Research Article

A Hybrid and Secure Priority-Guaranteed MAC Protocol for Wireless Body Area Network

Sana Ullah, Muhammad Imran, and Mohammed Alnuem

College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Correspondence should be addressed to Sana Ullah; sanajcs@gmail.com

Received 26 November 2013; Accepted 7 January 2014; Published 23 February 2014

Academic Editor: Honggang Wang

Copyright © 2014 Sana Ullah et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper introduces a hybrid and secure MAC protocol (PMAC) for WBAN. The PMAC protocol uses two contention access periods (CAPs) for accommodating normal and life-critical traffic and one contention-free period (CFP) for accommodating large amount of data packets. The priority-guaranteed CSMA/CA procedure is used in the CAP period, where different priorities are assigned to WBAN nodes by adjusting the backoff window size. In addition, a set of security keys is used to prevent illegal access to the network. Analytical expressions are derived to analyze the average delay, power consumption, throughput, and packet loss probability of the PMAC protocol. Results derived from these expressions are validated by computer simulations.

1. Introduction

Wireless body area networks (WBANs) are captivating significant attention from research and industrial communities. They provide unprecedented and limitless opportunities for medical and nonmedical applications [1, 2]. Medical applications employ implantable or wearable tiny devices in, on, or around the human body for continuous health monitoring such as predicting contingency abnormal condition and treatment of chronic diseases including diabetes and hypertension. Non-medical applications include interactive body computing, information exchange, social networking, monitoring forgotten things, entertainment, monitoring of athletes, education, or assessing soldier fatigue and battle readiness. Most of these applications require WBAN to stay operational for a longer period of time which necessitates power-efficient network operation. For example, a diabetic patient requires round-the-clock real-time glucose monitoring over a period of years to decades in order to avoid catastrophic consequences such as stroke or a heart attack that may result in death. This requires WBAN node to continuously monitor and report glucose level for timely action. Nodes of WBAN primarily rely on low power batteries that hinder their operation over longer period of time. Therefore, power-efficient network operation is extremely crucial for prolonging network lifetime.

Medium access control (MAC) protocols play a critical role in extending network lifetime by controlling the dominant sources of energy waste such as packet collisions, overhearing, idle listening, and control packet overhead. Most of the existing MAC protocols for WBAN are categorized into contention- and schedule-based MAC protocols. In contention-based MAC protocols, nodes compete for the channel to transmit the data; carrier sensor multiple access with collision avoidance (CSMA/CA) protocol is the best example of contention-based MAC protocols where the nodes contend for the channel using a random backoff period. These protocols are scalable and do not require establishing infrastructure. However, they are unable to handle emergency situations where multiple nodes (with the same priorities) are triggered to send life-critical data. Schedule-based MAC protocols divide the channel into multiple fixed or dynamic slots, which are used for data transmission. These protocols reduce idle listening and overhearing; however, they incur significant protocol overhead.

This paper proposes a hybrid and secure MAC protocol (PMAC) for WBAN. The PMAC protocol supports two contention access periods (CAPs) and one contention-free period (CFP). In the CAPs, the operation is mainly based on a priority-guaranteed CSMA/CA procedure, where different WBAN nodes are assigned different priorities. These priorities are adjusted by tuning the contention window...
(CW) size. Depending on the application requirements, the CAPs may also employ the slotted-ALOHA protocol. The CFP is used to carry large amount of data packets to the coordinator. The PMAC protocol uses a set of security keys including master key (MK) and pairwise temporal key (PTK) in order to prevent adversaries from gaining resource allocation information and from corrupting the CFP slots. The performance of the PMAC protocol is analyzed using both analytical and simulation-based methods. The results are derived in terms of average delay, power consumption, throughput, packet loss probability, and number of corrupted CFP slots.

The rest of the paper is organized into the following sections. Section 2 presents the related work. Section 3 explains the basic operation of the PMAC protocol. Sections 4 and 5 present the analytical approximations and performance results. The final section concludes our work.

2. Related Work

Multiple research efforts are dedicated to the development of novel MAC protocols for WBANs. Some of these efforts analyzed existing technologies such as IEEE 802.15.4 [3], while others have proposed new techniques for power-efficient communication in WBANs. The authors of [4] investigated the suitability of IEEE 802.15.4 MAC protocol for WBANs; however, their analysis was confined to periodic and asymmetric traffic. In [5], the authors proposed a random access protocol that supports quality of service for multiuser mobile WBANs. This protocol addressed inter-WBAN interference and energy wastage problems caused by network mobility and provided support for latency and energy control. The authors of [6] proposed a reliable power-saving mechanism that strives to reduce collisions and idle listening. They also proposed a distributed queuing MAC protocol and evaluated its performance for different network loads [7, 8]. The performance of IEEE 802.15.6-based CSMA/CA procedure was investigated in [9] where the minimum delay and maximum throughput for different narrow band frequency bands were derived. The authors of [10, 11] developed an analytical model to evaluate the performance of contention-based WBANs. They developed a Markov chain to model backoff procedure of IEEE 802.15.6 under saturated and nonsaturated conditions. Their study also investigated the effectiveness of exclusive and random access phases. A similar study was conducted in [12] where the authors investigated the impact of different periods on the IEEE 802.15.6 superframe structure. They considered saturated and error prone channel and developed a Markov chain for analyzing different traffic loads on the IEEE 802.15.6 networks. In [13], the authors studied the integration of radio frequency identification (RFID) technology with WBANs and concluded that RFID-based wakeup methods can play a significant role in extending the network lifetime to years. A superframe-level time hopping scheme for WBAN with variable contention access period was presented in [14]. While maintaining the similar interference mitigation, the proposed scheme improved performance of WBAN in terms of energy dissipation, latency, and spectrum efficiency. The authors of [15] recently proposed an adaptive time division multiple access (TDMA) protocol based on periodic wake up schedules, which efficiently handles overhearing and idle listening problems in WBANs. Another study presented in [16] proposed a traffic-aware dynamic MAC protocol that dynamically adjusts wake-up intervals based on traffic status register bank. The dynamic wake-up intervals save extra power consumed by idle listening, overhearing, collisions, and unnecessary beacon transmission. A priority-based TDMA protocol is presented in [17], where the transmission schedules are based on priorities of data packets. This protocol dynamically adjusts the superframe structure according to the traffic load, thereby minimizing power consumption of the network.

3. PMAC Protocol

The following sections discuss the general description, priority-guaranteed resource allocation, and security support of PMAC protocol.

3.1. General Description. The PMAC protocol operates in a beacon-enabled mode, where beacons are transmitted at the end of each superframe. The superframe consists of a beacon, two contention access periods (CAP1 and CAP2), and one contention-free period (CFP) as given in Figure 1. The beacon is used for resource allocation information. It also carries security codes in order to allocate resources to legitimate users. The CAP1 considers a priority-guaranteed CSMA/CA procedure for data transmission. The operation of the priority-guaranteed CSMA/CA is partially based on IEEE 802.15.6 standard [18]. The CFI has an optional period for slotted-ALOHA protocol (this is not considered in our analysis). Depending on the application requirements, the slotted-ALOHA protocol may be used to send short data and command frames. For example, for low-traffic situations, the slotted-ALOHA may be used to allocate resources to nodes in the CFP period. The CFP period consists of multiple TDMA slots and is used for a large amount of data packets including streaming data. The CAP2 is an optional period which is used to finish the pending transmission of CAPI. This period is also used to inform the coordinator of incomplete transmission in the previous CFP slots. In addition, the PMAC considers a one-hop star topology network with uplink traffic only. The entire operation of the network is controlled by the WBAN coordinator.

3.2. Priority-Guaranteed Resource Allocation. For resource allocation, the coordinator continuously broadcasts beacons to all nodes, and only active nodes are able to receive the beacons. The PMAC protocol allows low duty cycle nodes to remain in sleep mode in order to save their energy (consumed by beacon overhearing). The nodes which have no data to send or receive do not need to wakeup and receive the beacons. The nodes requiring the allocation of TDMA slots send a request to the coordinator in the CAP period. Upon receiving the request, the coordinator allocates TDMA slots
in the CFP period of the following superframe. Figure 2 shows the beacon format of PMAC protocol. The details of each field are present in [18].

In the CAP period, the PMAC protocol employs the priority-guaranteed CSMA/CA procedure. The procedure of this protocol is based on IEEE 802.15.6 standard [18] where the node sets the backoff counter to a random integer that is uniformly distributed over \([1, CW]\) where \(CW \in (CW_{\text{min}}, CW_{\text{max}})\). Traditional CSMA/CA procedure initially sets its backoff counter to a random integer selected from a fixed-size CW. Because WBAN may have different nodes with different priorities, the use of a fixed-size CW is not a reliable approach, for example, electrocardiogram and blood pressure nodes may have high and low priorities, respectively. The priority-guaranteed CSMA/CA prioritizes all the nodes by assigning different \(CW_{\text{min}}\) and \(CW_{\text{max}}\) values to them as given in Table 1.

Nodes having high priorities will have a small CW and those having low priorities will have a large CW. Once the backoff counter is selected, the node starts decrementing this counter for each idle CSMA slot. Once the backoff counter reaches zero, the node transmits the data. If the channel is busy due to a frame transmission, the node locks its backoff counter until the channel becomes idle. Unlike IEEE 802.15.6 CSMA/CA where the CW is doubled for even number of failures, the CW in the priority-guaranteed CSMA/CA is doubled for each failure. Figure 3 shows the resource allocation of a priority-guaranteed CSMA/CA procedure.

### Security Support

Since WBANs are mostly used for health applications, attacks on these networks may create serious circumstances for their users. Each WBAN must be able to support strong security protocols in order to enable secure communication on the channel. In addition, these protocols must also be able to address other security issues such as data confidentiality, data authentication, data freshness, data availability, and secure management. The security mechanism of the PMAC protocol is based on security levels: (1) unsecured communication level, where the data is transmitted in unsecured frames, (2) authentication level, where the data is transmitted in secured authentication with no encryption, and (3) authentication and encryption, where the data is transmitted in authenticated and encrypted frames. The PMAC protocol uses a master key (MK) for establishing a secure communication. The MK is pre-shared between the nodes and the coordinator. Once the pre-shared MK is activated during association, the nodes generate a pairwise temporal key (PTK) for a single session upon mutual agreement. The frames are then authenticated and encrypted using the AES-128 counter. The secure MK and PTK keys prevent adversaries from penetrating into the network and from manipulating different active and passive attacks including backoff manipulation and replay attacks.

### Analytical Approximations of PMAC

Let \(i = (0, 1, 2, \ldots, 7)\) represent the priority class of the nodes in the CAP period (CFP periods are not considered in the analysis) and let \(n_i (i = 0, 1, \ldots, N - 1)\) be the number of finite stations in the priority \(i\) class. Let \(r_i\) represent the probability that a node transmits in the priority \(i\) class. The probability \(p_i\)
that $n_i$ senses the channel busy in the backoff stage is given by [19]

$$p_i = 1 - \left[ \sum_{x=0}^{i-1} (1 - \tau_x)^{n_x} \right] \left( 1 - \tau_i \right)^{n_i - 1} \left[ \sum_{x=i+1}^{N-1} (1 - \tau_x)^{n_x} \right].$$ (1)

The probability $\sigma$ is that the channel is busy or there is an ongoing transmission during a slot time is given by

$$\sigma = 1 - \left[ \sum_{x=0}^{N-1} (1 - \tau_x)^{n_x} \right].$$ (2)

The transmission probability $\tau_i$ is given by the fraction of average number of attempts $E[A_i]$ for the priority class $i$ to the average number of backoff $E[B_i]$ that a node needs to transmit the data successfully. According to [19], the expressions for $E[A_i]$ and $E[B_i]$ are given by

$$E[A_i] = \sum_{j=0}^{M_i} \left[ j p_i^j (1 - p_i) \right].$$ (3)

The probability that the data is successfully transmitted after $j$th retry is $p_i^j (1 - p_i)/(1 - p_i^{M_i} + 1)$, where $M_i$ is the retry limit of $n_i$ in the priority class $i$. The number of backoff slots in the $j$th retry is $\sum_{x=0}^{i} (W_{i,x} - 1)/2$. The expression for $E[B_i]$ is given by

$$E[B_i] = \sum_{j=0}^{M_i} \left[ p_i^j (1 - p_i) \right] \left[ \sum_{x=0}^{j} (W_{i,x} - 1) \right]/2.$$ (4)

The probability $\tau_i = E[A_i]/E[B_i]$ can be used to solve (1) and (2).

4.1. Average Delay. The average delay $E[D_{PMAC}]$ includes the delay of the packet when it arrives at the queue and the delay of the successful transmission. It is given by

$$E[D_{PMAC}] = E[B_i] \delta + E[W_i] + T_D + 2T_T + 2T_C$$ (5)

where $T_D, T_T, T_C$, and $\delta$ represent the data packet transmission time, the turn around time, control packet transmission time, and empty slot time, respectively. The $E[W_i]$ is the mean waiting time of the packets for priority class $i$. According to the nonpreemptive M/G/1 priority queuing system, $E[W_i]$ is given by

$$E[W_i] = \frac{\rho E[R]}{[1 - \sum_{j=0}^{i} \rho_j] [1 - \sum_{j=0}^{i} \rho_j]},$$ (6)

where $\rho = [E[B_i] + T_D + 2T_T + 2T_C]/L$ is the traffic intensity and $E[R]$ is the residual service time. The variable $L$ represents the average interarrival time of the packets.

4.2. Average Power Consumption. The average power consumption $E[P_{PMAC}]$ includes the power consumed during idle $P_{IDLE}$, transmit $P_{TX}$, and receive $P_{RX}$ states. The $E[P_{PMAC}]$ is given by

$$E[P_{PMAC}] = \left[ P_{IDLE} (L - E[D_{PMAC}]) + P_{TX} T_D + P_{RX} (T_S + 2T_T + 2T_C) \right]/(L + E[D_{PMAC}]),$$ (7)

where $T_S$ is the time to switch from idle to transmit or receive states.

4.3. Throughput. The saturated throughput $ST_i$ is fraction of average transmission time in a slot for a priority class $i$ to the total slot duration [20]. It is given by

$$ST_i = \frac{\psi_i E[P]}{[1 - \sigma] \delta + \psi T_b + [\sigma - \psi] T_{COL}},$$ (8)

where $T_b$ and $T_{COL}$ represent the average time the channel is sensed busy due to a successful transmission and due to a collision, respectively [21]. In addition, $E[P]$ is the average packet length. The $\psi_i$ is the successful transmission probability occurred in a slot time for a priority class $i$ and $\psi$ is the successful transmission probability in a slot time. According to [19], the expressions for $\psi_i$ and $\psi$ are given by

$$\psi_i = n_i \tau_i (1 - \tau_i)^{n_i - 1} \left[ \sum_{x=0}^{N-1} (1 - \tau_x)^{n_x} \right],$$ (9)

$$\psi = (1 - \sigma) \left[ \sum_{x=0}^{N-1} n_i \tau_x \right]/[1 - \tau_x] \sum_{x=0}^{N-1} n_i \tau_x.$$ (9)

For PMAC, the expressions for $T_b$ and $T_{COL}$ are

$$T_b = PHY + MAC + SIFS + DIFS + 2p + T_c + T_D,$$

$$T_{COL} = PHY + MAC + DIFS + T_D,$$ (10)

where PHY, MAC, SIFS, DIFS, and $p$ represent the physical layer header, MAC layer header, short interframe spacing, distributed coordination function (DCF) interframe spacing, and propagation delay, respectively.
Table 2: Simulation parameters (the symbol rate is calculated based on [18]).

| Parameter | Value |
|-----------|-------|
| CCA       | 63/Symbol rate |
| $M_0$     | 4     |
| $M_1$     | 7     |
| CSMA slot length | CCA + 20 $\mu$s |
| MAC footer | 16 bits |
| Propagation delay $p$ | 1 $\mu$s |
| $P_{\text{IDLE}}$ | 5 $\mu$W |
| $P_{\text{RX}}$ | 1.8 mW |
| $T_S$     | 0.4 ms |
| $T_C$     | 1.9 ms |
| $E[P]$    | 245 bytes |
| PHY       | 31 bits |

5. Performance Results

The basic operation of the PMAC protocol is simulated in an independent C++ simulator. The nodes generate uplink Poisson traffic in a star topology network. Initially, we consider two priority classes (class 0 and class 1) for performance analysis; however, the analysis is valid for all types of priority classes. The $CW_{\min}$ and $CW_{\max}$ for priority classes 0 are 16 and 64 and for priority class 1 are 16 and 32, respectively. The simulation parameters are listed in Table 2. We are interested in analyzing the PMAC protocol in terms of the following parameters.

(i) Average Delay. This is the average delay of a packet in the queuing, backoff, and transmit states for a priority class $i$.

(ii) Average Power Consumption. This is the average power consumed in the backoff, transmit, and receive states for a priority class $i$.

(iii) Throughput. This is the saturation throughput of WBAN.

(iv) Packet Loss Probability. The packet loss probability $P_{\text{LOSS}}$ is the probability of a packet when it fails at $M_i + 1$ attempts and is derived as $P_{\text{LOSS}} = P_{\text{TX}}^{M_i+1}$.

(v) Number of Corrupted CFP Slots. This is the total number of CFP slots that are corrupted by an attacker. The attacker first listens to the beacon in the beginning of the superframe period and grabs knowledge about the slot boundaries of CFP period. Once the CFP slots are known, the attacker creates interference in these slots.

Figure 4 shows the average delay as a function of number of nodes in priority class 0 and class 1. Because class 0 has longer waiting and queuing delays, its average delay is comparatively more than that of class 1. In addition, when the number of nodes increases, the average delay increases; this is because of increase in packet loss and collision probabilities. In addition, the average power consumption for class 0 is more than that of class 1 for a few number of nodes as illustrated in Figure 5. However, when the number of nodes in a high priority class is increased (for a fixed CW), the power consumption will eventually increase and will be much higher than that of a low priority class. This figure also shows the average power consumption of IEEE 802.15.4 protocol, which is much higher than class 0 and class 1. This is due to the fact that all nodes in IEEE 802.15.4 network compete for the channel with the same priorities. The saturation throughput is shown in Figure 6, where class 0 has much higher throughput than that of class 1 and class 2. The latter two classes have small CWs and therefore have high chances of collisions. Since class 0 has a low retry limit, it is unable to transmit all packet successfully and has a higher packet loss probability as illustrated in Figure 7. The trend in Figure 7, however, depends on the number of retry limit $M_i$. Figure 8 shows different attacks on the CFP slots of the superframe, where the attacker corrupts the CFP slots by gaining the resource allocation information through beacons. It can be seen that proper authentication and encryption procedure is able to prevent most of the CFP attacks. This is due to the use of secure MK and PTK keys which do not allow adversaries to grab beacons and to penetrate the CFP slots.

6. Conclusion

This paper introduced a hybrid and secure MAC protocol which prioritizes the nodes by using a priority-guaranteed
CSMA/CA procedure in the CAP period. The priorities are adjusted according to the CW. The PMAC protocol used CFP periods for large amount of data packets. Analytical approximations were derived to analyze the performance of CAP period in terms of average delay, power consumption, throughput, packet loss probability, and number of corrupted CFP slots. The analytical approximations were validated by computer simulations. In future, we will derive analytical approximations for the CFP period and will study its feasibility for multimedia WBANs.

**Conflict of Interests**

The authors declare that they have no conflict of interests.

**Acknowledgment**

This work was supported by the Research Center of College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia, through the Research Project no. RC121244.

**References**

[1] S. Ullah, H. Higgins, B. Braem et al., "A comprehensive survey of wireless body area networks: on PHY, MAC, and network layers solutions," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[2] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[3] IEEE, 802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs) Used in or around a Body, IEEE, Piscataway, NJ, USA, 2006.

[4] N. F. Timmons and W. G. Scanlon, "Analysis of the performance of IEEE 802.15.4 for medical sensor body area networking," in *Proceedings of the 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON’04)*, pp. 16–24, Santa Clara, Calif, USA, October 2004.

[5] S. Cheng, C. Huang, and C. C. Tu, "RACOON: a multiuser QoS design for mobile wireless body area networks," *Journal of Medical Systems*, vol. 35, no. 5, pp. 1277–1287, 2011.

[6] B. Otal, L. Alonso, and C. Verikoukis, "Highly reliable energy-saving mac for wireless body sensor networks in healthcare systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 553–565, 2009.

[7] B. Otal, L. Alonso, and C. Verikoukis, "Towards energy saving wireless body sensor networks in health care systems," in *Proceedings of the IEEE International Conference on Communications Workshops (ICC ’10)*, pp. 1–5, May 2010.

[8] B. Otal, L. Alonso, and C. Verikoukis, "Design and analysis of an energy-saving distributed MAC mechanism for wireless body sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, Article ID 571407, 13 pages, 2010.

[9] S. Ullah, M. Chen, and K. Kwak, "Throughput and delay analysis of IEEE 802.15.6-based CSMA/CA protocol," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3875–3891, 2012.
[10] S. Rashwand, J. Mišić, and H. Khazaei, “IEEE 802.15.6 under saturation: some problems to be expected,” *Journal of Communications and Networks*, vol. 13, no. 2, pp. 142–148, 2011.

[11] S. Rashwand and J. Mišić, “Performance evaluation of IEEE 802.15.6 under non-saturation condition,” in *Proceedings of the 54th Annual IEEE Global Telecommunications Conference (GLOBECOM ’11)*, pp. 1–6, Houston, Tex, USA, December 2011.

[12] S. Rashwand and J. Mišić, “Effects of access phases lengths on performance of IEEE 802.15.6 CSMA/CA,” *Computer Networks*, vol. 56, no. 12, pp. 2832–2846, 2012.

[13] S. Ullah and A. Alamri, “A secure RFID-based WBAN for healthcare applications,” *Journal Medical Systems*, vol. 37, Article ID 9961, 2013.

[14] Z. Jian, L. W. Hanlen, A. Y. Wang, and H. Xiaojing, “Superframe-level time-hopping system with variable contention access period for wireless body area communications,” in *Proceedings of the IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC ’11)*, pp. 2178–2182, Toronto, Canada, September 2011.

[15] A. Rahim, N. Javaid, M. Aslam, U. Qasim, and Z. A. Khan, “Adaptive-reliable medium access control protocol for wireless body area networks,” in *Proceedings of the Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON ’12)*, pp. 56–58, 2012.

[16] M. M. Alam, O. Berder, D. Menard, and O. Sentieys, “TAD-MAC: traffic-aware dynamic MAC protocol for wireless body area sensor networks,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 2, no. 1, pp. 109–119, 2012.

[17] I. Anjum, N. Alam, M. A. Razzaque, M. M. Hassan, and A. Alamri, “Traffic priority and load adaptive MAC protocol for QoS provisioning in body sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 205192, 9 pages, 2013.

[18] IEEE 802. 15. 6, Wireless Medium Access Control (MAC)and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs) used in or around a body, 2012.

[19] Y. Xiao, “Performance analysis of priority schemes for IEEE 802.11 and IEEE 802.1 le wireless LANs,” *IEEE Transactions on Wireless Communications*, vol. 4, no. 4, pp. 1506–1515, 2005.

[20] S. Ullah, M. Chen, and W. Alsalih, “Performance analysis of contention access period of IEEE 802.15.3 MAC protocol,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 13, no. 3/4, pp. 158–166, 2013.

[21] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535–547, 2000.
