An Energy Model for the IoT: Secure Networking Perspective

Filipe Conceição[1,2], Nouha Oualha[2], and Djamal Zeghlache[1]
[1] CEA, LIST, Communicating Systems Laboratory, 91191 Gif-sur-yvette Cedex, France
[2] Télécom SudParis, Institut Mines-Télécom, 9 rue Charles Fourier, 91011 Evry, France
Email: filipe.conceicao@cea.fr, nouha.oualha@cea.fr, djamal.zeghlache@telecom-sudparis.eu

***Abstract*—An energy model for Internet of Things devices is proposed. The model is based on security mechanisms that are constantly used but never accounted for to allow for longer term conclusions on the energetic cost of security. It is suitable for networking scenarios by slicing the energy spent by a device in individual connections with other network elements. It presents a three phase view of a connection with external network elements: establishment, active communication phase and termination. It maps security mechanisms and offers the ability to quantify the costs of security algorithms in all the phases. It enhances the traditional models by introducing security as a basis and being suitable for networking considerations. Simulation results are presented that show better visibility of a device's energy consumption while networking in cooperation scenarios and due to security options, using Bluetooth's Low Energy most secure mode of operation.**

***Index Terms*—Energy Model, Security, IoT**

I. Introduction

The limitations and constraints of some devices in the Internet of Things (IoT) and Machine-to-Machine (M2M) networks are a major concern in research. Several articles can be found in the literature studying the topic, providing mechanisms for increased energy efficiency and savings. These often include routing strategies to achieve these goals. Their application results in less energy consumed by devices and by consequence, by their networks. Works presented in [1], [2] are examples.

A common limitation of constrained devices is the battery capacity. Recent works propose energy harvesters to extend the battery as an energy source or in some applications to replace them, still maintain a device operating properly throughout its life time [3], [4]. But in order for this to work, the device's energy consumption must be known. This information can then be used for several purposes like battery or energy harvester dimensioning, task scheduling or any type of energy efficient strategies design. Works presented in [1], [2] are examples of these strategies where routing mechanisms are designed to achieve minimum power cost while relaying data from a source node to a destination. However, they also aim at maximizing network lifetime by keeping a balanced distribution of residual energy of the network nodes, sometimes rejecting the path with lowest cost.

In networks with energy harvesting capabilities, rejecting the best path for the balance objective may not be the correct decision. Energy harvesting predictions may change the path choice, even in low energy cases, if an immediate energy intake is foreseen. Same with a device's networking load. A device with several networking tasks has its battery level reduced faster than a device with a light load. Therefore, better understanding an IoT device's energy consumption is fundamental.

The energy consumption models in the literature divide a device into hardware blocks. Examples are presented in [5]–[7] where the models follow a behavioral pattern of acquiring data by means of transducers (Sensing Block), data processing in a controller unit (Processing Block), networking (Communications Block) and internal processes of the Operating System (OS) [8]. The energy consumed by each block is then summed to obtain the device's total consumption. This quantification method is not helpful in the design of energy saving strategies while networking because it does not provide means to observe the impact of the networking load. Therefore, in this paper, we propose quantifying energy consumption based on networking tasks, treating each network connection separately.

When starting new connections, procedures to establish a security context (e.g., session keys) are usually executed. They are mandatory for authentication purposes so that unauthorized access to the network (or free riders) can be prevented through entity or message authentication, for data integrity purposes which should be guaranteed against malicious alterations of data as well as passive threats such as transmission errors originated by noisy channels. They are also mandatory for confidentiality, to guarantee that only the intended or authorized parties can access information.

The energetic cost of security operations may be relatively low in the case of symmetric cryptography, but the cost of asymmetric techniques is not [9]. And after a security context is established between two devices, other security related costs like ciphering or message authentication consume energy while networking. Available data on the energy cost of related cryptographic primitives focus on quantifying single operations [9],

[10], which is not enough to understand the implications and energy cost that security has in the long term.

Due to these considerations, we propose in this paper an energy model for IoT devices based on security mechanisms that slices the energy consumed by a device on each connection with other network nodes. The contributions presented in this work are 1) an energy model for IoT devices is presented that slices the energy spent by each connection making it suitable for networking scenarios, 2) the model provides an energetic quantification method for the establishment, maintenance and termination of a connection with another network node, via the cost of cryptographic mechanisms, 3) the model provides a quantification method for security algorithms executed while a connection is active and 4) simulation results from cooperation scenarios in IoT are presented, showing the usefulness of the model for both networking and security considerations.

As of the rest of the paper's organization, Section II presents and describes the model and Section III presents scenarios, results observed and conclusions of the results using the proposed energy model.

II. Energy Model

An IoT device in a network can have several connections at the same time with other network elements. We propose to quantify each one of them separately. At a point in time, summing the energy consumption of each the n active connections, $E_C(i), i \in 1, 2, ...n$, with the energy spent by the OS in its routine tasks, E_{OS}, equals the total energy consumption of the device. This relation is given by Eq. 1.

$$E_{IoTd} = \sum_{i=1}^{n} E_C(i) + E_{OS} \tag{1}$$

Each connection between two devices comprises three phases. First, for security reasons, the establishment of security contexts for subsequent communication is performed. With the security context established, the connection is in the active phase and the devices now exchange data. While the connection is active, it can happen that the keys in use are renewed or the connection itself is no longer needed, and they are revoked. The energy consumed by connection establishment, its maintenance and termination is denoted as E_{CEM}. The energy consumed in the secure, active phase is denoted as E_{SC}. E_{Com} denotes the energy consumed in radio communications. Finally, each connection added can increase the energy consumption due to application related tasks. This is denoted as E_{App}. Eq. 2 summarizes the energy consumed for each connection i.

$$E_C(i) = E_{CEM}(i) + E_{SC}(i) + E_{App}(i) + E_{Com}(i) \tag{2}$$

The radio interface can be connection dependent and may use different power levels. The amount of data sent and received is usually different as well. We therefore distinguish between energetic cost at transmission and reception, $E_{T\text{x}}$ and $E_{R\text{x}}$ respectively. Eq. 3 defines the cost of communications.

$$E_{Com}(i) = E_{T\text{x}}(i) + E_{R\text{x}}(i) \tag{3}$$

Sensing and actuation tasks can be further included in the model, added in Eq. 2. However, the focus of this work is the security and networking aspects, and we therefore omit it.

A. The role of security

As a fundamental part in all phases of a connection, security plays a vital role in this model. Therefore, E_{CEM} and $E_{SC}(i)$ are further detailed. E_{CEM} is the sum of asymmetric and symmetric connection establishment procedures, E_{ACE} and E_{SCE}, with the maintenance cost, E_{CM}. Termination cost is considered to be part of E_{CM} as it is usually a memory deletion operation with a very low energy cost. Eq. 4 reflects this cost for each connection.

$$E_{CEM} = \sum_{i=1}^{n} E_{ACE}(i) + E_{SCE}(i) + E_{CM}(i) \tag{4}$$

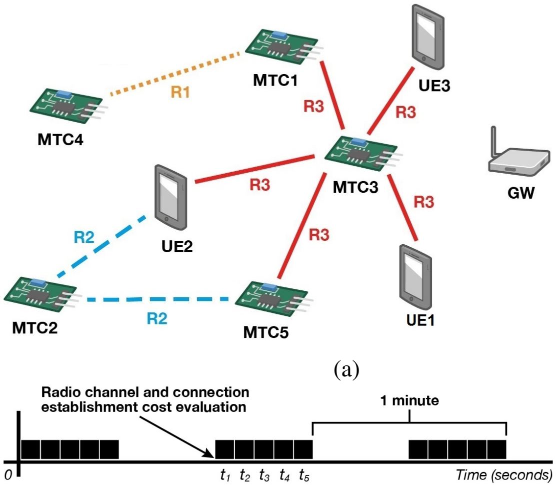
While in the active phase, the cost of security services like ciphering, integrity protection and data source authentication, e.g., using a Message Integrity Codes (MIC) or digital signatures are considered and denoted by, respectively, E_{Ciph}, E_{Int} and E_{Auth}. Entity authentication costs, if they exist in the active phase, are included in E_{CM}. Eq. 5 further details the costs of the active phase, that are therefore translating security operations that are done continuously for devices networking.

$$E_{SC} = \sum_{i=1}^{n} E_{Ciph}(i) + E_{Int}(i) + E_{Auth}(i) \tag{5}$$

III. IoT scenarios model application

In this section, an attempt is made to reproduce cooperation scenarios in IoT networks that can be strategies for energy saving like in [1], [2] or to increase other network performance aspects like Packet Delivery Ratio (PDR). An illustration of the considered connections is shown in Fig. 1a.

In the first case, devices cooperate with neighbor nodes providing routing services if their radio channel conditions offers energy savings. In the latter, there is an energy budget to spend on maximizing the number of concurrent transmissions. However in both cases, because it is fundamental to establish a security context, $E_{CEM} \neq 0$. In particular, we consider that devices


MTC4
R1
MTC1
R3
UE3
R3
MTC3
GW
R3
R3
UE2
R2
R3
UE1
MTC2
R2
MTC5
Radio channel and connection establishment cost evaluation
1 minute
0
t_1 t_2 t_3 t_4 t_5
Time (seconds)

(a)

(b)

Fig. 1: (a) General scenario system model.
(b) Periodic Updates representation.

establish security contexts using the symmetric algorithm Advanced Encryption Algorithm (AES) making $E_{SCE} \neq 0$ or in addition, Elliptic Curve Diffie-Hellman (ECDH) can also be used and in that case $E_{ACE} \neq 0$. While in the active phase, encryption and decryption of data using AES is considered making $E_{Ciph} \neq 0$. This choice of protocol and algorithm matches Security Mode 1 Level 4 of Bluetooth Low Energy (BLE) security, that enforces an authenticated device pairing with encryption and is the recommended to be used by the National Institute of Standards and Technology (NIST) [11]. Channel conditions between devices and GW are assumed static and thus, $E_{T\text{x}}/E_{R\text{x}}$ are constant. As the goal is to show that the weight of the security procedures on establishing and during a connection will impact in time the energy consumption of the overall network and should not be neglected, we consider $E_{App}(i) = E_{OS} = 0$. Table I lists the non zero parameters used in Eqs. 3, 4 and 5 in each of the scenarios presented in the following subsections. Values were taken from [9], [10]. Radio links are modeled with normal distributions where a value is generated at each time slot.

The devices can be Machine Type Communications (MTC) devices or User Equipments (UEs) and they can communicate directly, like introduced in [12]. MTC devices are performing Periodic Updates (PU), i.e., MTC devices transmit updates to a GW on a regular basis with constant frequency and data size [13] as illustrated in Fig. 1b. A frequency of $60s$ between data sending is used where the first $5s$ are used to transmit and receive information. After and until the next PU, the device's state is in an Idle state. The daily energy consumption is then monitored. $1s$ granularity is used for simplicity as it does not change the achieved numerical results, that were obtained using MATLAB.

TABLE I: Simulations' parameters

Parameter	Value (Units)
$B_{T\text{x}}/B_{R\text{x}}$	2
E_{SCE}/E_{ACE}	7.83 (1)$/276.70$ (2)
E_{Ciph}	1.21 (1)
$GW \rightarrow E_{T\text{x}} = E_{R\text{x}}$	9 (1)
$R_1 \rightarrow E_{T\text{x}} = E_{R\text{x}}$	$N \sim (2; 0.3)$ (1)
$R_2 \rightarrow E_{T\text{x}} = E_{R\text{x}}$	$N \sim ([3, 12]; 0.03)$ (1)
$R_3 \rightarrow E_{T\text{x}} = E_{R\text{x}}$	$N \sim (2; 0.4)$ (1)

$B_{T\text{x}}/B_{R\text{x}}$ - Data Tx/Rx at each time slot (Bytes).
E_{SCE}/E_{ACE} - Cost of key establishment via symmetric/asymmetric algorithms (J).
E_{Ciph} - Cost of encryption/decryption of data (J/Byte).
$E_{T\text{x}}/E_{R\text{x}}$ - Energy consumed to Tx/Rx data (J/bit).
(1) $- \times 10^{-6}$
(2) $- \times 10^{-3}$

A. Networking load

In this case, MTC_1 sends PU to the GW at the same time it relays PU from neighbor node MTC_4, also to the GW and every time it is requested, through link R_1. The daily energy consumption of MTC_1 is observed and plotted in Fig. 2 as a function of how often MTC_4 requests PU relaying. Without relaying data for MTC_4, the daily energy consumption represented by the direct GW reference line that is constant as it is independent of the frequency of the relaying requests.

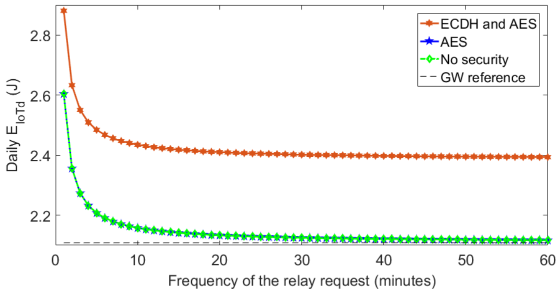


Fig. 2: Energy consumption with and without relaying

The cost of relaying data with no security context establishment, considering AES only and both ECDH and AES is also shown. As expected, the less often MTC_1 relays data, the less energy it consumes. But the plot shows different energy efficiency zones where 1 minute deviation in the frequency of the relay requests greatly impacts the energy consumed before the 15 minutes frequency but after, the impact becomes smaller until it is almost negligible at 60 minutes. This illustrates well that the networking load of a device needs to be considered when deciding to include it or not in a routing paths. It may cause it to advertise as a relay despite having a low battery level if the network load is low as well. In the inverse sense, having a higher network load may cause it not to advertise despite having a reasonable battery level and this can only be observed if connections are quantified separately, instead of quantifying the total consumption only. This idea can also be extended to multiple MTC devices requesting relaying service at the same time instead of always the same device, at different request frequencies. In both cases, single or multiple relay requests, it shows networking load can have a significant impact on keeping the distribution of residual node energy balanced.

B. *Security establishment budget*

Despite the available routing strategies, nodes are not always available to relay data. The probability of their availability changes with applications, networking scenarios, energy levels, mobility models, etc. In a smart city context, mobility of users is a characteristic of the networking scenario causing the probability of having a relay UE available to change. MTC devices with energy harvesting capabilities have at times full battery and the capability to harvest more energy and at others, low battery levels and no possibility to harvest energy. In this section, 3 different probabilities for MTC_2 to have a new relay available through R_2 are evaluated, 10%, 50% and 90%. MTC_2 decides to relay the PU by evaluating R_2 immediately before instant t_1 (only the first time slot is evaluated), adding E_{CEM} due to a new secure connection establishment, comparing it with the GW link cost and choosing the lowest cost.

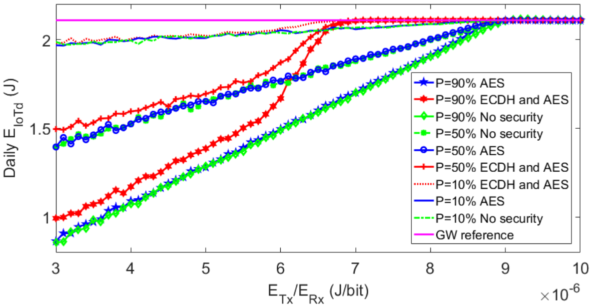


Fig. 3: Energy savings for different relaying probabilities

Daily energy consumption is shown in Fig. 3. With a 10% probability for relay availability, energy savings are around 7%. With 90% relay availability, energy savings are up to 60% for these conditions. However, if load balancing techniques are applied like in [2], energy savings are partially lost because the relays will at times refrain from relaying data. AES-based key establishment has a very small impact on the energy consumption and relaying decision. ECDH however has a noticeable impact. In this section only, the cost of ECDH was $E_{ACE} = 10 * E_{SCE}$, instead of the one listed in table I. Using the value in the table, E_{CEM} would be so high, that the device would never relay packets. This would change if the GW link radio cost was much higher. However, the simulations' parameters were selected to fit resource constrained MTC devices [10] and they show clearly that protocols like ECDH for key agreement can be energetically unaffordable for them, although the recommended BLE security mode imposes their use.

The plot also points out what is the security budget for connection establishment in these conditions, in terms of the difference between the radio link cost for R_2 and the GW link. This may be extremely useful for a device because it gives information on how to choose the security mechanisms to apply as a function of the radio cost of the available relays or inversely, to discard relays due to security requirements.

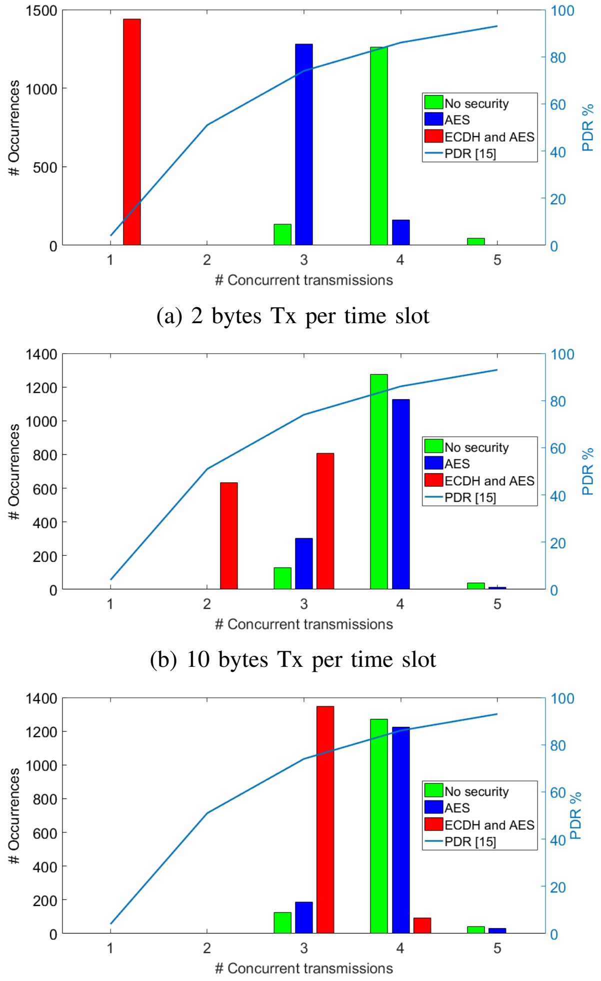
C. *Concurrent transmissions*

In this section, the energy consumed sending PU to the GW is an energy budget, B, that shall not be exceeded. MTC_3 has 5 devices offering lower radio cost via R_3 link. The five similar links are a simulation of smart city scenarios where often people holding UEs concentrate close to MTC devices leaving after a while, e.g. public transportation stops, imposing new connection establishments. MTC_3 maximizes the number of relays to send the PU concurrently without exceeding the energy budget. Concurrent transmissions reduce the negative impact of packet loss by increasing PDR [14].

Evaluation of the radio channels is done as in Fig. 1b. Starting from the relay with the lowest cost and increasing, MTC_3 will transmit the PU to as many relays as possible, given that $E_{CEM} + E_{Com} < B$. Fig. 4 plots histograms quantifying how many times one or more relays were used to transmit PU daily, for different PU sizes. If more than one was used, redundant data was carried. Work presented in [15] shows simulation results with the PDR as a function of the number of concurrent transmissions. This result is used in the plots to link PDR to the number of relays used by MTC_3.

If no security is considered, results remain unchanged. If only AES-based key establishment is considered, there is a visible difference in its impact on PDR between 2 and 10 Bytes. From 10 to 20 Bytes, the difference is less noticeable. If ECDH is executed as well, its impact on PDR is clear from 2 to 10 and from 10 to 20 Bytes, showing that the weight of ECDH has a clear impact on the effort of increasing PDR.

As the PU size increases, increasing E_{SC}, the PDR increases as well showing a trade off between E_{SC} and E_{CEM} creating a relation between the two. Conclusions can be drawn that PDR is increased by reducing E_{CEM}, increasing E_{SC} or a compromise between the two opting e.g., to use different security mechanisms other than the ones considered in this work or buffering more PU data before sending it.



(a) 2 bytes Tx per time slot

(b) 10 bytes Tx per time slot

(c) 20 bytes Tx per time slot

Fig. 4: Histograms - Daily number of occurrences for different concurrent transmissions

IV. Conclusion

In this paper an energy model for IoT devices was presented. The model serves as a tool to quantify the energy cost of establishing connections and of their active phase, treating each connection separately. It quantifies the cost of all modern cryptography algorithms that are constantly being executed while a networking connection is established, active and then terminated. The model proves to be useful in diverse networking scenarios where techniques like load balancing or minimum thresholds for battery level constraints are applied, due to the lack of visibility on the impact of single connections. Presented results allow to draw conclusions on the energy budget for security establishment, for energy saving and PDR improvement strategies. They show as well that BLE recommendations for security may not be affordable to constrained devices.

Acknowledgements

This work received funding from the European Unions Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 675891 (SCAVENGE).

References

[1] J. Luo, J. Hu, D. Wu and R. Li. "Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks", in *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 112-121, Feb. 2015.

[2] K. Machado, D. Rosário, E. Cerqueira, A. Loureiro, A. Neto and J. Souza. "A Routing Protocol Based on Energy and Link Quality for Internet of Things Applications", in *Sensors*, 13(2): 1942-1964, 2013.

[3] S. Chalasani and J. M. Conrad, "A survey of energy harvesting sources for embedded systems," *IEEE SoutheastCon 2008, Huntsville*, AL, 2008, pp. 442-447.

[4] W. Seah, Z. Eu and H. Tan, "Wireless sensor networks powered by ambient energy harvesting (WSNHEAP) Survey and challenges," *1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, Aalborg, 2009, pp. 1-5.

[5] B. Martinez, M. Montn, I. Vilajosana and J. D. Prades. "The Power of Models: Modeling Power Consumption for IoT Devices", *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5777-5789, Oct. 2015.

[6] Q. Wang, M. Hempstead and W. Yang. "A Realistic Power Consumption Model for Wireless Sensor Network Devices", *3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, 2006, pp. 286-295.

[7] W. Du, F. Mieyeville and D. Navarro. "Modeling Energy Consumption of Wireless Sensor Networks", *5th International Conference on Systems and Networks Communications*, 2010, pp. 94-98.

[8] SCAVENGE-Sustainable Cellular Network Harvesting Ambient Energy. "WP2Energy Models", SCAVENGE-Sustainable Cellular Network Harvesting Ambient Energy, 2018, [Online]. Available: http://www.scavenge.eu/wp-content/uploads/2018/02/D2.1.pdf. [Accessed: May. 30, 2018]

[9] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha. "A study of the energy consumption characteristics of cryptographic algorithms and security protocols", in *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128-143, Feb. 2006.

[10] G. de Meulenaer, F. Gosset, F. X. Standaert and O. Pereira. "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Avignon, 2008, pp. 580-585.

[11] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen, K. Scarfone, "Guide to Bluetooth Security", National Institute of Standards and Technology (NIST), Gaithersburg, 2017.

[12] F. Conceição, N. Oualha and D. Zeghlache. "Security Establishment for IoT Environments in 5G: Direct MTC-UE Communications", *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Montreal, 2017.

[13] N. Nikaein, M. Laner, K. Zhou, P. Svoboda, D. Drajic, M. Popovic and S. Krco. "Simple Traffic Modeling Framework for Machine Type Communication", *ISWCS 2013; The Tenth International Symposium on Wireless Communication Systems*, Ilmenau, Germany, 2013, pp. 1-5.

[14] B. X. Yen, D. T. Hop and M. Yoo. "Redundant transmission in wireless networked control system over IEEE 802.15.4e", *The International Conference on Information Networking 2013 (ICOIN)*, Bangkok, 2013, pp. 628-631.

[15] S. Yu, X. Wu, P. Wu, D. Wu, H. Dai and G. Chen. "CIRF: Constructive interference-based reliable flooding in asynchronous duty-cycle wireless sensor networks", *IEEE Wireless Communications and Networking Conference (WCNC)*, Istanbul, 2014, pp. 2734-2738.