Performance and Energy-Tuning Methodology for Wireless Sensor Networks Using TunableMAC

Udoh, E. and Getov, Vladimir

This is a copy of the author's accepted version of a paper subsequently to be published in the proceedings of the IEEE Int. Conference on Communications, Computing, Cybersecurity, and Informatics, CCCI 2020. Virtual - online, 03 - 05 Nov 2020.

The final published version will be available online at:

https://ieeexplore.ieee.org/

Performance and Energy-Tuning Methodology for Wireless Sensor Networks Using TunableMAC

Ekereuke Udoh
Distributed and Intelligent Systems Research Group
University of Westminster
London, United Kingdom
w1562173@my.westminster.ac.uk

Vladimir Getov
Distributed and Intelligent Systems Research Group
University of Westminster
London, United Kingdom
v.s.getov@westminster.ac.uk

***Abstract*— Energy-efficiency and performance are at the forefront with regards to wireless sensor networks due to the resource-constrained nature of the sensors on the network. Most of the energy in a sensor is consumed by the radio and this therefore creates the need for a more efficient use of the Media Access Control (MAC) layer which controls access to the radio. The Castalia framework which runs on the OMNET++ simulation platform provides a MAC layer protocol – TunableMAC – which is used in this paper for tuning of performance and consumed power. Our goal is to improve as much as possible the performance/energy balance in terms of resources used up by security features, while attempting to preserve the overall lifespan of the wireless sensors. This paper investigates performance parameters for TunableMAC such as energy consumed, latency, throughput and network lifetime based on simulated temperature sensors. A 5-step methodology is proposed that can be helpful for minimizing the impact of denial-of-sleep (DOS) attacks. Hence, the benefit of this research is that it feeds into the development of a novel MAC protocol that is energy-aware and can autonomously guard against energy drain attacks such as DOS attacks.**

Keywords—TunableMAC protocol, performance tuning, OMNET++, wireless sensor networks, energy aware

I. INTRODUCTION

Wireless sensor networks (WSNs) can be used in resource-constrained environments where there is limited or no access to external energy sources e.g. underwater exploration and battlefield surveillance. In addition, the sensors are also constrained in terms of resources such as battery life as well as low memory due to their miniature size and need for portability [2]. To conserve energy, these sensor nodes go into sleep mode to save energy. This makes them prone to energy-drain attacks such as DOS attacks which prevent the sensors from sleeping, thereby draining their energy, and reducing their lifespan significantly from 3.5 years to 3 days [4].

In [5], DOS attacks are classified into six methods: sleep deprivation, barrage, synchronization, replay, collision, and broadcast attacks. These attacks are possible due to vulnerabilities like frame collisions, message overhearing and idle listening [3]. To mitigate these attacks, certain approaches have been proposed and compared, however the evaluation of these approaches are qualitative in nature with a focus on their strengths and weaknesses [5].

Although this paper focuses on TunableMAC as a form of test bed for analysing and tuning the changes in performance, it is imperative to look at the existing approaches to curbing DOS attacks. This is discussed in Section II. Section III discusses the research methodology, followed by a discussion of the results in Section IV. Section V concludes the paper and outlines directions for future work.

II. RELATED WORK

A generic framework that optimizes the performance of existing clustering protocols (e.g. UHEED) by using Simulated Annealing and K-Beam algorithms is proposed in [21]. However, this is mainly aimed at clustering and routing protocols. In [22], the relationship between node density and certain network parameters such as received signal strength indicator (RSSI) and Link quality indicator (LQI) are analysed, with reference to DOS attacks.

Gateway MAC (GMAC) was designed to protect against broadcast attacks [13] which are usually targeted at the MAC layer. GMAC focuses on the network architecture as a way of conserving energy and reducing the risk of DoS attacks by using cluster-based approach, making it better than SMAC, TMAC and BMAC in terms of network lifetime. However, it is relatively low in terms of autonomy as it focuses on the MAC layer of the network.

In [8], the hash-based scheme, which also uses a cluster-based approach, is proposed to be better than the random vote scheme and round robin scheme. This evaluation is based on the time and energy consumed in order to select a cluster head.

In [4], Clustered Adaptive Rate Limiting (CARL) approach is designed to protect against an unauthenticated broadcast attack. It does this by using a host-based intrusion system which classifies incoming packets based on authentication tests and anti-replay checks. Furthermore, it limits the rate at which the radio remains active as a way of minimizing the broadcast attack, however this method can affect performance by limiting valid packets from being received.

The Fake Schedule Switch Scheme (FSSS) involves a node initiating a fake schedule switch if it does not receive an acknowledgment after sending a message [12]. This tricks the attacker into launching their attack at the wrong time and could minimize collision, exhaustion, and broadcast attacks. However, this is applicable with MAC protocols that support Request-to-Send (RTS) and Clear-to-Send packets (CTS).

In [9], the Secure Wakeup Scheme (SWS) is proposed which assumes that a radio can perform some checks on the validity of a packet while the sensor node is still in sleep state. The radio is assumed to be able to store a list of tokens with which it compares the tokens sent to it. While this seems

energy-efficient, it is not clear how the radio achieves this and how much energy is spent.

The Absorbing Markov Chain (AMC), proposed in [14], is a mathematical model which can be useful for detecting a DOS attack by making some probabilistic calculations on the expected death time of a sensor network while monitoring the network flow. However, this method only is limited to detecting the attack, without any controls or measures to mitigate it.

A Hierarchical Collaborative Model (HCM) proposed in [2] utilises distributed anomaly detection whereby the load of detecting the anomaly is spread across multiple nodes to minimise the burden on a single node. To achieve this, nodes are categorised in various roles and clusters. The weakness of this model is that packet overhead may be high in some cases.

The Cross-Layer Mechanism (CLM) as the name implies focuses on data gathered from multiple layers of the network – MAC, network, and physical layers. They use a combination of routing table, RSSI and data fragment rejection to detect sleep deprivation attack, replay attack and barrage attack, respectively. However, this mechanism has only been tested on one protocol (SMAC) and only works in scenarios where RTS and CTS are supported.

In [11], the Two-tier Secure Scheme (TSS) is proposed with a strong focus on reducing the complexity of the security process and conserving energy while trying to tackle power exhausting attacks, specifically forge and replay attacks. It uses a hash-chain generated dynamic session key which is useful for authentication and encryption.

The Zero-Knowledge Protocol (ZKP) [10] is used alongside the interlock protocol for authentication via key transfer. The protocol claims to protect against man-in-the-middle and replay attacks. However, there is no research on the energy costs of this approach, especially as it involves RSA key generation and hash generation and distribution.

III. Performance Tuning Methodology

The performance tuning methodology was used to evaluate WSN MAC protocols based on their performance via simulation experiments using OMNET++ and the Castalia framework. The methodology is divided into 5 steps:

1. Decide on what performance metrics to measure
2. Decide on TunableMAC parameters to use
3. Choose a set of values for each parameter
4. Choose scenario and run simulations
5. Build a predictive model based on results

A. Performance Metrics

Certain performance metrics had to be used and these metrics include:

Latency. This has to do with any form of delay that happens during communication in the wireless sensor network. Latency is measured in units of time – e.g. seconds.

Throughput. As mentioned earlier, this is defined as the amount of data successfully transferred from the source to destination within a given period. Throughput is usually measured in bits/second. However, in the simulator, this is referred to as the transmitted packets per time it took to transmit those packets.

Consumed energy. This is the total amount of energy used to transmit data from a source to its destination. The unit for consumed energy is joules/bit.

Network Lifetime. This is how long the nodes on a network can stay alive from the point when they start working to the point where the nodes fail due to energy-drain attacks.

B. TunableMAC Parameters

This section explains the various parameters of TunableMAC parameters that can be tuned [20].

Justification for choosing TunableMAC. One of the main reasons for using TunableMAC was the flexibility it gives, allowing a user to alter a number of parameters (8 to 10) in order to suit the network needs.

Duty cycle. The duty cycle is expressed as a percentage or fraction of time for which the node listens or for which the node is active in duty.

Listen interval. While duty cycle is a fraction of time the node listens, listen interval is the actual time for which the node listens.

Beacon Interval Fraction. The presence of a duty cycle means that a node that wants to transmit to sleeping nodes needs to wake up those nodes. This can be done using beacons as a form of preamble before sending the actual message.

Probability of transmissions. This is used alongside the number of transmissions or retransmissions to calculate the expected number of successful transmissions per node.

Number of transmissions. This has to do with the number of times data is transmitted.

Random Transmission Offset. This is the random time for which a node delays before information is transmitted.

Retransmission Interval. This is the interval between transmissions and is also expressed as an integer data type.

Backoff Type. Based on CSMA technique, a node backs off each time the channel is busy. How long the node backs off is determined by the back-off type.

C. TunableMAC Limitations

There is no security to prevent DOS attacks as nodes can be kept awake through a stream of beacons. TunableMAC does not support unicast and this leads to a waste of energy as information is always sent to all neighbouring nodes. Finally, it does not support RTS/CTS: Therefore, there is no form of collision avoidance.

IV. Wireless Sensor Network Simulation Results

A. Introduction

This simulation involves 16 temperature sensors arranged in the form of a grid. These sensors sample their temperature readings when it gets above 15 degrees. Any node that senses a value above the threshold then broadcasts this value. The value propagation which records how many of the nodes received the broadcasted value is then recorded for each node. Energy consumed by the node is also recorded as

well as the number of packets transmitted by the nodes. In this scenario, only one node senses temperature beyond 15 degrees. The results are dependent on a number of parameters associated with the TunableMAC protocol used in the scenario. The parameters include duty cycle, beacon interval fraction, and TX Power.

TABLE I. TUNABLE PARAMETERS USED

	Duty Cycle	Beacon Interval Fraction	TX Power
1	0.02, 0.05, 0.1, 0.5, 0.8	1.0	0dBm
2	0.1	0.02, 0.05, 0.1, 0.5, 0.8	0dBm
3	0.1	1.0	-15, -10, -5, -1, 0

B. *Varying Duty Cycle*

TABLE II. THROUGHPUT RESULTS

Duty Cycle = 0.02	Duty Cycle = 0.05	Duty Cycle = 0.1	Duty Cycle = 0.5	Duty Cycle = 0.8
0.992	0.975	0.992	0.933	0.867

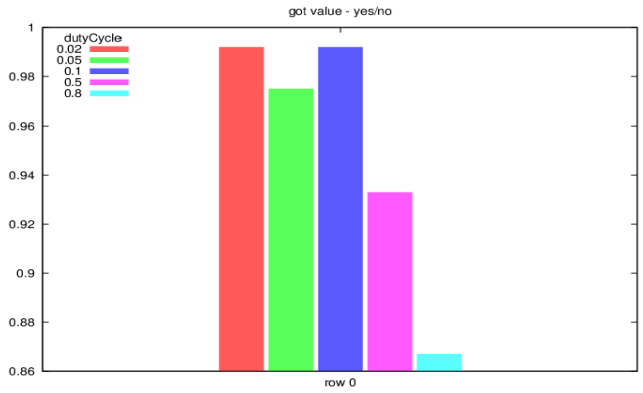

Fig. 1. Throughput values based on duty cycles.

The graph in Fig.1. shows the value propagation which indicates how many of the nodes received the propagated value as the duty cycle is varied. One point to note is that the change in value propagation is not linear and this is due to the variations and randomness in the start times of the nodes (lack of synchronization of sleep cycles). In [18] one of the ways to ensure synchronization of schedules is for each node to send a SYNC message to other nodes to make them aware of its schedule. The main irregularity lies between the second and third bar from the left, where the duty cycle is 0.05 and 0.1 respectively. However, the graph still shows at large that the value propagation reduces as duty cycle increases. The lowest value is 0.867 which happens when the duty cycle is at the highest relatively (0.8).

TABLE III. CONSUMED ENERGY RESULTS

Duty Cycle = 0.02	Duty Cycle = 0.05	Duty Cycle = 0.1	Duty Cycle = 0.5	Duty Cycle = 0.8
0.146	0.124	0.143	0.376	0.557

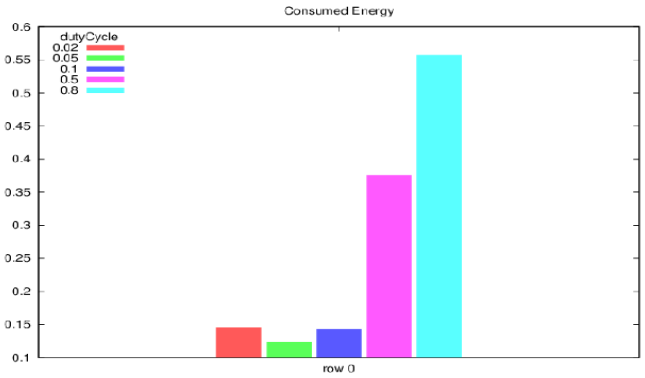

Fig. 2. Energy consumption based on duty cycles.

The graph in Fig. 2 shows the effect of duty cycling on energy consumption. It is clear, that energy consumption increases as the duty cycle increases meaning that the relatively highest consumed energy happens when duty cycle is 0.8. The more a node listens, the more energy it consumes. In [19] the authors conclude in their results and discussions that energy consumption increases as duty cycle increases. Among the three parameters (duty cycle, beacon interval faction and transmit power), the duty cycle relatively has the greatest impact on energy consumption with its highest being 0.557.

TABLE IV. TRANSMITTED PACKETS

Duty Cycle = 0.02	Duty Cycle = 0.05	Duty Cycle = 0.1	Duty Cycle = 0.5	Duty Cycle = 0.8
117.017	45.825	22.808	3.733	1.733

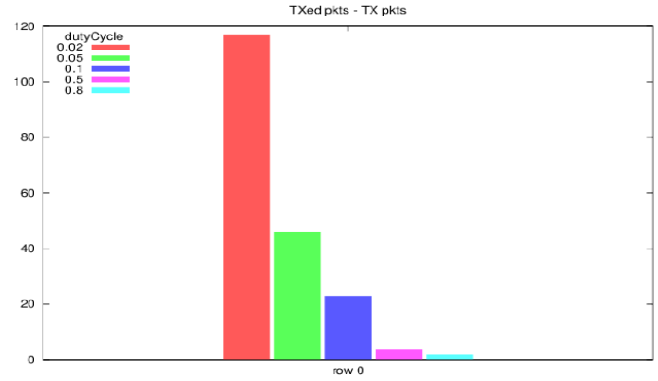

Fig. 3. Transmitted packets based on duty cycles.

The graph in Fig. 3 shows the impact of the duty cycle on the transmitted packets. Apparently, the lower the duty cycle, the higher the transmitted packets. This is due to the fact that a node spends less time listening and therefore can send more data.

C. *Varying Beacon*

TABLE V. THROUGHPUT VALUES

Beacon Fraction = 0.02	Beacon Fraction = 0.05	Beacon Fraction = 0.1	Beacon Fraction = 0.5	Beacon Fraction = 0.8
0.183	0.242	0.304	0.813	0.912

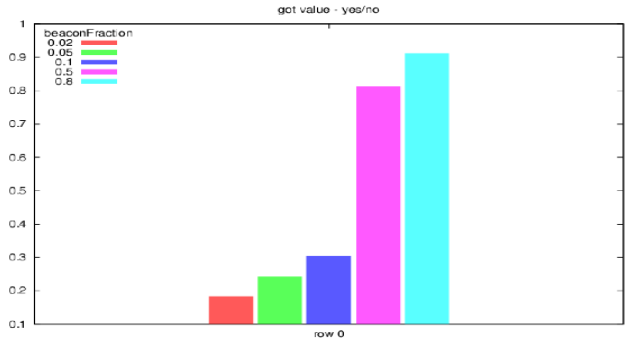

Fig. 4. Througput based on beacon interval fraction.

The graph in Fig. 4 shows the effect of the beacon interval fraction on the value propagation. Value propagation increases as the beacon fraction increases. This means that more nodes are likely to receive the propagated value when more beacons are sent.

TABLE VI. CONSUMED ENERGY

Beacon Fraction = 0.02	Beacon Fraction = 0.05	Beacon Fraction = 0.1	Beacon Fraction = 0.5	Beacon Fraction = 0.8
0.134	0.135	0.135	0.137	0.142

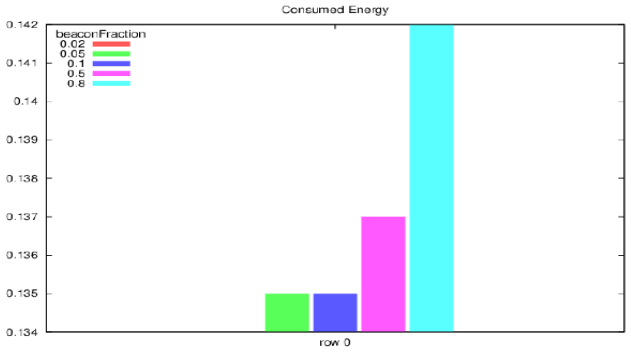

Fig. 5. Consumed energy based on beacon interval fraction.

The graph in Fig. 5 shows the impact of the beacon interval fraction on the consumed energy. The higher the beacon interval fraction, the higher the energy consumed.

TABLE VII. TRANSMITTED PACKETS

Beacon Fraction = 0.02	Beacon Fraction = 0.05	Beacon Fraction = 0.1	Beacon Fraction = 0.5	Beacon Fraction = 0.8
0.367	0.725	1.217	9.75	17.337

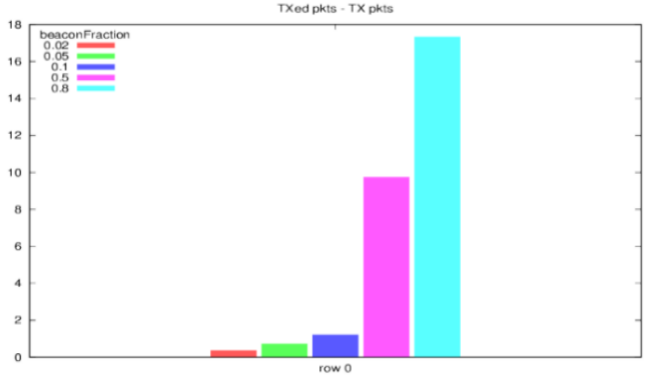

Fig. 6. Transmitted packets based on beacon fraction.

The graph in Fig. 6 shows the effect of varying the beacon interval fraction on the transmitted packets. The higher the beacon interval fraction, the higher the number of transmitted packets.

D. *Varying TX Power*

TABLE VIII. THROUGHPUT RESULTS FOR TX POWER

TX Power = -15dBm	TX Power = -10dBm	TX Power = -5dBm	TX Power = -1dBm	TX Power = 0dBm
0.063	0.113	0.558	0.954	0.979

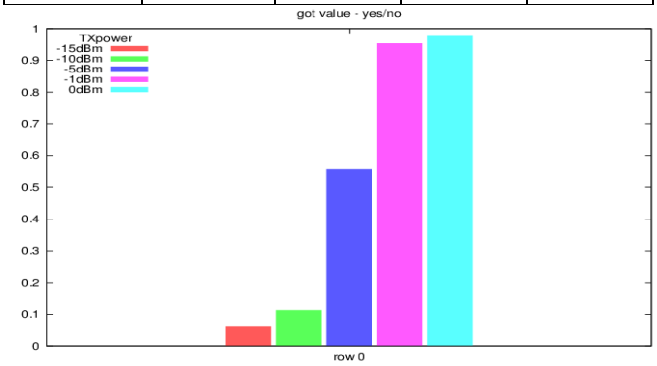

Fig. 7. Throughput based on transmission power.

Fig. 7 shows the effect of varied transmitted packet on the value propagation and it clearly indicates that the value propagation increases as the radio transmit power increases.

TABLE IX. CONSUMED ENERGY FOR TX POWER

TX Power = -15dBm	TX Power = -10dBm	TX Power = -5dBm	TX Power = -1dBm	TX Power = 0dBm
0.135	0.135	0.138	0.143	0.143

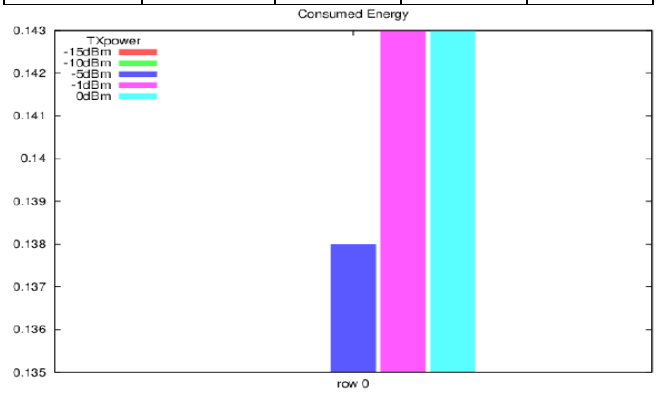

Fig. 8. Consumed energy based on varied TX power.

Fig. 8 shows the effect of the radio transmit power on the consumed energy. The energy increases as the transmit power increases. Hence, the reason why most radios for wireless sensor networks do not exceed 0dBm of transmit power.

TABLE X. TRANSMITTED PACKETS FOR TX POWER

TX Power = -15dBm	TX Power = -10dBm	TX Power = -5dBm	TX Power = -1dBm	TX Power = 0dBm
1.438	2.587	12.842	21.946	22.521

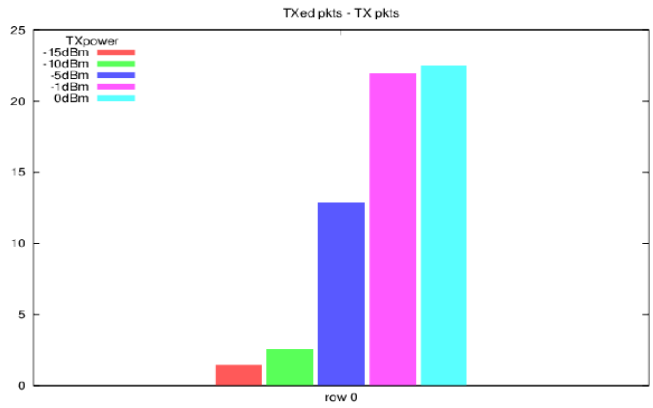

Fig. 9. Transmitted packets based on TX power.

Fig. 9 shows the effect of varying the transmit power on the number of transmitted packets. It is evident that the higher the transmit power, the higher the packets transmitted. There is a huge difference between the change in TX packets from 15dBm to -10dBm and then from -10dBm to -5dBm. Transmit power can be said to be directly proportional to the value propagation, consumed energy and transmitted packets.

V. Conclusion and Future Work

This paper contributes a thorough investigation of the impact of certain parameters on various aspects of a wireless sensor network thereby giving more insight as to where to focus on in terms of increasing energy-efficiency. This then makes it easier to decide which of the parameters to tune in order to increase energy-efficiency with minimal effect on throughput which can be measured from the value propagation. Following this approach, we introduce a novel 5-step methodology to minimize the thread of DOS attacks.

Ongoing research makes use of this methodology as part of developing an energy-efficient and autonomous protocol to tackle energy-drain attacks like DOS attacks. This research opens up opportunities to look into how such an energy-efficient and self-adaptive protocol which protects sensors from energy-drain attacks (denial-of-sleep attacks) can be developed.

References

[1] V. Kumar, S.B. Dhok, R. Tripathi, and S. Tiwari, “Cluster size optimization with Tunable Elfes sensing model for single and multi-hop wireless sensor networks,” Int. Journal of Electronics, vol. 104, no. 2, pp. 312–327, 2017.

[2] T. Bhattasali, R. Chaki, and S. Sanyal, “Sleep deprivation attack detection in wireless sensor network,” Int. J. Comput. Appl., vol. 40, no. 15, pp. 19–25, 2012.

[3] M. Brownfield, Y. Gupta, and N. Davis, “Wireless sensor network denial-of-sleep attack,” Proc. 6th Annual IEEE SMC Information Assurance Workshop, pp. 356–364, IEEE Xplore, 2005.

[4] D.R. Raymond and S.F. Midkiff, “Clustered adaptive rate limiting: Defeating denial-of-sleep attacks in wireless sensor networks,” Proc. IEEE Military Communications Conference (MILCOM), pp. 1–7, IEEE Xplore, 2007.

[5] D.E. Boubiche and A. Bilami, “A defense strategy against energy exhausting attacks in wireless sensor networks,” J. of Emerging Technologies in Web Intelligence, vol. 5, no. 1, pp. 18–27, 2013.

[6] J. Rezaei, “Best-worst multi-criteria decision-making method,” Omega, vol. 53, pp. 49–57, 2015.

[7] L. Xu and J.B. Yang, “Introduction to multi-criteria decision making and the evidential reasoning approach,” Manchester School of Management, 2001.

[8] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, M. Kandemir, and R. Brooks, “The sleep deprivation attack in sensor networks: Analysis and methods of defense,” Int. J. Distrib. Sens. Networks, vol. 2, no. 03, pp. 267–287, 2006.

[9] R. Falk and H.J. Hof, “Fighting insomnia: A secure wake-up scheme for wireless sensor networks,” Proc. 3rd Int. Conf. on Emerging Security Information, Systems and Technologies (SECURWARE), pp. 191–196, 2009.

[10] S. Naik and N. Shekokar, “Conservation of energy in wireless sensor network by preventing denial-of-sleep attack,” Procedia Computer Science, vol. 45, pp. 370–379, 2015.

[11] C.T. Hsueh, C.Y. Wen, and Y.C. Ouyang, “A secure scheme against power exhausting attacks in hierarchical wireless sensor networks,” IEEE Sens. J., vol. 15, no. 6, pp. 3590–3602, 2015.

[12] C. Chen, L. Hui, Q. Pei, L. Ning, and P. Qingquan, “An effective scheme for defending denial-of-sleep attack in wireless sensor networks,” Proc. of 5th Int. Conference on Information Assurance and Security, IAS’09, pp. 446–449, IEEE Xplore, 2009.

[13] M.I. Brownfield, “Energy-efficient wireless sensor network MAC protocol,” PhD Thesis, Virginia Tech, 2006.

[14] T. Bhattasali and R. Chaki, “AMC model for denial-of-sleep attack detection,” Journal of Recent Research Trends, pp. 1–4, 2012.

[15] B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, “Energy cost of security in an energy-harvested IEEE 802.15.4 wireless sensor network,” Proc. 3rd Mediterranean Conference on Embedded Computing (MECO), pp. 198–201, IEEE Xplore, 2014.

[16] S. Isaiadis and V. Getov, “Integrating mobile devices into the Grid: Design considerations and evaluation," Proc. of Euro-Par 2005 Conference, LNCS, vol. 3648, pp. 1080–1088, Springer, 2005.

[17] S. Panichpapiboon, G. Ferrari, and O.K. Tonguz, “Optimal transmit power in wireless sensor networks,” IEEE Transactions on Mobile Computing, vol. 5, no. 10, pp. 1432–1447, 2006.

[18] T. van Dam and K. Langendoen, “An adaptive energy-efficient MAC protocol for wireless sensor networks,” Proc. 1st ACM International Conference Embedded Network Sensor System, pp. 171–180, ACM, 2003.

[19] R. Tahar, A. Dhraief, A. Belghith, H. Mathkour, and R. Braham, “Autonomous and adaptive beaconing strategy for multi-interfaced wireless mobile nodes,” Wireless Communications & Mobile Computing, vol. 16, no. 12, pp. 1625–1641, Wiley, 2016.

[20] B. A. Networks, “User's Manual,” March 2011.

[21] A. Alchihabi, A. Dervis, E. Ever, and F. Al-Turjman, “A generic framework for optimizing performance metrics by tuning parameters of clustering protocols in WSNs,” Wireless Networks 25, pp. 1031–1046, Springer, 2019.

[22] E. Udoh and V. Getov, "Performance analysis of denial-of-sleep attack-prone MAC protocols in wireless sensor networks," Proc. 20th Int. Conference on Computer Modelling and Simulation (UKSim-AMSS), pp. 151–156, IEEE Xplore, 2018.