today's commercial market. Nowadays wireless technology has become a part of our life, all present applications are being upgraded to support wireless technology and all upcoming applications are being manufactured with integrated wireless support. Wireless technology has become a basic requirement.

All the wireless applications need over-the-air accessibility of up to 100m of area that can be provided by IEEE 802.11 [1] which supports over-the-air interface between the wireless client and a base station or between two wireless clients. Demand for wireless LAN hardware has experienced phenomenal growth during the past several years, evolving quickly from novelty into necessity. As a measure of this expansion, WLAN chipset shipments in 2010 surpassed the 500-million-unit mark, a more than tenfold increase from 2005 shipments of less than 10 million units. Shipments of 802.11e will Surge Ahead of 802.11g in the Wi-Fi Chipset Market in 2015 along with 802.11n.

Thus far, demand has been driven primarily by users connecting notebook computers to networks at work and to the Internet at home as well as at coffee shops, airports, hotels, and other mobile gathering places. As a result, Wi-Fi technology is most commonly found in notebook computers and Internet access devices such as routers and DSL or cable modems. In fact, more than 90 percent of all notebook computers now ship with built-in Wireless LAN.

These new uses, as well as the growing number of conventional WLAN users, increasingly combine to strain existing Wi-Fi networks. Fortunately, a solution is close at hand. The industry has come to an agreement on the components that will make up 802.11n, a new WLAN standard that promises both higher data rates and increased reliability, and the IEEE standards-setting body is ironing out the final details. The load in a WLAN is rarely evenly divided among all access points. Most mobile nodes may be associated with one access point while neighboring access points could be lightly loaded or idle. Though the specification is not expected to be finalized, the draft is proving to be reasonably stable as it progresses through the formal IEEE review process.

II. OBJECTIVE & MOTIVATION

A. Objective

The main objective here is to detect and punish the malicious wireless station. Along with it the following operations can be performed, it detects the packet dropped while traversing from different nodes, and checks weather the node is active or inactive. When a node is found malicious it will be punished for 20 seconds, after that it will be activated or punished again randomly. Here malicious station means the one which is trying to alter the integrity of data. By detecting the malicious station, the quality of service can be improved, by letting the honest data to be sent. Application is implemented in java programming language along with java creator tool.

B. Motivation

The main motivation has emerged with a deliberate consideration of the amount of work still remaining to provide the real-time data transmission support, with required QoS. Contemporary wireless devices should be equipped with functionality for supporting Quality of Service (QoS)

applications such as voice or video streaming services. Unfortunately, most widely used Medium Access Control (MAC) protocols, IEEE 802.11a/b/g, could not satisfy these requirements because they do not provide assurance for fluent QoS For example, the Distributed Coordination Function (DCF) in the legacy IEEE 802.11 series could not guarantee performance for multimedia applications because it only works as a contention-based channel coordination function. As an alternative, the Point Coordination Function (PCF) has been proposed to provide a contention-free period. During this period, the access point (AP) grants a contention-free channel access to each wireless station with the polling mechanism based upon a round-robin scheme. However, it is observed only one polled station can transmit data in each polling interval [2]. This causes unpredictable beacon delay, and it does not allow other stations to fairly access the shared medium to transmit their data. More importantly, it does not include any mechanism to prioritize transmissions among the different data flows. Here along with detection and punishment of malicious wireless stations packet dropped, path traversed and it also checks weather the node is active or inactive.

III. RELATED WORK

IEEE 802.11e is an approved amendment to the IEEE 802.11 standard that defines a set of Quality of Service enhancements for wireless LAN applications through modifications to the Media Access Control (MAC) layer. The standard is considered of critical importance for delay-sensitive applications, such as Voice over Wireless LAN and streaming multimedia. The amendment has been incorporated into the published IEEE 802.11-2007 standard. 802.11 is an IEEE standard that allows devices such as laptop computers or cellular phones to join a wireless LAN widely used in the home, office and some commercial establishments.

Protocol misbehavior has been studied in various scenario different communication layers and under several mathematical frameworks. The previous approaches propose a sequence of conditions on some available observations for testing the extent to which MAC protocol parameters have been manipulated. The advantage of the scheme is its simplicity and easiness of implementation, although in some cases the method can be deceived by cheating peers, as the authors point out. The approach presupposes a trustworthy receiver, since the latter assigns to the sender the back-off value to be used. The receiver can readily detect potential misbehavior of the sender and accordingly penalize it by providing less favorable access conditions through higher back-off values for subsequent transmissions. A decision about protocol deviation is reached if the observed number of idle slots of the sender is smaller than a pre-specified fraction of the allocated back-off. The sender is labeled as misbehaving if it turns out to deviate continuously based on a cumulative metric over a sliding window. This work also presents techniques for handling potential false positives due to the hidden terminal problem and the different channel quality perceived by the sender and the receiver.

Misbehavior detection has been studied at the network layer for routing protocols as well. The work in [12] presents the watchdog mechanism, which detects nodes that do not forward packets destined for other nodes. The pathrater mechanism evaluates the paths in terms of trustworthiness and helps in avoiding paths with untrusted nodes. The technique presented in [3] aims at detecting malicious nodes by means of neighborhood behavior monitoring and reporting from other nodes. A trust manager, a reputation manager and a path manager aid in information circulation through the network, evaluation of appropriateness of paths and establishment of routes that avoid misbehaving nodes. Detection, isolation and penalization of misbehaving nodes are also attained by the technique above. Node misbehavior can be viewed as a special case of denial-of- service (DoS) attack or equivalently a DoS attack can be considered as an extreme instance of misbehavior. DoS attacks at the MAC layer are a significant threat to availability of network services. This threat is intensified in the presence of the open wireless medium. In [7], the authors study simple DoS attacks at the MAC layer, show their dependence on attacker traffic patterns and deduce that the use of MAC layer fairness can mitigate the effect of such attacks. They describe vulnerabilities of 802.11 and show ways of exploiting them by tampering with normal operation of device firmware.

A. DCF and Illustration of Possible Misbehavior

DCF uses CSMA/CA (carrier sense multiple access/collision avoidance) for resolving contention among multiple hosts accessing the channel. A host with data to transmit on the channel selects a random backoff value from range [0,CW/4], where CW (Contention Window) is a variable maintained by each host. While the channel is idle, the backoff counter is decremented by one after every time slot (time slot is a fixed interval of time defined in IEEE 802.11 standard) and the counter is frozen when the channel becomes busy. A host may access the channel when its backoff counter is decremented to zero. After the backoff counter is decremented to zero, the sender host may reserve the channel for the duration of the data transfer by exchanging control packets on the channel. The sender first sends an RTS (Request to Send) packet to the receiver host. The receiver responds with a CTS (Clear to Send) packet and this exchange reserves the channel for the duration of data transmission (RTS-CTS exchange is optional in IEEE 802.11). Both the RTS and the CTS contain the proposed duration of data transmission.

CTS (or both) are required to defer transmissions on the channel for the duration specified in RTS/CTS. After a successful RTS/CTS exchange, the sender transmits a DATA packet. The receiver responds with an ACK packet to acknowledge a successful reception of the DATA packet. If a host's data transmission is successful, the host resets its CW to a minimum value (CWmin); otherwise, if a host's data transmission is unsuccessful (detected by the absence of a CTS or the absence of an ACK), CW is doubled, subject to a

maximum of CWmax. Some strategies misbehaving hosts may use to obtain an unfair share of the channel include:

- Selecting backoff values from a different distribution with a smaller average backoff value, than the distribution specified by DCF (e.g., by selecting backoff values from the range [0, CW/4] instead of [0,CW] or by always selecting a fixed backoff of one slot).
- Using a different retransmission strategy that does not double the CW value after collision.

Such selfish misbehavior can seriously degrade the throughput of well-behaved hosts, this paper, they propose modifications to IEEE 802.11 for simplifying the detection of such misbehaving hosts and for penalizing hosts detected to be misbehaving.

B. Bianchi's Model

In the 802.11 protocol, the fundamental mechanism to access the medium is called distributed coordination function (DCF). This is a random access scheme, based on the carrier sense multiple access with collision avoidance (CSMA/CA) protocol. Retransmission of collided packets is managed according to binary exponential backoff rules. The standard also defines an optional point coordination function (PCF), which is a centralized MAC protocol able to support collision free and time bounded services. DCF describes two techniques to employ for packet transmission. The default scheme is a two-way handshaking technique called basic access mechanism. This mechanism is characterized by the immediate transmission of a positive acknowledgement (ACK) by the destination station, upon successful reception of a packet transmitted by the sender station. Explicit transmission of an ACK is required since, in the wireless medium, a transmitter cannot determine if a packet is successfully received by listening to its own transmission.

In addition to the basic access, an optional four way handshaking technique, known as request-to-send/clear-to-send (RTS/CTS) mechanism has been standardized. Before transmitting a packet, a station operating in RTS/CTS mode "reserves" the channel by sending a special Request-To-Send short frame. The destination station acknowledges the receipt of an RTS frame by sending back a Clear-To-Send frame, after which normal packet transmission and ACK response occurs. Since collision may occur only on the RTS frame, and it is detected by the lack of CTS response, the RTS/CTS mechanism allows increasing the system performance by reducing the duration of a collision when long messages are transmitted. As an important side effect, the RTS/CTS scheme designed in the 802.11 protocol is suited to combat the so-called problem of Hidden Terminals, which occurs when pairs of mobile stations result to be unable to hear each other.

In order to model the misbehaving wireless stations, it specified some malicious cases where the cheater could fix its contention window. A game-theoretic approach was used to investigate the selfish behaviors with the Nash equilibrium. However, they assumed the network is always in the saturated condition which would be infeasible in the practical situation.

C. Predictable Random Backoff (PRB)

PRB operates as follows. Initially, a node with a data packet to transmit randomly chooses a *cwi* from [0, *CW*min]. Upon a successful data transmission, if both *cwi* and $\alpha l \times cwi$ are less than *Wt*,2 a lower bound of the contention window for the next *cwi*+1 selection will be assigned as in (1).

$$CWi+1 \text{ lb} = \alpha l \times CWi \text{ lb}. \quad (1)$$

In case *cwi* is selected as 0, *CW*lb is set to a pre-specified value *CW*spec lb . Otherwise, *CW*lb will be set to a default value.3 Therefore, the node needs to select *cwi*+1 from [*CWi*+1 lb − 1, *CW*min] for the next transmission. In the presence of a failed transmission due to collision or packet errors, the upper bound *CW*ub is doubled, and *cw* is selected from [*CWi*+1 lb − 1, min(2*i*min+*nf* − 1, 2*i*max − 1)], where *nf* is the number of failed transmissions.

Host misbehaviors in MANETs can be classified into the following two categories: 1) selfish misbehavior and 2) malicious misbehavior. A selfish host can deliberately misuse the MAC protocol to gain more network resources than well-behaved hosts. The node can benefit from this behavior through the following three scenarios: obtaining a large portion of channel capacity, reduced power consumption, and improved quality of service, e.g., low network latency. To mitigate the impact of selfish nodes on the network performance, particularly those smart nodes a new adaptive and predictable algorithm, called predictable random backoff (PRB), that is based on minor modifications of the IEEE 802.11 binary exponential backoff (BEB) was proposed.

D. DOMINO: Detecting MAC Layer Greedy Behavior

DOMINO, software to be installed at the access point, is developed. This includes multiple modules to detect various kinds of misbehaviors by wireless stations. However, they could not show cases relevant to EDCA in IEEE 802.11e networks. MAC greedy behavior consists in modifying the operation of the IEEE 802.11 protocol by failing to follow communication procedures. It requires a modification of the IEEE 802.11 MAC protocol in a way that is incompatible with the current standard. Such an approach is practically unfeasible. It gives control to the receiver over the sender by making the former assign backoff values to the latter in both the detection and the correction schemes.

Given the number of possible attacks and their mutual independence, DOMINO needs to be implemented only at the AP. DOMINO periodically collects traffic traces of active user stations during short intervals of time called monitoring periods. A series of tests, each aimed at detecting a particular misbehavior technique, determines if the analyzed traffic

presents behavior anomalies. These anomalies can be considered as the symptoms of the corresponding misbehavior. The outputs of these tests are then fed into a Decision Making Component (DMC) that decides whether a given station is cheating. If so, the operator is informed. MAC greedy behavior consists in modifying the operation of the IEEE 802.11 protocol by failing to follow communication procedures or changing parameters defined in the standard. Hence, it is important to distinguish misbehavior techniques according to the type of traffic they target.

The modular architecture presents several advantages. First, the tests as well as the decision making component can be implemented using several algorithms depending on the required accuracy and the tolerable complexity. Second, new tests for potential yet undiscovered misbehaviors can be easily added.

Hence, the proposed DOMINO approach opens the door to new misbehavior techniques, including misbehaving receivers and collusion between sender and receiver. It creates communication and computation overhead. The first is due to the addition of new frame header fields and the second to the detection and correction schemes that have to compute backoff and, in some cases, penalties for each individual frame of the sending station. This may result in the measured backoff being larger than the assigned one and, hence, leave the cheater undetected.

IV.IEEE 802.11E FOR QUALITY OF SERVICE

Among these task groups, 802.11e is a task group that is working to provide the QoS support, in WLAN, for the transmission of real-time data. IEEE802.11e introduces the new Hybrid Coordination Function (HCF) for the medium access, which consists of the contention based Enhanced Distributed Channel Access (EDCA) for prioritized QoS along with contention free HCF Controlled Channel Access (HCCA). The HCF combines the methods of PCF and DCF, which is the reason it is called hybrid. These new functions are built on DCF defined in the 802.11 legacy model as shown in Figure 2.18. The station that operates as the central coordinator for all other stations within the QoS supporting BSS (QBSS) is called the Hybrid Coordinator (HC). According to 802.11e, QoS enabled station is known as QSTA while QoS enabled access point is known as QAP.

IEEE802.11e provides some basic improvement in legacy 802.11 MAC which includes; an 802.11e station that obtains medium access must not utilize radio resource for duration longer than a specified limit. This important new feature is known as transmission opportunity (TXOP) which refers to the time duration in which a registered station has the right to deliver MSDU. A TXOP is defined by its starting time and duration. TXOP obtained via contention based medium access are referred to as EDCA-TXOP while TXOP obtained by the HC via controlled medium access is referred as HCCA-TXOP or polled TXOP. The IEEE 802.11 is a standard that defines the specifications of both Physical (PHY) and Media Access Control (MAC) layers of WLAN. According to that standard mandatory distributed coordination function (DCF) and an optional point coordination function (PCF) are the two medium access coordination functions at MAC layer. The IEEE 802.11 based WLAN is initially designed only for the best effort data traffic i.e. it does not provide any support for real-time traffic. While if we want to use wireless components in industrial automation, where reliable and time conscious communication is a key factor, the real-time behavior must be considered because whether it is Ethernet or wireless, industrial automation system has rigorous requirements on quality of service (QoS) such as jitter and delay. As described in jitter value lower then 1 ms and delay lower than 10 ms is required in process control application.

The IEEE 802.11 [1] standard was introduced in 1999, After that IEEE established different task groups that are working to provide the enhanced features in WLAN, among these task groups is one task group by the name of 802.11i, focusing on enhanced security and authentication mechanisms of WLAN, similarly 802.11n, which tries to support a maximum (throughput) of at least 100 Mb/s. 802.11f, proposing an inter-AP protocol to allow stations to roam between multi-vendor access points. 802.11e is a task group that is working to provide the QoS support, in WLAN, for the transmission of real-time data. The comprised standards fall within the scope of layer one PHY or physical layer and layer two data link layer of the Open Systems Interconnection (OSI) reference model and specify the data link layer in two sub layers, the Logical Link Control (LLC) and Medium Access Control (MAC).IEEE802.11e introduces the new Hybrid Coordination Function (HCF) for the medium access.

Figure.1 Shows structure of IEEE 802.11e super frame shows structure of the 802.11e super frame which consists of the contention-free period operated by HCCA, and the contention period operated by both HCCA and EDCA.

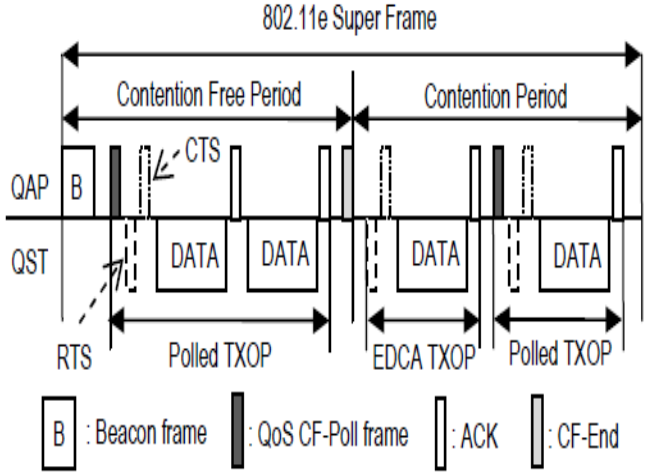

Figure 1: IEEE 802.11E Super Frame

The beacon frame includes network parameters which can be used for the contention between wireless stations. The polled TXOP with HCCA can be acquired through the negotiation phase between QSTA and QAP using a TSPEC frame. Once the HC at the QAP determines the TXOP-granted QSTA, it schedules the polled TXOP duration used by the QAP, and informs the QSTA by sending a QoS CF-Poll frame. When the contention-free period ends, QAP broadcasts the CF-End frame to all QSTAs to initiate the contention period with EDCA.

With EDCA, high priority traffic has a higher chance of being sent than low priority traffic: a station with high priority traffic waits a little less before it sends its packet, on average, than a station with low priority traffic. This is accomplished by using a shorter contention window (CW) and shorter arbitration inter-frame space (AIFS) for higher priority packets. A TXOP time interval of 0 means it is limited to a single MAC service data unit or MMPDU.

As part of 802.11e, an additional random access protocol that allows fast collision resolution is defined. The HC polls stations for MSDU Delivery. For this, the HC requires information that has to be updated by the polled stations from time to time. Controlled contention is a way for the HC to learn which station needs to be polled, at which times, and for which duration. The controlled contention mechanism allows stations to request the allocation of polled TXOPs by sending resource requests, without contending with other EDCF traffic. For fast collision resolution, the HC acknowledges the reception of request by generating a control frame with a feedback field to the requesting stations.

V. Enhanced Distributed Channel Access (EDCA)

With EDCA, high priority traffic has a higher chance of being sent than low priority traffic: a station with high priority traffic waits a little less before it sends its packet, on average, than a station with low priority traffic.

This is accomplished by using a shorter contention window (CW) and shorter arbitration inter-frame space (AIFS) for higher priority packets. In addition, EDCA provides contention-free access to the channel for a period called a Transmit Opportunity (TXOP).

A TXOP is a bounded time interval during which a station can send as many frames as possible (as long as the duration of the transmissions does not extend beyond the maximum duration of the TXOP). If a frame is too large to be transmitted in a single TXOP, it should be fragmented into smaller frames.

The use of TXOPs reduces the problem of low rate stations gaining an inordinate amount of channel time in the legacy 802.11 DCF MAC. A TXOP time interval of 0 means it is limited to a single MAC service data unit or MMPDU.

VI. Limitations of Previous Work

Contemporary wireless devices should be equipped with functionality for supporting Quality of Service (QoS) applications such as voice or video streaming services. Unfortunately, most widely used Medium Access Control (MAC) protocols, IEEE 802.11a/b/g, could not satisfy these requirements because they do not provide assurance for fluent QoS For example, the Distributed Coordination Function (DCF) in the legacy IEEE 802.11 series could not guarantee performance for multimedia applications because it only works as a contention-based channel coordination function.

As an alternative, the Point Coordination Function (PCF) has been proposed to provide a contention-free period. During this period, the access point (AP) grants a contention-free channel access to each wireless station with the polling mechanism based upon a round-robin scheme. However, it is observed only one polled station can transmit data in each polling interval [2].

In addition, in AP's perspective, there is no efficient way to determine the volume of data that will be transmitted from the polled station. This causes unpredictable beacon delay, and it does not allow other stations to fairly access the shared medium to transmit their data. More importantly, it does not include any mechanism to prioritize transmissions among the different data flows. Also the existing system did not guarantee the integrity of data which was sent in the network which was the most challenging and important task to be accomplished.

Future Enhancement & Proposed Work's Advantages

The drawbacks of the existing work can overcome by proposing a malicious detection algorithm. In the proposed scheme the detected malicious node is deactivated or punished for some time, so that the honest stations can continue to transfer their data without any interruption. Here, malicious station is the one which is trying to change the integrity of the data. The system will find out such stations and punish them so that the integrity of the data does not change.

Along with it the following operations can be performed, it detects the packet dropped while traversing from different nodes, the path traversed and checks whether the node is active or inactive. When a node is found malicious it will be punished for 20 seconds, after that it will be it activated or punished randomly.

Using the proposed methodology, possible misbehavior of the system can be avoided, hence improving the quality of service and also the integrity of the system. Since all the network scenarios can be controlled by the network administrator, it will be easy to handle active, inactive and malicious nodes.

REFERENCES

1] IEEE 802.11 WG, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification," IEEE 1999.

[2] S. Mangold, S. Choi, G. Hiertz, O. Klein, and B. Walke, "Analysis of IEEE 802.11e for QoS support in wireless LANs," *Proc. of IEEE Wireless Communication*, December 2003, pp. 40–50.

[3] C. Assi, A. Agarwal, and Y. Liu, "Enhanced per-flow admission control and QoS provisioning in IEEE 802.11e Wireless LANs," *IEEE Transactions on Vehicular Technology*, 57(2): 1077–1088, March 2008.

[4] P. Kyasanur, and N. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks," *Proc. of IEEE DSN*, June 2003, pp.173–182.

[5] P. Kyasanur, and N. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *IEEE TMC*, 4(5):502–516, September-October, 2005.

[6] M. Cagalj, S. Ganeriwal, I. Aad, and J. Hubaux, "On selfish behavior in CSMA/CA networks," *Proc. of IEEE INFOCOM*, March 2005, pp. 2513–2524.

[7] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE J-SAC*, 18(3):535–547, March 2000.

[8] L. Guang, C. Assi, and A. Benslimane, "Modeling and analysis of predictable random backoff in selfish environments," *Proc. of ACM MSWiM*, October 2006, pp. 86–90.

[9] IEEE Computer Society, "IEEE Std 802.11e. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2005.

[10] F. Schreiber, "Effective Control of Simulation Runs by a New Evaluation Algorithm for Correlated Random Sequences," *AEÜ Int'l. J. Elec. and Commun.*, vol. 42, no. 6, 1988, pp. 347–54.

[11] D. Gu and J. Zhang, "A new measurement-basedfs admission control method for IEEE 802.11 wireless local area networks," in *Proc. 14th Int. Symp. Pers., Indoor, Mobile Radio Commun.*, 2003, pp. 2009–2013.

[12] Data communications and networking by Behrouza A.Forouzan.

[13] W.-Y. Choi, "A centralized MAC-level admission control algorithm for traffic stream services in IEEE 802.11e wireless LANs," *Int. J. Electron. Commun.*, vol. 58, no. 4, pp. 305–309, Jul. 2004.

[14] I. Aad, J. P. Hubaux, and E. W. Knightly, "Denial of service resilience in ad hoc networks," in *Proc. ACM Mobicom*, Sep. 2004, pp. 202–215.

[15] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of nodes: Fairness in dynamic ad-hoc neTworks)," in *Proc. ACM Symp.Mobile Adhoc Netw. Comput. (MOBIHOC)*, Lausanne, Switzerland, Jun. 9–11, 2002.

[16] M. Balazinska and P. Castro, "Characterizing Mobility and Network Usage in a Corporate Wireless Local-Area Network," Proc. MobiSys, May 2003.

[17] M. Cagalj, S. Ganeriwal, I. Aad, and J.P. Hubaux, "On Selfish Behavior in CSMA/CA Networks," Proc. IEEE INFOCOM, Mar. 2005.