RANDOM MAC OPTIMIZATION FOR IOT COMMUNICATION

[1]Reem Abdullah Alkhateeb, [2]Shroog Ageel Alshammari, [3]Kusum Yadav
[1]Computer Science and Engineering Department, University of Ha'il , Hail, Kingdom of Saudi Arabia
r.alkhateeb@uoh.edu.sa, [2]shr.alshammari@uoh.edu.sa, [3]kusumasyadav0@gmail.com,

ABSTRACT— *These days, the use of networks has become part of our daily lives, especially with the spread of the Internet of Things which consists of low-capacity devices that cooperate to perform specific tasks. This can be used to facilitate our life during this current era which is full of technology. Furthermore, network design must be developed to eliminate the need for a central coordinator. The absence of a central coordinator greatly simplifies the design of the network, especially in the case of a vast number of connected devices; however, this may cause collisions between data packets sent from different devices at the same time. Nevertheless, collisions can be resolved through multiple mechanisms for instant ALOHA derivatives. However, these type of mechanisms does not solve the problem 100%, but it makes the performance better...*

I. INTRODUCTION

The In the world of networking, the internet is not considered new; however, it can be said that there is a new technological revolution in the science of networks called the 'Internet of Things' (IoT), which allows the internet to reach the world of everyday, material things. It has become a fixture in certain industries, as the technology can be used for business applications in place of humans, and also plays a significant role in health – these are the most prominent areas that the internet of things deals with. Besides, IoT allows devices and servers to talk to each other in new, more interconnected ways [4, 5]. It is possible to say that the IoT is a system of interconnected computing devices, machines, objects, and people who are provided with unique identifiers and the ability to transmit data across a network without the requirement for human-to-human or human-to-computer communication [1, 2]. There are around 9 billion interconnected devices, and this number is expected to reach 24 billion by 2020, which suggests new opportunities for marketing, greater competencies, and enhanced experiences [2].

The most important aspect of network science is the 7-layer OSI model, consisting of the physical layer, the data link layer, the network layer, the transport layer, the session layer, and the application layer. In this study, there will be a focus on the data link layer that has the IEEE 802 protocol family, particularly the media access control layer (MAC), which is responsible for sending packet data to and from the network interface card, and to and from another shared remote channel [6]. An open protocol stack represents the key to implement the vast world of services and applications that the market provides day by day, thanks to the ever-going technological innovation: for instance, in smart grid, environmental and energetic monitoring, smart transportations, and healthcare scenarios, which are only just few examples of the market fields that already largely benefit of the IoT paradigm and its innovative features. Both industrial and scientific communities have shown a great interest in the complex scenario of IoT/M2M services, because of the large number of issues as well as of opportunities it carries along. Both communities look forward to a larger use of the advantages that the satellites may offer: in fact, the fraction of the M2M traffic delivered via satellite is continuously increasing in size [1, 2]. It is known that in the age of the internet there is an enormous number of devices connected simultaneously to the network, which helps to facilitate our daily lives. The reason for concern about MAC is the lack of central coordination, which makes network design much simpler and performs better. Therefore, the development of access control protocols is required to overcome challenges in existing network infrastructure and protocol stacks used – for instance, ALOHA protocols, which are the easiest and most well-known [6, 7]. Besides, Irregular Repetition Slotted ALOHA (IRSA), a derivative of the ALOHA protocol, is currently considered the best solution to reduce collision. It raises the level of throughput, which works on the principle of random repetition to the packets that have been transmitted [4, 8]. It is also one of the Random Access protocols which have traditionally represented a general solution for the collision. As the IRSA has a space for each user, it is equipped with temporary storage space of limitless size to store packets that have not yet been sent or received correctly and without a collision. This is considered a development of the Contention Resolution Diversity Slotted ALOHA protocol (CRDSA).

II. HISTORY OF THE INTERNET OF THINGS(IOT)

The history of the internet stretches back to the middle of the last century. By the 1960s, the first packet switching networks were developed, including the development of the ARPANET network. ARPANET was a technology launched by the US Department of Defense in the 1960s to connect universities and research institutions, to exploit the capabilities of computers available at the time. The first network used TCP (both of these technologies have become a focal point in the creation of the internet) [1, 2, 9]. With the development of the internet came its availability for civilian purposes, and in the 1990s, a new internet era would emerge, namely the World Wide Web. Following this, mobile internet became globally widespread during the 2000s, and the most recent development – the Internet of Things (IoT) – was introduced between 2007 and 2009. This development has subsequently become an active science field in the world of networks and computing, as it consists of many interconnected smart devices that facilitate our lives. It is possible to say that IoT integrates things through specific systems to facilitate communication between devices, humans, and other devices including machines, sensors, and various artificial intelligence tools[1, 2, 10]. This type of communication can result in the creation of a vast amount of data that is stored, processed, and displayed to deal with it by setting the radio frequency. The importance of this field lies in the fact that it is involved in the running of many areas such as health, education and industrial sectors and helps to improve them, as shown in Figure 1.

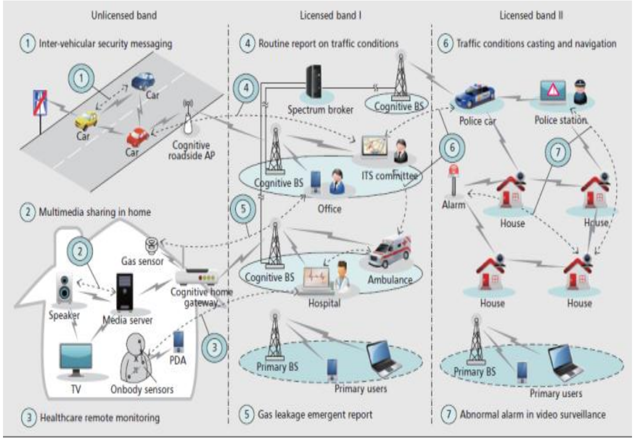

Figure.1.The IoT application [7]

NIC expects that "by 2025, Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more". It highlights upcoming opportunities that will arise, starting from the idea that "big demand connected with technology advances could drive general diffusion of an Internet of Things (IoT) that could, like the present Internet, provide an invaluable thing to economic development." Because of that, this field has attracted the attention of many researchers in networking[11]. Besides, it considered that this technology has become an integral part of our daily lives since there is a connection via the internet between many machines and devices. The system of communication is manufactured by platforms designed using cloud computing, as these platforms receive device applications through the internet, thus the decision is taken to collect the data from this connection. The devices around us can also be controlled using intelligent devices that have greatly enhanced the world of technology, and all this can happen through IoT. Some of the features of IoT include [12, 13]:

- Multitude: The vast number of devices that can be connected, even if there is no interaction with humans.
- Scalability: The possibility and ease of modifying the protocols used to communicate easily and quickly without wasting time and effort while preserving their characteristics.
- Variation: This is based on the way of working from the connection of various devices, which we can use in several areas and are scalable in growth; also, the introduction of new devices that can be utilized in new and different fields.
- Disappearance: Lack of need for direct human intervention is what enables hidden systems to make decisions based on data.
- Criticality: The criticality of use is possible in cases where devices are used for critical situations, such as in the health industry in saving a human life. This can be considered a challenge faced by this type of technology.
- Level of power: Trying to reduce the amount of energy needed to power devices with limited access to power.
- Cohabitation: Relative to the wide range of designs consisting of several devices that rely on this technology; focus must be on the side of coexistence and integration in these designs.
- Cost: To achieve widespread usage, the prices of these connected devices must be accessible to users to attract customers which can be obtained by connecting small, low-cost devices to carry out large tasks.

Because of the phenomenal growth expected of the Internet of Things over the next few years, it is worth considering the factors which will help to make communication between devices low cost and be able to perform substantial tasks smoothly. These factors include the use of protocols that assist in achieving the goal of communication between these devices, and the identification of methods utilized by controlling the communication between potential devices. Further, there is a need to contribute to the design of low-cost, low-complexity technologies [12,13].

III. IoT Protocols

In the field of IoT, devices communicate with each other using internet protocols that determine the method of sending and receiving data between these devices. Therefore, many protocols have been proposed to implement a connection between the different devices and provide solutions within specific mechanisms, such as CoAP, REST, XMPP, AMQP, MQTT, DDS, and others [14]. The lack of a protocol that can handle machine-to-machine, machine-to-server, and server-to-server communication has led to fragmentation among many protocols. In contrast, fragmentation is a major impediment to the development of new services that require the integration of multiple internet services to provide horizontal integration of services. The importance of protocols is to control or limit communication problems, such as the following [14]:

- Spectrum scarcity: There is a huge number of connected devices already in use, and considering this number is supposed to reach up to 50 billion devices by 2020, this creates a great challenge for communication networks regarding the congestion spectrum. Therefore, it is possible to use the current spectrum more efficiently to avoid potential spectrum shortages and to support large-scale data transfer.
- Interference: the presence of many connected devices causes overlapping between the networks, which adversely affects the process of data transfer. Thus, ways to limit these problems must be developed and implemented to achieve the best connection without losing any data.
- Coverage issues: The issue of network coverage is a major concern in the world of networks. Because wireless coverage is not always guaranteed, especially in the industrial and scientific domain, this issue can be effectively overcome through the dynamic access of the spectrum to spread better ranges. This will be discussed in more detail later in the thesis.
- Device heterogeneity: The diversity of networks regarding applications requires the use of a variety of protocols as well as the diversity of data sent and received. This requires intelligent handling of these data, so the devices must be smart enough to communicate with others. Additionally, there are a variety of new applications such as home multimedia distribution systems, smart roads for future intelligent transport systems, and broadband services in public areas.
- Network delay and losses: Data transfer delay is a thorny issue when designing a network, which determines how long it takes to transfer data over the network from one node or endpoint to another. Network delays are regularly

short; for example, the end-to-end delay of a network across countries is about 30 milliseconds. However, loss of network packets necessitates network designers to check for injuries, and to resend if necessary. The different round-trip time is added for a resend and response request[14]. Therefore, it must identify the IoT protocol stack which has taken a great deal of time in delaying to develop a protocol stack that meets the communication requirements, while keeping the protocols as simple as possible. Moreover, there is a need to build a single structure that replaces the proprietary approach through a transparent end-to-end structure. This structure must meet the essential requirements of a protocol stack which is capable of handling large amounts of information, queries, and accounts, and utilizing new data processing models, stream processing, data collection, and extraction, all of which are sustainable by telecommunication standards, including[6]:

- Low energy: The majority of devices require a low power connection because the vast majority of these devices operate by the battery, and cannot pull power from the source of energy. Thus, the COME protocol must show a low power consumption rate.
- A highly reliable protocols stack: To maintain privacy and to integrate things seamlessly into the internet, they need to provide the same reliability used on the internet – with the additional requirement that reliability works out as efficiently as possible[6].

When there is a monition for the protocol stack, it should monition the layer of this stack. The IoT protocol stack can be divided into four layers: application layer, transport layer, network layer, and data link layer, as shown in Figure 2.

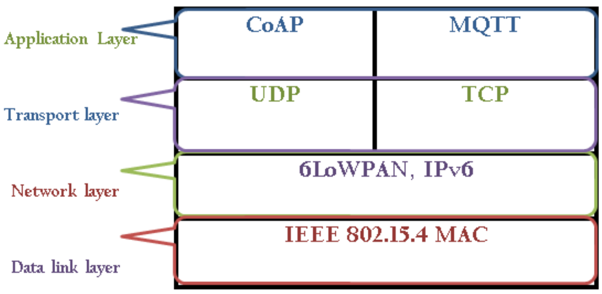

Figure 2. The IoT Protocol Stack

- **Application Layer Protocols**

The application layer is considered the top layer, and this layer provides software services to ensure communication between other application programs on the network. There is a focus on two protocols, namely the CoAP protocol (Constrained Application Protocol), introduced by the IETF Constrained RESTful Conditions (CoRE) working society. Second is the MQTT protocol (Message Queuing Telemetry Transport), which was developed by IBM in 1999 [6].

- **CoAP Protocol**

This protocol is useful for low-energy or battery-powered devices as it is a good choice for this kind of equipment. It has an exchange of requests and responses in an un-synchronous way. All headers, methods, and status codes are binary encoders; it effectively handles the need for ultra-lightweight protocol and constant connectivity capability. Furthermore, it uses UDP coupe [6][15].

- **MQTT Protocol**

This is a highly efficient protocol for low bandwidth devices and high latency networks. It takes the publish/subscribe messaging method, which is extremely lightweight and ideal for connecting small devices to restricted networks. In addition to its effective bandwidth, agnostic data, and its continuous session awareness, it is also considered very simple, offering few control options [16].

- Transport Layer Protocols

The transport layer is considered as an end-to-end connection, controlling two endpoints by using the Windows concept to determine how much information should be sent between endpoints. The technique of IoT focuses on the use of UDP. This is because it is lighter and much faster compared to TCP. Additionally, it is also considered as a communication protocol and does not come with the flexibility features of the encoder which makes it unique, making it suitable for the restricted environment of devices and sensors [6].

- **Network Layer or Internet Layer**

This layer can be considered as it aims to achieve efficiency with low-energy budgets such as IPv6 and low power wireless (6LoWPAN) networks. Also, there are real decisions about how the hardware may declare what functions are being implemented and the assumptions that are proposed about their role in the network. The overlay that IPv6 provides over the network 6LoWPAN is a set of protocols that can be used to integrate limited hardware resources into systems [6].

- **Data Link Layer**
- **IEEE 802.15.4 (MAC) Layer**

IEEE 802.15.4 is a set of standards that detail the variety of wireless personal area networks and focuses on communications between devices in a restricted environment in the case of low power, low memory, and low bandwidth [6, 17]. The MAC layer has also attracted the attention of researchers, which can be divided into three sections:

- **Contention-based Protocols**

This could also be called Random Access (RA) protocols. The simplest protocols send packets at the ready for data transmission and reduce collision. Data exchange can only begin if the channel is not busy sending another; otherwise, the transmission will have a delay. But in the event of a collision, data cannot be recovered in the future due to destructive interference between transmitters. The probability of data loss in such protocols is very high, which significantly affects the throughput. The most well known of these protocols are pure ALOHA and slotted ALOHA, which can achieve a maximum throughput of 18% for ALOHA and 36% for slotted ALOHA [18].

- **Contention-free Protocols**

Contention-free protocols can also be called Dedicated Access (DA) protocols. These can be considered as the protocols that allocate resources to terminals to eliminate collisions. Part of the time or part of the frequency bandwidth is assigned to a node, whether temporary or permanent and does not allow other nodes in the network to use them [19]

.

- **Hybrid Protocols**

This protocol is used to maximize the benefit of DA and RA as it tries to combine simplicity with productivity. This category of protocols also achieves the highest utilization and production of IoT of resolved users to have a sudden jump from a low value to a much higher value after a single time slot. The avalanche point gives the possible maximum throughput.

IV. RELATED WORK

There will be presenting a study on the protocols that limit interference and collision problems in the Internet of Things, which are discussed to avoid collisions. Because of this, the satellite protocols are mainly based on the ALOHA protocol and its developments. The major issues that affect the design, deployment, and performance of the IoT are as follows [1, 2, 20]:

- Medium Access Scheme
- Energy Management
- Transport Layer Protocol
- Cost
- Security
- Real-time Traffic Support with QoS provisioning

In this thesis, there will be a focus on the Medium Access Scheme, which has many characteristics for instant Energy Efficiency, Scalability, Adaptability, Low Latency and Predictability, and Reliability. It can be considered as being primarily responsible for regulating access to the shared medium.

- **Medium Access Scheme**

The Media Access Control scheme is one of two sublayers that designed the Data Link Layer of the OSI model. The MAC layer is responsible for transferring data packets to and from one Network Interface Card (NIC) to another across a shared channel. The MAC sublayer uses MAC protocols to guarantee that packets sent from different stations across the same channel do not collide. Moreover, many devices can recognize each other in the same physical link in the data link layer through the MAC addresses that are assigned to all ports on the switch. The MAC address is routed through the MAC algorithm as a secret key input, and an arbitrary longitudinal message is documented. A MAC address can be identified with a 12-digit hexadecimal number (48 bits in length). Additionally, the LAN nodes use the same communication channel for transmission. The MAC subclass consists of two primary responsibilities: data encapsulation, including frame assembly before transmission and frame parsing/error detection, during and after the reaction; and media access control, including the start of frame transmission and recovery from transmission failure. Moreover, as mentioned earlier, it is divided into three types, and the focus will be on Random Access Schemes and its protocols. Before identifying the types of Mac protocols, Successive Interference Cancellation (SIC) should be discussed [3, 17, 19].

- **Successive Interference Cancellation (SIC)**

Recently there has been considerable interest in the application of SIC which was initially applied to the Slotted ALOHA frame. SIC also can significantly improve and increase throughput by solving several collisions that affect throughput performance. The function of the recipient is to resolve the individual values received in the frame, and the indicators contained in those Singletons assist this. In this way, the corresponding interventions are eliminated in other slots, and other Singletons may be detected. This process is repeated until no more Singletons are detected or all user messages are resolved in this frame. Furthermore, it has demonstrated huge potential capacity and performance improvements, and there are other performance metrics rather than throughput, for example, delay, which is critical in some networks. SIC improves the throughput performance of networks; however, it may worsen its delay performance [4, 21].

- **Random Access Schemes**

Random Access schemes can be used to transfer data immediately, which may interfere with some of the data being transmitted. New mechanisms to eliminate overlap were also considered to resolve differences in data loads to reduce the loss of transmitted data. For example, these mechanisms are cracked ALOHA protocols (SA). It can be seen that most of the previous work on ALOHA systems is based on the assumption that when one packet is sent in a given period, it is always received correctly, and in the case of two or more transmissions, all packets are damaged. This is in addition to the concept of repeating the data packet twice (or more) within the same frame, to increase the probability of transmission successfully. This process may allow you to decrypt a different splash code sent in the same slot. Moreover, there are methods to solve the problem of data collision, which will be identified in more detail later, and the performance of these different methods is studied as determined as Random Access based on ALOHA. This chapter only views synchronous RA protocols, ignoring the ALOHA protocol, which is an asynchronous one. Examples of synchronous RA protocols include Slotted ALOHA, Diversity Slotted ALOHA, Contention Resolution Diversity Slotted ALOHA (CRDSA), and Irregular Repetition Slotted ALOHA (IRSA) [8, 22, 23].

- ALOHA

It can be said that the first copies of the Random Access protocols is pure ALOHA protocol, which is very straightforward and asynchronous, and was introduced in 1970 at the University of Hawaii. The data is sent as soon as it is ready, and the user waits for an acknowledgment (ACK) message from the receiver. Pure ALOHA does not verify whether the channel is busy before transmission. This way, it is possible that a collision between the packets of data that have been sent could occur. However, a node can monitor the broadcasts on the medium, even it's own, and determine whether the transmitted frames were received or not. Therefore, there is a need to recognize the attempt to resend at the transmission stations later on. When collisions occur, this will retransmit the data packet; otherwise, if the packet has been successfully delivered, the receiver responds with an acknowledgment. The efficiency of transmission of this protocol does not reach 100% of the communication channel's capacity. An effort is successful if the inter-attempt intervals on both sides exceed 1 (for unit duration packets) to calculate the successful of the attempt P (success) = e-g (n) e-g (n) = e-2g (n). Furthermore, the throughput of the success rate can be calculated using this equation: throughput= g (n) e-2g (n) and to find the max: throughput at g(n) = 1/2, throughput = 1/2e ~ 0.18, which is equivalent to 18% of the communication channel's capacity [8, 24].

- **Slotted ALOHA**

Slotted ALOHA is the first of the synchronous protocols of the Random Access protocols, introduced in 1972. In slotted ALOHA, time is subdivided into slots, and there will be a transit-only at the start of a slot. Moreover, the partial collision is avoided by the synchronization expedient. This organization divides the probability of a collision and increases throughput. So, the maximum throughput is double the amount obtained for pure ALOHA; this is because, in slotted ALOHA, possible collisions are half of the number of collisions that happen in pure ALOHA. The throughput can be calculated as if packet x is successfully delivered:

Prob{x is successfully delivered}

= Prob{No other packets within the vulnerable period T}

= e^-Np

Throughput = Np . e^-Np;

Which achieves the highest point 1/e = 36% when R = Np = 1 as shown in Fig. 3 [8].

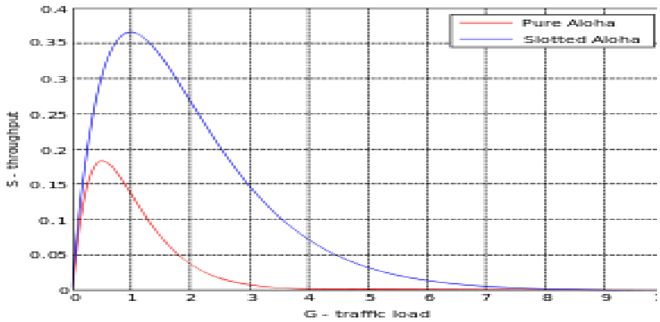

Figure 3 Pure ALOHA Performance Compared with Slotted ALOHA Performance[27]

- **Diversity Slotted ALOHA**

Diversity slotted ALOHA can be considered a derivative and support for SA, which was introduced in 1981. DESA either is used to send two or more identical copies to the channel, on different frequency channels or spaced at random intervals. The probability of receiving the original burst may increase because it is possible to decode one of the replicas correctly to retrieve the original information by reducing the number of retransmissions necessary to deliver the burst at the end. If the sender does not receive the acknowledgment from at least one of any of those replicas, it will wait again for the random time and will be restarted by the sending methods. Using two replicas is as productive as possible. Additionally, this method can increase the throughput performance. At present, this type of protocol is commonly used in satellite networks for initial station access or for sending short packets via a common medium [23].

- Contention Resolution Diversity Slotted ALOHA

CRDSA was introduced in 2007. It can be classified as an innovative DSA enhancement and an implementation of the sequential overlap elimination algorithm to achieve greater productivity of SA and DSA. As in DSA, each replica has indications of the position of the other copies in the frame. When a replica is decrypted correctly in the destination, other methods can be subtracted; that is, the interference cancellation can be applied. Thus, depending on time slots and frequency slots, there will be a specified frame size value and number of users per frame. If any user sends data, there will be two replicas to be sent with a random number of the frequency interval and the random number of the time slot that will indicate each replica. The other version that will successfully move will cancel the other, and equal the value of the frame with intervals that multiply with the intervals and user per frame. The frame size will be divided by two because each user sends two identical ones. Therefore, interference occurs if two packets are sent at the same frequency and one-time slot, so in this case, there will be no interference because each replica will be sent at a deferred frequency. Burst collisions are cleared up through a simple yet effective iterative Interference Cancellation (IC) approach that uses frame composition information from the replica bursts. The collided packets can be resolved by using successive interference cancellation (SIC) which is very useful. The main CRDSA advantages lie in the improved packet loss ratio and reduced packet delivery delay performance versus channel load, jointly with a much higher operational throughput compared to SA and DSA. CRDSA offers a significant performance gain concerning SA and DSA, which can reach up to 50% [23]. Thanks to the use of SIC, CRDSA offers a large performance gain concerning SA and DSA.

- **Irregular Repetition Slotted ALOHA (IRSA)**

The importance of wireless networks emerging from ALOHA has increased with the widespread use of the internet and progress in communications systems, as well as the increase in the number of wireless devices as mentioned previously. This growth has attracted more attention to ALOHA because it is a low-complexity protocol. However, pure ALOHA is not enough and cannot handle the huge number of users effectively. Therefore, many improvements have been proposed over the years. Irregular Repetition Slotted ALOHA (IRSA) is a new evolution of the ALOHA protocol that also sends each user a variable number of copies of their packets at each MAC frame with priority classes. Furthermore, collisions can be solved by eliminating overlapping interference using cleanly received copies. In this way, close productivity can be achieved close to the standard maximum output value of one value on the collision channel. As previously mentioned, CRDSA works on replicating packages. To convert the principle of variable frequency, the scheme [5] was called Irregular Repetition Slotted ALOHA (IRSA). In particular, it turns out that the ERS diagram can be equivalent by a binary diagram, and SIC can be seen on the dissecting decomposition on a binary diagram, similar to decoding the peeling symbols on the diagrams on the binary orthologue. This connection allows tools to borrow graphs for analysis and improvement of IRSA; its performance significantly reduces considerable lengths in the frame, as well as large size of the population. The development of density (DE) and error model can be predicted to show the rate analysis for loss of packets for the Lings can frame framework by conducting a block analysis [6 - 8]. The optimum frequency distribution was for DE, resulting in significant improvements in performance (for large frames) concerning CRDSA. On the other hand, since users in the IRSA service transfer replicas in their packages at randomly selected intervals, the probability distribution determines the number of replicas sent per slot – not controlled by the system designer, but fully determines the average number of frequencies and load. As previously mentioned, CRDSA achieves a maximum throughput, defined as the probability of successful packet transmission per slot, of T = 0.55; while the peak throughput for Framed Slotted ALOHA is just T = 0.37. While the transmitted replicas are different from user to user, this scheme is dubbed Irregular Repetition Slotted ALOHA (IRSA). Furthermore, IRSA operation can be described as borrowing concepts from graph symbols such as the spread of belief at the package level to resolve collisions. It, therefore, provides the representation of a chart that allows rapid and high-quality analytical characterization of IRSA performance. Tests and scientific convergence (SIC) show that the IRSA may provide productivity equal to T = 0.97 if an appropriate degree distribution is chosen and the number of available intervals is greater than the number of competing devices [4, 8].

V. OVERVIEW

This study is based on the principle of CRDSA, which is a Random Access technique that utilizes a specific number of replicas to transmit within a MAC frame. Furthermore, it follows this system to avoid a collision. Using this mechanism requires a pointer that points to the replica, and if one replica has received, it will cancel the other. Although CRDSA is not considered the best solution to the collision, it does upgrade the level of throughput performance. It also follows the same principle as the IRSA, but with a random number of replicas according to classes with priority performing better when throughput is compared.

Table.1Transmission Probability Distribution [25]

Index	Transmission Probability Distribution
1	$0.5102x^2 + 0.4898x^4$
2	$0.5631x^2 + 0.0436x^3 + 0.3933x^5$
3	$0.5465x^2 + 0.1623x^3 + 0.2912x^6$
4	$0.5x^2 + 0.28x^3 + 0.22x^8$
5	$0.08x^3 + 0.14x^4 + 0.3x^5 + 0.17x^6 + 0.14x^7 + 0.17x^9$
6	$0.4977x^2 + 0.2207x^3 + 0.0381x^4 + 0.0756x^5 + 0.0398x^6 + 0.0009x^7 + 0.0088x^8 + 0.0068x^9 + 0.0030x^1 + 0.0429x^{14} + 0.0081x^{15} + 0.0576x^{16}$

The study will start by generating a scenario to evaluate the performance of CRDSA within a MAC frame. Each user has to transmit two replicas of the same packet in a random time slot and frequency slot into the same MAC frame. Each replica has a pointer, which indicates the entire slot occupied by the bursts. Whenever one packet is successfully decoded at the receiver, the pointer is extracted, and the potential interference contribution caused by the replica on the corresponding slot is removed,

such as in the slot where the packet is decoded. The SIC technique proceeds until either all bursts have been successfully decoded, or until a maximum number of iterations has been reached. This technique is fundamental for improving the performance of the protocol, but at the same time introduces a temporal delay proportional to the maximum number of iterations done by the receiver [26].

In addition to creating a scenario that studying the performance of the IRSA protocol, which is considering to send a random number of the replica within classes that determine the priority in a random time slot and frequency slot. Following the same principle used in CRDSA, whenever a replica has successfully been received, the other replicas will be canceled. The SIC technique proceeds until all packets have been successfully received. It can be considered as a modification of the CRDSA scenario, which will lead to a comparison of the throughput performance in each protocol, resulting in the best way for data transmission without collision and improving the transmission of large quantities of data in a single system.

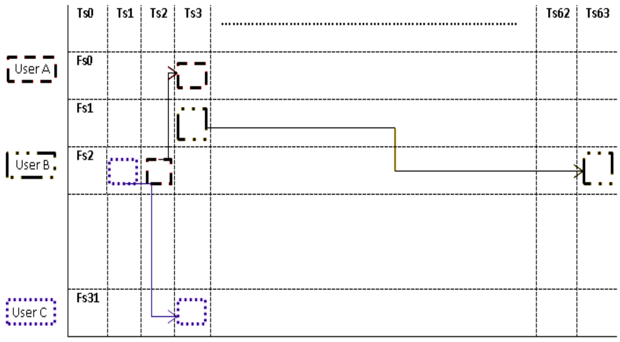

Figure 4 How the Number of Slots are Determined

VI. SYSTEM MODEL

- **CRDSA**

As stated, the scenario used to study the performance is CRDSA. The basic idea is to send data packets with identical replicas, which are two with a pointer, to achieve greater performance. Furthermore, the frame duration (Tf) is considered, which consists of n time slot F of frequency slot that will determine the value of the frame size and the number of the users per frame. The principle works as follows to determine the slots number: Slots=Timeslots*Frequency Slots. Furthermore, two replicas are randomly generated, with the first replica slots equal to a random number of time slots and frequency slots. There will be assigned further slots for the second replica, which will be a random number of timeslots and frequency slots. However, there will be a condition, which is the first replica slot ≠ second replica slot. For example, a frame with 64-time slots and 32 frequency slots, as shown in Figure3, means that the number of slots will be64*32 and the replica will be sent at a random time slot and frequency slot. Also, each replica will be randomly given a probability number.

Identifying a pointer K for both replica of packet as [preamble, pointer] where preamble is Time Slot and Frequency Slot of other replica as follows:

S={s11(x1,y1),s12(x1,y2),s21(x2,y1),s22(x2,y2),sts fs(xts,yfs)}

S is a cell which include many arrays s=[k ts fs] where k is a pointer for two replica so

s(ts1,fs1)=[k1 ts2 fs2]

s(ts2,fs2)=[k1 ts1 fs1] and so on.

For SIC state where a collided packet is detected, s array will be s(x,y)=[0 0 0] to decode and extract the true packet. On the other hand, the elements of the array are removed for a clean packet.

Using the successive interference cancellation (SIC) technique, there will be the detection of collision packets and the elimination of replicas of the successively received packet. The counter must be set, along with a maximum number of iterations: Nitr=1 to max iteration and Nitr = Nitr

+1 for every interference canceled packet. The normalized load can be calculated as G = packet load/slots where packet load is between 0 and the number of slots and the throughput = number of successive received packets per frame/slots. Calculate the average to approximately 200 tests to the iteration counter to know the average of the interference packets [26].

- **IRSA**

IRSA is considered here as the scenario used to study the performance of CRDSA with modifications. The basic idea is to send data packets with an identical replica to achieve greater performance. Furthermore, the frame duration is Tf which consists of n time slot F of frequency slot that will determine the value of the frame size and the number of users per frame. The principle is to determine the slot numbers by Slots=Timeslots*Frequency Slots. Furthermore, there is a creating to S cell has Time Slots * Frequency Slots dimension and Status matrix for each slot so the statuses are non-negative integers as follows:
0: Slot is idle.
1: Slot is ready to transmit
2: The packet collides.
The replica will be sent in a randomly selected time slot and frequency slot. Besides, giving each replica a random probability number depending on the simulation result will allow a study of the performance of the transmission protocol, which is examined in different conditions and different transmission possibilities. Generating several replicas depending on Table 1.
To determine the performance, the number of slots with values of ones in the Status Matrix will be collected, which refers to the number of packets without collision.

Successive Status = $\sum_{n=0}$ Status (where result = 1)

Replication of packets received as a graph-based representation must also be removed, thanks to a successive interference cancellation (SIC) algorithm that facilities the detection of the collision packets. Additionally, setting the iteration counter and a maximum number of iterations: Nitr=1 to max iteration and Nitr = Nitr +1 for every interference canceled signal will calculate the normalized load G = packet load/slots where packet load is between 0 and number of slots.
The throughput = number of successive received packets per frame/slots.
The average of the interference packets can be worked out by calculating the average to approximately 200 tests of the iteration counter.

I. RESULTS

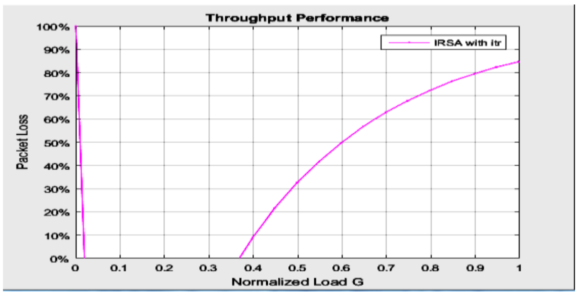

Figure 5 Packet Loss Rate of IRSA with Iteration

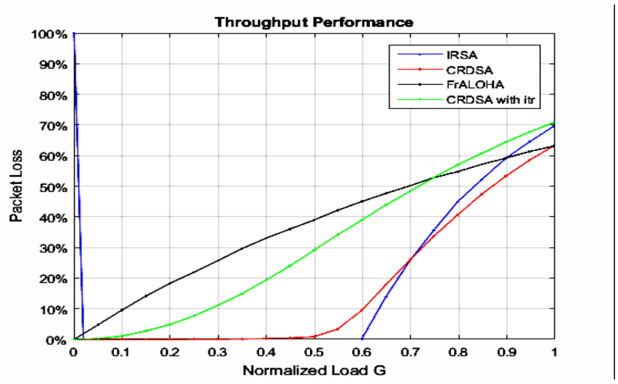

Figure 6 Packet Loss Rate of IRSA, ALOHA, and CRDSA

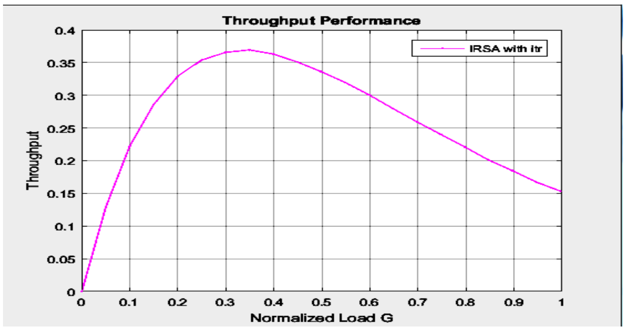

Figure 7 Throughput of IRSA with Iteration

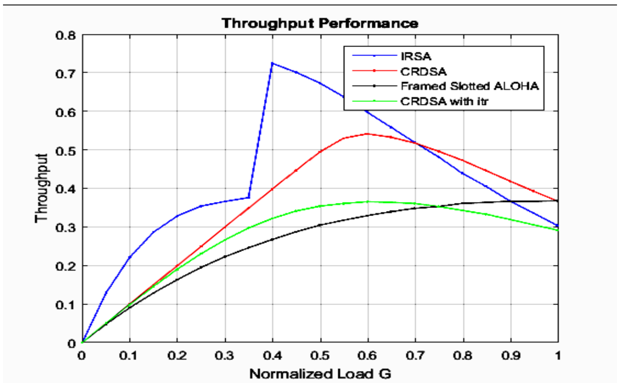

Figure 8 Throughput of IRSA, ALOHA and CRDSA

The CRDSA system, which was introduced, is simulated in MATLAB. The simulation examines the MAC layer, and the MATLAB code is shown in the Appendix. CRDSA access frame setting with time slots is set as 64, and the frequency slot is set as 32 because it is a Random Access simulation and each result is taken from the mean of 200 test results.

II. PERFORMANCE EVALUATION

Figure5 and Figure6 show the throughput performance of six schemes, which are indicated by the packet loss rate versus normalized load. The Magenta curve represents the IRSA scheme with maximum iteration set as one. Figure6 shows the blue curve representing the IRSA scheme without any maximum iteration set, which means the iteration will stop if the system achieves 100% throughput or no clean packet in the sample memory. The black curve represents the original frame ALOHA, while the green curve is the CRDSA scheme with maximum iteration set as one. The red curve represents the CRDSA scheme without any maximum iteration set, which means the iteration will stop if the system achieves 100% throughput or no clean packet in the sample memory. Furthermore, from Figure6 it can also be seen that the original frame ALOHA is already starting to lose packet compared to CRDSA – the red curve only starts losing packets when the load is larger than approximately 45%. Besides, we can see that the CRDSA packet loss rate increases significantly after 50% load, but it is still better than frame ALOHA. Moreover, comparison with IRSA shows it has the best performance because it only starts to lose packets after 60%. Figures 7 and 8 show the frame utilization of six schemes mentioned above with increased normalized load. For frame ALOHA, it achieves its maximum utilization of around 37% when the load is full. In comparison, CRDSA achieves maximum frame utilization when the load is close to 60%. For CRDSA without maximum iteration set, throughput is able to achieve 40% of the frame slots. Furthermore, comparison with IRSA shows that it achieves maximum frame utilization when the load is nearly 70%. For IRSA without maximum iteration set, Figure 8 illustrates that the IRSA throughput with maximum iteration is able to achieve 60% of the frame slots. Figures6 and7 demonstrate that IRSA can achieve much lower packet loss rate and higher frame utilization than both original frame ALOHA and CRDSA. Additionally, they also provide configuration suggestions for Load Relief schemes and frame size setting. For example, if frame resource is quite precious, frame size could be set as a relatively small number, and Load Relief schemes should control the normalized load no more than 0.7 at most of the time. On the other hand, if throughput performance is primary, frame size could be slightly increased, combined with Load Relief schemes control, to make the normalized load no more than 0.6. However, the cost of the IRSA scheme is the uncertainty of time delay and power consumption caused by increasing iteration. Therefore, actual operation iteration should be limited. However, over small iteration, limitation would sabotage IRSA performance like one-iter IRSA in Figures 5, 6, 7, and 8. The following analysis is of the suitable maximum iteration set of IRSA.

III. CONCLUSION AND FUTURE WORK

IoT technology has revolutionized the world of communications; this technique saves valuable time and effort and helps us adapt to the era of speed. Considering the high importance of this technology, it must be developed, especially in the area of Random Access protocols. Furthermore, the different protocol types indicate evolution, and thus many models have been published for these different protocols. It is expected that IoT technologies will improve even further over the coming years, and studies will increase in this area. This paper discussed several ideas, algorithms, and techniques to improve the performance of protocols through the development of random transport protocols. Analytical and experimental analyses were presented, highlighting promising solutions.

As shown in the results, the performance of the IRSA was better than CRDSA, which was with a particular number of iterations with assigned numbers called probability. A possible solution is to add another random number to each user which can act as a block number to prevent the user from choosing this number when selecting the random number employed in the probability variables. For example, there will be a user number m which will go to send the replicas with a probability number k. However, if we assign a number to prevent the users from independently selecting a particular number, it will skip that number and never use it. From this principle, it can be seen how collisions between data packets can be avoided. This step can lead to avoiding each user from using a particular slot which may improve the throughput performance.

REFERENCES

[1] "The internet of things: Between the revolution of the internet and the metamorphosis of objects." Vision and Challenges for Realising the Internet of Things (2010): 11-24.

[2] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.

[3] Xia, Feng, et al. "Internet of things." International Journal of Communication Systems 25.9 (2012): 1101.

[4] Toni, Laura, and Pascal Frossard. "Prioritized random MAC optimization via graph-based analysis." IEEE Transactions on Communications 63.12 (2015): 5002-5013.

[5] Zanella, Andrea, et al. "M2M massive wireless access: challenges, research issues, and ways forward." Globecom Workshops (GC Wkshps), 2013 IEEE. IEEE, 2013.

[6] Aijaz, Adnan, and A. Hamid Aghvami. "Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective." IEEE Internet of Things Journal 2.2 (2015): 103-112.

[7] Zhang, Yan, et al. "Cognitive machine-to-machine communications: visions and potentials for the smart grid." IEEE network 26.3 (2012).

[8] Paolini, Enrico, Gianluigi Liva, and Marco Chiani. "Coded slotted ALOHA: A graph-based method for uncoordinated multiple access." IEEE Transactions on Information Theory 61.12 (2015): 6815-6832.

[9] Abbate, Janet Ellen. "From ARPANET to Internet: A history of ARPA-sponsored computer networks, 1966--1988." (1994).

[10] Domingo, Mari Carmen. "An overview of the Internet of Things for people with disabilities." Journal of Network and Computer Applications 35.2 (2012): 584-596.

[11] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[12] Boswarthick, David, Omar Elloumi, and Olivier Hersent, eds. M2M communications: a systems approach. John Wiley & Sons, 2012.

[13] Wu, Geng, et al. "M2M: From mobile to embedded internet." IEEE Communications Magazine 49.4 (2011).

[14] Al-Fuqaha, Ala, et al. "Toward better horizontal integration among IoT services." IEEE Communications Magazine 53.9 (2015): 72-79.

[15] Shelby, Zach, Klaus Hartke, and Carsten Bormann. "The constrained application protocol (CoAP)." (2014).

[16] Thangavel, Dinesh, et al. "Performance evaluation of MQTT and CoAP via a common middleware." Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on. IEEE, 2014.

[17] Bianchi, Giuseppe, Luigi Fratta, and Matteo Oliveri. "Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs." Personal, Indoor and Mobile Radio Communications, 1996. PIMRC'96., Seventh IEEE International Symposium on. Vol. 2. IEEE, 1996.

[18] Sharma, Gaurav, Ayalvadi Ganesh, and Peter Key. "Performance analysis of contention based medium access control protocols." IEEE Transactions on Information Theory 55.4 (2009): 1665-1682.

[19] Busch, Costas, et al. "Contention-free MAC protocols for wireless sensor networks." International Symposium on Distributed Computing. Springer, Berlin, Heidelberg, 2004.

[20] Rayes, Ammar, and Samer Salam. "The Internet in IoT—OSI, TCP/IP, IPv4, IPv6 and Internet Routing." Internet of Things From Hype to Reality. Springer International Publishing, 2017. 35-56.

[21] Weber, Steven P., et al. "Transmission capacity of wireless ad hoc networks with successive interference cancellation." IEEE Transactions on Information Theory 53.8 (2007): 2799-2814

[22] Raychaudhuri, D. "Performance analysis of random access packet-switched code division multiple access systems." IEEE Transactions on Communications 29.6 (1981): 895-901.

[23] Munari, Andrea, et al. "The throughput of slotted ALOHA with diversity." Communication, Control, and Computing (Allerton), 2013 51st Annual Allerton Conference on. IEEE, 2013.

[24] Stefanovic, Cedomir, PetarPopovski, and DejanVukobratovic. "Frameless ALOHA protocol for wireless networks." IEEE Communications Letters 16.12 (2012): 2087-2090.

[25] Laura Toni and Pascal Frossard. Prioritized random MAC optimization via graph-based analysis. arXiv preprint arXiv:1501.00587, 2015.

[26] Wei Ye, John Heidemann, and Deborah Estrin. An energy-e cient MAC protocol for wireless sensor networks. In INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications So-cieties. Proceedings. IEEE, volume 3, pages 1567{1576. IEEE, 2002.

[27] Wikipedia,(2014):“ALOHAnet”https://en.wikipedia.org/wiki/ALOHAnet.[Accessed 23 September. 2017].