ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/335104959

Towards a Reliable Modulation and Encoding Scheme for Internet of Things Communications

Conference Paper · October 2019

DOI: 10.1109/AICT47866.2019.8981775

CITATIONS
7

READS
644

5 authors, including:

Parham Sadeghi
Sharif University of Technology
6 PUBLICATIONS **12** CITATIONS

Bardia Safaei
Sharif University of Technology
25 PUBLICATIONS **399** CITATIONS

Amir Mahdi Hosseini Monazzah
Iran University of Science and Technology
45 PUBLICATIONS **670** CITATIONS

Alireza Ejlali
Sharif University of Technology
154 PUBLICATIONS **2,495** CITATIONS

SEE PROFILE

All content following this page was uploaded by Bardia Safaei on 13 August 2019.

The user has requested enhancement of the downloaded file.

Towards a Reliable Modulation and Encoding Scheme for Internet of Things Communications

Parham Sadeghi*, Bardia Safaei†, Kimia Talaei‡, Amir Mahdi Hosseini Monazzah§ and Alireza Ejlali‖

*†‡‖Department of Computer Engineering, Sharif University of Technology, Tehran, Iran
Email: {*psadeghi,†bsafaei, ‡ktalaeikh}@ce.sharif.edu
§School of Computer Science, Institute for Research in Fundamental Sciences, Tehran, Iran
Email: §monazzah@ipm.ir
‖Department of Computer Engineering, Sharif University of Technology, Tehran, Iran
Email: ‖ejlali@sharif.edu

***Abstract*—As the emergence of Internet of Things (IoT) brings the realization of ubiquitous connectivity ever closer, our reliance on these applications gets more important. Nowadays, such connected devices could be found everywhere, from home appliances to industrial control systems and environmental monitoring applications. One of the main challenges in IoT infrastructures is that of reliability, which emboldens itself in the context of Low-power and Lossy Networks (LLN) as they are inherently prone to packet loss as a result of their environmental and design constraints. Therefore, reliability of IoT devices becomes crucially important. With communication, the most important consideration in these infrastructures, the reliability of the links plays the main role in the overall reliability of the system. An aspect of link reliability lies within the modulation and encoding schemes used for the transmission of data. There are various types of such methods supported by the de facto IEEE 802.15.4 protocol, but few of them are in actual widespread deployment. In this paper, we explore three of these modulation schemes along with four of the well-known encoding techniques for three different deployment scenarios and then we evaluate the results to propose the most admirable couple for establishing a reliable communication infrastructure in IoT applications.**

***Index Terms*—Internet of Things, Modulation, Encoding, Reliability**

I. Introduction

The Internet of Things (IoT) paradigm has brought about the possibility of interaction between an enormous amount of physical objects via an Internet based communication infrastructure, which could lead into remarkable advances in the quality of the human lives. The idea behind this emerging field is to supply a vast variety of low-power and resource constraint physical objects with sensors, actuators, processing units and networking capabilities, enabling them to interact and exchange collected data through wireless mediums [1]. The IoT infrastructure is mainly characterized by proneness to packet loss, energy-constrained devices, and unreliable communication links. As a result, reliability has always been one of the major challenges of IoT systems and this only heightens the importance of employing high-level schemes to improve reliability.

The Architecture of IoT encompasses a number of operational layers, which the network layer and its routing protocols plays a critical role in providing a reliable communication for delivering data packets from their sources to their intended destination(s) [2]. Nevertheless, the link reliability in the underlying layers has always been a bottleneck for wireless communication systems. With the advent of IoT paradigm in different portable and ad-hoc wireless applications, this has only increased in importance as communication consumes about 800 to 1000 times more energy than the processing and this makes re-transmission a hefty price to pay in these energy constrained devices [3]. In addition to the environment specifications, the link reliability is highly dependent on the underlying communication infrastructure and the modulation and encoding schemes used within it, which has led many researchers to study this field thoroughly [4]. Unfortunately, such efforts have been narrow in their vision to the best of our knowledge.

Even before the start of the standardization trend of IoT (which still has not yet fulfilled), most of the protocols relied on the IEEE 802.15.4 physical layer for their communication, as it was well defined, easy to use and cheap to implement. This physical layer specification has gone through many revisions and the most current version and implementations support Offset Quadrature Phase Shift Keying *(OQPSK)*, Binary Phase Shift Keying *(BPSK)* and Gaussian Frequency Shift Keying *(GFSK)* modulation modes, of which GFSK is the easiest and cheapest to implement. Alongside these methods, there are encoding schemes from the the Medium Access Control *(MAC)* layer. The standard for IEEE 802.15.4 MAC mandates the MANCHESTER encoding [5] but other protocols have modified this encoding scheme to meet their own criteria as some wish to ignore many reliability concerns in order to reduce the power consumption [3].

Considering the fact that the cognitive radio is a relatively new phenomena and of no use in IoT devices due to their energy constraints; here, we first try to compare the most popular modulation schemes to find out which one best fits to the IoT infrastructures as this part is always implemented in hardware. Afterwards, we compare the encoding schemes, which may be implemented in either software or hardware. Our experiments and observations have been done through extensive simulations in three different scenarios, i.e., open filed, warehouse, and indoor applications, in order to evaluate the link reliability under each scenario. Our aim in this paper is to propose a scheme that performs well in all of the

scenarios as they are mostly studied separately, but the real-world implementations are a mixture of all of these cases. This will in turn help the network designers to choose the optimal combination based on their intended criteria.

The rest of the paper is organized as follows: section II describes the building blocks of an IoT infrastructure with focusing on communications, section III will provide a brief overview of the literature and their scope, with focusing on their pros and cons. Section IV will elaborate on our methodology and experimental setup, which has been used to reach our evaluations. In section V, the observations along with the results will be discussed in each of the scenarios. Finally, Section VI will conclude the paper and makes some remarks on our future endeavors.

II. Building Blocks of IoT

There are several necessary components central to a successful IoT implementation. According to [6], these functional requirements could be categorized into six fundamental elements as follows:

1) Identification and Addressing: Each object within the network must be assigned with a unique identifier to facilitate traceability, control and monitoring of objects. In recent years different identifying methods such as Ubiquitous Codes *(uCodes)* [7], Electronic Product Codes *(EPC)* [8], [9] and European Article Number *(EAN)* [10] have been proposed. Nevertheless, due to the key distinguishing point between IoT and its predecessor Wireless Sensor Networks (WSN), it is necessary to determine the exact sources and destinations of transmissions in the IoT network globally [11]. In this regard, there should be addressing mechanisms, which enable the nodes to route their gathered information through middle layers towards their destinations. These addressing techniques are almost built upon IPv6, which could be made more efficient in terms of their header overhead and power consumption by using compressing mechanisms, i.e., 6LoWPAN [12].

2) Sensing and Actuating: There are three theories on the relation between IoT and Cyber Physical Systems (CPS): 1) IoT = CPS, 2) IoT $\subset$ CPS, and 3) IoT $\supset$ CPS. Independent from our perspective, which centers around the second approach, two concepts of IoT and CPS have major similarities. Hence, according to the definition of CPS, these systems are mainly operating based on feedback loops, where sensors monitor the physical environment and send their collected data towards central data warehouses to be processed. Afterwards, appropriate instructions will be sent back to the deployed actuators in the environment based on the extracted information, so they could take appropriate actions. This process will be iterated until a certain deadline or event is met. In this regard, in such systems, the identified objects should be equipped with either sensors or actuators. Storing and processing such a huge volume of data with relatively different types, deadlines, and processing requirements, gathered from an enormous number of sensors is a serious challenge in IoT systems [13]. This issue has motivated designers to integrate cloud platforms into the IoT frameworks as an effective solution to creat new generation of technologies such as fog and edge computing.

3) Communication: Utilization of efficient communication technologies is fundamental to the IoT as it enables the heterogeneous devices to communicate with each other without human intervention [14]. As it has been depicted in Fig. 1, there are many wired and wireless communication technologies, which have been exploited in IoT infrastructures. Nevertheless, due to the type of IoT applications, the communication of embedded devices in IoT are mainly based on wireless mediums. Examples of widely used wireless communication technologies include IEEE 802.11 [15], [16], Bluetooth Low Energy *(BLE)*, Near-Field Communication *(NFC)*, and IEEE 802.15.4 [17]. The main challenge in such infrastructures is the concept of reliability, which is directly affected by the deployment environment. Typically, IoT systems are deployed in relatively harsh and dynamic environments with various sources of signal distructions such as interference, noise, physical obstructions, and factors such as fading and scattering. These parameters could lead into distortion or loss of data packets in the network. Accordingly, IoT systems are also known as the Low-power and Lossy Networks *(LLN)* [18]. These technologies could be employed in different IoT infrastructures with different dimensions, i.e., Personal Area Network *(PAN)*, Local Area Network *(LAN)*, Metropolitan Area Network *(MAN)*, and Wide Area Network *(WAN)*. In this regard, the most reliable communicating technologies should be employed in different layers of the IoT architecture (including the physical and perception), to overcome these challenges [14].

4) Computation: Generally speaking, computations are handled via hardware or software, but the main bottleneck in the calculations will be certainly upon the existing hardware platforms in an IoT system. Similar to any other embedded device, an IoT platform must be provided with a core processing unit such as a micro-controller or a Field-Programmable Gate Array *(FPGA)* to perform necessary tasks with energy efficient techniques, e.g., task scheduling and power management methods [19]. The amount of process on the gathered data depends on the type of the system from a broader view. In typical IoT infrastructures, the nodes have severe resource limitations in terms of energy, processing capabilities and storage. In such systems, to handle the processing operations on the gathered data, exploiting the cloud servers is unavoidable. Nevertheless, in recent years, due to the emergence of IoT applications with high demand of response time, e.g., Remote Healthcare Monitoring Systems *(RHMS)*, in contrast with the cloud-based IoT systems, a part of the calculations should be handled in the IoT nodes themselves to reduce the imposed latency and provide a more resource efficient infrastructure [1], [20]. In such technologies, which are called fog computing, the collected data will be partly processed before the information is sent to the data center [21].

5) Services: The IoT services are divided into four main categories [6], [22], [23]: I) Identity related services which aim to identify connected objects within the network; II) Information Aggregation Services that perform the required pre-processing on the raw collected data; III) Collaborative-Aware Services that make use of the data to perform the necessary actions; IV) Ubiquitous Services that provide the

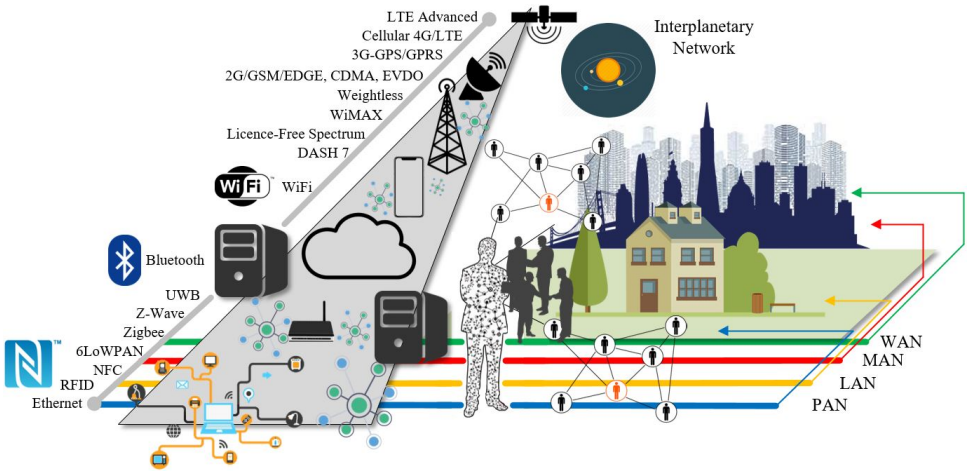

Fig. 1: Communications Technologies in Internet of Things

latter at anytime to anyone who requires that service [6].

6) Semantics: Once the data is transferred to a cloud platform or a data warehouse, it needs to be analyzed and transformed into interpretable knowledge, based on which the corresponding actions can be taken.

Ever since the emergence of IoT, a vast variety of challenges have been faced, many of which are still active areas of research. Some of the main challenges include massive scaling of IoT as the number of IoT devices is increasing drastically (it has been estimated that there will be more than 9 devices per person at the end of 2025 [14]), achieving an adequate level of robustness and reliability despite the noisy infrastructure, privacy and security issues due to openness of the system, and designing an IoT architecture that facilitates connectivity, communication and supports a whole range of applications [24]. Meanwhile, the reliability is on a high importance due to its broad range of impacts on the provided Quality of Service (QoS) to the subscribing users in the IoT system. Hence, it should be considered in different levels of abstraction with a high degree of attention.

III. Related Works

The topic of link reliability has been thoroughly studied throughout the years and is a well established area of research. A major portion of the topics related to this field have had a narrow vision and to the best of our knowledge, such a comparative study has not been conducted before. Although the study and modelling of wireless channels is an old one, the authors in [25] proposed one of the most comprehensive methods concerning low power links. These links are commonly modeled using a disk approximation [3] in higher layers, which is very inaccurate; so they try to use models previously developed for cellular networks to analyze interference in transitional regions and estimate the transition error rate for low power radio applications. Further up the chain, [26] and [27] model the effects of GFSK modulation on Bit Error Rate *(BER)* and try to find analytical equation based on theory and empirical data and compare them to data obtained from experiments.

The following studies proposed theoretical methods for calculation of error rate while taking into account the GFSK modulation as the underlying modulation technique. In [26], the authors derive the frame error rate *(FER)* for Bluetooth transmissions in the presence of Electromagnetic Interference. In this study, the FER due to the GFSK modulation has also been taken into consideration. In [27], a practical method has been proposed to compute BER for a GFSK system. In both cases, the results obtained from theoretical equations have been verified with respect to the experimental results.

Other works such as [28] and [29] shift their focus and try to examine and compare the effect of more state-of-the-art M-ary modulation techniques like OQPSK on the BER. The effects of encoding schemes on the link reliability in LLNs is thoroughly discussed in [25], but this paper does not take into consideration the effects of scenarios in which these devices are going to be used and also utilizes a more computation heavy mode of SECDED code.

IV. Methodology

Based on the modular modelling methodology, each part of the model is constructed independently from others to facilitate ease of modification for other use-cases. The three main layers of this specification are the channel model, which is modelled by the path loss, the modulator which provides P_e and the encoder which calculates the final reliability. Each of these are further elaborated in the following:

A. Radio and Channel Model

The wireless channel models vary immensely in their complexity and range from the simple disk model to models considering diffraction and scattering of the signal, mostly used for cellular networks. Most models also include at least one empirical variable to better model the environment. The model used for this study is the log-normal path loss model represented in Equation 1 with Gaussian shadowing effect, which seems to model the radio channel of IoT devices accurately enough without being too complex to understand.

$$PL(d) = PL(d_0) + 10nlog_{10}(\frac{d}{d_0}) + X_\sigma \quad (1)$$

In this equation, d is the distance between sender and receiver and d_0 is the reference distance, equal to 1 meter in our case. n is an empirical variable called the path-loss exponent. X_σ is a Gaussian random variable with standard deviation σ which is also an empirical value considered constant only when the environment is not changing. At the receiver side, Signal to Noise Ratio *(SNR)* depends on the sender's power, path-loss and the thermal noise of the environment and is in the form of Equation 2.

$$\gamma(d) = P_{t_{dB}} - PL(d)_{dB} - P_{n_{dB}} \quad (2)$$

In Equation 2, $P_{n_{dB}}$ is the thermal noise and it's obtained from Equation 3, where k is the Boltzmann's constant, T_0 is the temperature in Kelvin, B is the bandwidth ($30KHz$ here) and F is the noise form reported by the chip manufacturer, considered $13dB$ in most IoT applications [25].

$$P_{n_{dB}} = 10log_{10}(k.T_0.B) + F + 1 \quad (3)$$

B. Modulation

Although IEEE 802.15.4 supports many modulation schemes across many frequency bands, the most widely used are OQPSK, BPSK and GFSK in the $2.4GHz$ range for their ease of use and cost-effective means of implementation. Each of these is further explained below.

1) OQPSK: This scheme works by shifting the phase of the modulator signal to create four different states and thus each symbol encodes two bits. In the OQPSK variant used in IEEE 802.15.4, the odd and even bits are offset by one bit-period, affording the advantage of lower amplitude change during transitions by avoiding the origin of signal constellation. As this is a Quaternary modulation, the probability of a corrupt bit is calculated from Equation 4, wherein Q is the tail distribution function of standard Gaussian distribution.

$$P_b = Q(\sqrt{\frac{2E_b}{N_0}}) \quad (4)$$

2) BPSK: Working on the same principle of changing phase to modulate symbols, this scheme has only one bit per symbol. This 180°phase difference gives it higher energy per symbol and makes it more suitable for noisy environment while halving the effective data rate. Equation 5 is used to calculate the corrupt bit probability of this scheme.

$$P_b = \frac{1}{2}efrc(\sqrt{\frac{E_b}{N_0}}) \quad (5)$$

3) GFSK: A departure from using the sinusoid's phase, this scheme uses two modulator signals, each encoding a bit. A Gaussian filter is used here to smoothen the transitions and reducing the side-band power. The bit error rate here is usually calculated from Equation 6.

$$P_b = Q(\sqrt{\frac{E_b}{N_0}}) \quad (6)$$

C. Encoding

Alongside the officially supported Non-Return-To-Zero *(NRZ)* encoding scheme, some proprietary protocols choose to use another scheme. Among these schemes are MANCHESTER, 4B5B and SECDED.

1) NRZ: A very simple encoding scheme, where 'one' is representing no changes in the signal state, while 'zero' is an indication of a change in the state of the signal. This method produces an encoded signal with the same baud rate as the base band signal but has no inherent self-clocking and needs additional techniques to avoid bit slips. For a frame length of f bits, the probability of its correct reception is given in Equation 7 which corresponds with our definition of link reliability.

$$R_{Phy} = (1 - P_b)^f \quad (7)$$

2) 4B5B: Used in telecommunications to achieve a moderate level of fault detection and self-clocking, a mapping of 4-bit data nibbles is done through a dictionary to 5-bits, which awards us a single bit error detection. By designing the dictionary to contain at least two transitions per 5 bits of output, the self-clocking aspect is achieved. Since this method produces a 25% overhead, the link reliability is obtained from Equation 8.

$$R_{Phy} = (1 - P_b)^{1.25f} \quad (8)$$

3) MANCHESTER: Designed to tolerate frequency errors and jitters and help the clock recovery by the most extreme case of self-clocking, this method works by finding the XOR product of the original data signal with the clock signal. Although this method is the main type of encoding used in IEEE 802.15.4, it carries with itself the disadvantage of having double the baud rate of NRZ encoding scheme, which may prove too much in some applications. The required equation to derive the link reliability has been given in Equation 9.

$$R_{Phy} = (1 - P_b)^{2f} \quad (9)$$

4) SECDED: Short for "Single Error Correction, Double Error Detection", it is a (4,7) hamming code with an additional parity bit. This encoding scheme is used to remedy the fact that the hamming distance of three in traditional hamming codes cannot always detect double bit errors if error correction is attempted, so a parity bit is added. The link reliability under this scheme is derived from Equation 10.

$$R_{Phy} = [(1 - P_b)^8 + (8P_e(1 - P_b)^7)]^{\frac{2f}{8}} \quad (10)$$

V. Experimental Setup and Evaluation

The most current revision of IEEE 802.15.4 uses the $2450MHz$ ~$2485MHz$ band with a bandwidth of $30KHz$ and a data rate of $250Kbps$. The transmission power can take on values of $100mW$, $10mW$ and $5mW$, while the old $1W$ and $20mW$ modes, which were used in $868MHz$ and $915MHz$ ranges are considered legacy and are rarely seen in new hardware chips.

We have considered three deployment scenarios in Matlab, which correspond to the path-loss exponent of equation 1

TABLE I: Reliability of Different Modulation Schemes (NoN)

Distance (m)	OQPSK	BPSK	GFSK
50	91	91	44
60	73	73	35
70	71	71	34
80	67	67	32
90	29	29	13
100	27	27	13

and give it values of 2 for an open outdoors scenery, 4 for open indoor scenarios typical of warehouses and 6 for closed indoor spaces like office buildings. The temperature has been considered as 23°Celsius for the outdoor and 27°Celsius for indoor situations to account for thermal noise. Furthermore, the frame length has been set to 52 bytes of data in all of the scenarios, not considering the preamble and start of frame delimiter.

Traditionally, OQPSK is used in more stable places as it has half the energy per bit than that of BPSK but twice the throughput for the same transmission energy overall. GFSK is only used where the hardware is highly cost constrained and it has to be extremely simplified, as it has the worst overall reliability. This is clearly shown in Table I, where the results are shown for an outdoor open space with MANCHESTER encoding and $10mW$ transmission power. The results are being presented in form of Number of Nines *(NoN)* notion in Table I. According to our observations, since OQPSK has established the most reliable communication among the other modulation schemes, in the following subsections, we have reported the overall reliability in each scenario with its respective encoding scheme.

A. $1^{st} Scenario : OpenFields$

This scenario is the traditional use-case of IoT as inherited from WSN. The results are reported for OQPSK and different modulation schemes with a transmission power of 10mW. The result for this part are in Fig. 2 and are in NoNs notion. As it could be seen, by increasing the distance between the sender and receiver, the overall reliability has been dropped significantly. Accordingly, different encoding schemes have behaved differently corresponding to the existing distance, which completely depends on the type of the IoT application. For instance, in case of having short distances, the NRZ is able to provide a better reliability, while in case of long distances (which is typical in outdoor applications), the SECDED encoding has dominated other schemes in terms of reliability. Hence, in open filed IoT applications, the SECDED encoding scheme would provide a more robust communication.

B. $2^{nd} Scenario : Warehouse$

This scenario best fits to the typical factories and Industrial IoT *(IIoT)* deployments. The results are reported for OQPSK modulation and different encoding schemes with a 100mW transmission power. The results are presented in Fig. 3, again in NoNs notion. According to our observations, in open indoor scenary applications, the SECDED has dominated the other encoding techniques in terms of reliability, specially in shorter distances.

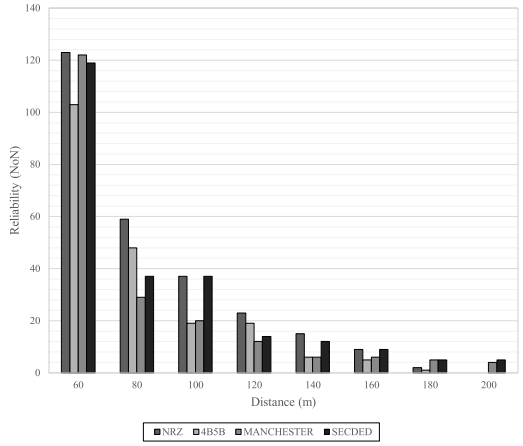

Fig. 2: Open fields scenery with 10mW transmission power and OQPSK modulation

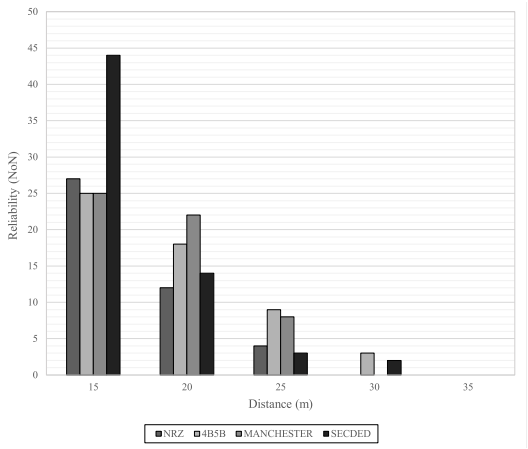

Fig. 3: Open indoors scenery, typical of warehouses and industrial buildings with 100mW transmission power and OQPSK modulation

C. $3^{rd} Scenario : Indoors$

Representing the envisioned future of IoT, this scenario will be the most common one in the coming future. A delegate of office and home space, the reliability of transmission is a crucial part yet, but will increase in importance as time goes by, specially for the RHMS Systems [1]. The results have been reported for the OQPSK modulation and different encoding schemes, with a 100mW transmission power. The results are presented in Fig. 4. Similar to what we have had in the last two scenarios, the SECDED encoding was able to also provide a better reliabilty in Indoor applications.

VI. Conclusion

Due to the importance of reliability in IoT communications, this paper tries to compare three of the most well-known modulation schemes along with four encoding techniques in three different deployment environments to propose the most admirable couple for conducting reliability in IoT communications. The results show that the link reliability

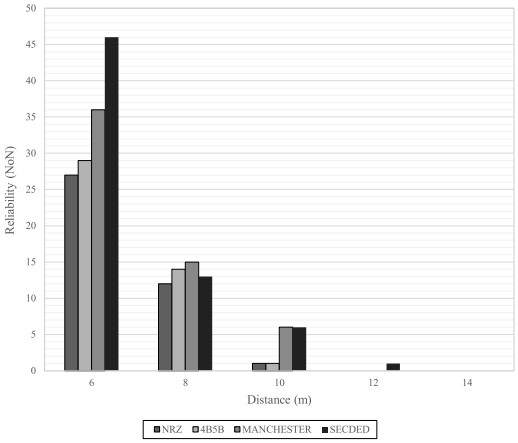

Fig. 4: Closed indoors scenery, typical of offices and homes with 100mW transmission power and OQPSK modulation

could be enhanced using these methods but with a cost of energy overhead due to transmission of redundant information and the required processing for the encoding and decoding procedures. The results here show that SECDED provides a better link reliability compared with MANCHESTER, but it is rarely used, as the leap in the reliability cannot be justified by the processing overhead that it imposes to our resource constrained processor. Further more, our observations have indicated that the OQPSK modulation scheme is able to establish a more robust communication in wireless systems. It should be mentioned, since the analytical model proposed here follows the modular modeling methodology, it could be easily combined with the models from higher layers to create a more comprehensive and detailed representation of the network. Many of the analytical models for the MAC layer in IEEE 802.15.4, only use the simple disc model, which can reduce their accuracy and therefore, the inclusion of our model could help to alleviate this problem.

REFERENCES

[1] B. Safaei, A. A. M. Salehi, M. Shirbeigi, A. M. H. Monazzah, and A. Ejlali, "Pedal: power-delay product objective function for internet of things applications," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*. ACM, 2019, pp. 892–895.

[2] B. Safaei, A. M. H. Monazzah, T. Shahroodi, and A. Ejlali, "Objective function: A key contributor in internet of things primitive properties," in *2018 Real-Time and Embedded Systems and Technologies (RTEST)*. IEEE, 2018, pp. 39–46.

[3] P. Di Marco, C. Fischione, F. Santucci, and K. H. Johansson, "Modeling ieee 802.15. 4 networks over fading channels," *IEEE Transactions on Wireless Communications*, vol. 13, no. 10, pp. 5366–5381, 2014.

[4] J. Miranda, R. Abrishambaf, T. Gomes, P. Gonçalves, J. Cabral, A. Tavares, and J. Monteiro, "Path loss exponent analysis in wireless sensor networks: Experimental evaluation," in *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*. IEEE, 2013, pp. 54–58.

[5] "IEEE 802.15.4 - IEEE Standard for Low-Rate Wireless Networks, C/LM - LAN/MAN Standards Committee," *IEEE Std.*, 2015.

[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[7] N. Koshizuka and K. Sakamura, "Ubiquitous id: standards for ubiquitous computing and the internet of things," *IEEE Pervasive Computing*, no. 4, pp. 98–101, 2010.

[8] D. L. Brock, "The electronic product code (epc)," *Auto-ID Center White Paper MIT-AUTOID-WH-002*, pp. 1–21, 2001.

[9] L. Atzori, A. Iera, and G. Morabito, "Siot: Giving a social structure to the internet of things," *IEEE communications letters*, vol. 15, no. 11, pp. 1193–1195, 2011.

[10] P. Hu, H. Ning, T. Qiu, Y. Zhang, and X. Luo, "Fog computing based face identification and resolution scheme in internet of things," *IEEE transactions on industrial informatics*, vol. 13, no. 4, pp. 1910–1920, 2016.

[11] B. Safaei, A.-A. M. Salehi, A. M. H. Monazzah, and A. Ejlali, "Effects of rpl objective functions on the primitive characteristics of mobile and static iot infrastructures," *Microprocessors and Microsystems*, 2019.

[12] N. Kushalnagar, G. Montenegro, C. Schumacher *et al.*, "6lowpan: Overview, assumptions, problem statement and goals. draft-ietf-6lowpan-problem-01. txt," *IETF Internet Draft*, 2005.

[13] B. Safaei, S. G. Miremadi, and S. A. Chamazcoti, "Implicit effect of decoding time on fault tolerance in erasure coded cloud storage systems," in *2016 International Computer Science and Engineering Conference (ICSEC)*. IEEE, 2016, pp. 1–6.

[14] B. Safaei, A. M. H. Monazzah, M. B. Bafroei, and A. Ejlali, "Reliability side-effects in internet of things application layer protocols," in *2017 2nd International Conference on System Reliability and Safety (ICSRS)*. IEEE, 2017, pp. 207–212.

[15] "IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications." [Online]. Available: https://doi.org/10.1109/ieeestd.2012.6178212

[16] "IEEE standard for information technology—telecommunications and information exchange between systems local and metropolitan area networks—specific requirements - part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications." [Online]. Available: https://doi.org/10.1109/ieeestd.2016.7786995

[17] "IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (LR-WPANs)." [Online]. Available: https://doi.org/10.1109/ieeestd.2011.6012487

[18] S. Kamalijam, A. Arvandi, M. Ashtarayeh, B. Safaei, and A. M. H. Monazzah, "A novel lna circuit in the l band with the purpose of increasing gain in gsm & gps in wireless multi-receiver systems," in *2019 2nd International Conference on Communication Engineering and Technology (ICCET)*. IEEE, 2019, pp. 112–116.

[19] M. Ansari, A. Yeganeh-Khaksar, S. Safari, and A. Ejlali, "Peak-power-aware energy management for periodic real-time applications," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2019.

[20] F. Samie, L. Bauer, and J. Henkel, "Iot technologies for embedded computing: A survey," in *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*. ACM, 2016, p. 8.

[21] ——, "From cloud down to things: An overview of machine learning in internet of things," *IEEE Internet of Things Journal*, 2019.

[22] X. Xiaojiang, W. Jianli, and L. Mingdong, "Services and key technologies of the internet of things," *ZTE Communications*, vol. 2, p. 011, 2010.

[23] M. Gigli and S. G. Koo, "Internet of things: Services and applications categorization." *Adv. Internet of Things*, vol. 1, no. 2, pp. 27–31, 2011.

[24] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[25] M. Zuniga and B. Krishnamachari, "Analyzing the transitional region in low power wireless links." in *SECON*, vol. 4, 2004, pp. 517–526.

[26] S. Malisuwan, J. Santiyanon, and J. Sivaraks, "The performance of bluetoothtm transmissions in electromagnetic interference environment," *International journal of the computer, the internet and management*, vol. 11, no. 2, pp. 1–14, 2003.

[27] M. Shimizu, N. Aoki, K. Shirakawa, Y. Tozawa, N. Okubo, and Y. Daido, "New method of analyzing ber performance of gfsk with postdetection filtering," *IEEE transactions on communications*, vol. 45, no. 4, pp. 429–436, 1997.

[28] B. O. Omijeh and I. Eyo, "Comparative study of bit error rate of different m-ary modulation techniques in awgn channel," *American Journal of Networks and Communications*, vol. 5, no. 5, pp. 82–90, 2016.

[29] M. S. Jaipreet Kaur, Hardeep Kaur, "Comparison of ber for various digital modulation schemes in ofdm system," *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)*, vol. 5, no. 4, apr 2016.

View publication stats