Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 7, pp. 2771–2778
DOI : 10.47974/JIOS-2331

Energy harvesting enabled cryptographically secure MAC design for IEEE 802.15.6 WBANs

Anita Shukla [†]
Department of Basic Sciences & Humanities
Pranveer Singh Institute of Technology
Kanpur 209305
Uttar Pradesh
India

Ankit Jain [*]
Department of Electronics & Communication Engineering
Pranveer Singh Institute of Technology
Kanpur 209305
Uttar Pradesh
India

Sneha Khoria [§]
Department of Computer Science & Engineering
Pranveer Singh Institute of Technology
Kanpur 209305
Uttar Pradesh
India

Hema Singh [‡]
Department of Basic Sciences & Humanities
Pranveer Singh Institute of Technology
Kanpur 209305
Uttar Pradesh
India

[†] *E-mail:* shukla.anita27@gmail.com
[*] *E-mail:* ankit2483jain@gmail.com (Corresponding Author)
[§] *E-mail:* snehakhoria@gmail.com
[‡] *E-mail:* hemasingh11@gmail.com

Awanit Kumar [@]
Rohit Maheshwari [#]
Department of Computer Science and Engineering
Career Point University
Kota 325003
Rajasthan
India

Abstract

Wireless Body Area Network (WBAN) uses Cryptographic Security for the protection of sensitive information stored and transmitted between body-worn devices (i.e. medical devices). Although Cryptographic Security is important, the WBAN needs to provide a reliable method of communicating and an efficient method of consuming energy in order to provide next-generation healthcare and wearable technologies, especially within the Medical/Nursing Industry, as well as assistive technology, such as sports monitoring solutions. Recently, continued advancements within the area of Energy Harvesting Technologies have enabled the WBAN to provide sustainable operation through the use of Energy Harvesting from Body Motion, Heat, and/or Ambient Sources, thereby extending the lifetime of a WBAN Network. Due to the random availability of harvested energy, however, IEEE 802.15.6 MAC protocol performance is impacted due to its emphasis on using a back-off strategy when "saturated." This paper presents Discrete-Time Markov Chain (DTMC) Analytical Model for performance assessment of cryptographically protected IEEE 802.15.6 MAC protocols operating in Energy Harvesting WBANs. The Analytical Model was developed to include MAC Back-off behavior and the cryptographic processing overhead of the MAC protocol.

Subject Classification: *Primary 68P20, Secondary 68T99.*

Keywords: *Cryptographic security, Wireless body area networks (WBAN), IEEE 802.15.6, Energy harvesting, Discrete-time markov chain (DTMC), MAC protocol, Performance analysis.*

1. Introduction

Due to the increasing age of the world's population (in 2013 the world demo consisted of 11.7% of people who were 60 years or older, and this percentage was projected to increase to 21.1% by 2050 according to the UN [1]), there will be an increased need for secure and energy-efficient solutions to monitor patients and their medical conditions with constant oversight and long-term management of chronic and life-threatening ailments associated with aging. Approximately 75% of the global case rates of Non-Communicable Diseases (NCDs) which accounted 68% of total number of death tolls worldwide during 2012, occur among persons 60 years of age and older [2]. The prolonged nature of these injuries or illnesses leads to a need for an increased degree of monitoring, increased healthcare use, and increased healthcare spending the highest percentage of which in the US has been estimated to have reached

[@] *E-mail:* `itsawanitkumar@gmail.com`
[#] *E-mail:* `rohit.maheshwari27@gmail.com`

17.9% of GDP in 2012 [3]. With recent advancements in wireless technology and sensor technology, there is now the possibility of conducting remote continuous health monitoring of individuals where secure transmission of data allows for early detection of diseases and thereby reducing the occurrence of hospitalizations and treatment expenses while increasing the quality of life of patients [4]. WBANs consist of collections of sensors attached to an individual, allowing for the remote monitoring of an individual's vital signs, and the ability to perform automated actions like delivering medications and exchanging secured data using cryptography. Likewise, data must be secured to ensure confidentiality, integrity, and authenticity in order to create and maintain trust and reliability. The IEEE 802.15.6 standard [5] describes physical layer and medium access control (MAC) layer for ultra-low-power WBANs. This standard is planned for very low data rates, energy constraints, and a need for reliability. The most common network topology used in WBANs is star topology all nodes communicate with central WBAN hub. Two-hop communication is also supported [6], which helps address the problem of increased signal attenuation through the body due to tissue absorption, body movement, and shadowing. In addition, these technological advances have enabled the development of multi-hop cooperative communication techniques to improve network performance by increasing communication link quality and decreasing latency and packet loss [7, 8]. The limitations imposed by the battery lifetime of WBAN devices are the biggest challenges to providing an energy-efficient solution, since changing out a worn-down battery is not always practical for wearable or even implantable devices. Therefore, energy-efficient MAC protocols [9-12] have been developed to help reduce power consumption while still allowing for the provision of Quality of Service (QoS) and maintaining high levels of security.

2. Background Study

The IEEE 802.15.6 standard addresses wireless communication in WBAN, specifying that multiple types of service for different information will be provided. As this standard outlines the different User Priorities (UPs) assigned to a variety of signals, including emergency signals, it provides a means to guarantee Quality of Service (QoS) when transmitting data in close proximity to other individuals' bodies or equipment.

2.1 *Summary of IEEE 802.15.6 MAC protocol*

In IEEE 802.15.6, three different modes for MAC (Medium Access Control) Operations exist, with the most commonly used mode being Beacon Mode with Superframes. Here, a wireless body area network (WBAN) is divided into equal-length synchronous time slots called Superframes, which begin with a Beacon frame and include a total of seven phases: Exclusive Access Phase One (EAP1), Random Access Phase One (RAP1), Managed Access Phase (MAP), Exclusive Access Phase Two (EAP2), Random Access Phase Two (RAP2), Managed Access Phase (MAP), and Contention Access Phase (CAP) (IEEE 802.15.6). The phases for each superframe can be seen in

Figure 1. The exclusive access phase can only be accessed by the node with the highest Priority (EAP) and if there is any CAP remaining then the B2 frame must be sent first (as an indication) after MAP has been completed. In addition, Resources are typically allocated within the MAP Phase via Polling.

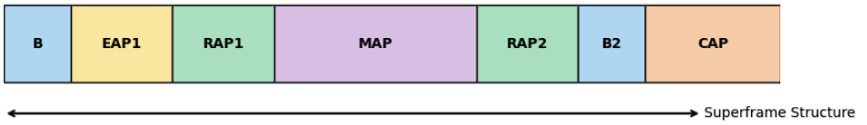

Figure 1
Superframe Structure for Beacon Mode

2.1.1 CSMA/CA mechanism

According to the IEEE 802.15.6 standard, only 8 different types of user priorities are allowed for nodes. These priorities are assigned based on different characteristics of user being utilized to send data to node. Although nodes send data to the channel at these different user priority levels, they transmit data to the channel using the CSMA/CA method. To do this, each node will maintain a backoff counter that is based on W_k, where W_k represents the window size for the backoff counter when the node is sending data to UP_k. To create the backoff counter, the node will generate a random integer from 1 through W_k. W_k can change as a function of the number of retries (r), which is calculated as below.

$$W_k(r) = \begin{cases} CW_{k,min} & r = 0 \\ W_k(r-1) & r = odd, r \le m \\ min\{CW_{k,max,} 2W_k(r-1)\} & r = even, r \le m \end{cases}$$

Here: $W_k(r)$ = Contention window size for priority class k at retry stage r
$CW_{k,\min}$ = Minimum contention window
$CW_{k,\max}$ = Maximum contention window
r = Retransmission attempt m = Maximum retry limit

There are numerous reasons a node's Backoff Counter may be locked or unlocked. A node's Backoff Counter will be "locked" if;

a) The backoff counter is reset by the system or the value drops to 0.
b) The node is attempting to listen, and the channel is busy or occupied by other nodes.
c) The time is currently not found in RAP, CAP or EAP.

3. Analytical Model

The section will first describe an energy harvesting model used by sensor nodes. Next, we will construct a discrete time Markov chain (DTMC) model to represent how the CSMA/CA-based medium access control (MAC) protocol defined in the IEEE 802.15.6 Standard works with an Energy Harvesting (EH) based Wireless Body Area Network (WBAN). We will also use the DTMC to derive closed form equations for evaluating performance of WSAN when the

sensors are harvesting energy. Finally, we will assume that the WSAN is operating at full capacity, or saturation.

3.1 *Cryptographically Secure Energy harvesting model*

In this section, we assume that each Node's energy is harvested from an energy Harvesting (EH) Model which is cryptographically secure, which follows a Poisson Distribution whereby the energy arrival at energy buffer of each node is distributed according to the Poisson Distribution. As for the energy buffer of every node, we assume it has infinite capacity. Performance analysis is simplified by converting EH from the Poisson process into a Bernoulli process. If there is less energy arriving than one Eunit, then it is regarded as zero. In addition, while a node is busy transmitting or sensing a packet, the node can also charge or recharge itself with additional energy. Therefore, the following equations represent the relationship between energy harvesting, energy storage and energy depletion.

$$E(t) = \begin{cases} E(t-1) & P_1 \\ E(t)+1 & P_0 = 1 - P_1 \end{cases}$$

Here, t is the index of time slot and E(t) is the state of the energy buffer.

3.2 *Discrete-Time Markov Chain model*

The procedure of CSMA/CA MAC protocol prescribed by (IEEE) 802.15.6 standard can be represented by a Discrete-Time Markov Chain (DTMC) model. It has been shown that during the Clear Channel Assessment (CCA) period, amount of power used is roughly equal to that consumed by transmission. Therefore, it can be assumed that both channel sensing and packet transmission consume equal amounts of energy Eth; thus, depicts DTMC model for CSMA/CA MAC protocol.

The contention technique implemented by the MAC protocol is expressed as a series of discrete transitions between different states, some of the state transition probabilities that have identical representations are absent from this representation. Each system state in the model can be completed in end of every time slot. A state's representation is tuple comprising 4 distinct components, with representation written in the format of {k, i(t), j(t), q(t)}. First, the user priority. Second, nth number of retries. Thirdly, the actual value of the backoff counter. Fourth, value of state of the energy buffer. Should this energy buffer reach a value of N, then it is used up immediately by the node when performing a CCA or for transmitting data when backoff counter value is greater than 1. When backoff counter value has reached 1, the node is to perform an immediate delivery of data once the backoff counter value becomes 0. State A to state B transition probability is denoted as P(A|B), and the following equations represent the probabilities associated with a few of the critical state transitions in the Discrete-Time Markov Chain.

$$P(k,i,j,q|k,i,j,q) = P_0 \qquad j \geq 2, q \leq (N-1) \; or \; j = 1, q \neq 2N$$

$$P(k,i,j,q+1|k,i,j,q) = P_1 \qquad j \geq 2, q \leq (N-1) \; or \; j = 1, q \neq 2N$$

$$P(k,i,j,q|k,(i-1),0,N) = P_q h_k / W_{k,i} \qquad i \neq 0, j \neq 0, q \epsilon (0,1)$$

$$P(k,0,j,q \mid k,i,0,N+1) = P_{q-1}(1-h_k)/W_{k,0},$$
$$i \neq m, j \neq 0, q \in (1,2)$$

$$P(k,0,j,q \mid k,m,0,N) = P_q / W_{k,0}, j \neq 0, q \in (0,1)$$

$$P(k,0,j,q \mid k,m,0,N+1) = P_{q-1}/W_{k,0}, j \neq 0, q \in (1,2)$$

$$P(k,i,j-1,q \mid k,i,j,N) = P_q(d_k f_k), j \geq 2, q \in (0,1)$$

$$P(k,i,j,q \mid k,i,j,N) = P_q(1-d_k f_k), j \geq 2, q \in (0,1)$$

$$P(k,i,0,q \mid k,i,1,2N) = P_{q-N}(d_k f_k), q \in (N, N+1)$$

$$P(k,i,1,q \mid k,i,1,2N) = P_{q-N}(1-d_k f_k), q \in (N, N+1)$$

Using transition probabilities provided above, determine steady-state probabilities of the DTMC by applying the property which uses that sum of all steady-state probabilities is 1.

$$\sum_{i=0}^{m} \sum_{q=N}^{N+1} b_{k,i,0,q} + \sum_{i=0}^{m} \sum_{q=N}^{2N} b_{k,i,1,q}$$
$$+ \sum_{i=0}^{m} \sum_{j=2}^{W_{k,i}} b_{k,i,j,N} + \sum_{q=0}^{N-1} \sum_{i=0}^{m} \sum_{j=1}^{W_{k,i}} b_{k,i,j,q} = 1$$

Probability of packet transmission τk and probability of CCA Pcca, k is determined as;

$$\tau_k = \sum_{i=0}^{m} \sum_{q=N}^{N+1} b_{k,i,0,q}$$

$$P_{cca,k} = \frac{P_1 \sum_{i=0}^{m} \frac{(W_{k,i}+1)}{2} h_k{}^i}{N\left[d_k f_k \sum_{i=0}^{m} h_k{}^i + \sum_{i=0}^{m} \frac{(W_{k,i}+1)}{2} h_k{}^i\right]}$$

Collision probability after transmitting hk including probability of channel being idle, dk, are defined as below,

$$h_k = 1 - (1-\tau_k)^{n_k - 1} \prod_{i \neq k, i=0}^{7} (1-\tau_i)^{n_i}$$
$$d_k = (1-\tau_k)^{n_k - 1} \prod_{i \neq k, i=0}^{7} (1-\tau_i)^{n_i}$$

The transmission probability Ptr, the probability of successful transmission of one node in UPk Psu,k, and probability of successful transmission in WBAN Psu is given below;

$$P_{tr} = 1 - \prod_{i=0}^{7} (1-\tau_i)^{n_i}$$
$$P_{su,k} = \tau_k d_k f_k = \tau_k f_k (1-\tau_k)^{n_k - 1} \prod_{i \neq k, i=0}^{7} (1-\tau_i)^{n}$$
$$P_{su} = \sum_{i=0}^{7} C_{n_i}^{1} P_{su,i} = \sum_{i=0}^{7} n_i \tau_i d_i f_i$$

4. Conclusion

This work presents DTMC model for the IEEE 802.15.6 MAC protocol in WBANs including energy-harvesting nodes. This study serves as an initial step toward assessing performance of IEEE 802.15.6 MAC protocol in WBANs equipped with energy-harvesting capabilities. Mathematical model validates the accuracy and effectiveness of suggested analytical approach aimed at evaluating the IEEE 802.15.6 MAC protocol under energy-harvesting conditions. For

future work, we plan to incorporate a more realistic energy arrival model and also address the unsaturated scenario, where packets arrive at each node according to a data arrival process, such as a Poisson arrival model.

References

[1] United Nations, Department of Economic and Social Affairs, Population Division, *World Population Ageing 2013*, Tech. Rep. ST/ESA/SER.A/348. New York, USA: United Nations (2013).

[2] World Health Organization, *Global Status Report on Noncommunicable Diseases 2014*. Geneva, Switzerland: WHO Press (2014).

[3] A. Chatterjee, S. Kubendran, J. King, and R. DeVol, *Chronic Disease and Wellness in America: Measuring the Economic Burden in a Changing Nation*. Santa Monica, CA, USA: Milken Institute (2014).

[4] E. Kartsakli, A. S. Lalos, A. Antonopoulos, S. Tennina, M. Di Renzo, L. Alonso, and C. Verikoukis, "A survey on M2M systems for mHealth: A wireless communications perspective," *Sensors,* vol. 14, no. 10, pp. 18009–18052 (2014), doi: 10.3390/s141018009.

[5] IEEE Computer Society, *IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks*, IEEE Std. 802.15.6-2012, pp.1–271 (Feb. 29, 2012), doi: 10.1109/IEEESTD.2012.6161600.

[6] A. Lalos, A. Antonopoulos, E. Kartsakli, M. Di Renzo, S. Tennina, L. Alonso, and C. Verikoukis, "RLNC-aided cooperative compressed sensing for energy-efficient vital signal telemonitoring," *IEEE Trans. Wireless Commun.,* vol. 14, no. 7, pp. 3685–3699 (2015), doi: 10.1109/TWC.2015.2435934.

[7] G. Arrobo and R. Gitlin, "New approaches to reliable wireless body area networks," in *Proc. IEEE Int. Conf. Microwaves, Communications, Antennas and Electronics Systems* (COMCAS), Tel Aviv, Israel, pp. 1–6 (2011), doi: 10.1109/COMCAS.2011.6105779.

[8] E. Kartsakli, A. Antonopoulos, A. Lalos, S. Tennina, M. Di Renzo, L. Alonso, and C. Verikoukis, "Reliable MAC design for ambient assisted living: Moving the coordination to the cloud," *IEEE Commun. Mag.,* vol. 53, no. 1, pp. 78–86 (2015), doi: 10.1109/MCOM.2015.7010516.

[9] C. Li, B. Hao, K. Zhang, Y. Liu, and J. Li, "A novel medium access control protocol with low delay and traffic adaptivity for wireless body area networks," *J. Med. Syst.,* vol. 35, no. 5, pp. 1265–1275 (2011), doi: 10.1007/s10916-011-9682-5.

[10] M. Ameen, J. Liu, S. Ullah, and K. S. Kwak, "A power-efficient MAC protocol for implant device communication in wireless body area networks," in *Proc. IEEE Consumer Commun. Netw. Conf.* (CCNC), Las Vegas, NV, USA, pp. 1155–1160 (2011), doi: 10.1109/CCNC.2011.5766534.

[11] K. S. Kwak and S. Ullah, "A traffic-adaptive MAC protocol for WBAN," in *Proc. IEEE GLOBECOM Workshops*, Miami, FL, USA, pp. 1286–1289 (2010), doi: 10.1109/GLOCOMW.2010.5703420.

[12] S. Banakar, V. Ramuloo, L. Vegi, A. Kumar, R. Maheshwari, and N. Singh, "Spectral graph theory for large-scale network topology optimization in cloud computing," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 7, pp. 2899–2906 (2025), doi: 10.47974/JDMSC-2560.

Received December, 2025