Impact of Duty Cycle Protocols on Security Cost of IoT

Sultan Alharby, Jeff Reeve, Alex Weddell, Nick Harris
Electronics and Computer Science Department
Southampton University
Southampton, UK
sa1c15, jsr, asw, nrh@ecs.soton.ac.uk

***Abstract*—With the evolution of IoT embedded devices and their broad application, security has become crucial. Security comes at a cost to these limited devices in terms of energy. However, evaluating security cost is not straightforward, as there are many factors involved, such as the employed security services and type of hardware. This research studies the impact of duty cycle protocols on security cost in IoT embedded devices. It begins by evaluating the cost of security on a per-packet basis, and then evaluates how duty cycle protocols could affect security cost. The research demonstrates the relationship between duty cycle protocols and security cost, which could be a source of confusion when measuring the actual security cost in a real scenario.**

***Index Terms*—Security Cost, Duty Cycle Protocol, Energy Consumption**

I. Introduction

The concept of the Internet of Things (IoT) has received much attention over the last five years. It is predicted that the IoT will influence every aspect of our lifestyles in the near future [1] . The IoT embedded devices are one of the key enablers of the operation of IoTs, allowing data to be collected from the surrounding environment. However, due to their limited resources, nature of deployment and unattended operation, IoT embedded devices are vulnerable to various types of attack. Security is paramount and essential for reliable and safe communication between IoT embedded devices [2] [3]. Therefore, utilising the limited resources available to protect the communication between these embedded devices is a complex task. These embedded devices are usually equipped with small batteries [4], which makes energy conservation crucial. Security cost is not straightforward [5], as many factors affect the obtained result such as the employed security services and type of hardware.

In this research, security cost is defined as the energy consumption which is additional to the packet transmission for security services. Most published researches have studied the cost of security based on packet-basis. Most of these studies has focused on studying the extra bytes added by security and the required time for Microcontroller Unit (MCU) to process complex security algorithms. This methodology is important and has been demonstrated by many researchers. Evaluation by this methodology has shown that security services such as encryption, replay protection and authentication add overhead to the packet being transmitted [6] [7] [8]. This overhead is expressed by the extra time required by radio to transmit the added bytes for authentication service and the time needed by the MCU to process complex encryption/decryption and authentication algorithms. However, this overhead is just represents the cost of security for transmitting one packet with the security header, and therefore is only part of the actual security overhead. What is missing is the impact of duty cycle protocols on the cost of security.

This research focuses on how duty cycle could affect the security cost at the data link layer. There are many different types of duty cycle protocols for an IoT embedded system, and these protocols ensure that radio is turned off as much as possible, while allowing different embedded devices to communicate. Security services affect radio energy consumption and therefore their cost is affected by the duty cycle. This has been neglected by previous researches when evaluating security cost. To study whether duty cycle protocols affect the security cost at data link layer, we must first understand the cost of security per packet, and prove that security does add cost in terms of energy. This will help us to understand the communication and computation overhead added by security. Then, it is necessary to study the work mechanism of the employed duty cycle protocol to investigate whether it affects security overhead.

II. Related Work

Many researchers have studied the cost of security for IoT embedded devices at the data link layer. In [7] the cost of encryption algorithms with different modes of operation has been studied. The evaluation uses MicaZ and TelosB hardware. The results show the cost of different types of symmetric encryption. Another research, conducted by [9], proposes an optimised implementation of Advanced Encryption Standard (AES) which uses a hardware accelerator with different modes of operation. The research compares it with software implementation in terms of energy consumption, and concludes that hardware implementation is more efficient. In [10], the authors have studied and compared AES, RC5 and RC6 encryption, and the results indicate that, among the three

evaluated encryption algorithms, AES is the most expensive in terms of energy consumption. These researches are useful for explaining the security cost on a per packet-basis. However, what is missing is an evaluation of the impact of duty cycle on the security cost. The cost of security depends on the number of security services invocation. Hence, duty cycle protocols might affect the overall security cost. This, to the authors knowledge, is the only research that evaluates the relationship between duty cycle protocols and security cost for IoT embedded devices.

III. IEEE 802.15.4 Security Specification

In this section we present the security services covered in the evaluation. IEEE 802.15.4 security specification is used in this research to measure the security cost of IoT embedded devices. This is the most widely used security specification in IoT embedded devices at the data link layer. IEEE 802.15.4 defines the security requirements in the data link layer [11], and supports security techniques to protect the wireless communication from possible attack. These techniques assure the confidentiality, integrity, authenticity and replay protection on a per-frame basis [12]. IEEE 802.15.4 offers two operational modes: a beacon-enabled mode, and a non-beacon enabled mode [13]. In the former case, the network communication is managed by a coordinator [11]. The coordinator sends regular beacons to synchronise embedded devices and manage all communication. With beacon-disabled mode, every embedded device can access the channel through a CSMA/CA protocol which is the used mode in this evaluation. IEEE 802.15.4 security layer is controlled at the data link layer, and the security requirements are specified at the application layer [11]. If no security mechanism is chosen at the application layer, then communication will be unsecured.

IEEE 802.15.4 offers a security suite which supports eight different security levels, as shown in Table I. Each security level supports specific security requirements and has a different frame format. These security levels generally offer no security, encryption only (AES-CTR), authentication and integrity only (AES-CBC-MAC), or all three security services: encryption, integrity and authentication (AES-CCM). AES-CBC-MAC uses three different MIC lengths: 4, 8 and 16 bytes [14]. Also, CCM supports a high level of security with the option of 4, 8 and 16 bytes. MIC is used to guarantee that data has not been changed, and also guarantee that data has originated from a legitimate source. The length of MIC represents the strength of integrity and authentication. The name of each level consists of two to three parts. The first part indicates the cryptography scheme (AES if security parameters is enabled). The second part indicates the mode of operation used in the cryptography scheme. The last part, if applicable, indicates the Message Integrity Code (MIC), which can be of varying length. Advanced Encryption Standard (AES) cipher is used in the standard with a fixed block size of 128 bits and different key lengths of 128, 192 or 256 bits [13]. However, the employed key length is 128 bits. An unsecured frame consists of three fields: a MAC header with 7 to 23 bytes, data payloads with 0 to 115 bytes, and Frame Check Sequences (FCS) with 2 bytes [12]. A secured frame has one more field named Auxiliary Security Header (ASH), with 5 to 14 bytes. This is in addition to the Message Integrity Code (MIC) if authentication is enabled. One of the contents of ASH is the Frame Counter with 4 bytes for replay attack detection. Frame counter is set by the outgoing frame at the transmitter side. The frame counter field is checked at the receiving embedded devices, and is accepted if the value is higher than the previous received value.

TABLE I
Security Suites, Reproduced from [15]

SiuteID	Describtion	Security Services	MIC Length
0	No Security	Null	0
1	AES-CBC-MAC-64		4
2	AES-CBC-MAC-64	Authentication	8
3	AES-CBC-MAC-128		16
4	AES-CTR	Encryption only	0
5	AES-CCM-32	Authentication	4
6	AES-CCM-64	and	8
7	AES-CCM-128	Encryption	16

IV. Experimental Setup

This research uses the Contiki OS developed by a world-wide community of experts.Contiki is a highly portable open source OS and runs on many different wireless sensor platforms. It supports a simulator called Cooja [16], which allows developers to debug and simulate their applications on large-scale networks. Cooja is used in this research for simulation. Cooja provides a means of estimating the power consumption of the radio and MCU. The Powertrace tool [17], which is supported in Contiki, is used to provide detailed information about where power is being consumed (transmission, receiving, etc), and calculates the time each component spends in a particular mode. Cooja can emulate real hardware. Sky hardware is emulated in the simulator. The two components affected by security services are the MCU and radio. Hence, the following formula is used to measure the energy consumed by security:

$$E_{sec} = E_{sec-compu} + E_{sec-comm} \quad (1)$$

where E_{sec} the energy consumed by security, $E_{sec-compu}$ computes the energy consumed by MCU for security, and $E_{sec-comm}$ the energy required by the radio to send the extra bytes neccessary for security. The cost of transmitting a packet without security services will be used as a *baseline* to calculate security cost. A higher security level is associated with higher security services, which will generally consume more energy. Each security level will be evaluated in terms of energy, and the difference between the current and baseline level is the security cost for that particular security level. The current drawn by Tmote sky components in different modes is required

to calculate energy consumption. Tmote sky uses cc2420 as transceiver and MSP430 as a micro-controller. The current drawn by these components is shown in Table II.

TABLE II
TYPICAL CURRENT CONSUMPTION FOR TMOTE SKY

Component	Current drawn
MCU- Active state	2.4mA
Radio - Transmitting mode	17.4mA
Radio - Receiving mode	19.7mA

The parameters which used in this evaluation are shown in Table III

TABLE III
SIMULATION PARAMETERS

Parameter	Value
Platform	Tmote Sky
MAC protocol	CSMA
Radio Duty Cycle	ContikiMAC
Payload	24 byte
Transmission range	50 Meters
TX/RX success ratio	100%
Radio	CC2420
Microcontroller unit (MCU)	MSP430

Energy consumption for each component can be measured by calculating the time each component spends in a certain mode (receiving, transmitting, idl...). The following formula is used to achieve this:

$$E = Energest\_Value * Voltage * Current \\ / RTIMER\_SECOND * runtime \quad (2)$$

Where, E is the amount of energy consumed by an embedded device's component in a particular mode, $Energest\_Value$ is the difference in ticks between two interval times, and $RTIMER\_SECOND$ is the number of ticks per second, which is equal to 32768 ticks/second in this simulation. The evaluation has been repeated for each security level. The results are shown in Table IV

V. SECURITY COST

Table IV shows the energy consumption of both MCU and radio when transmitting a packet with 24 bytes payload for all IEEE 802.15.4 security levels. As can be seen from the table IV and Figure 1 that radio is the main contributor to energy consumption. It constitutes 73.7% of the total energy consumption at level 0, and 88.5% at security level 7. This indicates the important of duty cycle protocol as it responsible for controlling radio. MCU consumes only 12% at level 0, and this increases as the code grows in complexity with higher security levels. In general the security cost at the first three levels fluctuates between 31.54%, at security level 1, and 60.46% at top security level based on the MIC lengths[4, 8, 16 bytes]. Increasing the MIC length used for authentication would keep the radio active for longer, allowing more bytes to be sent. This explains the great energy consumption when enabling authentication. The cost of security at the fourth level is almost 33% since only encryption is supported. The last three security levels support authentication, encryption, integrity, and replay protection attack. Hence, they are the most energy consuming levels among all security levels. The only difference between the last three levels is authentication length, which can be as described in the first three levels 4, 8, and 16 bytes. The results shows an overhead added by security services which could shorten the network lifetime significantly.

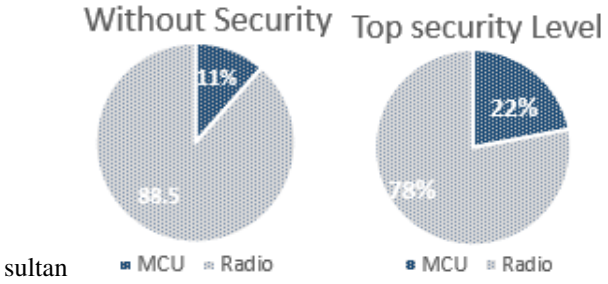

Fig. 1 Radio consumption vs MCU consumption for level 0 and 7

VI. DUTY CYCLE PROTOCOLS

The main objective of duty cycle protocols is to disable the radio as often as possible [18], while allowing low power devices to communicate with each other at minimum requirement. This technique of controlling the radio state to save energy is called duty cycling [19]. To achieve this, several protocols have been proposed in the literature which trade-off these requirements and extend the network lifetime. These protocols can be classified into synchronous, asynchronous and semi-synchronous duty cycles [20], in relation to the mechanism employed to control the radio module. In a synchronous scheme embedded devices are time synchronised [20], hence all embedded devices wake up and sleep at a set time. Contrary to this, asynchronous embedded devices do not need to work simultaneously, and they have no agreed wakeup/sleep schedule. A semi-synchronous duty cycle combines the two methods by grouping neighbour embedded devices into a synchronised cluster where different clusters communicate with each other asynchronously. This research will discuss duty cycle from the perspective of security cost.

A. Impact of Duty Cycle on Security Cost

Security cost is based on the number of security services invocation, which in this case AES. The relation between security cost and duty cycle is that some duty cycle protocols increase the number of transmitted packet by re-transmission. This means greater AES invocation, which in-turn leads to greater energy consumption. To clarify, a typical duty cycle protocol, named ContikiMAC [18], is discussed as an example. This protocol uses an asynchronous mechanism, and supports two methods of transmission: unicast and broadcast.

TABLE IV
ENERGY CONSUMPTION OF TRANSMITTING ONE PACKET WITH A PAYLOAD OF 24 BYTE IN DIFFERENT SECURITY LEVELS

Security level	MCU energy consumption (μJ)	Radio energy consumption (μJ)	Total energy consumption (μJ)	Percentage of increased security overhead over non-secure packet (%)
0	9.53	73.28	82.81	-
1	24.01	84.91	108.926	31.54%
2	24.15	92.39	116.54	40.72%
3	24.32	103.546	127.87	54.4%
4	28.95	81.24	110.19	33%
5	28.5	83.8	112.3	35.6%
6	29.11	90.80	119.91	44.8%
7	29.33	103.55	132.88	60.46%

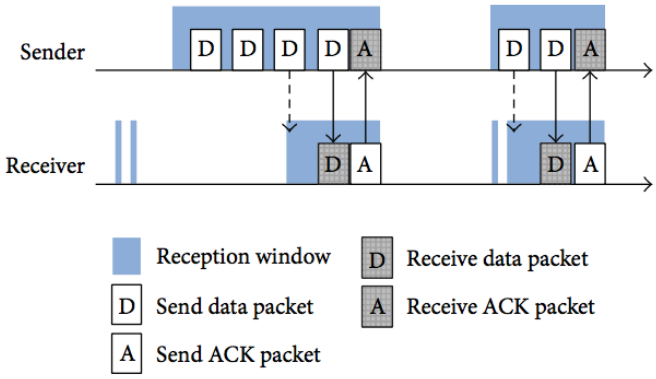

Fig. 2 Unicast transmission of Contiki-MAC.

Fig. 3 Unicast transmission of Contiki-MAC.

1) Unicast Transmission: In a unicast transmission, as shown in Figure 2, the sender checks the channel before transmission, and if it is free, the whole packet is sent repeatedly until the receiver wakes up and returns an acknowledgement. It is clear that successful delivery of one packet might require the transmission of many packets from the sender side. With every packet transmission the employed security services are invoked. Hence, the energy consumption for security processes is increased by the ContikiMAC duty cycle. To evaluate that in the simulation, we will conduct an experiment containing two nodes. Each node transmits packets to the other node. The employed duty cycle protocol in this experiment is ContikiMAC. Figure 3, which obtained from the simulator, shows the transmission for both $node1$ and $node2$. As can be noticed that one successful packet delivery requires multiple transmissions. The figure shows that, $node1$ transmits 4 packets before the receiver $node2$ wakes up and sends an acknowledgement, whereas $node2$ needs to send 7 packets before receiving acknowledgement from $node1$. The number of AES invocations in node 1 is less than in node 2. This retransmission is repeated with each packet delivery, which clearly demonstrates the effects of duty cycle on security cost.

To evaluate the effect of duty cycle on security cost, the PowerTracker tool supplied with the Cooja simulator is used. PowerTracker can present a detailed information on the total time the radio spends in active, receiving and transmitting modes. Figure 4 depicts the percentage of duty cycle for both $node1$ (Sky1 in the figure) and $node2$ (Sky2 in the figure) in all three modes. The $node1$ radio module is active for 5.72% of the time, while the radio in $node2$ is active for 6.87%. In both nodes, most energy is consumed during transmission mode, which explains the retransmission and AES invocations effects on the actual packet energy consumption. Security cost fluctuates between 31% and 60% per packet based on the selected security level, and this means that with each transmission attempt caused by duty cycle, there is extra overhead for security. Hence, the the actual security cost evaluation should take duty cycle into consideration.

Mote	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky 1	5.72%	1.39%	0.37%
Sky 2	6.87%	2.41%	0.37%
AVERAGE	6.29%	1.90%	0.37%

Fig. 4 Duty cycle evaluation for the two nodes.

To get more realistic evaluation for actual implementation, the number of delivered packets versus the retransmission tries for each node have been recorded for five minutes, as shown in Figure 5. Each node delivered 306 successful packets to the other node. However, $node1$ retransmitted 1224 packets to get the 306 packets delivered, while in $node2$ 2142 packets. This significant difference in retransmission is definitely affect the number of security features invocations, and consequently, affect the total security energy consumption.

2) Broadcast Transmission: in contrast, the broadcast transmission in ContikiMAC constantly sends the same packet repeatedly for a full interval wake-up time to ensure that all embedded devices have received the packet. There is no acknowledgement in the broadcast transmission, as illustrated in Figure 6. This mechanism consumes more energy compared to unicast transmission, as the security

features will be invoked repeatedly for a full interval wake-up time.

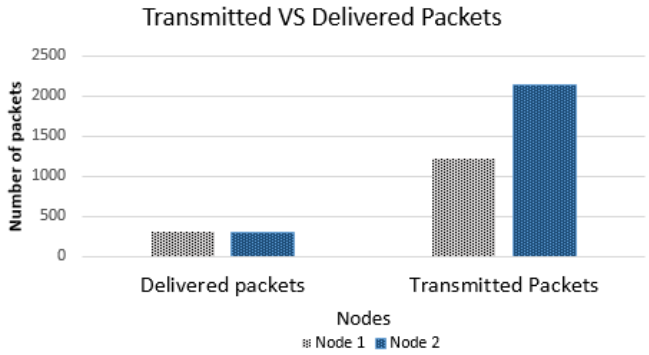

Fig. 5 Comparison between delivered and transmitted packets.

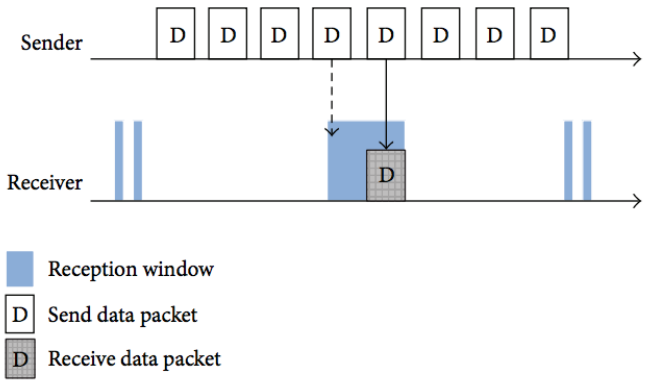

Fig. 6 Broadcast transmission of ContikiMAC.

The duty cycle protocols do not always affect the security cost; this depends on their work mechanism. The ContikiMAC protocol, as discussed previously, sends the whole packets repeatedly which requires multiple security invocations. Other protocols may use different mechanism allow for transmission to take place only when the receiver is active, so there is only one transmission for packet delivery. This is better in terms of security cost as there is only one security services invocation. For example, X-MAC [21] and LPL(Low Power Listening) [22]protocols uses short and long pre-amble to guarantee that the embedded receiver device has sufficient time to detect the pr-eamble and remain active before transmitting any packet from the sender. Hence, there is only one packet transmission, which means only one AES invocation.

VII. CONCLUSION

Security is crucial to IoT embedded devices. However, security comes at a cost to these constraint devices. The main issue here is that the exact security cost is still not known, as there are many influencing factors, such as the utilised security services and the used duty cycle protocol. This research has highlighted the impact of duty cycle protocols on security cost, an area which has been neglected by previous papers. First, it evaluates the security cost on a per packet-basis, and then prove that it adds significant overhead. The results show that security cost depends on the number of security features which are invoked. The research goes on to evaluate how duty cycle protocols could affect security cost. It clarifies the effect of increasing the number of AES invocations by some duty cycle protocols. Also, It has shown that not all duty cycle protocols affect security cost, and that this depends on the number of packet retransmissions for a single packet. Different duty cycle protocols lead to different results. Therefore, engineers should take duty cycle into consideration when evaluating security cost.

REFERENCES

[1] J. A. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, feb 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6774858/

[2] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," in *Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on*. IEEE, 2011, pp. 308–311.

[3] S. Sciancalepore, G. Piro, E. Vogli, G. Boggia, and L. A. Grieco, "On securing ieee 802.15. 4 networks through a standard compliant framework," in *Euro Med Telco Conference (EMTC), 2014*. IEEE, 2014, pp. 1–6.

[4] S. K. Singh, M. Singh, and D. Singh, "A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks," *International Journal of Advanced Networking and Application (IJANA)*, vol. 2, no. 02, pp. 570–580, 2010.

[5] S. Alharby, N. Harris, A. Weddell, and J. Reeve, "The security trade-offs in resource constrained nodes for iot application," *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 12, no. 1, pp. 52 – 59, 2018. [Online]. Available: http://waset.org/Publications?p=133

[6] N. Dziengel, N. Schmittberger, J. Schiller, and M. Günes, "Secure communications for event-driven wireless sensor networks," in *Proc. of the 3rd Int. Symp. on Sensor Networks and Applications SNA*, 2011.

[7] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Computer Networks*, vol. 54, no. 17, pp. 2967–2978, 2010.

[8] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "Minisec: a secure sensor network communication architecture," in *Proceedings of the 6th international conference on Information processing in sensor networks*. ACM, 2007, pp. 479–488.

[9] C. Panait and D. Dragomir, "Measuring the performance and energy consumption of aes in wireless sensor networks," in *Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on*. IEEE, 2015, pp. 1261–1266.

[10] A. Trad, A. A. Bahattab, and S. B. Othman, "Performance trade-offs of encryption algorithms for wireless sensor networks," in *Computer Applications and Information Systems (WCCAIS), 2014 World Congress on*. IEEE, 2014, pp. 1–6.

[11] S. Saleem, S. Ullah, and K. S. Kwak, "A study of ieee 802.15. 4 security framework for wireless body area networks," *Sensors*, vol. 11, no. 2, pp. 1383–1395, 2011.

[12] R. Daidone, G. Dini, and G. Anastasi, "On evaluating the performance impact of the ieee 802.15. 4 security sub-layer," *Computer Communications*, vol. 47, pp. 65–76, 2014.

[13] I. Standard and I. C. Society, "IEEE Standard for Local and metropolitan area networks Part 15 . 4 : Low-Rate Wireless Personal Area Networks (LR-WPANs) IEEE Computer Society S ponsored by the," *IEEE Std 802.15.4-2011*, vol. 2011, no. September, pp. 1–294, 2011. [Online]. Available: http://ieeexplore.ieee.org/servlet/opac?punumber=6012485

[14] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the internet of thingsa comparison of link-layer security and ipsec for 6lowpan," *Security and Communication Networks*, vol. 7, no. 12, pp. 2654–2668, 2014.

[15] A. V. Taddeo, M. Mura, and A. Ferrante, "Qos and security in energy-harvesting wireless sensor networks," in *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on*. IEEE, 2010, pp. 1–10.

[16] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Local computer networks, proceedings 2006 31st IEEE conference on*. IEEE, 2006, pp. 641–648.

[17] A. Dunkels, J. Eriksson, N. Finne, and N. Tsiftes, "Powertrace: Network-level power profiling for low-power wireless networks," 2011.

[18] A. Dunkels, "The ContikiMAC Radio Duty Cycling Protocol," SICS, Tech. Rep., 2011. [Online]. Available: http://soda.swedish-ict.se/5128/1/contikimac-report.pdf

[19] J. Saraswat and P. P. Bhattacharya, "Effect of duty cycle on energy consumption in wireless sensor networks," *International Journal of Computer Networks & Communications*, vol. 5, no. 1, p. 125, 2013.

[20] R. C. Carrano, D. Passos, L. C. Magalhaes, and C. V. Albuquerque, "Survey and taxonomy of duty cycling mechanisms in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 181–194, 2014.

[21] M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-mac: a short preamble mac protocol for duty-cycled wireless sensor networks," in *Proceedings of the 4th international conference on Embedded networked sensor systems*. ACM, 2006, pp. 307–320.

[22] J. L. Hill and D. E. Culler, "Mica: A wireless platform for deeply embedded networks," *IEEE micro*, vol. 22, no. 6, pp. 12–24, 2002.