Performance Analysis of Denial-of-Sleep Attack-Prone MAC Protocols in Wireless Sensor Networks

Udoh, E. and Getov, Vladimir

https://doi.org/10.1109/UKSim.2018.00038

Performance Analysis of Denial-of-Sleep Attack-Prone MAC Protocols in Wireless Sensor Networks

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* — Wireless sensor networks which form part of the core for the Internet of Things consist of resource constrained sensors that are usually powered by batteries. Therefore, careful energy awareness is essential when working with these devices. On the other hand, the presence as well as the absence of security features implemented in resource constrained sensors can have negative effects on their energy consumption. Indeed, the introduction of security techniques such as authentication and encryption, to ensure confidentiality and integrity of data, can place higher energy load on the sensors. However, the absence of security protection could give room for energy-drain attacks such as denial-of-sleep attacks which has a higher negative impact on the life span (availability) of the sensors than the presence of security techniques. This paper focuses on denial-of-sleep attacks by simulating three Media Access Control (MAC) protocols – Sensor-MAC, Timeout-MAC and TunableMAC – under different network sizes. We evaluate, compare, and analyse the received signal strength and the link quality indicators for each of these protocols. The results of our simulation provide insight into how these parameters can be used to detect a denial-of-sleep attack. Finally, we propose a novel architecture for tackling denial-of-sleep attacks by propagating relevant knowledge via intelligent agents.**

Keywords* — *Denial-of-sleep attacks, wireless sensor networks, RSSI, LQI, energy-aware IoT, energy efficiency, autonomy, security

I. INTRODUCTION

The Internet of Things (IoT) is an emerging trend which is predicted to rapidly expand in the nearest future. In the simplest terms, the IoT represents the concept of having literally any device as part of the internet. While the current internet is somewhat limited to the conventional computers such as desktop computers, laptops, tablets and mobile phones, the IoT would consist of sensor-based devices thereby allowing for any device with a sensor to be connected to the internet. While the internet consists of human-to-machine communication, the IoT includes machine-to-machine communication as these devices may need to talk to each other in certain contexts. This then makes IoT applicable to many sectors such as agriculture, medicine, manufacturing, education, transport and many other sectors.

Practically, any device can be connected to the internet, and if this is the case the developers face many challenges related to the quality of service such as interoperability, scalability, security, performance, intelligence, and energy efficiency. This research narrows the focus to three of these concerns: energy efficiency, autonomy, and security.

One of the major components of the IoT is a Wireless Sensor Network (WSN) which consists of resource-constrained sensor nodes that usually sense different types of data from the environment and then transmit to a base station. Because of their resource-constrained nature, they are very prone to certain attacks called denial-of-sleep attacks.

Denial-of-sleep attacks are considered to be one of the most dangerous attacks which can reduce the life span of sensors from years to days [1]. Sensors usually go into sleep mode as a way of conserving energy. These attacks work by keeping the nodes awake and preventing them from going into sleep mode thereby draining the energy of the nodes [3].

Various methods are used to carry out a denial-of-sleep attack. These are commonly classified as sleep deprivation, barrage, synchronization, replay, collision and broadcast attacks [4]. These attacks take advantage of vulnerabilities such as frame collisions, message overhearing and idle listening [2]. On the other hand, various approaches have been proposed to detect and prevent denial-of-sleep attacks. Existing comparisons of these approaches are qualitative in nature with a focus on their strengths and weaknesses [4].

The aim of the research is to compare and analyse the results of three simulated protocols – Sensor-MAC (SMAC), Timeout-MAC (TMAC) and TunableMAC – based on performance metrics such as the Received Signal Strength Indicator (RSSI) and the Link Quality Indicator (LQI).

The rest of this paper is organized as follows. Section II throws light on related work in the area of evaluation of denial-of-sleep attack-prone MAC protocols. Section III

provides a discussion of the methodology for the research work. Section IV follows with a review and evaluation of the existing approaches based on certain specified criteria. Then, Section V describes our analysis and discussion based on the results of the Castalia framework on the OMNET++ Simulator. Section VI introduces our proposed approach which provides more autonomy than existing approaches. Finally, Section VII concludes the article and outlines directions for future work.

II. RELATED WORK

Recent work [17] compares SMAC, TMAC and 802.11 in terms of energy consumption and the results show that TMAC saves 25% more energy than SMAC. In another project [18], the same protocols are compared, however, more performance metrics are looked into such as end-to-end delay, packet delivery ratio and throughput and similarly, TMAC does better than SMAC. In [19], SMAC, TMAC and CSMA/CA are compared in terms of energy saving and peak load handling. The findings show that TMAC takes the lead in terms of energy saving but does not do as good as SMAC and CSMA/CA in terms of peak handling.

With respect to RSSI and LQI data, pattern recognition methodologies and clustering methods are used in [21] to process the data in order to find out the number of nodes in an unknown neighbouring WSN. This is done with the intention of maintaining network security. While RSSI indicates the strength of the signal, LQI indicates the quality of the signal. In [22], the limitations of RSSI which include being affected by environmental factors such as reflection, refraction, electromagnetic fields and diffraction are discussed. Hence, there's a need for another metric such as LQI, which is not affected by these environmental factors as much as RSSI. Combining these two metrics would guarantee more valid results.

III. METHODOLOGY

Existing approaches are classified in terms of their semantics and function and are then reviewed. Secondly, three protocols vulnerable to denial-of-sleep attacks are simulated in OMNET++ and Castalia framework to measure the RSSI and the LQI parameters of these three protocols under three network sizes. The simulation scenario is a bridge with three different sizes (40m, 200m and 1000m) and nodes (7 nodes, 34 nodes and 154 nodes respectively). The average value for the RSSI for all nodes is measured for each of the three MAC protocols under the three bridge sizes. The same is done for the LQI. The protocols simulated are discussed below:

SMAC is a duty-cycle based MAC protocol which has a fixed listen interval. One of the disadvantages of this is that of there is very low traffic the energy is wasted during the listen phase. On the other hand, if there is very high traffic, throughput may be hindered as the listen time may not be enough. Therefore, there is a need to have an adaptive listen time which TMAC provides. Another challenge with SMAC is that the duty cycle parameters are decided in advance and this may not be suitable for networks with rapidly changing topologies. Another challenge is that it does not have random offset and therefore there may be collisions during broadcasts and Request-To-Send/Clear-To-Send does not work for broadcasts [2].

The TMAC protocol has two major strong areas. One of them is the adaptive listening interval which adapts the listen interval according to the traffic level. Another strong point is the future-request-to-send technique which addresses the early sleeping problem. However, in order to conserve energy, TMAC sends messages between small periods of time and this may have an effect on throughput in high traffic-load networks.

TunableMAC [16] is a protocol that was provided along with the WSN Framework, Castalia. As the name implies, this algorithm is tuneable and allows 12 of its parameters to be tuned. This protocol can simulate many duty-cycling protocols, but it does not support unicast. It uses CSMA for its transmission, therefore its persistence and backing off policies can be tuned. Its duty cycle can also be tuned as well as the train of beacons that can be used to wake up potential receivers.

IV. REVIEW OF EXISTING APPROACHES TO DENIAL-OF-SLEEP ATTACKS

A. Protocols

The MAC layer of the OSI model is usually exploited by denial-of-sleep attacks and the Gateway-MAC (GMAC) is a protocol developed to guard specifically against broadcast attacks [12]. GMAC saves a lot of energy via its centralised cluster management approach and has a better network lifetime than other protocols such as the SMAC, TMAC and Berkeley-MAC (BMAC).

Zero Knowledge Protocol (ZKP) works with the interlock protocol for key transfer and helps to tackle main-in-the-middle and replay attacks [9]. This protocol is not energy-efficient enough as it combines authentication and interlock protocol as part of its protection. It does not apply enough intelligence in tackling a variety of attacks

B. Schemes

The hash-based scheme protects against barrage attacks and works by protecting cluster heads against intrusion [7]. Similar to GMAC, it works by protecting the cluster heads against intrusion which is energy-efficient but not autonomous enough to guard against attacks to sensors other than the cluster heads. CARL classifies incoming packets based on authentication tests and anti-replay checks [3]. This is energy-efficient and relatively positive on throughput but has a relatively low autonomy because of its use of current host-based intrusion detection methods which do not take the distributed nature of

sensors into consideration. If there is a high amount of traffic more than anticipated by the protection mechanism, then the rate limiting may go out of hand thereby even negatively affecting throughput. The fake schedule switch scheme uses the RSSI measurement aid in protecting against collision, exhaustion and broadcast attacks [11]. It works by increasing the energy usage of the attacker which may affect throughput if the fake schedule switch is not done accurately. Although there is some form of autonomy in this method, throughput remains at stake. The secure wake-up scheme finds a way to authenticate messages while ensuring that a node doesn't change to active state [8]. This is quite energy efficient in nature but due to its way of working make affect network throughput if proper authentication is not done in keeping a sensor from waking up which could negatively affect throughput. Two-tier secure scheme (TSS) integrates with a MAC protocol in addition to using a hash-chain to counter replay and forge attacks [10]. While this may affect more than one layer, it may have a negative effect on energy-consumption and even on throughput.

C. Models

The Absorbing Markov Chain (AMC) approach is a mathematical model which is used in calculating the expected death time of a sensor network and using that to determine the presence of a denial-of-sleep attack [13]. While this may have some form of autonomy in its approach, it may affect network throughput because of its procedural complexity and may sometimes not be energy-efficient. The hierarchical collaborative model (HCM) uses anomaly detection technique to detect denial-of-sleep attacks using a distributed approach whereby workload is spread across components in a hierarchical manner [1]. Its anomaly detection technique is quite static in nature and may not be intelligent enough to detect some attacks which may function below the threshold. Cross Layer Mechanism (CLM) focuses not just on the MAC layer as in the case of GMAC, but also focuses on the network and physical layers [4]. It also uses RSSI like in the fake schedule-switch scheme to prevent replay attacks. It is quite low on autonomy as it doesn't consider a variety of scenarios and can have a negative impact on throughput.

V. RESULTS AND ANALYSIS

For RSSI, the higher the value, the higher the signal strength. For the LQI parameter, the lower the value, the better the quality. Figures 1-6 show the RSSI and LQI for SMAC, TMAC and TunableMAC respectively. Figures 7 and 8 show the three protocols in two graphs for RSSI and LQI respectively.

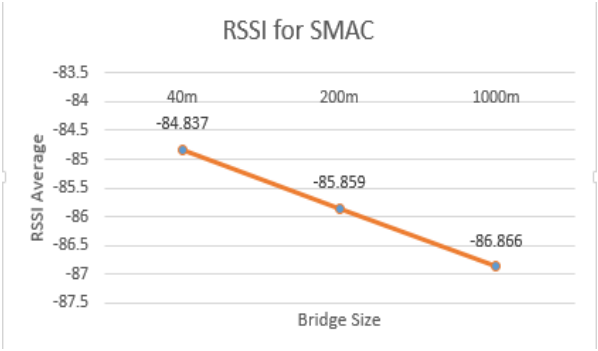

Fig. 1. RSSI for SMAC protocol under three network sizes

Figure 1 shows how the RSSI parameter gets weaker as the network size increases for the SMAC protocol. It is important to note that SMAC has a fixed-duty cycle

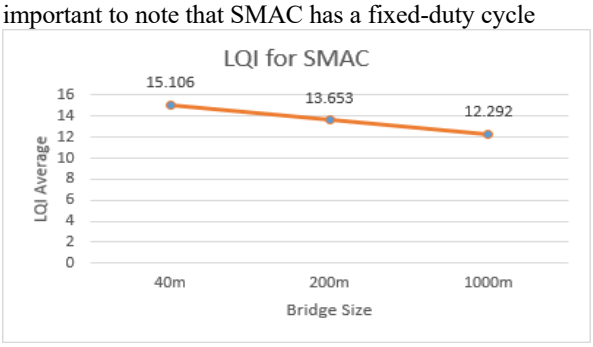

Fig. 2. LQI for SMAC under three network sizes

Figure 2 shows how the link quality gets better with increase in network size for the SMAC protocol. While TMAC performs better than SMAC in terms of RSSI under the 40m bridge - as seen in Figures 1 and 3, SMAC performs better than TMAC in terms of LQI - as seen in Figures 2 and 4.

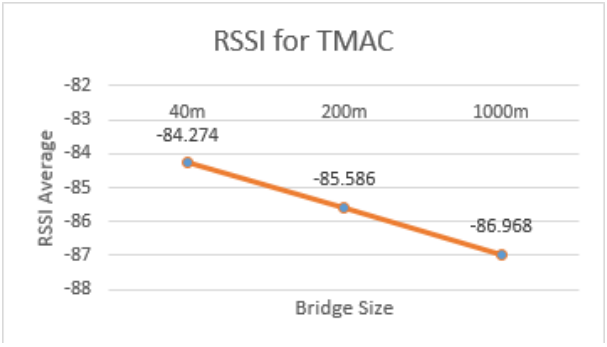

Fig. 3. RSSI for TMAC under three network sizes

Figure 3 shows how the signal strength reduces as the network size increases. Compared to Figure 1, the RSSI parameter for the 40m bridge in Figure 3 is slightly stronger than that of Figure 1. The only exception is in the 1000m bridge where SMAC performs better.

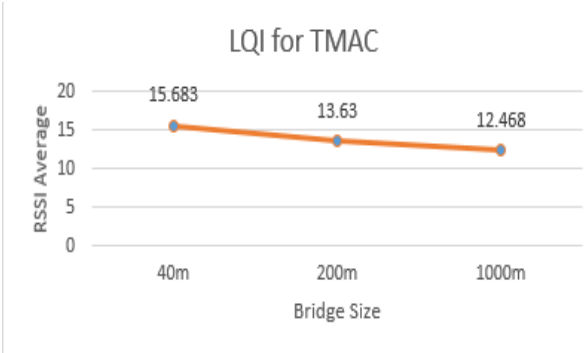

Fig. 4. LQI for TMAC under three network sizes

Figure 4 shows how the link quality improves as the network size increases. Overall, the LQI for TMAC is lesser than that of SMAC.

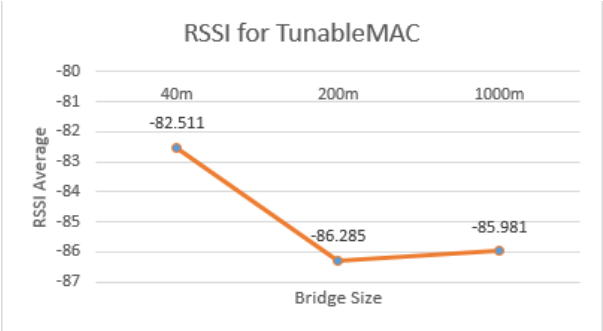

Fig. 5. RSSI for TunableMAC under three bridge sizes

In Figure 5, signal strength weakens as the network size increases from 40m to 200m but then the signal strength slightly gets better with the 1000m bridge. The RSSI for the 40m bridge is stronger than in Figure 1 and Figure 3 and also stronger, overall, than SMAC and TMAC.

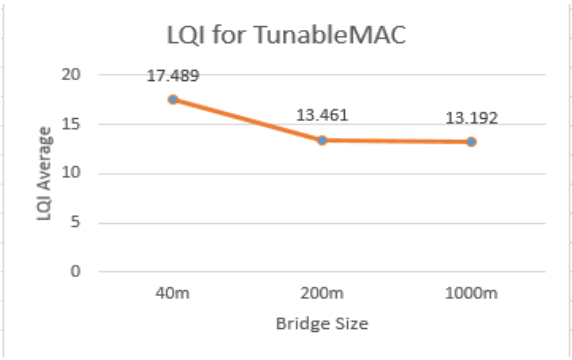

Fig. 6. LQI for TunableMAC under different bridge sizes

In Figure 6, the link quality gets better as the network size increases. The overall LQI for TunableMAC is weaker than SMAC and TMAC.

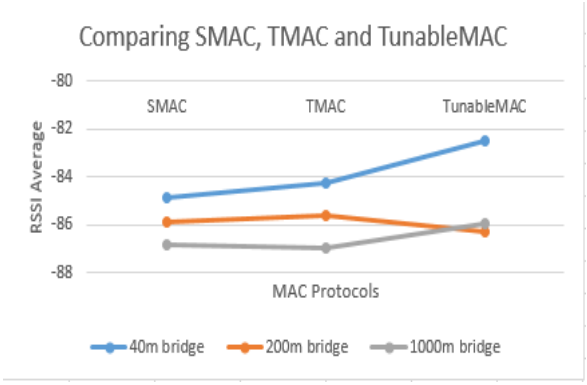

Fig. 7. Comparing RSSI for SMAC, TMAC and TunableMAC

In Figure 7, RSSI is strongest in the 40m bridge with TunableMAC having the best performance. In the 1000m bridge, TunableMAC also has the strongest signal strength among the three protocols. Only in the 200m bridge does this trend with TMAC having the strongest RSSI parameter followed by SMAC.

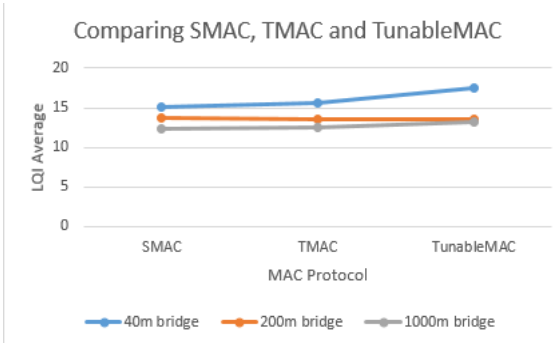

Fig. 8. Comparing LQI for SMAC, TMAC and TunableMAC

In Figure 8, the 1000m bridge has the best link quality with SMAC having the strongest link quality. SMAC also maintains the strongest link quality in the 40m bridge but performs differently in the 200m bridge where TunableMAC has the best performance.

VI. PROPOSED AUTONOMOUS APPROACH

In addition to the aforementioned results, an approach is proposed that could help curb and minimize the impact of a denial-of-sleep attack.

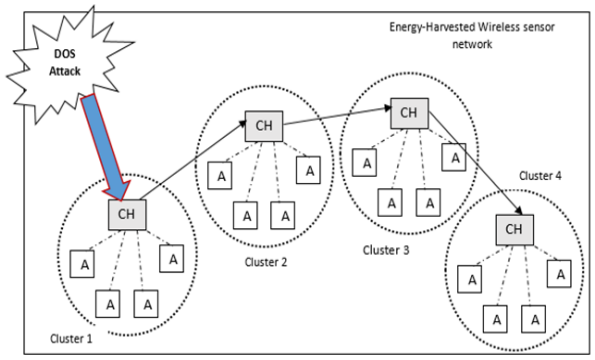

Fig. 9. Proposed WSN architecture for intelligent agents

Figure 9 shows the architecture of the proposed approach [20] which is an improvement of two existing approaches – GMAC and HCM. As discussed earlier, while GMAC and the hash-based scheme use centralized approach via cluster heads, HCM and the distributed wake-up scheme use a distributed architecture. Although these approaches seem very useful, they do not take into consideration the size of the network especially on a large scale.

Our proposed architecture is based on a combination of both the centralized and the distributed approach. It would involve the use of intelligent agents whereby each sensor becomes an agent which can sense data and take responsive action with the workload dynamically distributed among them. However, this would not function optimally with the current battery-powered sensors, but rather an energy harvested IEEE 802.15.4 WSN [14]. This is necessary because the dynamic distribution would lead to an increase in processing power thereby consequently increasing energy costs.

Earlier work [15] introduced the concept of virtual clusters whereby nodes are grouped into the same subnet and presented as a single resource. The WSN will be dynamically divided into clusters with cluster heads appointed for each cluster. In this approach, if a sensor encounters or senses a denial-of-sleep attack, it immediately takes responsive action and also broadcasts the information to the rest of the appointed cluster heads via a "rumour" approach which may consume more bandwidth than processing power. The "rumour" approach is coined from the term "routing by rumour", which explains the semantics of distance-vector routing protocols whereby each router sends messages to its nearest neighbour until the information propagates to all the routers. In this case, the cluster heads send information to the nearest cluster head and it continues that way until the information gets to all the cluster heads which then pass the information to their clusters. The cluster heads then relay this information to the sensors in their clusters.

VII. CONCLUSION AND FUTURE WORK

The novelty of this paper lies in the simulation results and the comparisons between the three protocols as well as the new proposed architecture for tackling denial-of-sleep attacks. As discussed in Section II, although there have been comparisons of SMAC and TMAC, as well as analysis of RSSI and LQI data, however, no research to the best of our knowledge has compared these protocols in the context of what impact they have on RSSI and LQI values.

In the future, the RSSI values would be used as a parameter in detecting denial-of-sleep attacks. This would be achieved via the following steps:

A. Use RSSI to measure distance between nodes

The RSSI parameter can be used to tell the distance between nodes and this can be useful in knowing how far a node is from the sink.

B. Use the distance measurements to assign nodes to real clusters

Knowing the distance between nodes can also enable clustering to be done among nodes. This would allow creation of real clusters and allows for nodes closest to each other to be in the same cluster.

C. Establish a threshold value for the RSSI and throw an alert when there is an anomaly

Studying the RSSI values can also help detect a malicious node by observing an abnormal pattern in the RSSI values which would detectable if there is a threshold value.

Furthermore, more research can be done in the TunableMAC protocol to find out what other parameters influence its high performance for the majority of the results. The TunableMAC is a good protocol to investigate especially because of its tuneable parameters which allows for a lot of experimenting to see the effect of certain changes. The throughput and latency aspects of the protocols can also be analysed to observe the relationship these parameters. Finally, this can lead to the development of an improved secure and energy-efficient WSN MAC protocol.

REFERENCES

[1] T. Bhattasali, "Sleep Deprivation Attack Detection in Wireless Sensor Network," Int. J. Comput. Appl., vol. 40, no. 15, pp. 19-25, 2012.

[2] 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.

[3] D.R. Raymond and S.F. Midkiff, "Clustered Adaptive Rate Limiting: Defeating Denial-of-sleep Attacks In Wireless Sensor Networks," Proc. of IEEE Military Communications Conference (MILCOM), pp. 1-7, IEEE Xplore, 2007.

[4] 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.

[5] J. Rezaei, “Best-Worst Multi-Criteria Decision-Making Method,” Omega, vol. 53, pp. 49-57, 2015.

[6] L. Xu and J.B. Yang, “Introduction to Multi-Criteria Decision Making and the Evidential Reasoning Approach,” Manchester School of Management, 2001, https://php.portals.mbs.ac.uk/Portals/49/docs/jyang/XuYang_MSM_WorkingPaperFinal.pdf.

[7] 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 Int. J. Distrib. Sens. Networks, vol. 2, no. 03, pp. 267–287, 2006.

[8] R. Falk and H. J. Hof, “Fighting insomnia: A secure wake-up scheme for wireless sensor networks,” Proc. 2009 3rd Int. Conf. Emerg. Secur. Information, Syst. Technol. Secur. 2009, pp. 191–196, 2009.

[9] 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.

[10] 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.

[11] 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. 5th Int.# Conference on Information Assurance and Security, IAS’09, pp. 446-449, IEEE Xplore, 2009.

[12] M. I. Brownfield, “Energy-efficient Wireless Sensor Network MAC Protocol,” PhD Thesis, Virginia Tech, 2006, http://hdl.handle.net/10919/26749.

[13] T. Bhattasali and R. Chaki, “AMC Model for Denial of Sleep Attack Detection,” Journal of Recent Research Trends, pp. 1-4, 2012, http://arxiv.org/abs/1203.1777.

[14] 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, 2014.

[15] 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.

[16] B. A. Networks, “User’s Manual,” March, 2011.

[17] A. Pratama, R. Munadi, and R. Mayasari, "Design and Implementation of Flood Detector Using Wireless Sensor Network with Mamdani's Fuzzy Logic Method", Proc. 2nd Int. Conference on Information Technology Information Systems and Electrical Engineering (ICITISEE), pp. 192-197, 2017.

[18] A. Roy and N. Sarma, “Performance Evaluation of Synchronous Energy Efficient MAC Protocols for Wireless Sensor Networks,” Proc. Of 2nd Int. Conference on Communication, Computing and Security [ICCCS-2012], pp. 806-813, Procedia Technology, 2012.

[19] G. P. Halkes, T. van Dam, and K. G. Langendoen, “Comparing Energy-Saving MAC Protocols for Wireless Sensor Networks,” Mobile Networks and Applications, vol. 10, no. 5, pp.783-791, Springer, 2005.

[20] E. Udoh, V. Getov, A. Bolotov, “Sensor Intelligence for Tackling Energy-Drain Attacks on Wireless Sensor Networks,” Proc. Of 23rd Workshop on Automated Reasoning: Bridging the Gap between Theory and Practice, University of Liverpool, 2016, http://westminsterresearch.wmin.ac.uk/17129/1/ARW-16-Udoh-Getov-Bolotov.pdf.

[21] Y. Wang, I.G. Guardiola, X. Wu, “RSSI and LQI Data Clustering Techniques to Determine the Number of Nodes in Wireless Sensor Networks,” International Journal of Distributed Sensor Networks, 2014, https://doi.org/10.1155/2014/380526.

[22] R. Grossmann, J. Blumenthal, F. Golatowski, D. Timmermann, “Localization in Zigbee-based Sensor Networks,” Proc. 1st European ZigBee Developers Conference (EuZDC '07), München, Germany, 2007.