Risk Analysis of Personal Data Loss in Wireless Sensor Networks

Anastasiya Doroshenko[1], Kvitoslava Obelovska[1] and Olha Bilyk[1]

[1] *Lviv Polytechnic National University, S. Bandera str. 12, Lviv, 79013, Ukraine*

Abstract

Data protection has always been a key issue in wireless sensor networks. However, with the entry into force of the General Data Protection Regulation (GDPR) on 25 May 2018, new requirements to the collection, transmission, and protection of personal data have been added to the handling of data in wireless sensor networks. This is due to the spread of IoT and Wireless Body Area Sensor Networks (WBAN) in smart homes, smart cities, applications that track physical activity and human health where the most of the data collected, transmitted, and processed are not only personal but also fall into the category of sensitive data defined in the GDPR. Accordingly, the risks of losing this data are much higher, and minimizing the loss of packets with such data is a particularly urgent task. The methodology for improving the performance of networks, focused on reducing packet loss is given on the example of sensor networks. The bottleneck of sensor wireless networks is access to a shared physical medium. There are many protocols to control access to the physical environment, the protocol choice can be important in terms of packet loss. The L-MAC sensor network protocol, which belongs to the class of scheduled protocols, and the B-MAC protocol, which belongs to the category of contention based, were studied and compared. For specific networks, results of the research showed a significant dependence of the number packets lost on the choice of MAC-sublayer protocol and on the protocol settings. When configuring the protocol, the SlotDuration parameter was used as a variable during network optimization. Research conducted using the Discrete Event Simulator OMNeT++ and INET framework.

Keywords

GDPR, Wireless Sensor Network, MAC protocol, packet loss, personal data.

1. Introduction

The use of sensor networks has spread particularly rapidly in the IoT, smart cities and homes, and in medicine and the daily lives of most people in recent years. More and more gadgets that we use every day collect certain data and share it with each other. Sensors of temperature and humidity, gas and water, heartbeat, and human pressure in real-time exchange information with our smartphones and computers, which allows you to remotely control your home, prevent emergencies, or monitor human well-being. However, with the entry into force on May 25, 2018, the General Data Protection Regulation (GDPR) added to the generally accepted requirements for

CITRisk'2021: 2nd International Workshop on Computational & Information Technologies for Risk-Informed Systems, September 16–17, 2021, Kherson, Ukraine

EMAIL: anastasia.doroshenko@gmail.com (A.Doroshenko); kvitoslava.m,obelovska@lpnu.ua (K.Obelovska); olha.bilyk.knm.2018@lpnu.ua (O.Bilyk)

ORCID: 0000-0002-7214-5108 (A.Doroshenko); 0000-0002-8714-460X (K.Obelovska); 0000-0002-3589-5401 (O.Bilyk)

data transmission over wireless networks, which are caused by the requirements of the GDPR. In particular, one of the main requirements is the security of the personal data of the user, which are processed by the controller.

The article considers the problem of improving the security of data transmission in wireless sensor networks, namely - the process of controlling access to the physical environment during the transmission of sensitive personal data of the user in real-time. To reduce the risk of losing personal data during transmission, it is necessary to minimize the number of lost packets, thus avoiding their retransmission.

The main contributions of this paper can be summarized as follows:

- identified the types of personal data and sensitive personal data transmitted in wireless sensor networks, as well as described the features of working with them by the GDPR;
- it is revealed that the performance of the MAC-sublayer for the wireless sensor network depends on the media access protocol category and is different for different network size;
- it is also has been shown that that use of the protocol L-MAC, which belongs to the scheduled protocols, can provide total number of packets received 40 % more than when using the B-MAC protocol from the category of contention based;
- based on simulation, the conditions under which the parameter optimization for the B-MAC and L-MAC protocols could significantly decrease packet loss on MAC-sublayer, are determined.

2. Related Works

With continuing developments in miniaturization and battery design, wireless sensor networks (WSN) are poised to become common technology in our daily lives. Low cost and flexibility of deployment make WSN well suited for a wide variety of military, environmental, healthcare, and commercial applications. Some WSN applications, such as monitoring patients in hospitals or weapons targeting in battlefront require end-to-end data confidentiality [1-3].

Wireless transmission method in wireless sensor networks has put forward higher requirements for private protection technology.

Data protection in WSN is one of the main requirements that must be provided at the highest level. There are various methods and approaches for data protection in wireless sensor networks. However, since WSN are made up of many resource limited sensor nodes, they are typically unable to sustain the high volumes of data transmissions. In particular, to reduce communication overhead in term of number of messages transmitted in the sensor network and to reduce computational overhead due to arithmetical operation in providing encryption and decryption in private data aggregation, in [4] proposed a privacy-preserving data aggregation in WSN.

In [5] proposing to use in-network data aggregation, where sensor data from multiple nodes can be combined before being forwarded to neighboring nodes; and thus, energy consumption can be reduced significantly. But in situations where sensor nodes privacy is non-negotiable, data aggregation cannot be implemented at the cost of security. Therefore, there is a strong need for secure data aggregation protocols designed to fit the unique properties and considerable constraints of WSNs. In [5] proposed a novel solution for the secure aggregation of data in WSNs based on probabilistic homomorphic encryption. By combining with a unique encoding function, their solution guarantees the privacy of sensor data, while also greatly reducing communication costs.

However, aggregation is a very energy-intensive operation that significantly reduces energy efficiency of WSN. Energy efficient privacy preserving data aggregation is important in power

constrained wireless sensor networks. Existing hop by hop encrypted privacy preserving data aggregation protocols does not provide efficient solutions for energy constrained and security required WSN due to the overhead of performing power consuming decryption and encryption at the aggregator node for the data aggregation and the increased number of transmissions for achieving data privacy. The decryption of data at the aggregator node will increase the frequency of node compromise attack. Thereby aggregator node reveals large amounts of data to adversaries. Therefore, in [6] was proposed privacy homomorphism-based privacy preservation protocol achieves non delayed data aggregation by performing aggregation on encrypted data. Thereby decreases the node compromise attack frequency. The main aim of research was to provide a secure data aggregation scheme which guarantees the privacy, authenticity and freshness of individual sensed data as well as the accuracy and confidentiality of the aggregated data without introducing a significant overhead on the battery limited sensors [7].

According to the packet loss problem of private protection algorithm based on slice technology, in [6] was described the data private protection algorithm with redundancy mechanism, which ensures privacy by privacy homomorphism mechanism and guarantees redundancy by carrying hidden data. It selects the routing tree generated by Collection Tree Protocol as routing path for data transmission. By dividing at the source node, it adds the hidden information and also the privacy homomorphism. At the same time, the information feedback tree is established between the destination node and the source node. In addition, the destination node immediately sends the packet loss information and the encryption key via the information feedback tree to the source node. As a result, it improves the reliability and privacy of data transmission and ensures the data redundancy [8, 9].

The protection of personal data transmitted via WSN can be considered as a separate task. After all, a huge number of indicators that are transmitted from different sensors in a smart home or within a smart city can be used to identify users, analyze their behavior and make automated decisions. Starting from May 25, 2018, all these actions must be regulated by the GDPR and meet its requirements [10-11].

A smart home is a building in which ubiquitous computing and information technology are deployed to expect and respond to the occupants' needs and to enhance their every day's life. To achieve this goal, smart homes rely on WSN for collecting all kind of personal data. Nevertheless, information privacy is one of the most sensitive issues for users nowadays. Therefore, it becomes of utmost importance to ensure this privacy in smart homes. This is particularly challenging because of the specific characteristics of WSN (e.g. limited resources: energy, storage, computation, communication) and the specific smart home environment. In [7] overviewed existing techniques for content-based privacy and contextual-based privacy in smart home environments according to a set of proposed criteria.

Also, now Wireless Body Area Sensor Networks (WBAN) are becoming more and more popular and have shown great potential in real-time monitoring of the human body. With the promise of cost effective, unobtrusive, and unsupervised continuous monitoring, WBAN have attracted a wide range of monitoring applications such as healthcare, sport activity and rehabilitation systems. However, in using the advantage of WBAN, a number of challenging issues should be resolved. Besides open issues in WBAN such as standardization, energy efficiency and Quality of Service, security and privacy issues are one of the major concerns. Since these wearable systems control life-critical data, they must be secure. Nevertheless, addressing security in these systems faces some difficulties. WBANs inherit most of the well-known security challenges from WSN. However, typical characteristics of WBAN, such as severe resource constraints and harsh environmental conditions, pose additional unique challenges for security and privacy support. In

[12], was surveyed major security and privacy issues and potential attacks in WBAN and explained an unsolved quality of service problem which has great potential to pose a serious security issue in WBANs.

For different applications of WSN, the loss of data packets has its risks. In particular, for emergency monitoring and prevention systems, the loss of a package containing critical data means that appropriate actions to prevent or respond to an emergency will not be taken in time [10]. Loss of data in the WBAN medical direction can also lead to the fact that critical patient readings will not be processed in time, which can lead to fatal consequences.

On the other hand, according to the GDPR, data describing a person's whereabouts, physical and medical characteristics belong to sensitive personal data and must be protected with particular care. That is why the urgent task is to minimize data loss during simultaneous access to the physical environment in real-time [11].

3. Method and techniques of research

3.1. Enforcing GDPR regulation to wireless sensor networks

Data privacy in WSN remains a major concern of regulation bodies. The introduction of the European General Data Protection Regulation (GDPR) enables users to control how their data is accessed and processed, requiring consent from users before any data manipulation is carried out on their personal data by smart devices or cloud-hosted services (article 1 GDPR). The GDPR applies to the processing of personal data of data subjects in the Union in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not (article 3 GDPR) [9].

Following the privacy-by-design approach system should supporting GDPR compliance checking for smart devices. The privacy requirements of such applications are related to GDPR obligations of device and software systems operators (such as user consent, data protection, right to forget etc.) [12, 14].

In order to identify and minimize project data protection risks, it is recommended to conduct a Data Protection Impact Assessment (DPIA). DPIA is a way for organization to systematically and comprehensively analyze its processing and help to identify and minimize data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals [13].

A DPIA does not have to indicate that all risks have been eradicated. But it should help you document them and assess whether or not any remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals. A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

Table 1 described the correlation between WSN, WBAN and GDPR obligations and rights [14, 15].

Table 1
Correlation between WSN, WBAN and GDPR obligations and rights

GDPR obligations and rights	Article of GDPR	WSN	WBAN
Right to be informed	Article 15	+	+
Right of access	Article 15	+	+
Right to rectification	Article 16	+	+
Right to be forgotten	Article 17	+	+
Right to restriction of processing	Article 18	+	+
Right to be notified about rectification or erasure	Article 19	+	+
Right to data portability	Article 20	+	+
Right to object	Article 21	+	+
Right to deter automated decision-making	Article 22	+	+
Subject`s consent	Article 7	+	+
Child consent	Article 8	+	+
Privacy by design	Article 25	+	+
Breach Notification within 72h	Article 33	+	+
Data Privacy Impact Assessment	Article 35	+	+

DPIA is recommended to be performed if the system:

- use innovative technology;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice;
- track individuals' location or behavior;
- profile children or target marketing or online services at them;
- process data that might endanger the individual's physical health or safety in the event of a security breach.

Therefore, from the above we can conclude that for most tasks that use wireless sensor networks, risk assessment through the implementation of the DPIA is mandatory. Once the risks are identified, it is necessary to choose organizational and technical methods to minimize them. In particular, one of such methods is the selection of optimal parameters for data transmission via WSN to minimize the loss of packets with personal data.

3.2. Wireless networking technologies for data transmission

Wireless networking technologies are based on the use of a shared environment for data transmission. That is why the bottleneck of any wireless local area networks, wireless sensor networks have access to the physical medium. Management of access to the physical environment is regulated by the Media Access Control (MAC) sublayer of network architecture. The primary

task of any MAC protocol is to control the access of the nodes to the shared medium. There are four protocol categories as contention based, scheduling based, channel polling based, and hybrid [16] and a large number of MAC protocols specifically designed for this sublayer in wireless sensor networks [17, 18]. For research in this paper we have chosen the two most important categories: contention based and scheduling based. In the contention-based protocols the channel access policy is based on competition. Each time a node needs to send a packet, it tries to access the channel. These protocols cannot provide guaranteed access to the network. Schedule-based protocols can be scheduling packets on nodes or scheduling nodes to access a channel. Some of these protocols take battery charge into account when scheduling nodes.

We will focus in detail on the study of two protocols B-MAC and L-MAC, which respectively belong to contention-oriented and scheduling based.

B-MAC (Berkeley MAC) protocol is a carrier sense media access protocol that provides effective collision avoidance, high channel utilization and low power operation. L-MAC (Lightweight MAC) is an energy-efficient medium access protocol based on time-division multiple access to give nodes in the WSN the opportunity to communicate collision-free.

WSN optimization requires a lot of time and money if you do it directly with real sensors. That is why it is important to create models of wireless sensor networks for their research and optimization. As a tool we used OMNeT ++ Discrete Event Simulator using INET framework that contains the implementation of MAC protocols for wireless sensor networks [19, 20].

There are many network parameters, which are studied by various authors, such as the data transmission time [21], the number of retries and conflicts [22], reliability [23-25], data loss [22, 26, 27], network throughput, backoff time and delay [25, 28-30], energy consumption [31], etc. We mainly focused on how to reduce data loss. We compare B-MAC and L-MAC protocols in terms of the number of packets carried by the network. We want to find the values of the parameters for each protocol that lead to the best performance of the network in a particular scenario. We want to minimize packet loss, so we need to optimize the number of packets received by the server. Optimization of protocols will be performed depending on the parameter Slot Duration. For both protocols, we will select this parameter specifically for the available number of nodes in the network. We will find the value of the Slot Duration, at which the server will receive the maximum number of packets during the network.

4. Results of Experiment

4.1. The architecture of wireless sensor networks

We will conduct our experiment using two networks, which include 5 (Figure 1) and 10 (Figure 1) sensor nodes that send data packets to the server.

To begin with, we will conduct an experiment with both protocols, where each sensor will send data packets to the server with an interval of 1 second. The start time of sending the first packet of each node is determined by the exponential distribution in the range from 0 to 1 second:

.sensor.app[0].sendInterval = 1s

.sensor.app[0].startTime = exponential(1s).

For both B-MAC [19] and L-MAC [20], we will use a value of 0.1 second as the slotDuration parameter:

**.wlan[*].mac.slotDuration = 0.1s,

and the length of the message – 10 Byte:

.sensor.app[0].messageLength = 10 Byte.

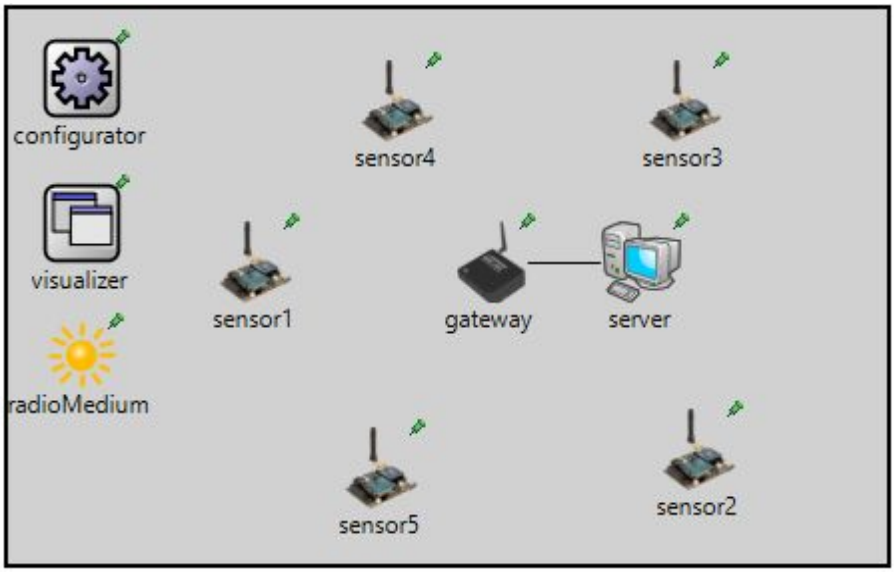


Figure 1: Network structure with 5 sensor nodes

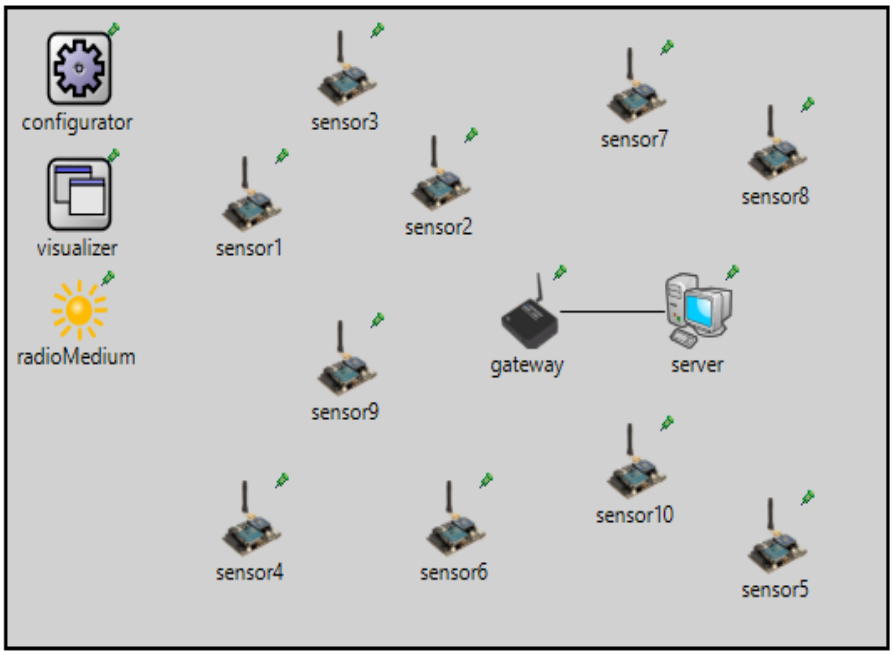


Figure 2: Network structure with 10 sensor nodes

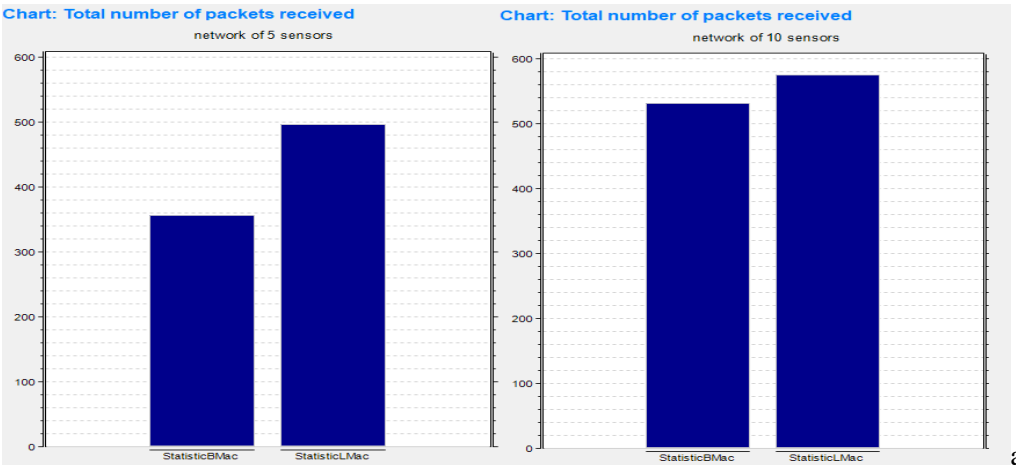
To increase the size of the statistical sample, we will repeat each experiment 10 times and then find and analyze the arithmetic mean of the number of packets delivered to the server.

The results of the simulation according to the settings and scenario described above are shown for networks with 5 and 10 sensors, respectively, in Figures 3 a) and 3 b) and Table 2.

Table 2

Comparison of the number of received packets for B-MAC and L-MAC protocols

	5 sensor nodes		10 sensor nodes	
Protocol	B-MAC	L-MAC	B-MAC	L-MAC
SlotDuration, sec	0,1	0,1	0,1	0,1
The number of packets received by the server	356	497	532	576



a)

b)

Figure 3: Total number of packets received: a) for the network of 5 sensor nodes; b) for the network of 10 sensor nodes

Analysis of the results shows that for the studied networks, the use of the L-MAC protocol provided more packets than the use of the B-MAC protocol for both networks. For a network with 5 nodes by 40%, and with 10 nodes – by 8%.

4.2. Optimizing for packet loss

Now we implement the process of optimizing the number of packets received by the server. The scenario of the experiment is as follows. For each protocol, change the slotDuration parameter in 0.01 second increments from 0.01 seconds to 1 second and count the number of packets the server will receive in 100 seconds of network operation. As mentioned earlier, repeat this experiment 10 times to increase the sample. With the best slotDuration parameter, the number of received packets by the server will be the largest, respectively, the number of lost packets is minimal.

4.2.1. B-MAC protocol

In the OMNET ++ environment for the B-MAC protocol, the condition of the above-described parameter changes and time constraints are set as follows:

**.mac.slotDuration = ${slotDuration=0.01..1 step 0.01}s
sim-time-limit = 100s
repeat = 10

5 sensors in the network

The results of starting the simulator in the above scenario using the B-MAC protocol for a network with 5 nodes are shown in Figure 4 and Table 3.

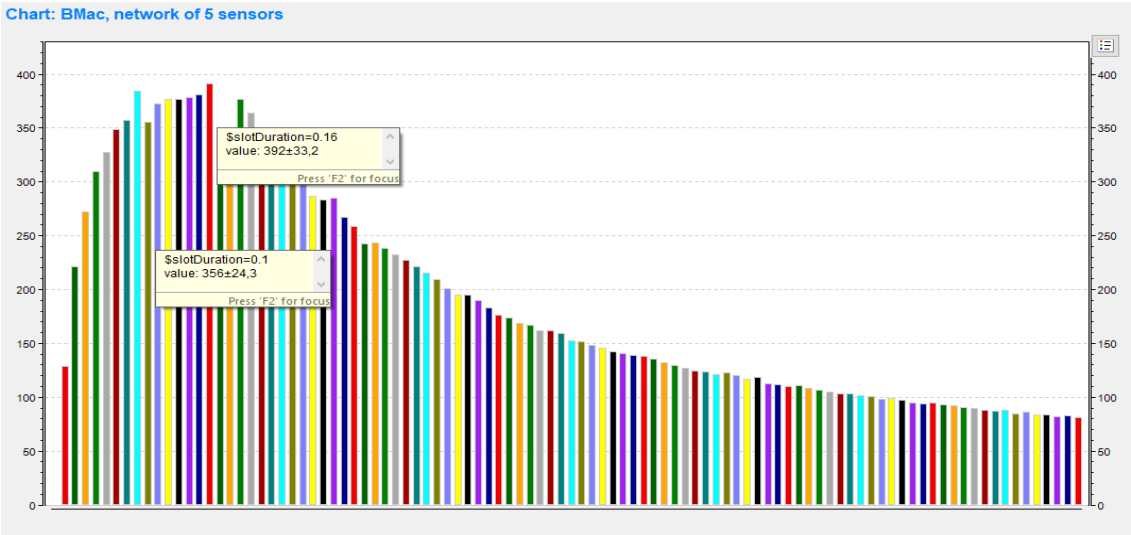


Figure 4: B-MAC statistics for a network of 5 nodes

Figure 4 illustrates the significant dependence of packets number received by the server, depending on the variable SlotDuration. We perform optimization in order to maximize the number of received packets. And as can be seen from Figure 4, the maximum number of packets received by the server averages 392 packets (392 ± 33.2). Before optimization, according to the previous experiment, this value was 356 packets (see Figure 4 or Figure 3 a)). For the network, which includes 5 sensors, when using the B-MAC protocol, the best option is to set the parameter Slot Duration = 0.16 seconds. At this value of the Slot Duration parameter, the number of received packets by the server will be the maximum and 10% more than before optimization.

Table 3

Comparison of the number of received packets for B-MAC and L-MAC protocols without and with SlotDuration parameter optimization

	5 sensor nodes				10 sensor nodes			
Protocol	B-MAC		L-MAC		B-MAC		L-MAC	
	optimization		optimization		optimization		optimization	
SlotDuration, sec	0,1	0,16	0,1	0,05	0,1	0,07	0,1	0,05
The number of packets received by the server	356	392	497	497	532	624	576	994

10 sensors in the network

In Figure 5 shows the results of a similar experiment for a network with 10 sensor nodes. The graph on fig 5. shows that the best value of the SlotDuration parameter for this network is 0.07 seconds. The average number of packets received by the server, with a SlotDuration value of 624 packets. An interval of 0.06 seconds also gives a very close to optimal number of received packets. The data of both optimization experiments, as well as the results of the optimization results are summarized in Table 3.

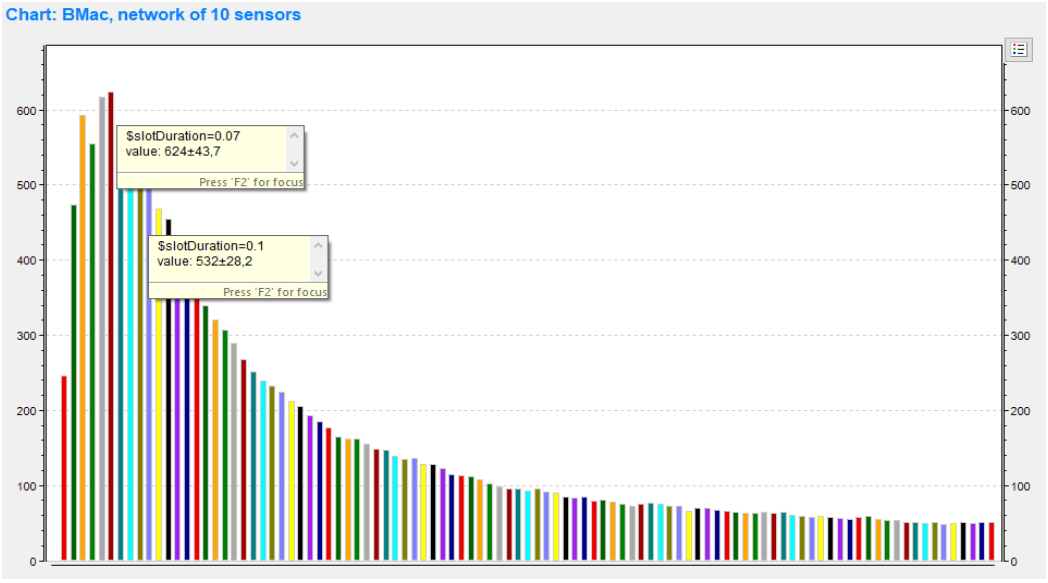


Figure 5: B-MAC statistics for a network of 10 nodes

Comparison of the results before and after optimization shows that for the B-MAC protocol for both five- and 10-node networks, the number of packets received by the server due to optimization increased significantly, by 10% and 17% respectively.

We will conduct similar studies for the L-MAC protocol.

4.2.2. L-MAC protocol

For the L-MAC protocol, the change of the SlotDuration parameter will be set in the same way as in the experiment with the B-MAC protocol:

**.mac.slotDuration = ${slotDuration=0.01..1 step 0.01}s

sim-time-limit = 100s

repeat = 10

5 sensors in the network

Figure 6 presents the results of the simulator in the script, which allows to maximize the number of packets received by the server using the L-MAC protocol. The variable parameter is the value of SlotDuration.

According to the graph on fig.6 when using the L-MAC protocol in a network with 5 nodes, the maximum value of the average number of received packets 497 was obtained for both Slot Duration = 0.05 and Slot Duration = 0.1 seconds, which is set by default. That is, optimization in

this case does not win. However, the nature of the curve indicates that a further increase in Slot Duration will lead to a sharp decrease in the number of received packets.

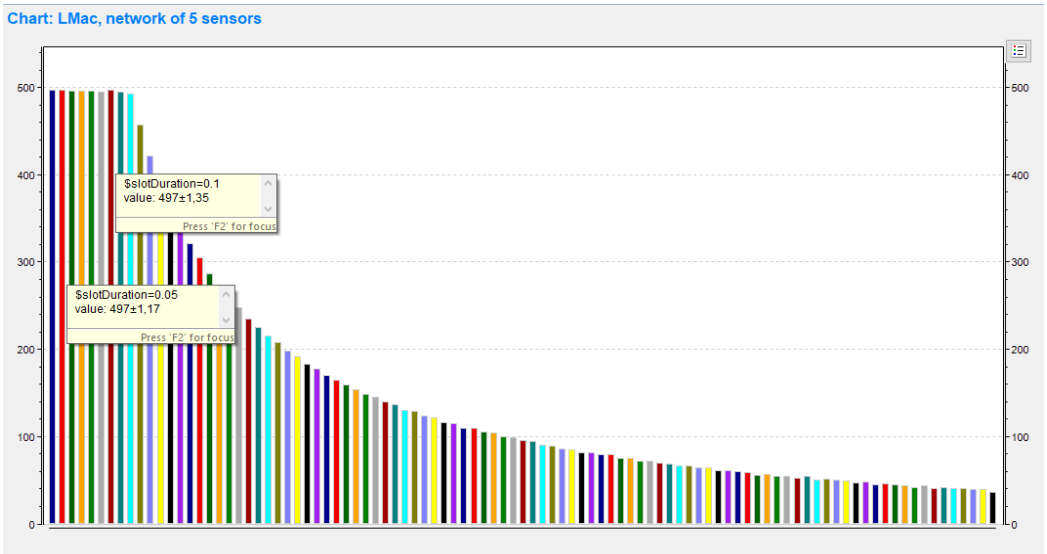


Figure 6: Statistics for L-MAC protocol in a network with 5 nodes

Find the optimal SlotDuration parameter for a network with 10 nodes.

10 sensors in the network

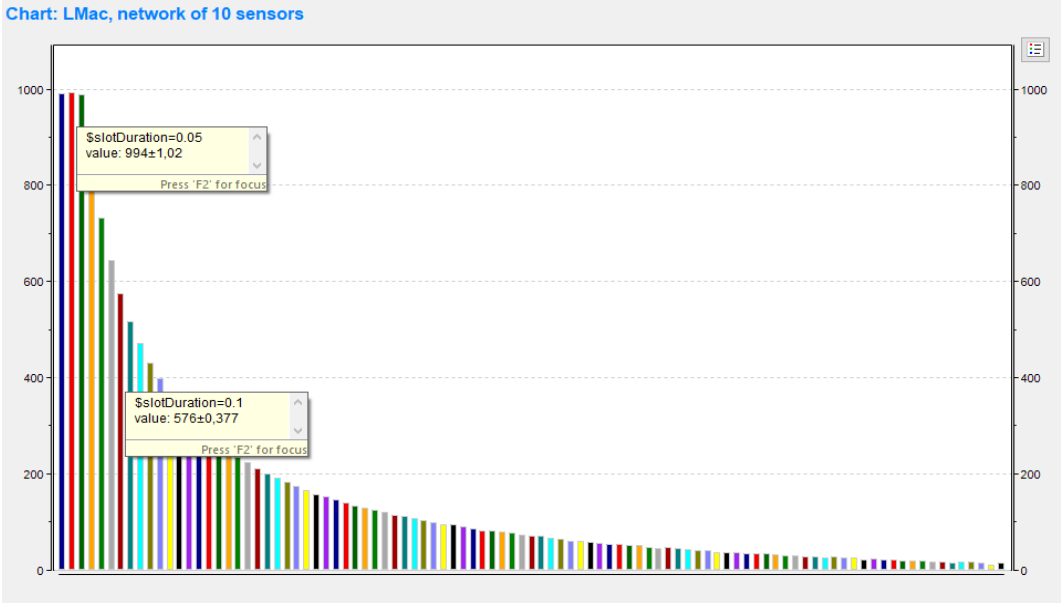


Figure 7: Statistics for L-MAC protocol in a network with 10 nodes

The best value of the SlotDuration parameter for this network is 0.05 seconds. The number of packets received by the server in this case is 994. This is 72% more than when the SlotDuration value is 0.1 second, set by default.

5. Discussions

As shown by the results in Figures 3a) and 3b) for the studied sensor networks, the L-MAC protocol, which belongs to the class of scheduled protocols, provides less packet loss on MAC-sublayer than when using the B-MAC protocol, which belongs to the category of contention based. Research shows for a network with 10 nodes, the number of received packets increased by 40 %, for networks with 5 nodes – by 8 %.

For quantitative analysis of the optimization results, the default value of the SlotDuration parameter was set to the default value of SlotDuration in the Simulator OMNeT ++ equal to 0.1 second. Figures 4-7 illustrate the optimization results depending on the SlotDuration parameter and illustrate the significant effect of this parameter on the number of lost packets for both the B-MAC protocol and the L-MAC protocol. Data analysis shows that this effect is different for networks with different numbers of nodes.

For the B-MAC protocol for both five- and 10-node networks, the number of packets received by the server due to optimization increased significantly, by 10% and 17% respectively.

For the L-MAC for five-node networks, optimization does not give a gain, because the accepted base value of SlotDuration in this configuration also provides the optimal result. Regarding the L-MAC protocol for ten-node networks, the optimization gave a significant improvement, namely an increase in the number of packets received by the server by as much as 72%.

6. Conclusion

Among the huge amount of data transmitted through wireless sensor networks, a significant part of personal data of people is transmitted, which, according to the GDPR, require special protection. The study concluded that it is particularly important for WSN and WBAN to identify the risks associated with the collection and transmission of sensitive personal data (such as information about a person's physical condition, indicators that determine his health, coordinates and location, etc.). To do this, it is advisable to identify all possible risks associated with compliance with the GDPR using DPIA.

The methodology for improving the performance of networks, focused on reducing packet loss, is given on the example of sensor networks. The bottleneck of sensor wireless networks, like other wireless networks, is access to a shared physical medium. There are many protocols to control access to the physical environment that can be divided into four protocol categories as contention based, scheduling based, channel polling based, and hybrid. Analysis of different categories protocol showed that for specific networks, the choice categories protocol can be important in terms of packet loss. Thus, for the studied sensor networks, the L-MAC protocol, which belongs to the class of scheduled protocols, provides less packet loss on MAC-sublayer than when using the B-MAC protocol, which belongs to the category of contention based. Research conducted using the Discrete Event Simulator OMNeT++ and INET framework show that for a network with 5 nodes, the number of received packets increased by 40 %.

Optimization of protocol settings allowed to reduce the number of lost packets considerably. The SlotDuration parameter was used as a variable during optimization.

Experiments have shown that for a certain type of measurement, the number of packets received by the server through optimization increased by both B-MAC and L-MAC by 17% and 72%, respectively.

7. Acknowledgements

This work was realized within the framework of the program Erasmus+ Jean Monnet Module “Data Protection in EU”' (611692-EPP-1-2019-1-UAEPPJMO-MODULE).

References

[1] S.S.Javadi, M.A.Razzaque, Security and Privacy in Wireless Body Area Networks for Health Care Applications, in: S. Khan, A.-S. Khan Pathan (Eds.), Wireless Networks and Security: Issues, Challenges and Research Trends, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 165–187. https://doi.org/10.1007/978-3-642-36169-2_6. https://doi.org/10.1007/978-3-642-36169-2_6

[2] A.Doroshenko, Analysis of the Distribution of COVID-19 in Italy Using Clustering Algorithms, in: 2020 IEEE Third International Conference on Data Stream Mining & Processing (DSMP), 2020, pp. 325–328. https://doi.org/10.1109/DSMP47368.2020.9204202. doi: 10.1109/DSMP47368.2020.9204202

[3] V.Sherstjuk, M.Zharikova, I.Sokol, Forest Fire Monitoring System Based on UAV Team, Remote Sensing, and Image Processing, in: 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), 2018, pp. 590–594. https://doi.org/10.1109/DSMP.2018.8478590

[4] V.Akila, T.Sheela, Preserving data and key privacy in Data Aggregation for Wireless Sensor Networks, in: 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), 2017, pp. 282–287. https://doi.org/10.1109/ICCCT2.2017.7972286

[5] J.Jose, M.Princy, J.Jose, PEPPDA: Power efficient privacy preserving data aggregation for wireless sensor networks, in: 2013 IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), 2013, pp. 330–336. https://doi.org/10.1109/ICE-CCN.2013.6528518

[6] P.Li, C.Xu, H.Xu, L.Dong, R.Wang, Research on data privacy protection algorithm with homomorphism mechanism based on redundant slice technology in wireless sensor networks, China Communications, 16 (2019), 2019, pp.158–170. https://doi.org/10.23919/j.cc.2019.05.012

[7] A.Alami, L.Benhlima, S.Bah, An overview of privacy preserving techniques in smart home Wireless Sensor Networks, 2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA), 2015, pp. 1–4

[8] S.A.Thompson, B.K.Samanthula, Optimized Secure Data Aggregation in Wireless Sensor Networks, in: 2017 15th Annual Conference on Privacy, Security and Trust (PST), 2017, pp. 394–3942. https://doi.org/10.1109/PST.2017.00055

[9] A.Doroshenko, Application of global optimization methods to increase the accuracy of classification in the data mining tasks, CEUR-WS.Org. 2353, 2019, pp. 98–109

[10] Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)", Op.europa.eu, 2020 [Online], Available: https://op.europa.eu/en/publicationdetail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/ language-en

[11] O.Tymchenko, B.Havrysh, O.Khamula, S.Lysenko, K.Havrysh, Risks of Loss of Personal Data in the Process of Sending and Printing Documents, CEUR-WS.org, vol. 2805, 2020, pp. 373–384
[12] S.S.Javadi, M.A.Razzaque, Security and Privacy in Wireless Body Area Networks for Health Care Applications. In: Khan S., Khan Pathan AS. (eds) Wireless Networks and Security, Signals and Communication Technology, Springer, Berlin, Heidelberg, 2013. https://doi.org/10.1007/978-3-642-36169-2_6
[13] S.Rizou, E.Alexandropoulou-Egyptiadou, K.E.Psannis, GDPR Interference With Next Generation 5G and IoT Networks, in IEEE Access, vol. 8, pp. 108052-108061, 2020. doi: 10.1109/ACCESS.2020.3000662
[14] J.Ortiz, P.J.Fernández, R.Sanchez-Iborra, J.B.Bernabe, J.Santa, A.Skarmeta, Enforcing GDPR regulation to vehicular 5G communications using edge virtual counterparts, in: IEEE 3rd 5G World Forum (5GWF), 2020, pp. 121-126. doi: 10.1109/5GWF49715.2020.9221248
[15] C.Saatci, E.Gunal, Preserving Privacy in Personal Data Processing, in: 1st International Informatics and Software Engineering Conference (UBMYK), 2019. DOI: 10.1109/ubmyk48245.2019.8965432
[16] A.S.Althobaiti, M.Abdullah, Medium Access Control Protocols for Wireless Sensor Networks Classifications and Cross-Layering, Procedia Computer Science, 65, 2015, pp. 4–16. https://doi.org/10.1016/j.procs.2015.09.070
[17] S.Alsamer, A.Aleesa, H.Saad, Y.Mohammed, M.Albadran, Contention and TDMA-based MAC wireless in scheduled and unscheduled settings. ARPN Journal of Engineering and Applied Sciences, vol. 11, no. 5, march 2016 ISSN 1819-6608, 2016, pp. 2859-2865
[18] CS Lee. Design by Improved Energy Efficiency MAC Protocol based on Wireless Sensor Networks. Journal of the KIECS. pp. 439-444, vol. 12, no. 3, Jun. 30 2017, t. 83, ISSN 1975-8170 eISSN, 2288-2189. http://dx.doi.org/10.13067/JKIECS.2017.12.3.439
[19] OMNeT++ Documentation: BMAC protocol, URL: https://doc.omnetpp.org/inet/api-current/neddoc/inet.linklayer.lmac.LMac.html
[20] OMNeT++ Documentation: LMAC protocol, URL: https://doc.omnetpp.org/inet/api-current/neddoc/inet.linklayer.bmac.BMac.html
[21] R.B.Agnihotri, N.Pandey, S.Verma, Analysis of behavior of MAC protocol and Simulation of different MAC protocol and proposal protocol for wireless sensor network, in: 2018 4th International Conference on Computational Intelligence & Communication Technology (CICT), 2018, pp. 1–6. https://doi.org/10.1109/CIACT.2018.8480373
[22] M.C.Ruiz, H.Macià, J.Calleja, New Proposals to Improve a MAC Layer Protocol in Wireless Sensor Networks, Informatica, 30, 2019, pp. 91–116. https://doi.org/10.15388/Informatica.2019.199
[23] K.S. Prabh, F. Royo, S. Tennina, T. Olivares, A MAC protocol for reliable communication in low power body area networks, Journal of Systems Architecture. 66–67 (2016) 1–13. https://doi.org/10.1016/j.sysarc.2016.04.001.
[24] V.Teslyuk, A.Sydor, V.Karovič, O.Pavliuk, I.Kazymyra, Modelling Reliability Characteristics of Technical Equipment of Local Area Computer Networks, Electronics, 10, 2021. https://doi.org/10.3390/electronics10080955
[25] A.R.Raut, S.P.Khandait, U.Shrawankar, Time-Critical Transmission Protocols in Wireless Sensor Networks: A Survey, in: N.R. Shetty, L.M. Patnaik, H.C. Nagaraj, P.N. Hamsavath, N. Nalini (Eds.), Emerging Research in Computing, Information, Communication and Applications, Springer Singapore, Singapore, 2019, pp. 351–364. https://doi.org/10.1007/978-981-13-5953-8_30

[26] R.Tkachenko, I.Izonin, N.Kryvinska, V.Chopyak, N.Lotoshynska, D.Danylyuk, Piecewise-linear Approach for Medical Insurance Costs Prediction using SGTM Neural-Like Structure, CEUR-WS.org, vol. 2255, 2018, pp. 170–179

[27] Y.Tsymbal, R.Tkachenko, A digital watermarking scheme based on autoassociative neural networks of the geometric transformations model, in: 2016 IEEE First International Conference on Data Stream Mining Processing (DSMP), 2016, pp. 231–234. https://doi.org/10.1109/DSMP.2016.7583547

[28] O.Leontyeva, K.Obelovska, Performance Analysis of IEEE 802.11 EDCA for a Different Number of Access Categories and Comparison with DCF, in: A. Kwiecień, P. Gaj, P. Stera (Eds.), Computer Networks, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 95–104

[29] O.Panova, K.Obelovska, An Adaptive ACs Number Adjusting Algorithm for IEEE 802.11 EDCA. In Proceedings of the 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015), Warsaw, Poland, 24–26 September 2015; pp. 823–826.

[30] V.Richert, B.Issac, N.Israr, Implementation of a Modified Wireless Sensor Network MAC Protocol for Critical Environments, Wireless Communications and Mobile Computing. 2017, 2017, 2801204. https://doi.org/10.1155/2017/2801204

[31] X.Liu, X.Du, M.Li, L.Wang, C.Li, A MAC Protocol of Concurrent Scheduling Based on Spatial-Temporal Uncertainty for Underwater Sensor Networks, Journal of Sensors, 2021, 5558078. https://doi.org/10.1155/2021/5558078