A METHOD FOR ESTIMATING RFID PROTOCOL EXECUTION TIME BASED ON FLOWGRAPH MODEL

TAN AIK THENG

UNIVERSITI SAINS MALAYSIA

2021

A METHOD FOR ESTIMATING RFID PROTOCOL EXECUTION TIME BASED ON FLOWGRAPH MODEL

by

TAN AIK THENG

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

September 2021

ACKNOWLEDGEMENT

First of all, the author of this dissertation would like to thank Associate Professor Zurinahni Zainol for supporting this research work. Next, the author would like to dedicate this dissertation to the late Mr. Tan Chek Hin, formerly a laboratory assistant at the School of Physics, Universiti Sains Malaysia. Subsequently, the author would like to thank the examination committee, Dr.Azizul Rahman Mohd Shariff, Associate Professor Cheah Yu-N, and Professor Zuriati Ahmad Zukarnain, who provided valuable comments and ideas content of this dissertation. The author would also like to thank all the committee members who were in charge of conducting the viva-voce examination session of this dissertation (Professor Mohd Zubir Mat Jafri, Professor Bahari Belaton, and Associate Professor Nurul Hashimah Ahamed Hassain Malim). Eventually, the author would like to take this opportunity to thank Dr. Lim Lian Tze, who shares valuable knowledge with the author of this dissertation in latex application for writing dissertations and articles.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

ACK Acknowledgement

AGT Agent

ARP Address Resolution Protocol

CBR Constant Bit Rate

CDF Cumulative Distributed Function

CGF Cumulant Generating Function

CTS Clear To Send

ID Identification

MAC Media Access Control

MGF Moment Generating Function

RFID Radio Frequency Identification

RAO Read Authentication Only Protocol

RTA Reader-then-Tag Authentication Protocol

RTR Routing

RTS Request To Send

UDP User Datagram Protocol

TCP Transmission Control Protocol

TAO Tag Authentication Only Protocol

TPG Traditional Polling Grouping

TRA Tag-then-Reader Authentication Protocol

LIST OF NOTATIONS

$M^{'}(0)$ non-defective time-to-event distributions

t_{gid} duration required to transmit group ID

t_{id} duration required to transmit RFID tag's ID

$t_{tag\ resp}$ duration required by RFID tag to transmit response

M_{ij} Moment generating function, i,j is an integer

P_{ij} Probability of Transisiton State, i,j is an integer

S_n State in flowgraph model, n is an integer

Y_n Sum of transmittance, n is an integer

KAEDAH BAGI MENGANGGARKAN MASA PELAKSANAAN PROTOKOL RFID BERDASARKAN MODEL GRAF ALIRAN

ABSTRAK

Protokol TPG direka cipta untuk mengelompokkan semua tag dengan cekap mengikut pemetakan yang tertentu sehingga tag dalam kumpulan yang sama akan mempunyai ID kumpulan yang sama. Dengan protokol TPG digunakan, pembaca RFID hanya menyiarkan ID kumpulan satu kali diikuti dengan ID tag RFID tanpa menghantar ID kumpulan yang sama berulang kali ke setiap tag RFID. Penyelesaian teori sedia ada yang dicadangkan untuk mengukur masa pelaksanaan protokol TPG tidak memberikan penyelesaian komprehensif. Ini termasuk masa tag RFID bertindak balas dan hanya boleh digunakan untuk mengukur waktu pelaksanaan protokol TPG dalam persekitaran pembaca RFID-ke-berbilang tag-RFID (satu-ke-banyak) tetapi tidak dalam persekitaran berbilang pembaca RFID-ke-berbilang tag-RFID (banyak-ke-banyak). Untuk mengatasi batasan persamaan protokol TPG sedia ada, model graf aliran dicadangkan dalam kerja penyelidikan ini untuk menganggarkan jumlah masa pelaksanaan protokol TPG dalam topologi rangkaian RFID banyak-ke-banyak. Penting untuk mengukur masa perlaksanaan protokol TPG dalam topologi rangkaian RFID banyak-ke-banyak kerana penggunaan protokol TPG tidak terhad hanya kepada topologi rangkaian RFID satu-ke-banyak. Penting untuk mengukur masa pelaksanaan protokol TPG dalam topologi rangkaian RFID banyak-ke-banyak kerana penerapan protokol TPG tidak terbatas hanya pada topologi rangkaian RFID satu-ke-banyak. Pada masa ini, topologi

rangkaian RFID banyak-ke-banyak digunakan secara meluas untuk memperbaiki kecekapan pengesahan. Oleh itu, pengukuran masa pelaksanaan protokol TPG dalam topologi rangkaian RFID banyak-ke-banyak adalah penting untuk menentukan kecekapan protokol TPG. Cadangan persamaan yang berasal dari model graf aliran untuk menganggarkan jumlah masa pelaksanaan protokol TPG boleh digunakan dalam tiga jenis topologi rangkaian RFID: satu-ke-satu (pembaca RFID dan tag RFID), satu-ke-banyak (pembaca RFID dan berbilang tag RFID), dan banyak-ke-banyak (berbilang pembaca RFID dan berbilang tag RFID). Untuk menilai persamaan yang dicadangkan bagi kerja penyelidikan ini, perisian simulator NS2 digunakan untuk mensimulasikan topologi rangkaian RFID satu-ke-satu (pembaca RFID dan tag RFID), satu-ke-banyak (pembaca RFID dan berbilang tag RFID), dan banyak-ke-banyak (berbilang pembaca RFID dan berbilang tag RFID) untuk mendapatkan masa pelaksanaan protokol bagi setiap simulasi topologi rangkaian, yang kemudiannya digunakan untuk membandingkan dengan hasil yang diperoleh dari persamaan yang dicadangkan. Untuk mensimulasikan persamaan kerja penyelidikan ini untuk setiap topologi rangkaian RFID melibatkan bilangan peranti RFID yang berlainan, parameter simulasi seperti kadar data membaca dan menulis antara peranti RFID dan masa melibatkan dalam paket data penghantaran udara protokol TPG digunakan berdasarkan sedia yang ada. Hasil pengukuran yang diperoleh antara simulator NS2, persamaan yang dicadangkan, dan persamaan yang dicadangkan TPG yang ada dijangka mempunyai kesilapan relatif. Perkakasan komputer seperti ukuran memori dan kelajuan prosesor yang digunakan dalam simulasi NS2 adalah faktor utama yang menyebabkan hasil pengukuran mempunyai toleransi. Walau bagaimanapun, hasil pengukuran menunjukkan bahawa bacaan ralat relatif tepu pada 1.6 % walaupun nod atau peranti RFID melebihi 10000 dalam simulasi NS2.

Oleh itu, hasil pengukuran toleransi perbandingan antara persamaan TPG yang dicadangkan yang ada, persamaan yang dicadangkan untuk kerja penyelidikan ini, dan simulator NS2 membuktikan bahawa kebolehpercayaan dan ketepatan persamaan yang dicadangkan dikembangkan dalam kerja penyelidikan ini.

A METHOD FOR ESTIMATING RFID PROTOCOL EXECUTION TIME BASED ON FLOWGRAPH MODEL

ABSTRACT

The TPG protocol designed to efficiently group all tags according to a given partition so that tags in the same group will have the same group ID. Using the TPG protocol; the RFID reader sends the group ID followed by the IDs of the RFID tags only once without repeatedly sending the same group ID to each RFID tag. An existing theoretical solution proposed to measure the execution time of the TPG protocol does not provide comprehensive solutions. For example, the missing solutions consider the RFID tag response time and can only be used to measure the TPG protocol execution time in the RFID reader-to-RFID tag (one-to-many) environment, but not in the RFID reader-to-RFID tag (many-to-many) environment. A flowgraph model is proposed in this research to overcome the limitations of the existing TPG protocol equation. It is essential to measure the execution time of the TPG protocol in a many-to-many RFID network topology because the application of the TPG protocol is not limited to a one-to-many RFID network topology. Currently, the many-to-many RFID network topology widely uses to improve authentication efficiency. Therefore, measuring the execution time of the TPG protocol in a many-to-many RFID network topology is essential to determine the efficiency of the TPG protocol. The proposed equations based on the flowgraph model to estimate the total execution time of the TPG protocol can apply in three types of RFID network topologies: one-to-one (RFID reader and RFID

tag), one-to-many (RFID reader and RFID tags), and many-to-many (RFID reader and RFID tags). The NS2 simulator software used to simulate one-to-one (RFID reader and RFID tag), one-to-many (RFID reader and RFID tags), and many-to-many (RFID reader and RFID tags) RFID network topologies to obtain the protocol execution time of each simulated network topology, which uses to compare with the results obtained from the proposed equations. To simulate the proposed equation of this research work for each RFID network topology that includes the different number of RFID devices. The simulation parameters such as the read and write data rate between RFID devices and the timing involved in the over-the-air transmission of the data packets of the TPG protocol are reused based on existing TPG's work. The measurement results obtained between the NS2 simulator, proposed equations, and existing TPG proposed equation foresee having relative errors. Computer hardware such as the size of memory and processor speed used in NS2 simulation is the main factor that causes the measurement results to have tolerance. However, the measurement results show that the relative error reading is saturated at 1.6% even though nodes or RFID devices are beyond 10000 in NS2 simulation. Hence, a comparison tolerance measurement results between the existing proposed TPG equation, the proposed equation of this research work, and the NS2 simulator prove that the reliability and accuracy of the proposed equation developed in this research work.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Radiofrequency identification (RFID) is considered one of the key technologies in future networks due to its many advantages, such as the low cost of 5 cents per day and wireless transmission without a line of sight (Zhang et al., 2015),(Al-Fuqaha et al., 2015). The technology is also ubiquitously used in many different applications such as warehouse management, object tracking, authentication, and inventory control (Bolic et al., 2010). Each object tags with a RFID tag that can be passive, semi-passive, or active. Each object is represented by a unique identity (ID). In comparison, semi-passive and active tags have internal power sources; passive tags power by harvesting radio frequency (RF) energy from RFID readers. Therefore, the passive tags have a limited communication range, are much cheaper than the others, and are our target in this study. Although RFID technology has created a multi-billion dollar market, the RFID-based industry still has many significant problems, such as evaluating RFID protocol performance in one-to-many and many-to-many RFID network topologies (Nguyen et al., 2017).

In one-to-many RFID network topology, it consists of many RFID tags and one RFID reader. On the other hand, many-to-many RFID network topology consists of many RFID tags and many RFID readers. There are many types of RFID protocols designed for different goals and purposes. The goals and purposes include reducing the collision rate between RFID tags or RFID readers, improving efficiency in terms of timing for sensory data collection from RFID tags based on assigned group identification and security. Examples of RFID protocols developed to avoid collision between RFID tags include the idle-dynamic frame slotted ALOHA (RTCI-DFSA) (Qu et al., 2019) algorithm and the Dynamic Arrival Scenarios Based algorithm at First-Come-First-Serve (DAS -DFSA) (Zhang, Tao, Yu, Xiao, Cai, Gao, Jia and Wen, 2019). To reduce collisions in RFID system, some modern research works such as (Mbacke et al., 2018),(Nafar and Shamsi, 2018),(Wu et al., 2019) and (Golsorkhtabaramiri et al., 2019) have been presented. To provide security solutions in RFID systems, state-of-the-art RFID grouping proof protocols such as (Dhailah et al., 2019),(Cherneva and Trahan, 2020),(Xu and Dang, 2019) and (Cherneva and Trahan, 2018) are proposed for RFID users. In this research work, state-of-the-art grouping protocols execution time investigated in terms of existing theoretical solutions can be improved or extended to support measurement grouping protocol's execution time in many-to-many RFID network topology.

Measuring the specific RFID protocol execution time in a real-world environment is challenging when dealing with a large-scale RFID system. A large-scale RFID system consists of scalable RFID readers and RFID tags. The measurement requires a complex setup and is costly to execute (J et al., 2019). The time efficiency for communication between RFID devices in different RFID network topologies is an important parameter to consider while designing a TPG protocol. The time efficiency helps to justify the performance and reliability of the TPG protocol in RFID systems (Dhailah et al., 2019). To determine the gap in the current theoretical measurement of RFID protocol execution time, investigating related work is essential to identify the problem sets. Examples of research related to the theoretical measurement of RFID protocol execution time include Missing-Tag Identification Protocols (Zhang et al., 2011), baseline protocol (Zheng and Li, 2013), Categorized Missing Tag Identification Protocol (CMTI) (Zhao et al., 2014), TPG protocol (Liu et al., 2016),Hierarchical-hashing Data Collection (HDC) protocol (Liu et al., 2019), Time-Efficient Cloning Attacks Identification Protocol (CAIP) (min Zhao et al., 2017), White Paper Protocol (Gong et al., 2017) and Query for Large Categories and Small Categories (QLS) protocol (Liu et al., 2020).

TPG protocol designs to allow an RFID reader to communicate with a group of RFID tags based on group identification. When a group of RFID tags has the exact group identification, the RFID reader sends data to specific group tags. The RFID reader does not need to repeatedly send the same data to RFID tags with the same group identifier. Compared with the research work of Missing-Tag Identification Protocols (Zhang et al., 2011), Baseline protocol (Zheng and Li, 2013), Categorized Missing Tag Identification Protocol (CMTI) (Zhao et al., 2014), Hierarchical-hashing Data Collection (HDC) protocol (Liu et al., 2019), Time-Efficient Cloning Attacks Identification Protocol (CAIP) (min Zhao et al., 2017), White Paper Protocol (Gong et al., 2017) and Query for Large Categories and Small Categories (QLS) protocol (Liu et al., 2020), the theoretical model of TPG protocol proposed by (Liu et al., 2016) is much simpler in terms of using variables. Therefore, the TPG protocol chooses as the basis for verification in this research work. Most of the existing theoretical models are only limited to the one-to-many RFID network topology. In fact, in the natural RFID user environment, many RFID readers have been used to improve the data collection efficiency of RFID tags.

A measurement between theoretical and practical approaches is required to obtain reliable measurement results of TPG protocol execution time in many-to-many RFID network topology. The TPG protocol plays a vital role in improving the performance of RFID-enabled applications Liu et al. (2016). For example, suppose RFID tags belonging to the same group share a standard group ID. In that case, the reader can transmit the same data to them at the same time, which saves much communication overhead compared to traditional unicast transmission Liu et al. (2016). When RFID tags are in the same group, it simplifies the sensory data collection process. In many practical scenarios (Liu et al., 2019), it is crucial to quickly and accurately collect sensory data from a large number of RFID tags equipped with sensors. For example, in cold chain logistics, if the reported sensory data of some food products are abnormal, must take appropriate countermeasures in time to avoid potential risks in terms of economic losses or even safety (Liu et al., 2019). The main concern in solving the sensory data collection problem is identifying all IDs in a short time (Nguyen et al., 2019). Therefore, measuring the time efficiency for the RFID sensory data collection protocol is essential to verify the performance (Liu et al., 2019). To calculate the specific execution time of the RFID sensor data collection protocol in one-to-many and many-to-many RFID network topologies, the measurement methods can use either a theoretical model, simulator software, or the setup of a natural environment (Doss et al., 2020). In supply chain management and Warehouse Management, the use of RFID systems with many-to-many RFID network topologies is critical concerning large capacity warehouses. The application of many-to-many RFID network topology in Supply Chain Management and Warehouse Management helps to reduce the processing time of object recognition in production operation, create electronic records of production in production management systems, and establish an information platform for sharing with users (Han et al., 2019).

1.2 Problem Statement

TPG protocol execution time measurement can conduct via three methods: hands-on measurement, network simulator software such as NS2, and existing TPG protocol modeling (Xiao, Chen, Liu, Cheng and Luo, 2019). Using network simulator software such as NS2 to estimate TPG protocol execution time in one-to-one, one-to-many, and many-to-many RFID network topologies is feasible. However, the latency timing of TPG protocol on NS2 simulator software depends on the PC's hardware profile, such as processor speed and memory size (Xiao, Zhang, Chen, Chen, Liu, Cheng and Luo, 2019). Therefore, comparing the measurement results between the theoretical and network simulator software is essential for obtaining better accuracy and reliable measurement results (Chen et al., 2018).

Moreover, the TPG protocol is part of the RFID protocol and classified as Transmission Control Protocol (TCP). Each RFID tag expects to send an acknowledgment to the RFID reader after receiving the data packet sent by the RFID reader (Wang et al., 2019). In the existing TPG protocol equation, the response time of the RFID tag to the RFID reader does not seem to be considered, which affects the accuracy and reliability of measuring the execution time of the TPG protocol in the one-to-many RFID network topology (R et al., 2018). Therefore, the theoretical model used to measure TPG protocol execution time in one-to-many RFID network topology needs to be improved and extended to achieve more reliable TPG protocol execution time measurement (A.Bonuccelli and Martelli, 2018).

TPG protocol is not limited to the one-to-many RFID network topology. It is also possible to see the involvement of the TPG protocol in the many-to-many RFID network topology. In view existing TPG protocol equation only supported in measuring the TPG protocol execution time in the one-to-many RFID network topology (Liu et al., 2016), a new theoretical model is needed to enable the measurement of the TPG protocol execution time in the many-to-many RFID network topology (F and H., 2018). A new theoretical model is required to measure the TPG protocol execution time in many-to-many RFID network topology, as it helps to determine the performance of TPG protocol in large RFID networks in terms of timing efficiency (Wang et al., 2020).

1.3 Objectives of Research

The objective of this research is to propose a suitable and flexible theoretical model to estimate the execution time of the TPG protocol in different types of RFID network topologies such as one-to-one (RFID reader and RFID tag), one-to-many (RFID reader and RFID tags), and many-to-many (RFID reader and RFID tags) to determine the latency measurement result between the proposed model, the existing TPG protocol model, and the NS2 simulation. Details of research objectives are defined as follows:

- Measuring the execution time of TPG protocol in different RFID network topologies based on the proposed model, existing TPG protocol modeling, and NS2 simulation for latency timing comparison.

- Propose a model using the flowgraph model to estimate the total execution time of the TPG protocol in

  (i) One-to-many RFID network topology - In view existing TPG protocol equation does not take into account the RFID tag response time; an improvement in the proposed TPG protocol equation is essential to improve the accuracy and reliable measurement of TPG protocol execution time.

  (ii) Many-to-many RFID network topology - In view existing TPG protocol equation does not support measurement of TPG protocol execution time in a many-to-many RFID network topology, a new proposed equation derived from overcoming the limitations of the existing TPG protocol equation.

1.4 Contributions from Research Work

The research work demonstrates the application of the flowgraph model as a theoretical method for estimating the execution time of the Traditional Polling Grouping (TPG) protocol in an extensive RFID system to gain insights. Moreover, the flowgraph model better illustrates the over-the-air TPG protocol event used as communication between RFID devices in different types of RFID network topology such as RFID reader-to-RFID tag, RFID tag-to-RFID reader, and RFID reader-to-RFID tag. The proposed idea contributes to the RFID industry as an alternative option to measure the execution time of TPG protocol and other RFID protocols.

1.5 Research Methodology

To achieve the objectives of the research work. Three general initiatives have conducted as follows:

1. Derivation of a proposed model - Identify suitable theoretical methods that can be presented in this research work to solve the current problem in the theoretical measurement of TPG protocol execution time. In this research work, the flowgraph model was chosen as the theoretical solution for estimating TPG protocol execution time in one-to-many and many-to-many RFID network topology. It provides solutions for time-to-event use cases. As a benchmark to derive the proposed models for estimating the TPG protocol execution time in one-to-many and many-to-many RFID network topologies, the TPG signaling protocol events in one-to-many and many-to-many RFID networks topologies fitted and represented as a flowgraph model. The parameters assigned in the flowgraph model, such as the read and write data rates between RFID devices, follow the definition of EPC Global. On the other hand, the TPG protocol simulation parameters as proposed by (Liu et al., 2016), such as the timing for an RFID reader sending the RFID tag (t_{id}) ID and the group ID (t_{gid}) reused on the proposed model. The reason is to achieve fair comparison measurement results between the proposed model and the existing TPG protocol model.

2. Simulation - Identify a suitable simulator to simulate each of the RFID network topologies under investigation. This initiative's objective was to compare the RFID protocol execution time between the proposed models and the simulator. Selection of the NS2 simulator software for the simulation activities of this re-

search work because it is very well known and license-free. To perform the simulation using NS2, the RFID network topology such as one-to-one, one-to-many, and many-to-many constructed using a TCL script. The contents of each TCL script implemented for each RFID network topology consists of setup simulation parameters, the assignment of the functionality of the nodes such as RFID reader or RFID tag, the setup of the connection between the nodes, and the duration of the simulation for each network topology. Once the TCL creates for each network topology, the Cygwin application uses to executes the Linux commands to generate the network animation and NS2 trace files. Then the NS2 simulation can begin, followed by the analysis of the NS2 trace files. To measure the execution time of the TPG protocol in the NS2 simulation, the script AWK creates analyzes the NS2 trace file.

3. Evaluation - To determine the reliability and accuracy of the execution time of the TPG protocol based on the proposed model, the relative error results obtained between the simulation of NS2, the existing TPG protocol model, and the proposed model for each RFID network such as one-to-one, one-to-many and many-to-many carefully comparing and analyzing. To compare the measurement results TPG protocol execution time in one-to-many RFID network topology, the proposed model of this research work, the NS2 simulation, and the existing TPG protocol model involved evaluation measurement results. To compare the measurement results of TPG protocol execution time in many-to-many RFID network topology, only measurement results obtained from the proposed model of this research work and the NS2 simulation are involved because the existing TPG proposed equation has limitations support in many-to-many RFID

network topology. By comparing TPG protocol execution time obtained from the NS2 simulation, the proposed model, and the existing TPG protocol proposal model, TPG protocol execution time latency in different types of RFID network topologies can determine.

1.6 Scope

This research mainly focuses on applying the flowgraph model as a theoretical method to estimate the TPG protocol execution time in different RFID network topologies, especially in large-scale RFID systems. Analysis of relative errors measurement results obtained between different approaches conducted to determine the reliability and accuracy of proposed equations. In terms of simulation activities, NS2 software uses to validate the measurement results obtained from the proposed equation.

1.7 Organisation of Thesis

The contents of the thesis organized as follows:

Chapter 2 contains general information about RFID devices, types of authentication in RFID protocol, types of graph-theoretical models, state-of-the-art measurements of RFID protocol execution time, and NS2 simulator software.

Chapter 3 shows in detail the process of deriving the proposed model used for estimating the total execution time of the TPG protocol in a one-to-many RFID network topology known as RFID reader-to-RFID tag environment.

Chapter 4 shows in detail the process of deriving the proposed model used for estimating the total execution time of the TPG protocol in a many-to-many RFID network topology, also known as RFID reader-to-RFID tags environment.

Chapter 5 discusses the measurement results obtained between the proposed models, the NS2 simulator software, and the existing theoretical solution for TPG protocol adopted in one-to-one, one-to-many, and many-to-many RFID network topologies. Measurement results obtained from different methods analyzed in terms of the percentage relative error. For the many-to-many RFID network topology, comparison measurement results only between the NS2 simulation and the proposed model because the theoretical solution for measuring the TPG protocol execution time is not supported.

Chapter 6 summarises the results of the research. It includes research limitations, research challenges, goals achieved, and future work.

CHAPTER 2

LITERATURE REVIEW & BACKGROUND INFORMATION

In this chapter, a literature review provides on various topics related to this research paper. The topics covered are RFID adoption, types of authentication in RFID protocol, state-of-the-art protocols for RFID sensor data collection, theoretical graph models, and NS2 simulator software.

2.1 Introduction to RFID

Three main devices are involved in the authentication of the RFID system: RFID tag, RFID reader, and RFID database. Authentication in an RFID system defines verifying a person, animal, or object sent from a trusted source. The functions of each RFID device are described in detail below:

1. **RFID database** - The function of an RFID database is to store the IDs of RFID tags. Each RFID tag program with a unique ID. Only an authorized RFID tag can pass through the verification process performed by an RFID database. Typically, an RFID database can serve multiple RFID readers simultaneously to have a better coverage area for receiving data (Jia et al., 2019).

2. **RFID reader** - It is used as a medium to transmit verified data sent by an RFID tag to an RFID database. Verified data successfully read by the RFID reader from the RFID tag is transmitted to the RFID database for verification (Jia et al.,

2019).

3. **RFID tag** - RFID tag is used to store a unique ID and represents an object or person. A person's information can describe as a unique ID, which holds in RFID database (Jia et al., 2019).

Figure 2.1 shows the process of how an RFID reader reads data from and writes data to an RFID tag. When the RFID reader sends data to an RFID tag, this defines as a write operation. When an RFID tag sends data to an RFID reader, this process defines as a read operation.

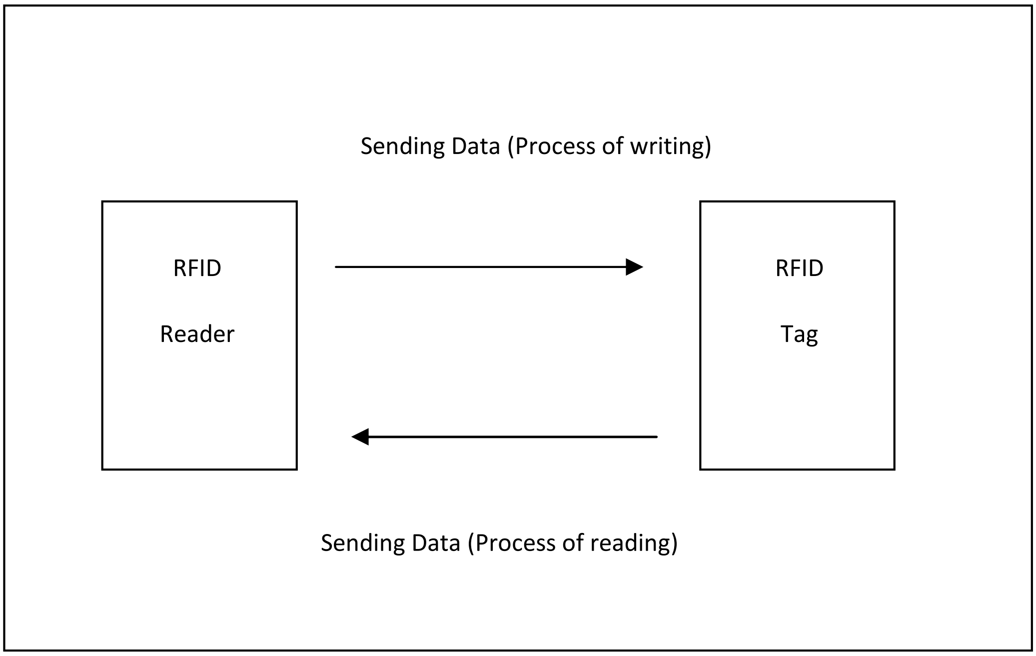

Figure 2.1: Reading or writing data on RFID devices

The types of channels that operate on RFID readers divided into control and data channels. The control channel is used for communication between RFID readers, while the data channel is for communication between the RFID reader and tag.

RFID is one of several technologies grouped under the term auto- ID processes that identify objects automatically with as little human intervention as possible (Zhang, Wang, Yu, Lyu, Mao, Periaswamy, Patton and Wang, 2019). An advantage of this technology compared to other traditional identification methods available to date is that no line of sight is required. The RFID tag can read the RFID tag wirelessly in any orientation, and it is the only technology that can read by multiple objects simultaneously (Zannas et al., 2018). The RFID tag consists of an antenna and a chip. The chip uses to store a unique serial number that represents a person or an item. An RFID database stores unique serial numbers that are assigned to authorize the RFID tag. The RFID reader equips with an antenna and a chip. It uses to establish communication with the RFID database to verify data from the RFID tag or write data to the RFID tag. The purpose of an antenna attached to the RFID tag and the RFID reader is to enable the sending or receiving of signals between the two. Figure 2.2 shows the authentication process involving the RFID database, RFID tag, an RFID reader in an RFID system.

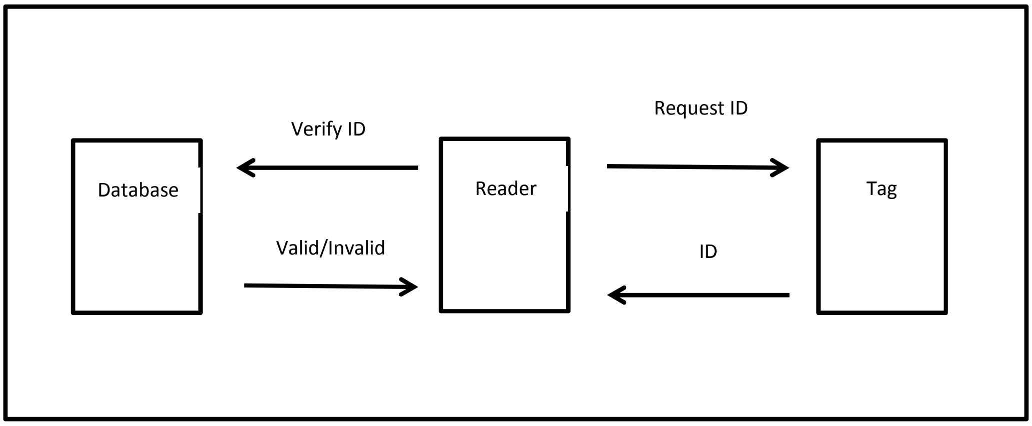

Figure 2.2: Authentication process in RFID system

A description of the authentication process in the RFID system as follows:

1. Initially, the RFID reader sends a signal to wake up the passive RFID tag and then requests a unique ID from the RFID tag.

2. Once the RFID tag is powered up; it sends a unique ID to the RFID reader.

3. RFID reader forwards a unique ID to the RFID database for verification.

4. After the received ID verifying, the RFID database informs the RFID reader of the validity of the ID.

Individual items can be identified, tracked, and categorized using the RFID system without human intervention.

2.1.1 Applications of RFID

The RFID system uses in various fields, such as the following:

- **Medical**: RFID tags placed on prescription pill bottles for visually impaired people. A special RFID reader provides audible information about the prescription's name, instructions, and warnings (Buffi et al., 2018).

- **animal identification**: Low-frequency RFID tags are implanted in animals, whether wild or domestic, can read to provide information such as sex, name, diseases, etc. (Buffi et al., 2018).

- **Tracking**: High-frequency RFID tags used to track library books, luggage, inventory, and even credit cards. American Express has a new service called Express Pay. The feature implemented on the blue credit card American Express uses RFID technology (Buffi et al., 2018).

- **geology**: RFID transceivers relay seismic information to RFID readers. The purpose is to simplify the process of data acquisition (Buffi et al., 2018).

- **Automotive**: Michelin has launched a program to embed RFID tags in their tires. In addition, Toyota and Lexus vehicles have a feature called the Smart Key option that uses an active RFID tag to allow drivers to unlock doors and roll down windows without taking the key out of their pocket (Buffi et al., 2018).

2.1.2 Types of RFID Tags

Three types of RFID tags are available on the market. The functionality of each type of RFID tag is as follows:

- Passive RFID tag - The passive RFID tag has no internal power supply, but a small electric current is generated in the antenna when an incoming signal reaches it. The amount of current generated by an electromagnetic field is enough to activate a passive RFID tag. Usually, it is enough to transmit simple information such as the ID number. Passive RFID tags can only activate from a distance of a few millimeters up to 6 meters.

- Active RFID tag - Active RFID tags contain an internal power source that enables a more extended read range and provides a large memory. The power source allows the active RFID tag to store information sent from a transceiver. In general, an active RFID tag size is larger than that of a passive RFID tag. Active RFID tag data can read from a few meters away, and the battery life is longer. The advantages of using active RFID tags include accuracy, reliability, and better performance in adverse environments such as humid or metallic environments (Ma et al., 2019).

- Semi-Passive RFID Tag - Semi-passive RFID tag uses an internal power source to monitor environmental conditions. However, it requires a radio frequency signal sent from the RFID reader to power it. An external power source uses to increase the signal strength of the semi-passive RFID tag and monitor environmental conditions such as temperature and shock. The other features are similar to those of the passive RFID tag (Ma et al., 2019).

The frequency ranges used for communication between RFID tags; an RFID reader divides into four categories: Low Frequency 125 or 134.2 kHz, High Frequency 13.56 MHz, UHF 868 to 956 MHz and Microwave 2.45 GHz (Athauda and Karmakar, 2019).

2.1.3 Classes of RFID Tags

Nowadays, there are six classes of RFID tags available in the market. RFID tags classify into class 0, class 1, class 2, class 3, class 4, and class 5. Each class has its specific reading and writing capabilities. Descriptions for each class of RFID tags as follows:

- **class 0** - Can only be used with passive RFID tags (read-only). It uses in the UHF band (Lin et al., 2018).
- **Class 1** - To write data once and read data many times on an RFID tag. It uses in UHF and HF bands (Lin et al., 2018).
- **Class 2** - Passive RFID tag uses to read and write data many times (Lin et al., 2018).

- **class 3** - RFID tag uses to read and write data attached to a sensor onboard. It uses to detect parameters such as temperature, pressure, and motion. It can be semi-passive or active (Lin et al., 2018).
- **Class 4** - RFID tag uses to read and write data with an integrated transmitter. It uses to communicate with other RFID tags or RFID readers (Lin et al., 2018).
- **class 5** - It is similar to the class 4 RFID tag. However, it has an additional function that uses to turn on other RFID tags or RFID readers (Lin et al., 2018).

2.1.4 Types of Authentication in RFID Protocol

In general, the authentication process in RFID protocol is essential to prevent counterfeiting (Yao et al., 2019). Descriptions for each type of authentication in RFID protocols as follows:

- RAO - The challenge c_1 sent by the RFID reader is a function of the key k. The RFID tag performs the same function with the same key k when it receives the challenge c_1. If the result generated by the RFID tag is equal to the challenge sent by the RFID reader, as shown in Figure 2.3, it accepts the RFID reader. Otherwise, it rejects the RFID reader (Li et al., 2019). The purpose of implementing the RAO protocol is to prevent an unauthorized RFID reader from accessing the RFID tag (Li et al., 2019).
- TAO - Upon receiving the challenge c_1 sent by the RFID reader, the RFID tag returns a response $R(c_1)$, which is a function of the challenge c_1. The RFID reader verifies the correctness of $R(c_1)$ via the RFID database and accepts the

RFID tag if it is correct or rejects the RFID tag if it is incorrect (Sun and Mu, 2019).

- TRA - It is a combination of RAO and TAO protocols. Initially, the RFID reader sends a random number c_1 as a challenge and receives the response $R(c_1)$ from the RFID tag. Next, it verifies the correctness of $R(c_1)$ using the RFID database (Sun and Mu, 2019). If it is correct, it accepts the RFID tag and proceeds with authentication by sending another challenge c_2 to the RFID tag. If not, it rejects and aborts the authentication process. If the RFID tag has already gone through the authentication process requested by the RFID reader, it verifies the challenge c_2 sent by the RFID reader. If it is correct, the RFID tag accepts it; if not, the RFID reader rejects it.

- RTA - Similar to the TRA protocol, the RTA protocol works with a combination of the RAO and TAO protocols. In TRA protocol, the RFID tag responds to the c_1 challenge without checking its validity. But the RTA protocol works with the RFID tag by first verifying the challenge $R(c_1)$ sent by the RFID reader before sending the response $R(c_1)$ to the RFID reader (Sun and Mu, 2019). If $R(c_1)$ is correct, the RFID tag accepts the RFID reader. If it is false, it rejects and aborts the authentication request. If the RFID reader has already passed the authentication requested by the RFID tag, it starts authenticating the RFID tag by checking the correctness of the response $R(c_1)$ using the RFID database. If it is correct, it accepts it; if not, it rejects the RFID tag.

General steps of TAO protocol used for the authentication process in RFID system as follows:

1. RFID reader sends a random number (c_1) to RFID tag.

2. Once the RFID tag receives the random number; it uses the secret key (k) to encrypt.

3. Encryption R(c_1) generated by RFID tag sent to the RFID reader.

4. Once the RFID reader receives the result of the encryption R(c_1) sent by the RFID tag, it cheques the correctness of R(c_1) via the RFID database and accepts the RFID tag if it is correct or rejects it if it is incorrect.

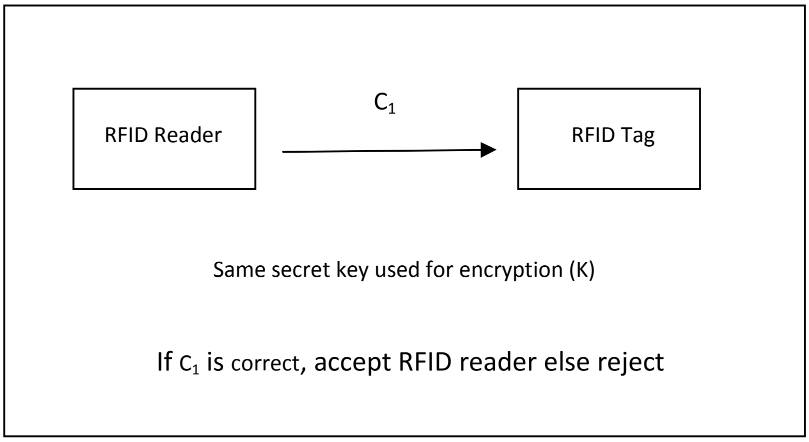

Figure 2.3: RAO Protocol

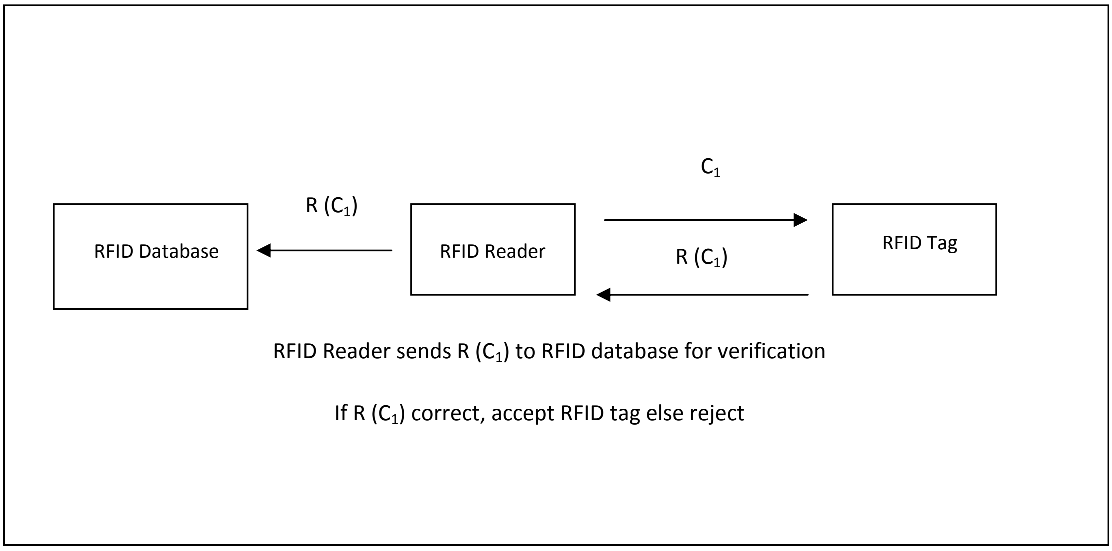

Figure 2.4: TAO Protocol

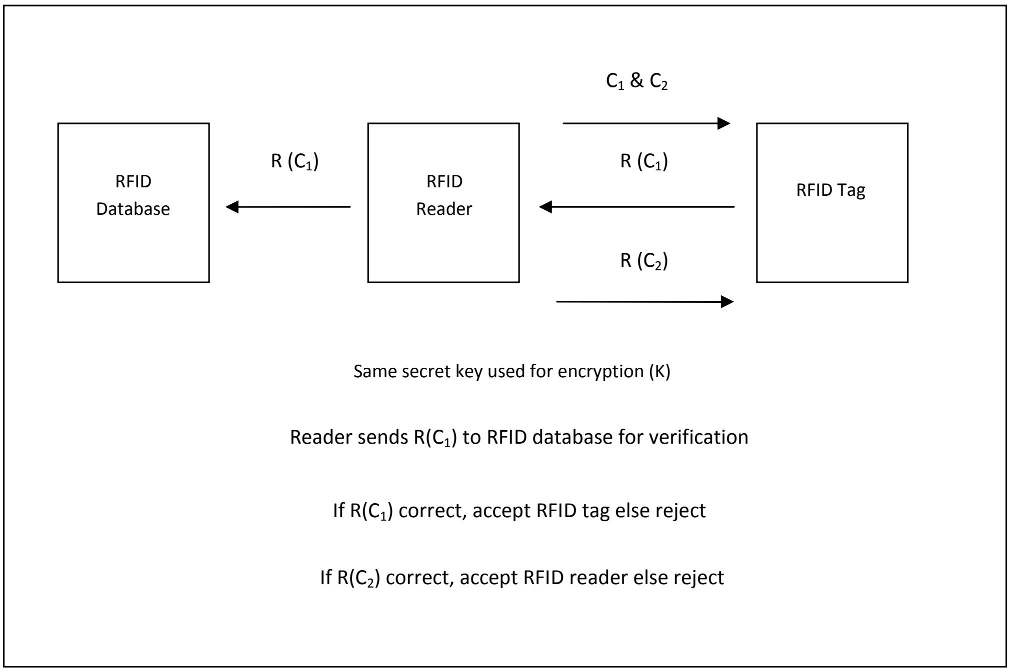

Figure 2.5: TRA Protocol

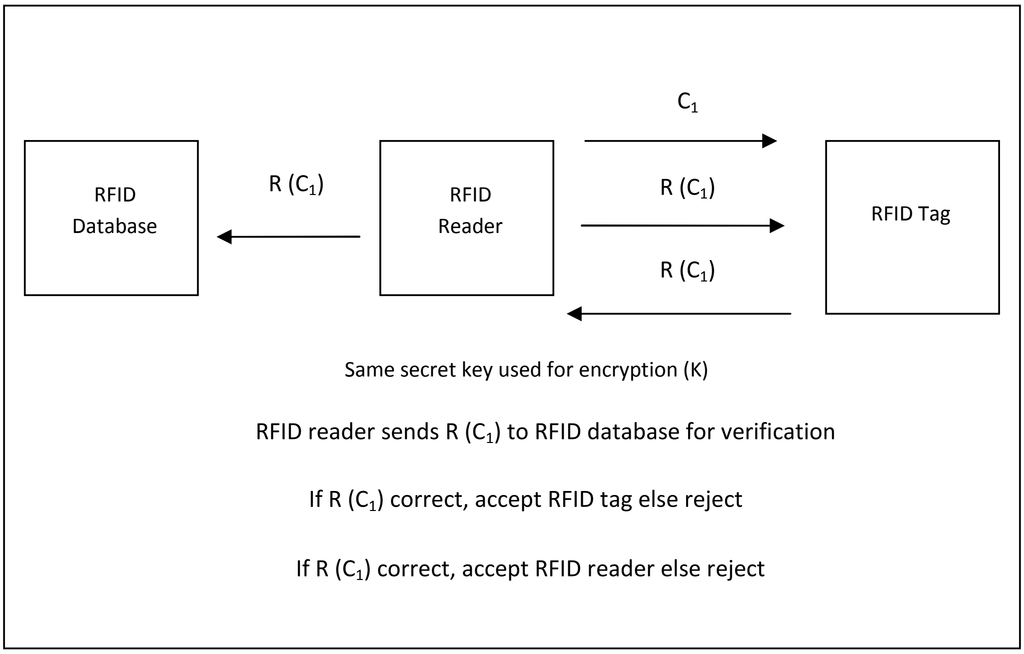

Figure 2.6: RTA Protocol

2.2 Anti-Collision Protocols

It is essential to consider collision scenarios between RFID devices in any designed RFID protocol using a particular RFID network topology. Anti-collision protocols are a set of rules for the successful transmission of information through a medium (Benny et al., 2018). These are critical to the performance of an RFID system (Benny et al., 2018). Without an anti-collision protocol, the response from different tags would collide, thereby prolonging the identification (Benny et al., 2018). ALOHA-based protocols are the most commonly used anti-collision protocols (Li et al., 2019). They are divided into ALOHA and slotted ALOHA protocols (Li et al., 2019).

2.2.1 ALOHA

A passive tag sends its unique ID as soon as it enters the field of a reader (Shen and Choo, 2018). In the ALOHA protocol, RFID tags attempt to communicate with the reader without checking the availability of the channel (Shen and Choo, 2018). The main drawback of this protocol is that a collision may occur if two tags send their frames (Ma et al., 2018) simultaneously. If a collision occurs, the frames sent will destroy (Ma et al., 2018). The only solution to avoid this collision is to resend the collided frames after an unknown amount of time (Ma et al., 2018). Here, the vulnerable period (period in which a collision can occur) is twice the frame length (Ma et al., 2018).

2.2.2 Slotted ALOHA

Implementation of Slotted ALOHA protocol is to improve the efficiency or throughput of the pure ALOHA protocol (Jiang et al., 2019). Unlike the pure Aloha, in the slotted ALOHA, the timeline is divided into slots of a certain length (Khalil et al., 2019). Therefore, it cannot transmit data whenever data is ready (HajMirzaei, 2019). Instead, tags can only transmit data at the beginning of a particular time slot (HajMirzaei, 2019). When the data to be transmitted is ready, it should wait for the start of the next time slot (Su et al., 2019). So this protocol is free from partial collisions. Slotted Aloha increases the efficiency compared to pure ALOHA (Su et al., 2019). The problem with this protocol is that collisions occur when more than one tag transmits at the beginning of the same slot, and also time synchronization is required (Su et al., 2019). The only solution is to retransmit the collided frames after waiting for an unknown amount of time (Zhou et al., 2019). The vulnerable time has reduced from twice the frame length in pure ALOHA to a single frame length (Zhou et al., 2019). Even though the collision rate has reduced compared to the pure ALOHA protocol, it still cannot eliminate collisions (Zhou et al., 2019).

2.2.3 Framed Slotted ALOHA

The main disadvantage of the slotted ALOHA algorithm is that it cannot work effectively when the number of RFID tags in the system increases (Yang et al., 2018). Thus, the Framed slotted ALOHA algorithm was proposed to overcome the problem (Yang et al., 2018). The biggest distinction of FRAME Slotted ALOHA's algorithm from pure slotted ALOHA's algorithm is that the RFID tag is only allowed to transmit its data in one of the slots of a frame (Parada et al., 2018). In other words, the RFID tag can only transmit its data in a frame at most once (Parada et al., 2018). A deliberate comparative study between Framed ALOHA and the Slotted ALOHA algorithm discussed in the paper (Parada et al., 2018).

2.2.4 Dynamic Framed Slotted ALOHA

The major drawback of Framed slotted ALOHA algorithm is the number of tags is always unknown to the reader because all the frames would have the same length, which means the number of slots in each frame is fixed (Wijayasekara et al., 2019). Therefore, two major problems will arise. Firstly, the number of slots a frame offers is far lesser than the number of available tags, and the second one is the condition where the number of slots of a frame offers is far larger than the number of RFID tags that are available (Wijayasekara et al., 2019). From the first scenario, as the tag amounts exceed slot availability, there may be collisions in all of the slots of a frame;