

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Institut National Polytechnique de Toulouse (INP Toulouse)

Discipline ou spécialité :

Réseaux, Télécommunications, Systèmes et Architecture

Présentée et soutenue par :

M. AHMAD KHALID

le lundi 13 novembre 2017

Titre :

A Secure Localization Framework of RAIN RFID Objects for Ambient Assisted Living

---

Ecole doctorale :

Mathématiques, Informatique, Télécommunications de Toulouse (MITT)

Unité de recherche :

Institut de Recherche en Informatique de Toulouse (I.R.I.T.)

Directeur(s) de Thèse :

M. FABRICE PEYRARD

M. EMMANUEL CONCHON

Rapporteurs :

M. ABDENNACEUR KACHOURI, ECOLE NALE D'INGENIEUR DE SFAX TUNISIE

M. SYLVAIN GIROUX, UNIVERSITE DE SHERBROOKE

Membre(s) du jury :

Mme BEATRICE PAILLASSA, INP TOULOUSE, Président

M. CLAUDE TETELIN, CNRFID, Membre

Acknowledgements

The work presented in this thesis was carried out at the Institut de Recherche en Informatique de Toulouse (IRIT) of the Ecole Supérieure d'Electrotechnique, d'Electronique, d'Informatique, d'Hydraulique et des Télécommunications (ENSEEIHT). I thank the IRIT team for welcoming me to the laboratory.

I would like to thank the Malaysian Government especially the Majlis Amanah Rakyat (MARA) and the Universiti Kuala Lumpur (UniKL) for their financial support that enables me to further my studies.

A special mention and gratitude to my Directeur de Thèse, Dr Fabrice PEYRARD for having accepted to direct this thesis and for all his invaluable advice and support. Also my deep gratitude to my second supervisor, Dr Emmanuel CONCHON, Maître de Conférence at the Université de Limoges. I thank both of them for their dynamism, scientific skills and availability throughout these four years which have enabled me to carry out my study smoothly.

I would like to express my sincere thanks to Prof Abennaceur KACHOURI, Professor at the Université de Sfax, Tunisia and Prof Sylvain GIROUX, Professor at the Université de Sherbrooke, Canada, who has given me the honour of accepting to be the rapporteur for this thesis and for providing me with their invaluable comments and insights.

I would also like to thank Prof Béatrice PAILLASSA, Professeur at the Université de Toulouse and Mr Clause TETELIN, Technical Director at the Centre Nationale de RFID (CNRFID) for their interest in my research by participating as the jury.

My love and gratitude goes to my wife, Irene Riana ISMAIL, who has been patient, encouraging and motivating me at all times during this

thesis work. I also thank my six children; Danial, Luqman, Anwar, Lutfi, Haris and Anaïs for supporting and cheering me up throughout my years here. My gratitude also goes to my mother and my late father for their encouragements and moral support.

I would also like to thank my colleagues and friends in the laboratory. Among them, I would like to thank Farouk, Mohamed, Hamdi, Aziz, Qiankun and Kuljaree. Last but not least, i would like to thank the administration team at the ENSEEIHT office, namely Sam, Isabelle and Annabelle for their kindness. I express my deepest gratitude to all and wish them well.

Abstract

Internet of things (IoT) is currently on our doorsteps. Numerous domains have benefited from this technology. It ranges from a simple application such as identifying an object up to handling a more complex system. The Radio Frequency IDentification (RFID) is one of the enabling technologies that drive the IoT to its position today. It is small, cheap and does not require any additional power sources. Along with its ubiquitous functionality, this technology enables the positioning of an object within a specific area. Ambient Assisted Living (AAL) is one of the many domains that benefit from the IoT. It aims at assisting elderly people in their daily routines by providing new assistive services in smart homes for instance. RFIDs in a smart home come as a great help to an elderly person, for example, to find an object that they misplaced. However, even with all its benefits in simplifying our lives, it is unfortunately double-edged where the advantage that it brings to an object could in turn go against itself. Indeed to be able to help the older adults to locate an object, the system requires certain data in relation to the positioning of the object and its identification. As the passive RFID tag coverage is very small, once its presence is detected, it is difficult to hide it. The ability of this technology in localizing objects gives an opportunity to a third person to take an advantage of the system.

In parallel with the persistent and constant need of privacy and secrecy by the users, the objective of this thesis consists of improving the privacy in localizing an object through a new protocol based on the latest version of the RFID second generation passive tag. The proposed protocol must be able to prevent an object from being identified and located by unauthorized parties or a malicious reader. The first

contribution of this work is the assessment of the RFID anti collision management. It is performed through the creation of an OMNET++ framework, modelled and built based on the latest RFID standard developed by GS1 and incorporated by ISO/IEC called Gen2V2 (RFID class 2 Generation 2 Version 2). It is a passive RFID tag that does not require any internal power sources to operate. It communicates using the UHF frequency. The Gen2V2 standard provides a list of cryptographical suites that can be used as a method to authenticate a tag and a reader. This new generation of tags is supported by an alliance of manufacturers called RAIN (RAdio frequency IdentificatioN) that promotes the adoption of the Gen2V2. The anti collision management overall performance is then compared with its theoretical value and four of its cryptographical suites namely PRESENT80, XOR, AES128 and cryptoGPS. Among the performances evaluated within the framework is the number of collisions and the duration required to interrogate a group of tags. Note that an addition of a localization functionality within the framework reveals that exchanged messages through wireless channel prior to the authentication can lead to a malicious localization of an object. To increase the localization privacy within AAL application, we propose therefore a second contribution which is a new localization method that is based on the current Gen2V2 standard exchanges by anonymizing the tag identity.

Résumé

Internet des objets (IoT) est actuellement à notre portée. De nombreux domaines ont bénéficié de cette technologie. Cela va d'une application simple, comme l'identification d'un objet jusqu'à la gestion d'un système plus complexe. L'identification par radiofréquence (RFID) est l'une des technologies qui a une part importante dans l'IoT aujourd'hui. C'est une technologie embarquée, peu onéreuse et qui ne nécessite aucune source d'alimentation supplémentaire dans le cas de tag passif. Avec sa fonctionnalité omniprésente, cette technologie permet d'identifier un objet dans une zone spécifique. L'Assistance et l'Autonomie des personnes à Domicile (AAL) est l'un des nombreux domaines qui bénéficient de l'IoT. Il vise à aider les personnes âgées dans leurs routines quotidiennes en fournissant de nouveaux services d'assistance dans les maisons intelligentes (smart home). La présence de RFID dans une maison intelligente est d'une grande aide pour une personne âgée et/ou déficiente, par exemple, pour l'aider à trouver un objet dans son environnement quotidien.

Cependant, parmi tous les avantages qu'apporte l'IoT dans notre vie quotidienne certains peuvent s'avérer de réels inconvénients en particulier la localisation et le respect de la vie privée. En effet, pour pouvoir aider les personnes âgées à localiser un objet, le système nécessite certaines données relatives au positionnement de cet objet, tout au moins son identification. Étant donné que la couverture de l'étiquette RFID passive est très faible, une fois sa présence détectée, il est difficile de la masquer. La capacité de cette technologie à localiser des objets donne l'occasion à une tierce personne de profiter du système.

Parallèlement au besoin persistant et constant de confidentialité par les utilisateurs, l'objectif de cette thèse consiste à améliorer la confi-

dentialité dans la localisation d'un objet grâce à un nouveau protocole basé sur la deuxième génération de RFID passive. Le protocole proposé doit pouvoir empêcher un objet d'être identifié et localisé par des parties non autorisées ou par un lecteur malveillant. La première contribution de ce travail est l'évaluation de la gestion anti-collision RFID. Elle est réalisée par la création d'un modèle OMNET++, construit sur la base de la dernière norme RFID développée par GS1 et adaptée par ISO / IEC appelé Gen2V2 (RFID classe 2 Génération 2 Version 2). Les étiquettes (tag) RFID passives conforment à Gen2V2 communiquent dans la bande de fréquence UHF (900MHZ) avec des portées de plusieurs dizaines de mètres. La norme Gen2V2 propose une liste de suites cryptographiques qui peuvent être utilisées comme méthodes pour authentifier une étiquette et un lecteur. Cette nouvelle génération d'étiquettes est soutenue par une alliance de fabricants appelée RAIN (RAdio frequency IdentifatioN) qui favorise l'adoption du Gen2V2. Nous évaluons dans cette thèse les performances globales du protocole anti-collision et nous comparons ensuite quatre de ces suites cryptographiques, à savoir PRESENT80, XOR, AES128 et cryptoGPS pour garantir l'authentification lecteur/tag. Parmi les performances évaluées dans ce modèle, nous nous sommes intéressé au nombre de collisions et à la durée requise pour interroger un groupe d'étiquettes. Nous avons intégré la fonctionnalité de localisation dans le modèle en s'appuyant sur les messages échangés avant l'authentification, ce qui peut conduire à une localisation malveillante d'un objet. Pour augmenter la confidentialité de la localisation au sein des applications AAL, nous proposons donc une deuxième contribution qui est une nouvelle méthode de localisation basée sur les échanges standard Gen2V2 en anonymisant l'identité de l'étiquette.

Contents

Abstract iii

Résumé v

Contents vii

List of Figures xi

List of Tables xiii

Acronyms xv

1 Introduction 1

1.1 Radio Frequency Identification (RFID) at a glance 2

1.2 Motivation 4

1.2.1 Research focus in IoT 5

1.2.1.1 Logistics 5

1.2.1.2 Retail 6

1.2.1.3 SmartHome 6

1.2.1.4 Healthcare 6

1.2.2 Application of the IoT to improve the Quality of Life 7

1.3 Simulation Model 8

1.4 Thesis Outline 8

2 State of the Art 9

2.1 General overview of Internet of Things (IoT) 9

2.2 Ambient Assisted Living (AAL) . . . 12
2.2.1 AAL Challenge . . . 13
2.2.2 AAL Technology . . . 14
2.3 Radio Frequency Identification (RFID) . . . 14
2.3.1 Radio Frequency Identification (RFID) air interface standards 15
2.3.1.1 Below 135kHz . . . 15
2.3.1.2 NFC 13.56MHz . . . 15
2.3.1.3 RFID 860MHz to 960MHz . . . 16
2.3.1.4 RFID 2.45GHz . . . 16
2.3.2 RFID Classification . . . 17
2.3.2.1 Active tags . . . 18
2.3.2.2 Semi active tags . . . 18
2.3.2.3 Passive tag . . . 19
2.3.3 RFID standard . . . 20
2.3.3.1 RFID Generation 1 . . . 20
2.3.3.2 RFID Class 1 Generation 2 Version 1 (C1G2) . . . 20
2.3.3.3 RFID Class 1 Generation 2 Version 2 (Gen2V2) . . . 21
2.3.4 RAIN RFID tag collision management . . . 23
2.3.4.1 Frame Slotted Aloha efficiency . . . 25
2.3.4.2 Collision Management Protocol . . . 26
2.3.5 RFID Identification . . . 28
2.4 Security . . . 29
2.4.1 Passive Attack . . . 30
2.4.1.1 Eavesdropping . . . 30
2.4.1.2 Relay attack . . . 30
2.4.2 Active Attack . . . 32
2.4.2.1 Desynchronization attack . . . 32
2.4.2.2 Man in the middle attack . . . 32
2.4.3 Authentication . . . 33
2.4.4 Advanced Encryption Standard: AES128 . . . 35
2.4.5 PRESENT-80 . . . 38
2.4.6 XOR . . . 43
2.4.7 cryptoGPS . . . 45

2.5 2D Tag Localization 48
2.5.1 Trilateration 49
2.5.1.1 Roundtrip Time of Flight (RToF) 50
2.5.1.2 Angle of arrival (AoA) 51
2.5.1.3 Received Signal Strength (RSS) 52
2.5.1.4 Phase of Arrival (PoA) 53
2.5.2 Trilateration calculation 53
2.6 Privacy 56
2.6.1 Localization Privacy with RFID tags 58
2.6.2 Privacy Threat in RFID localization 59
2.6.3 RFID Privacy Definitions 60
2.7 Conclusion 61

3 Gen2V2 Framework in OMNET++ 63
3.1 OMNET++ 63
3.2 OMNET++ structure 64
3.2.1 Network definition files (NED) 65
3.2.2 Simple module 66
3.2.3 Compound module 66
3.2.4 Communication channel 66
3.2.5 OMNET++ coding 67
3.2.6 OMNET++ troubleshooting 67
3.3 Gen2V2 framework 69
3.3.1 Gen2V2 hierarchy 71
3.3.1.1 Module: ModuleTag 72
3.3.1.2 Submodule: authenticationTag 73
3.3.1.3 Submodule: Radio Medium 73
3.3.1.4 Module: adversary 74
3.4 Anti-collision management 74
3.5 Cryptographic Suites within the framework 77
3.6 Cryptographical suites evaluation results 78
3.6.1 Evaluation parameters 78
3.6.2 Framework execution 79

3.6.3 Simulation results 79
3.7 RFID localization 81
3.7.1 Module: Server 82
3.7.2 Submodule: localization 83
3.7.2.1 Scenario 1: Wait for all tags 84
3.7.2.2 Scenario 2: Tag by tag 85
3.7.2.3 Scenario 3: Realtime update 88
3.7.2.4 Localization results 89
3.8 RFID tag privacy 90
3.9 Localization privacy 92
3.10 Conclusion 94

4 Conclusion and Perspectives **95**
4.1 Conclusion 95
4.2 Prespectives 96
4.2.1 Short term perspectives 96
4.2.2 Long term perspectives 97

Appendix **99**

Publications **105**

Bibliography **107**

List of Figures

2.1 The Internet of Things 9
2.2 Example of tags 11
2.3 Ambient Assisted Living 12
2.4 RFID frequency 17
2.5 RFID type 18
2.6 RFID classification 18
2.7 Gen2V2 communication exchange 21
2.8 ALOHA 23
2.9 Slotted Aloha Efficiency 26
2.10 Gen2V2 Collision Management Protocol 28
2.11 RFID security 30
2.12 Eavesdropping 31
2.13 Relay Attack 32
2.14 Man-in-the-Middle 33
2.15 RFID security classification 34
2.16 Gen2V2 Improvement 35
2.17 AES128 chart 36
2.18 AES128: Authentication protocol exchange between reader and tag 37
2.19 PRESENT-80: Protocol exchange between reader and tag 40
2.20 PRESENT80 chart 41
2.21 XOR: Protocol exchange between reader and tag 43
2.22 XOR chart 44
2.23 CryptoGPS chart 47
2.24 cryptoGPS: Protocol exchange between reader and tag 48

2.25 Roundtrip Time of Flight 50
2.26 AoA 51
2.27 Trilateration 54
2.28 Localization Privacy Topology 1 58

3.1 OMNET++ network definition 65
3.2 OMNET++ simple module 66
3.3 OMNET++ compound module 67
3.4 OMNET++: Event Log 68
3.5 Scenario 1: QueryAdjust at the end of the frame 69
3.6 Scenario2: QueryAdjust right after collision 70
3.7 ModuleTag Topology 72
3.8 NodeTag Topology 72
3.9 Collisios vs Q values 75
3.10 Total duration vs Q values 76
3.11 Reader's collision management 76
3.12 Slotted Aloha Efficiency 77
3.13 Efficiency comparison with 100 tags 78
3.14 Authentication duration fo 20 tags 80
3.15 Authentication duration for 100 tags 81
3.16 Localization Topology 82
3.17 Scenario summary 85
3.18 Scenario 1 86
3.19 Scenario 1 87
3.20 Scenario 2 88
3.21 Scenario 3 89
3.22 Localization duration 90
3.23 Gen2V2 91
3.24 Localization Privacy Topology 2 93

List of Tables

2.1 Tag classification vs resource 19
2.2 Q vs total slot number 24
2.3 Efficiency values 25
2.4 AES128 request format 38
2.5 AES: Substitution Box 39
2.6 AES: Shifting columns to the left 39
2.7 AES: MixColumns 39
2.8 PRESENT-80 Substitution box 42
2.9 PRESENT-80 permutation box 42

3.1 AES128 request format 79
3.2 Tag distance from readers 84

Acronyms

AAL	**A**mbient **A**ssisted **L**iving
ACK	**ACK**nowledgement
ADL	**A**ctivities of **D**aily **L**iving
AES	**A**dvanced **E**ncryption **S**tandard
AoA	**A**ngle **o**f **A**rrival
CSI	**C**ryptographic **S**uite **I**ndicator
ECDLP	**E**lliptic **C**urve **D**iscrete **L**ogarithm **P**roblem
EPC	**E**lectronic **P**roduct **C**ode
FSA	**F**ramed **S**lotted **A**LOHA
GE	**G**ate **E**quivalent
IoT	**I**nternet **o**f **T**hings
ISO	**I**nternational **S**tandards **O**rganization
NED	**NE**twork **D**escription
NFC	**N**ear-**F**ield **C**ommunication
PoA	**P**hase **o**f **A**rrival
PRNG	**P**seudo**R**andom **N**umber **G**enerator
RAIN	**RA**dio frequency **I**dentificatio**N**
RFID	**R**adio **F**requency **ID**entification
RN16	16 bits **R**andom **N**umber
RSSI	**R**eceived **S**ignal **S**trength **I**ndicator
RTLS	**R**eal **T**ime **L**ocation **S**ervices

RToF	**R**ound**T**rip **o**f **F**light
ToA	**T**ime **o**f **A**rrival
ToF	**T**ime **o**f **F**light
UHF	**U**ltra **H**igh **F**requency

1 Introduction

The invention of the computer and the introduction of the Internet result in almost everything to be connected together. The idea of connecting objects is developing at an incredible speed and now covers an unbelievable number of areas. The Internet of Things (IoT) has driven numerous improvements in various domains. Thanks to the Internet of Things, every object that is connected to a network could now be tagged with an identification and is able to answer to various conditions in a smart way.

Historically, it started in the logistic area where the primary objective was to tag and/or to record an object for inventory purpose and to manage various stocks and movement of both raw materials and final products. However, it was not an intelligent system as the function was only limited to keeping track of the amount of things in stock. As more and more specialised inputs such as sensors are included in the system, it began to open up to various other possibilities.

Smart Environment is the fruit of ideas on a controlled environment where every object is connected to other objects and is able to go from performing a simple and specific task to providing more complex services. As an example, the ubiquitous system could perform tasks such as maintaining the humidity level of an area with humidifier/dehumidifier sensors, maintaining the optimum temperature with the air conditioning sensors, or maintaining optimum light intensity level with light related sensors. Smart Home is one of the derivative results of the Smart Environment where several features such as light and temperature are automatically regulated based on the owners' preferences.

Through the use of IoT, every connected object could be tagged with an identification and an answer to various conditions in a smart way. Many objects are

embedded with RFID tags such as clothings and books. Tags are specifically attached or sewn into the items to indicate the price or to act as an anti-theft system. Now with the invention of nanotechnology, it is possible to incorporate nano-tags directly in the constituting material of the objects. As IoT relates to almost everything, one needs to consider the essential requirements that fit in every scenarios. As today's population age keeps increasing, we can see more and more elderly people trying to live independently in their own house. However, with age, staying safe and independent is a major challenge. Ambient Assisted Living (AAL) has among its principal aims to help these people to achieve this goal and IoT can be an interesting solution to achieve that. Localization is needed to support AAL , for example, to locate the person at a specific moment. This is to help in monitoring their behavior during the day and at night so that the system can learn what are the person's behaviors that are considered normal and decide either if the person requires any help or if and when he is not behaving 'normally'. This function is useful in order to optimize the number of contact hours required by a helper to spend with a person. Thus at the same time to maximize the number of person that the helper can handle. Another possible reason is to help an elderly person to locate their belongings within the house. Each object can be tagged and identified to make their life easier. However, this does not come without any inconvenience. Indeed, if the elderly person can easily locate and identify their belongings, any other person that has the same arrangements can also perform the same operation. This will make their belongings and all related information to be exposed to everybody. And this is one of the numerous reasons AAL application is not accepted nor adopted in the market. In order to improve the acceptance of the system, the overall security and privacy of the system need to be enhanced.

1.1 Radio Frequency Identification (RFID) at a glance

The idea of having the ability to manage an object from afar, either to gather information or to have full control of it has always inspired everybody. A simple example is the invention of the television remote control which facilitates the con-

trol of the television channels but does not require the user to be in the proximity to the television set.

Research on the identification of objects is not new. It has been going on for over ten years. It started with inventorying system, initially to replace the barcode system that requires physical access to the object as in a supermarket where the cashier system identifies the object one by one with the help of a hand held reader. It is based on a laser technology that requires a clear vision from the reader to the tag. It could be time consuming to identify each items.

Ever since its inception, RFID tag has been introduced and used in a numerous domains. For example, a tag serves as an identification tool for animals as defined in ISO standards [1, 2, 3] and/or any objects in general. A tag can also act as a method to authenticate the owner of an object in an access control system such as in a car immobiliser or parking/building entrance by using a MIFARE or NFC (Near Field Communication) card as a method of authentication (refer to ISO14443 [4]). Again, a tag can be used as a payment method due to the ability to authenticate the user. This feature is fundamental in order to guarantee secured transactions. Various industries have tried to propose their solutions in this matter, such as Apple Pay [5], Android Pay [6], Samsung Pay [7], Orange Cash [8]. Only time would tell the winner of this race.

The introduction of a Radio Frequency IDentifier helps to improve the productivity. It requires the item to be within the readers' communication range. Therefore no object handling is needed. This helps in reducing the amount of time needed to identify a group of items. On top of that, all items are uniquely identified. A few years later, the improving technology permits the use of wireless technology within the identification process. With this new technology, the development shifted from an object that could only identify itself, towards an object that could react based on a request. However, this enables everybody to hear the *conversation* done between the object and the *reader*. This creates a security issue to the system. Current researches are heading towards the security and privacy of the system. Many tries to handle the authentication of different component within the system and tries to identify how secure it is. Some researches focuses on the information exchanged. Could anybody intercept the data? What kind of data could be released? Could someone hijack the object? All of these issues will be

addressed in the following sections.

1.2 Motivation

The fear of not being able to ensure security and privacy of the connected object is slowing the adoption rate of the IoT in sensitive domains such as AAL. Earlier deployment does not consider the security and privacy parameters as a major issue. But, the risk exists due to the fact that the data exchange is going through a wireless communication channel. As a result, anybody could easily intercept the transmitted information.

On a positive side, a connected object offers endless possibilities to improve our day to day tasks in controlling machines, access and stocks. One could imagine that one day people could have their shopping list updated automatically as the stock in the refrigerator or the pantry reduces, their electrical appliances to switch on automatically during the lowest rate or to set their preferred environment before arriving home such as the air conditioning, lights, etc. and to set the microwave to reheat their food to be ready to be served.

With regards to senior persons' lives, they tend to be forgetful as they age and often misplaces their belongings. The current technology in the Internet of Things (IoT) can assist them in solving this issue. IoT covers various domain, including inventory. The inventory system is known for managing stocks. In the past, it served in monitoring stocks in a warehouse. Nowadays it can be applied to other groups of items such as groceries, medical supplies, etc. For an elder, the use of inventory in his daily living could prevent any shortage of things he owns or needs such as his medicine, for example, during the holiday period, where all pharmacies are closed. Tagging each of their belongings with an electronic tag does not only help in managing their inventory, but it can also assist them in recording the location of each item. It can be done systematically or based on ad hoc requests.

In order to reduce the burden on the system, it should have at least the last known position of the previous request. However, the frequency of the localisation process should be refined from one user to another. If the object is within a house and is not a mobile object, the detection could be done based on an ad hoc request. Otherwise, the detection could be configured once in every few seconds or minutes.

Theoretically, this can be done by sending a timely beacon signal.

The ability to position a tag is based on the detection of communication signal between the object and its sensor. The drawback of this method is that it is not only visible to the dedicated sensors, but it is also visible to all the other sensors within the range. Therefore, if there is no effort made to hide the position of the object, it is therefore virtually known to everybody. Hence, this could compromise the individual's privacy. This personal privacy includes information on their health condition, where a list of medications could reveal that they are currently being treated for a particular ailment. As a result, this could put the person in a disadvantaged situation or worse, he could be stigmatised because of his illness.

As the location of every object to the person could be known to everybody, for a burglar, it is like being able to pick a house to be burgled from a promotional brochure, where every item is listed in detail. It will be worse for the house owner if the burglar could even detect the location of the house's security alarm. The fact that whatever items in the house are easily located brings another issue, where within a limited time the burglar could identify the most expensive items.

1.2.1 Research focus in IoT

As the time progresses, the IoT research diversifies towards the development of services that could be beneficial to humankind. Our research focuses on domains that use the RFID technology. Therefore, we are interested in the evolution trend of the connected object in particular in areas such as leisure, logistics, transportation, retail, smart infrastructure, aeronautical industry, healthcare and environment.

1.2.1.1 Logistics

IoT derives a lot from the logistics domain. It helps to identify a particular object from a huge number of other objects. It is a very good example of RFID applications scenario in IoT. Its ability improves the inventory system by quickly determining if the raw material is about to be ordered and re-adjust the reorder level based on the availability of every component. It also reduces the burden of

stock tracking, inventorying and after sales services. Among research in focusing in improving the inventory accuracy is done by Helstrom et al. in [9] and Fan et al. in [10].

1.2.1.2 Retail

In retail sevices, RFID tags are used as an anti theft device. It prevents the merchandise from being stolen from the store. An unpaid item taken out from the store will trigger the alarm. As for the luxury items, the RFID tags are also used to prove the genuineness of the item. A counterfeiter can reproduce the object as similar as possible to the original one but can never duplicate the authenticity tag that is normally embedded within the item. The decision either to integate the RFID tag on the object is also discussed by Piramuthu et al. in [11].

1.2.1.3 SmartHome

To be fully functional, a SmartHome relies on the support of different technologies. The RFID offers the functionality such as the door access control with the help of a smart card, various services involving garments such as cloth sorting by color, material, events, etc. The unique identification of the garment can also help to identify the optimum conditions in washing machine, in the dryer and during the ironing process. In the kitchen, the refrigerator can communicate the quantity of a tagged item. During a shopping trip, the owner can interogate the refrigerator about the existing stock and determine what needs to be bought.

1.2.1.4 Healthcare

Healthcare is one of the domains that benefits the most from the recent improvement in IoT. It enables the monitoring of the patient to be more accurate. The monitoring can be performed continously by using a wearable RFID that can incessantly feed the system with specific readings such as the glucose level as proposed by Cho et al. in [12]. With the bodycentric RFID tag, the patient movement in the ward can also be monitored. The system can monitor all their gestures and behaviors in order to help to identify the possible symptoms. The system can also detect if the patient is passively lying on the bed or lying motionlessly in the toilet.

This scenario is possible with the help of the bodycentric RFID system similar to the one mentioned by Manzari et al. in [13]. The system can also suggest to the doctor possible illness based on the patient's symptoms. It can provide the correct medication and its optimum dosage as discussed by Jara et al. in [14]. The use of RFID can reduce the human error of misinterpreting the doctor's or the pharmacist's handwriting. Having a unique indentification also helps in keeping track of the patient's medical record.

1.2.2 Application of the IoT to improve the Quality of Life

In IoT, an object is assumed to be able to identify itself. Each object has a unique identity. It is also considered to be able to collect information of its surrounding, such as temperature, humidity, etc. It should be able to communicate with others through a wireless connection. It should be able to make a decision based on a given situation and based on the data gathered, it should be able to react accordingly.

IoT covers multiple domains. In the smaller scale, it includes assisting a senior person on a day to day chores in a smart environment for example by switching on and off the lights, heater, etc. The IoT can help a senior to stay in his resident without going to a retirement home.

DOMUS *(DOMotics at the Université de Sherbrooke)* is one of many laboratories that focuses in helping people with cognitive disorders either through AAL or Smart Home. As an example, to assist an elderly with Alzheimer Desease, the *"Nighttime Assistance System"* is proposed by Radziszewski et al. in [15, 16] in order to help calm the person and incite him to go to sleep thus minimizing nighttime wanderings. Along with that, Bergeron et al. in [17] concentrated on the positioning of an indoor object in Smart Home environment in order to enable the object tracking in the future.

In healthcare, the introduction of IoT technology helps in reducing human error in either the prescription or administration of drugs. In a bigger scale, IoT supports the industrial automation with millions of tags in managing raw materials, production, stocks and after sales services [18, 19, 20, 21, 22, 23].

1.3 Simulation Model

The work for this thesis concentrates on the improvement of RFID localization privacy. In order to do so, it requires a working RFID framework. Due to the lack of availability of the framework, the development of a framework in OMNET++ based on the current standard is then proposed. All RFID principal aspects such as the shared medium, anti collision management, security and authentication are included in the implementation.

1.4 Thesis Outline

This manuscript is organised by as follows:

Chapter 2 introduces the IoT concept, AAL definitions and challenges, RFID standards and related issues in security, localization, privacy and localization privacy. This chapter also covers four out of nine cryptographical suites that is available to be used with the current standard.

Chapter 3 focuses on the newly modeled Gen2V2 framework within OMNET++ simulator based on the current standard, the implementation of tag anti-collision management, several cryptographical suites, tag localization and tag localization privacy. It also covers all results related to the investigation published in [24] along with localization and localization privacy results.

Chapter 4 concludes the work and discusses the short term and the long term perspectives

2 State of the Art

This chapter presents a general review of the Internet of Things within the Ambient Assisted Living. A discussion on the Radio Frequency Identification (RFID) as the enabling technology and the possibility of maintaining secrecy, in particular regarding the localization of the connected things are presented.

2.1 General overview of Internet of Things (IoT)

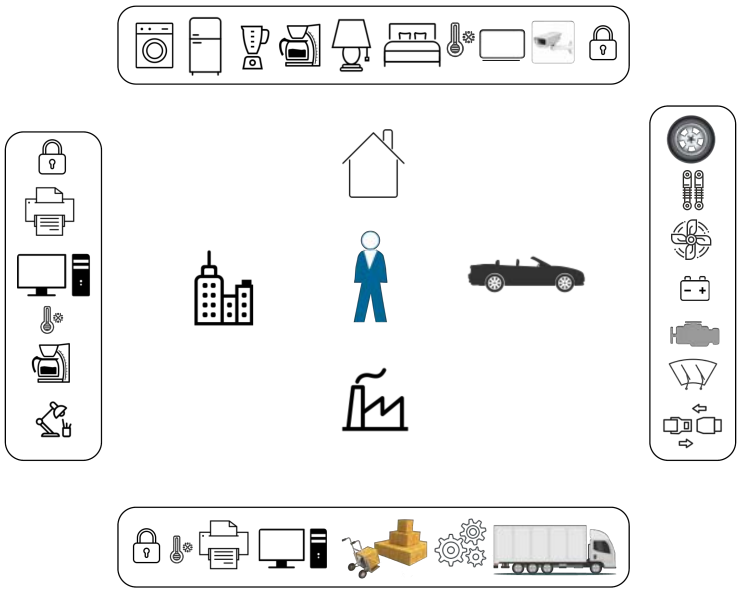

Figure 2.1 – Internet of Things

More and more connected objects are present in our daily activities thanks to the Internet of Things (IoT). These connected objects improve the productivity

of various tasks by providing their applications with relevant realtime data as depicted in Figure 2.1 such as the current quantity, current temperature, current humidity, current luminosity and security level that could be applied in various domains.

In order to provide better and broader services to the connected object in various domains, different communication technologies such as the RFID [25], Near Field Communication (NFC) [26], WiFi [27], ANT+ [28], Bluetooth [29], Zigbee (based on Personal Area Network (PAN) [30]) and Zwave [31] are used. Each connected object is uniquely identified so that the system is able to address the object when it is necessary. All the technologies stated above provide this functionality, including the RFID. NFC offers wireless data transfer in close proximity without requiring any pairing code. As an example of current applications, more and more credit cards, smartphones and smartwatches are embedded with NFC in order to encourage the use of electronic money. WiFi is one of the most popular, if not the most popular, wireless technology used nowadays. It is compatible to a broad range of devices such as computers, laptops, printers, televisions, game consoles, smartphones, etc. ANT+, Bluetooth, Zigbee and ZWave share the market in allowing simple connections between small devices through wireless connection without the need of having extended configuration. An advantage of ANT+ over Bluetooth is that it consumes less. Zigbee however, enables connection of more than 65000 nodes but with less transfer speed. Being the small brother of WiFi, Zigbee is able to support mesh network architecture in communication that enable all devices to be connected directly. ZWave concentrates on devices serves for home automation such as light bulbs, electric heater, etc.

A large number of academic papers cover the IoT phenomenon [18, 19, 20, 21, 22, 23]. The IoT includes vast domains such as logistics, access control, smart environment, medicine and healthcare. Each research brings a new insight from its own point of view. Its different aspects will be discussed further in the following sections.

Based on all the survey papers cited above, the IoT technology can be summarised as consisting of three main components;

- **Unique identification**

  Sensors and tags are samples of input devices. Sensors are usually designed

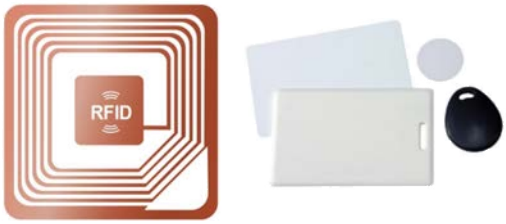

Figure 2.2 – Example of tags

to measure the changes in the environment (light, temperature, humidity, position, audio, video, voltage, current, etc.). Tags are intended to communicate an identity. They are predominantly passive (without embedded energy) and use contactless technologies such as Radio Frequency Identification (RFID) and Near Field Communication (NFC). Some tag examples are represented in Figure 2.2.

- **Communication channel**
  A communication channel mainly uses the radio medium such as Bluetooth, Zigbee and WiFi. Its objective is to enable the exchange of information with its environment. It transmits data to the global information system, which consists of local software applications for the data acquisition, data processing and data storage. This data can be distributed locally or centralized in the cloud environment.
- **Information system**
  The information system is the core of the overall system that provides services to the users. It manages the data collection by storing, modifying and removing data from the system. It controls the behavior of the system based on the feedback given by the input devices. As an example, to prevent any material shortage, a stock monitoring system can identify the quantity of a raw material and is able to schedule a new stock request while at the same time taking into consideration the time delivery before passing the order.

Having seen the existing main technologies in IoT, the next section will present the AAL environment in IoT.

2.2 Ambient Assisted Living (AAL)

As today's population age keeps increasing, older adults try to stay at home as long as possible. However, at a certain age, remaining safe while being independent is a major challenge. Ambient Assisted Living helps these people to achieve this goal.

Figure 2.3 briefly represents AAL in 4 groups of activities.

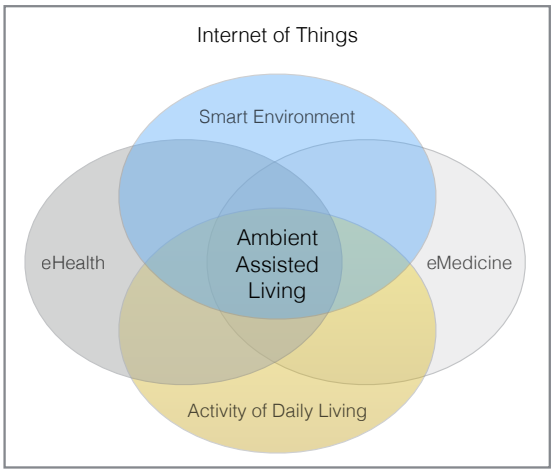

Figure 2.3 – Ambient Assisted Living within the IoT

- The objective of *the smart environment* is to manage the home access and comfortable ambience so that the elderly can feel safe and secure.
- *The e-Medicine* monitors the medication history. It records the patient's current status, the progress, the side effect encountered, the type of medications given, etc. It also serves as a reminder for the elderly person to take their medication, with a correct dosage and to report to their helper or the person in charge in their family or their pharmacist if the medication is about to finish.
- *The Activity of Daily Living (ADL)* describes their daily routine, such as cleaning, cooking, to move from one room to another, etc.
- *e-Health* helps in monitoring their health condition. It also helps to alert the relevant parties if the person requires a medical attention.

2.2.1 AAL Challenge

The primary challenge in AAL is the senior person's safety. The system is capable of monitoring their every action. If they are not performing their daily routines as usual or if their health deteriorates, multiple sensors will trigger a *preventive* action and notify the person in charge. This action shall minimise the risk of any possible dangerous situation such as a heart attack, an accidental fall, etc.

However, if anything happens without warning, the system shall detect the unfortunate event and notify the emergency status to the relevant parties. The relevant parties can be the family doctor, the ambulance services, and/or the relatives.

Another significant challenge is how to protect personal data. All these activities require continuous data collection. As every data of the senior person is vital, the system collects among others:

- Health related information
  - heartbeats
  - blood pressure
  - oxygen level
  - body temperature
- Medical information
  - drug prescriptions - drugs details, frequency of administration, amount/dosage.
- Personal environment preference
  - room temperature
  - room brightness
  - room humidity
- Object information
  - identification
  - current position

However, with the amount of data collected, it can be used against them. The medical information can reveal the person's illness. It can also be used as a leverage to get the upper hand in any negotiations. Section 2.6 will elaborate and discuss

this matter in detail.

Once the security and the protection of the personal data are assured, the implementation of the AAL shall see a bright future. The ability to help the elderly person to perform their daily activities are endless. Various researches have been done to help the senior persons' daily chores such as to cook, to go to the toilet, or to move from one room to another.

2.2.2 AAL Technology

Thanks to the technologies such as RFID, NFC, WiFi, ANT+, Bluetooth, Zigbee and Zwave (refer to IoT overview in section 2.1), AAL is able to help a senior person in their day to day routine. The smart environment uses sensors and switches to control the environment (detect, switch on, switch off). Other activities maximise the employment of passive RFID to reduce the cost of implementation.

In this work, we will concentrate on the RFID technology as the enabler of the AAL. The following chapter will present the RFID's general specifications followed by the RFID localization possibilities and how to ensure its security and privacy.

2.3 Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) drives most of the AAL solutions. It is made up of a system, a reader and a tag. The system stores and manages the information, the reader acts as the entry point to the system and the tag serves as an electronic identification agent attached to the object. Wyld in his book entitled "The Right Frequency for Government"(2005) [32] defined RFID as the technology that enables the identification of objects automatically by gathering data on these objects without any human intervention or data entry. The author also asserted that the RFID is not a new technology as it is actually a subset of the existing Radio Frequency technology that has been around since the 19th century and the idea came from an experiment dated back in 1886 by Frederick Hertz. The first known application of the RFID is the IFF (Identify Friend or Foe) during the World War II to identify an enemy aircraft. And since then, the RFID took a slow pace in being ready to be integrated in different domain. Among earlier applications

are in the domain of asset management, livestock tracking and transportation. Nowadays, almost every domain is touched by the RFID. However, for the past ten years the awareness about the RFID security has finally emerged.

Aligned with the same idea, according to CNRFID [33], RFID is defined as an automatic identification technology which uses radio-frequency electromagnetic fields in order to identify any objects that carry a tag whenever they get close to a reader. This identification includes the collection of the data contained in the tag by the reader. With the ability to read and collect the data from the tag, the reader also has the possibility to alter these data from the tag's memory. Currently the RFID standards are characterized by GS1 [34] and ISO standard organisations [35].

2.3.1 Radio Frequency Identification (RFID) air interface standards

Passive RFID tags have a limited communication range as described in ISO/IEC 18000 series of standard [36, 37, 38, 39, 40] and simplified in Figure 2.4. A passive RFID is capable of communicating within four frequencies :

2.3.1.1 Below 135kHz

Also known as Low Frequency (LF), this frequency standard is defined in ISO 11784 [1], ISO 11785 [2] and ISO/IEC 18000-2 [37]. The communication range is limited up to 0.1 meter. The main objective of this frequency is to ensure that a tag is in the vicinity of the reader. The tag is only capable of transmitting a small amount of data and the transmission rate is as low as 1 kbps. Typical application of this type of tag can be seen in the automotive industry, in the vehicle access control system or it is used as an animal identification tag. Its size is as small as a grain of rice.

2.3.1.2 NFC 13.56MHz

The second frequency range is at 13.56MHz (also called the High Frequency (HF)). The standard that is applied to this frequency range is the ISO/IEC 18000-

3 [38]. Among other types of technologies using the same frequency is the passive RFID [41], the proximity card as defined in ISO14443-2 [4], and the vicinity card as stated in ISO15693-2 [42]. The signal can go up to 0.1 meter. It has a higher data rate than the previous one (referring to [43], ISO 14443A has a maximum data rate of 106kbps, ISO 14443B has a maximum data rate of 847kbps and ISO 15693 has a maximum data rate of 26.4kbps). These types of cards are used mostly as library books identification system and as smart cards. They are commercially known as MIFARE and NFC.

2.3.1.3 RFID 860MHz to 960MHz

The third frequency range is between 860MHz to 960MHz (also called the Ultra-High Frequency(UHF)) as established in ISO/IEC 18000-6 [39]. It is the most commonly used tag frequency. It does not require a line of sight and can transmit high data rate (as mention in the standard [39], it has a maximum data rate of 40kbps). It can reach up to ten meters and is normally used in supply chains to track the stock flow. Since October 2013, GS1 (Global Standards) has ratified EPC Gen2v2, a new version of the widely used Gen2 Ultra High Frequency (UHF) RFID standard. Gen2v2 is backwards compatible with Gen2 but adds new features mainly for authenticating tags and readers as well as consumer privacy. These new features ease the adoption of RFID especially in application areas where the tag carries more information than only its identity. UHF is now an established technology, solutions can be reliably deployed for long read range, passive, and cheap. This new generation of tags is supported by an alliance of manufacturers called RAIN (RAdio-frequency IdentificatioN) [44]. The RAIN RFID Alliance is a non-profit organization that promotes awareness, education, and initiatives to accelerate the adoption of passive UHF RFID standards developed by GS1 (EPC Gen2) and incorporated by ISO/IEC (18000-63) [45] in business and consumer applications worldwide.

2.3.1.4 RFID 2.45GHz

Finally, the ISO/IEC 18000-4 [40] specifies the standard of the Super High Frequency(SHF) that operates at 2.45GHz which enables the communication range

of more than 10 meters. This tag focuses more on getting a bigger communication range and a bigger data rate but is more sensitive to electronic noise. It is mainly used in the vehicle fleet identification.

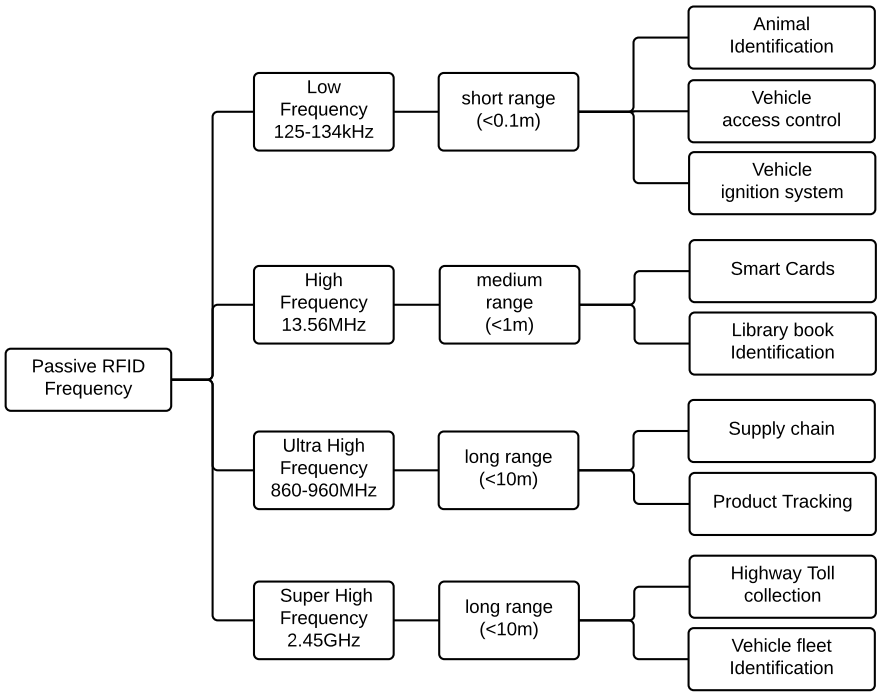

Figure 2.4 – RFID frequency

RFID classification does not stop at the frequency differences, it goes beyond that. A specific RFID only applies to a specific application and not to others. The frequency sharing is due to the availability of the frequency set by the government in a specific country. The effective classification of a RFID tag is based on its power sources. The following section discussed the matters elaborately.

2.3.2 RFID Classification

A RFID tag is categorized based on how it is powered, either fully powered, partially powered or without any internal power as illustrated in Figure 2.5. Furthermore the EPCglobal standard [46], the power-related RFID classification can be further extended into four functional classes that are based on the features supported by the tag. Figure 2.6 depicts the RFID categorization in detail where

it can be seen that there are three different kinds of tags: active, semi active and passive tags.

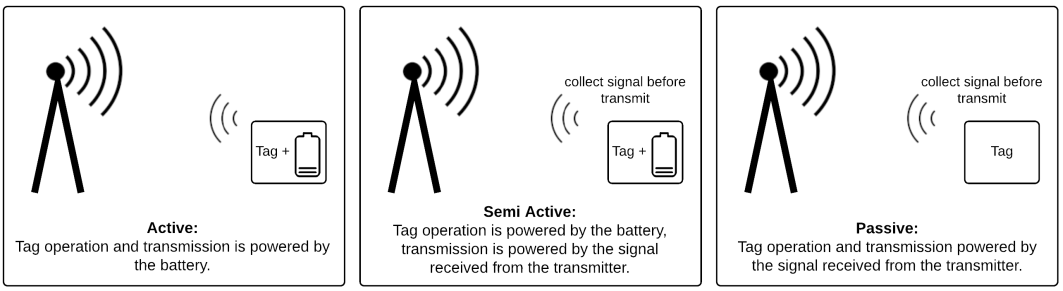

Figure 2.5 – RFID tag

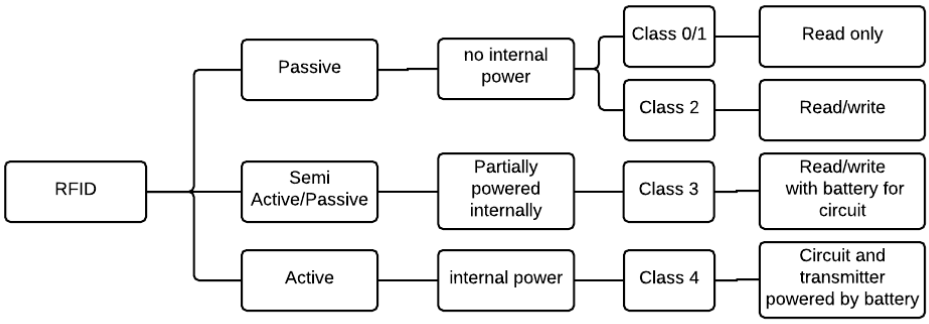

Figure 2.6 – GS1 RFID classification

2.3.2.1 Active tags

An active RFID tag includes an internal source of energy such as a battery to ensure that both the internal circuitry and the transmitter are available at all time. The class 4 tag represents the active tags that can initiate communications with readers or other tags without the need to wait to be energized by any signal.

2.3.2.2 Semi active tags

The semi active/semi passive tag collects energy from the reader to communicate. However, it depends on the internal power source to keep the internal

circuitry active. The class 3 tag represents the semi active tag. It is equipped with an identification, an internal memory for information storage and an authentication mechanism. It is also capable of controlling its confidential information within a controlled area with the help of the authentication mechanism.

2.3.2.3 Passive tag

A passive tag does not have an internal power source. Hence it collects the energy from the reader's request message and replied using the energy gathered from the signal. Passive tags are currently the most commonly used tags as they are low in cost and easily available. However, a passive tag can transmit up to ten meters because of the limited amount of energy collected from the signal that is sent by the reader.

Class 0, 1 and 2 represent the passive tags with the difference that the class 0 and class 1 are merely an identity tag and no other features are added. The only difference is that class 0 tags only provide identity as it is preprogrammed during the fabrication process and cannot be modified. The class 1 tags enable the user to modify the identification information on the tag once during the set up. The class 2 tags are equipped with the tag identification with an extended user memory and an access control authentication mechanism. These tags are capable of storing additional information rather than only the identity. They also control the access to a certain section of the memory area where confidential information can be stored.

	class 0	class 1	class 2	class 3	class 4
Active					x
Semi active				x	
Passive	x	x	x		

Table 2.1 – Tag classification vs resource

The CNRFID [33] does not differentiate between class 0 and class 1 tags. Dobkin in his book "The RF in RFID" [43] described further that initially, class 0 and class 1 operate on different protocols and are not compatible between each other. Furthermore, class 0 requires different frequency to transmit and to receive signals. Therefore the class 0 has been dropped to make way for the class 1 tags.

2.3.3 RFID standard

GS1 is a global non-profit organization that develops, creates and manages the EPC standard through EPCglobal [46]. This standard has been passed over by the Auto-ID Center that was founded in the Massachusetts Institute of Technology (MIT) in 1999. These standard characterizations will be explained further in the following section.

2.3.3.1 RFID Generation 1

The RFID generation 1 refers to the first standard proposed by Auto-ID Center. The main objective of this standard is to promote a common path towards a real standard compared to their predecessors; the barcode and the magnetic strip card. Through the Electronic Product Code (EPC), each object identification includes the manufacturer identification, the product category and a serial number. They also emphasized on the utilization of 900MHz frequency to achieve the best compromise between their cost, read range and capability.

2.3.3.2 RFID Class 1 Generation 2 Version 1 (C1G2)

In 2004, the Auto-ID Center handed over the EPC standard to the EPCglobal which then came out with a new standard called the ***Class 1 Generation 2*** (C1G2) and rendered the previous standard on class 0 and class 1 as obsolete. The standard dropped the class 0 from its specification.

Figure 2.7 described the association phase between a reader and a tag in the RFID Class 1 Generation 2. To simplify the communication exchanged between a reader and a tag, no collision has been considered in the best case scenario. It depicts both the current and the previous protocol communication standard exchange of the UHF tag. It starts by sending a query request from the reader to a tag. Considering the best case scenario where only one tag replies at one time, the tag will send a random number to the reader. Once the reader received the random number (RN16), the reader duplicates the same random number and sends it back to the tag. This response is used as the Acknowledge command (ACK) that indicates the tag that the reader has received the message and they can start

to communicate. Upon reception of this number, the tag will compare it with its own record. If numbers are identical, it will then release its identity. The identity sent is in the form of 96 bits EPC standard that described the manufacturer, the product category and it's serial number. The reader will then finish the inventory session by requesting another random number from the tag to be used for the following communication exchange.

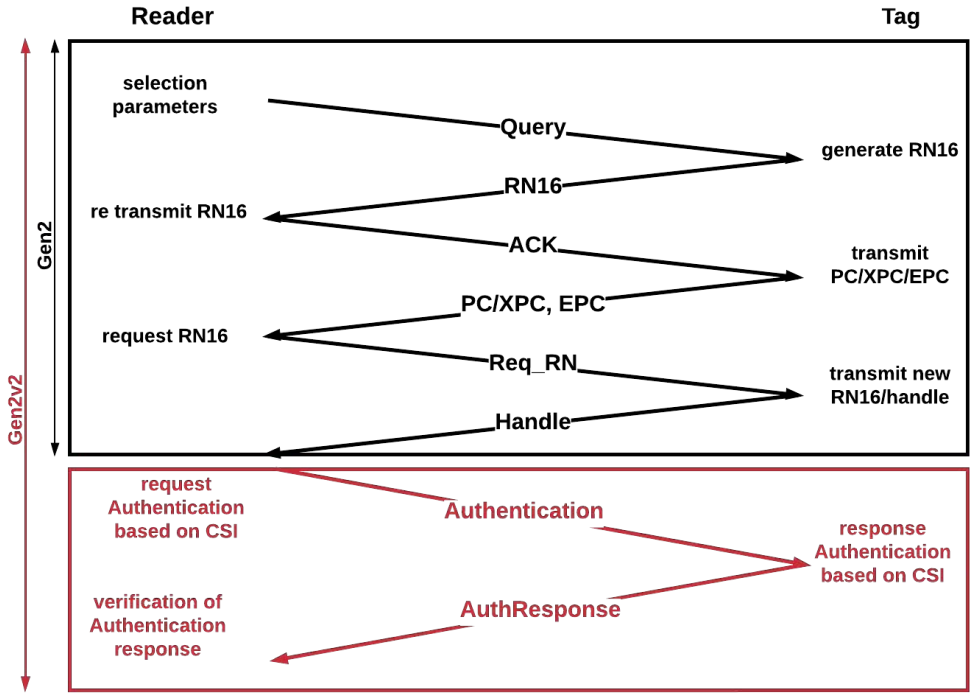

Figure 2.7 – Best case scenario communication exchange in Gen2V2

2.3.3.3 RFID Class 1 Generation 2 Version 2 (Gen2V2)

The current UHF RFID standard has been published in 2013 and is called the Generation 2 Version 2 (Gen2V2) [47]. The generation 2 refers to the class 2 tag that is described in Figure 2.6. It is designed to ensure backward compatibility with the previous version. The second generation improves the security and privacy of the tag owner. It limits the access to certain area of the passive tag memory by adding an authentication process. The UHF RFID tag has since become an

established technology that can propose reliable solutions for inexpensive and passive tags which can cater for a long read range. The novelty introduced by the second generation is presented in red. In all communication exchanges, the reader starts by selecting a set of tags that will participate in the communication session. This phase will be followed by an inventory phase where all requests regarding the identification and authentication are performed. The access to the extended memory can then be performed after the authentication process is successful. We can summarize the process in three phases:

- *Select*: to define the set of tag to be communicated.
- *Inventory*: the process of interrogating the selected tags.
- *Access*: the process of accessing tag's memory.

Figure 2.7 depicts the communication exchanges during the inventory phase. In this figure, we can see the similarities in the exchange process for the C1G2 tags as described in section 2.3.3.2 and the Gen2V2 tags. However, for Gen2V2, two additional processes were added which have further enhanced its security and privacy.

In Gen2V2, the reader will send an authentication request to the tag depending on the type of authentication selected at the beginning of the session. The tag prepares the answer and sends it accordingly to the reader. All communications after this authentication step are considered authenticated. More details about the procedure will be discussed in section 2.4 and 2.6

This authentication process enforces the next exchanges between the reader and the tag but does not provide privacy as the EPC is sent without any protection so that any attacker can know the identity of any tag.

The communication exchange in Figure 2.7 represents the best case scenario where only one tag communicates at a time (therefore no collision occurs). Unfortunately, it is not always the case. Since the communication medium is based on wireless technology, it is prone to collisions caused by messages sent simultaneously by tags or readers. A standard protocol is then required to solve this situation. The following section will discuss further the method to minimise the collision risk.

2.3.4 RAIN RFID tag collision management

The deployment of hundreds of RFID tags can generate a deadlock communication situation where two or more tags are responding to an initial request from a reader simultaneously. As a result, not a single receptor is capable of interpreting the message accurately due to collisions. Therefore, it requires a particular method to avoid the collision as proposed by in [48, 49]. Vogt in [48] proposed a method to detect the RFID tags without knowing its actual numbers. The implementation however, achieved only 90% accuracy.

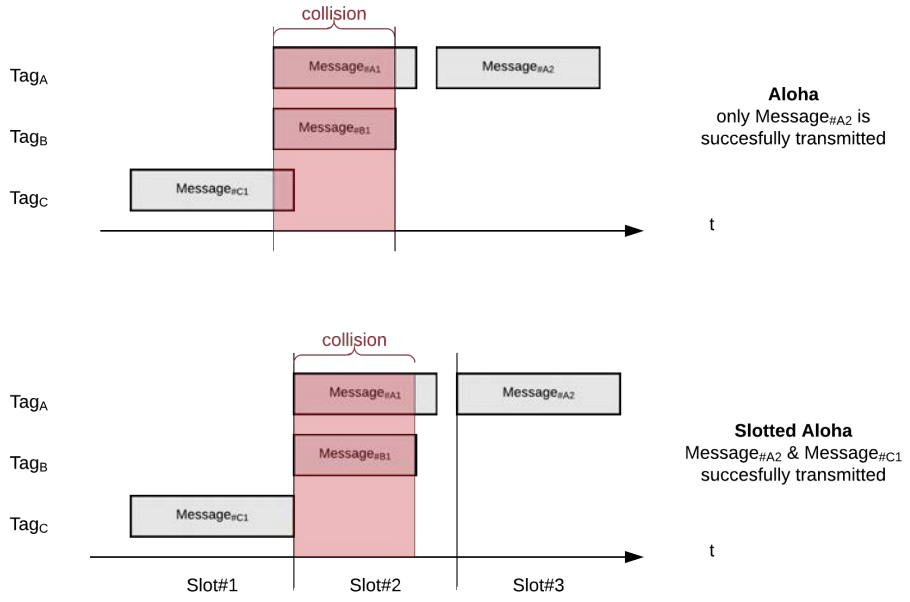

Figure 2.8 – Aloha vs Slotted Aloha

RFID tags communicate based on a protocol called the Frame Slotted Aloha (FSA). The protocol is a derivation of the famous Aloha protocol. In Aloha, a station can transmit a data as and when needed, therefore, collisions can occur at any time during a data transmission. It renders the communication channel to be inefficient. The Slotted Aloha improves collision management by dividing the transmission into time slots. So, a station can only transmit at the beginning

of a slot. This will reduce the collision possibility only at the beginning of the transmission rather than throughout the transmission duration. The Figure 2.8 describes the improvement achieved by using the Slotted Aloha. In both scenario, Tag_A sends 2 messages, A1 and A2, Tag_B and Tag_C send 1 message each, B1 and C1. Note that in comparison with the traditional Aloha, the Slotted Aloha, requires the current message to finish transmitting before allowing a new message to be sent. This, minimize the possibility of having a collision once a tag has started to transmit its message. The Frame Slotted Aloha also groups the slots in a frame and fixes the frame size in a form of 2^Q, where $Q\epsilon[0:15]$. Therefore the maximum frame size represents 32768 slots. (refer to Table 2.2). Lee et al. in [49] on the other hand, proposed an enhanced method of anti collision by changing the frame size dynamically by doubling it if 70% of the frame is filled with collision and dividing it by two if more than 30% of the frame is empty. They claim that it achieves more than 85% improvement over traditional Frame Slotted Aloha. In RFID application, the reader will define the frame size, while the tag selects a slot where it wants to communicate.

Q	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Slots	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768

Table 2.2 – Q vs total slot number

In order to simplify the implementation, Gen2V2 uses the term *slot counter* to represent the slot chosen by a tag. As previously mentioned in the last paragraph, a reader uses a Q value between 0 and 15 to indicate the frame size. A frame size is therefore between 1 to 2^Q. Table 2.2 indicates the total available slots for each Q value. As an example, when Q=3, the number of communication slots available is $2^Q = 8$. Therefore the tag can choose from 1 out of 8 possible slot for it to communicate with the reader. If the Q value is carefully chosen, the possibility of having two or more tags that try to communicate at the same time will be reduced. However, if the number of available slots is smaller than the number of tags, it will render the system inefficient.

2.3.4.1 Frame Slotted Aloha efficiency

A theoritical study has been performed to a population of 10 to 100 tags in order to obtained quantitative results sufficient enough in dimensionning set of RFID used in AAL [24]. The Frame Slotted Aloha efficiency is based on the number of tag (n) and the number of slots (N) available. The communication efficiency between tags within a slot is calculated based on the Equation 2.1. This efficiency, noted S, is the probability to have a successful transmission.

$$S = \frac{n(1-\frac{1}{N})^{n-1}}{N} \tag{2.1}$$

The communication efficiency of 10 tags, 50 tags and 100 tags are represented in the Figure 2.9. As mentionned by Tanenbaum and Wetherall in [50], the theoretical value for the maximum communication efficiency of FSA is at 38.6%. On the same note, the peak value of the graph moves along the x axis in accordance with the number of tags corresponding to the total slots available (refer to figure 2.9 and table 2.3);

Q	slots available	10 tags	50 tags	100 tags
2	4	18.7%	0%	0%
3	8	37.5%	9%	0%
4	16	34.9%	13.2%	1%
5	32	23.4%	32.9%	13.4%
6	64	13.5%	36.1%	32.8%
7	128	7.2%	26.5%	35.9%
8	256	3.7%	16.1%	26.5%

Table 2.3 – Efficiency values

As we go further, we notice that to get the maximum efficiency, the total number of slots available in a frame needs to be as close as possible to the number of tag. As an examples:

- 8 slots < **10 tags** < 16 slots
- 32 slots < **50 tags** < 64 slots
- 64 slots < **100 tags** < 128 slots.

This value will later be used as the guideline for the implementation of the simu-

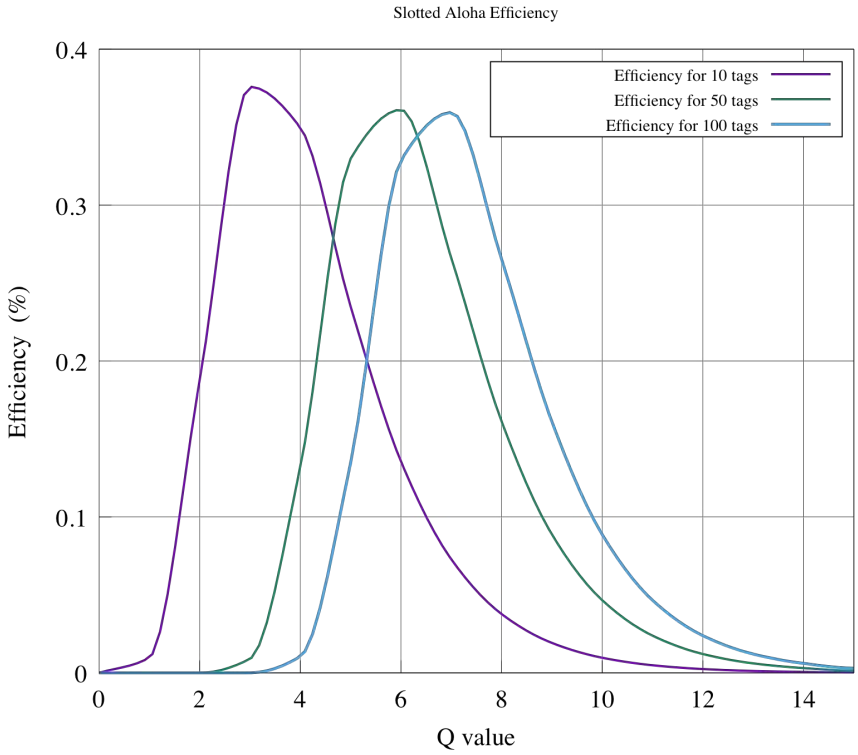

Figure 2.9 – Slotted Aloha Theoretical Efficiency

lation in chapter 3. It is interesting to know if the observation made based on the theoretical value will correspond to the simulated one.

2.3.4.2 Collision Management Protocol

As previously mentioned, the RFID collision management protocol is based on the FSA. It uses a slot counter to identify the slot number. In its implementation, only a tag with a slot counter zero is able to transmit any data. If a tag slot counter is different than zero, it decreases the slot counter number by one and wait for the next command. This creates a queue of tags that waits for their turn to communicate. Figure 2.10 explains the process further.

To start a session, a reader broadcasts a *Query* request with the frame size value as a parameter. The frame size is sent as a Q value which represents the frame size as 2^Q. The maximum Q value is set to be 15 at most (which represents 32768 slots). Each tag that receives the *Query* request generates a random number

within the frame boundaries that will serve as the slot counter.

If the slot counter is different than zero, the tag decreases the slot counter value by the decrement of one and waits for the next command from the reader. This step navigates through all slots of the frame one by one. If the slot counter is zero, the tag generates another random number (RN16) as a response for the query and sends it to the reader.

After sending the request, the reader monitors the communication channel to ensure that only one tag communicates at one time. There are three different possible scenarios.

The first scenario is when only one tag communicates during a slot. The reader successfully receives the random number (RN16) sent by the tag and it will echo the same value back to the tag as an indication that the message has been successfully received.

The second scenario is when there is a collision. It happens when more than one tag try to send a message simultaneously. The communication medium is then flooded with messages that make the signal unreadable for the reader. In this case, the reader ignores all messages and proceeds with another request called *QueryRep*. The *QueryRep* command indicates to the tag to decrease the slot counter by one. As mentioned previously, only tags with slot counter equal to zero can start transmitting data. Therefore this command positioned the tag a slot nearer to its goal (zero).

Finally, in the third scenario, if there is no communication that occurs during the slot duration, the reader will wait for a specific time out before broadcasting a new QueryRep command to all tags.

In any case, a tag will pass through the first scenario where it sends a random number (RN16) and wait for the answer. We can note also that the second and third scenario contribute to the communication channel inefficiency where the slot is not used for any communication. Finally, once the tag receives the acknowledgement command from the reader, it needs to identify itself to the reader. This identification process will be further discussed in the following section.

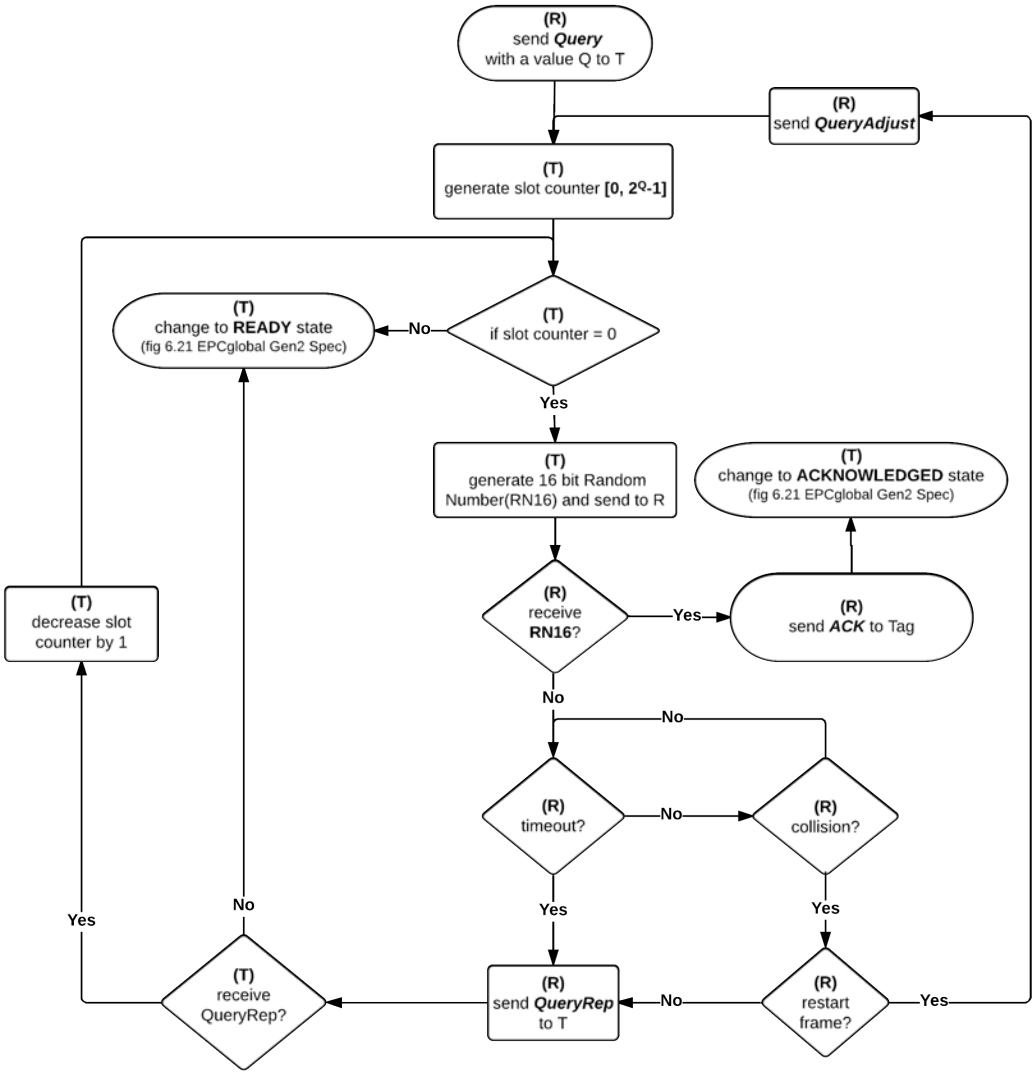

Figure 2.10 – Gen2V2 tag collision management

2.3.5 RFID Identification

Once collisions between tags are avoided, the reader can send the acknowledgement message to the active tag in the current slot. As described in Figure 2.10, the tag answers with its identity. The tag uses the Electronic Product Code (EPC) [51] as a unique identification. The EPC covers all type of RFID applications.

The EPC is represented in Internet Uniform Resource Identifier (URI). It is in

the form of:

urn:epc:id:scheme:12345678.234567.345.xxxx.xxxx

- urn: Uniform Resource Name
- epc: Electronic Product Code
- id: Identity
- scheme: epc format to be used

It is divided into several segments to guarantee the identity uniqueness. The first three segments are occupied by the EPCglobal standard parameters. It covers details such as the EPC length, version and generation. The fourth segment refers to the scheme to be used and the following segments are used for identification purposes. Scheme refers to the type of EPC implementation, such as for trading objects, logistics, automotive components, aerospace and defence sector, etc. As an example, the serialized global trade item number (SGTIN) refers to the trading item/product code.

The standardisation enhances a cross platform ability and enables the outgrowth of the IoT. Research trends on the fusion of the connected objects within the current internet network are discussed in [19] and [21]. The results of the fusion can offer a boom effect to the existing service-oriented application. Despite the bright future that awaits the IoT, all literatures cited previously had raised the same concern with regards to the security and privacy in IoT.

2.4 Security

Realising the gap that exists within the EPC C1G2 standard, the Gen2V2 protocol adds several commands to cater the security in RFID tags. Among others are to validate a tag or a reader during an association between a tag and a reader. This to ensure that only authorized tag or reader will take part in the conversation.

As RFID relies on the wireless communications, the same access medium is shared by every user and is therefore more vulnerable to security attacks.

In general, the security threats are classified into two categories: active attacks and passive attacks as depicted in Figure 2.11 the following sections will discussed

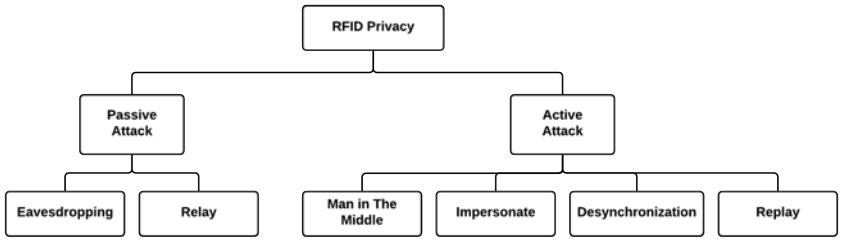

Figure 2.11 – RFID Security

further these attacks from a general standpoint as they are not specific to the health domain.

2.4.1 Passive Attack

A passive attack is an attempt to monitor and/or to capture information from a system. It has no impact on the end to end communication. It can also be considered as the preliminary step before an active attack where communications are captured for every transmission on the medium. Among the attacks that are considered passive are eavesdropping and relay attack.

2.4.1.1 Eavesdropping

Eavesdropping consists of capturing the conversation between two entities. As depicted in Figure 2.12, a third person behind the wall is secretly listening to Alice and Bob's conversation. In RFID, if the gathered data are not encrypted, it can be used to identify useful information such as the EPC. However, no modification of the exchanged data is made. Hancke in [52] performs a proof of concept on HF RFID eavesdropping.

2.4.1.2 Relay attack

The relay attack is the attempt to get access to a secure entity with the help of a legitimate security device. It is based on the assumption that the legitimate device must be close to the attacked system. It can enable the opponent to access the system while the device is not within range. This attack requires at least

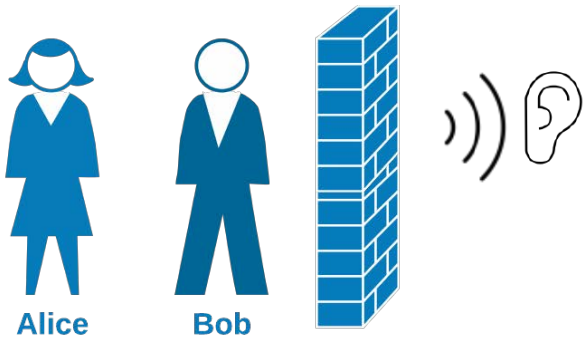

Figure 2.12 – Eavesdropping

two equipments that are able to impersonate the system and the device (refer to Figure 2.13).

When the adversary wants to access the locked item, it will send a request for the information from the proximity key through the device#1 which then forward the information to the device#2. With this given information, the adversary will finally be able to get into the locked item. It is considered a passive attack as it does not modify any messages from the actual device and the opponent is not required to understand the message. Silberschneider et al. in [53] demonstrate a relay attack using a HF RFID and a smart phone on an access control environment. Sportiello et al. in [54] give another example of a long range relay attack using two phones. In the case study performed by Francillon et al. in [55], the relay attack enables the possibility of stealing a vehicle by using two devices where an attacker with the first device within the car proximity, while his accomplice is in close range of the ligitimate car key. The accomplice should be near to the vehicle owner, therefore within the range of the car key. Therefore trick the vehicle immobilizer to believe that the vehicle RFID immobilizer.

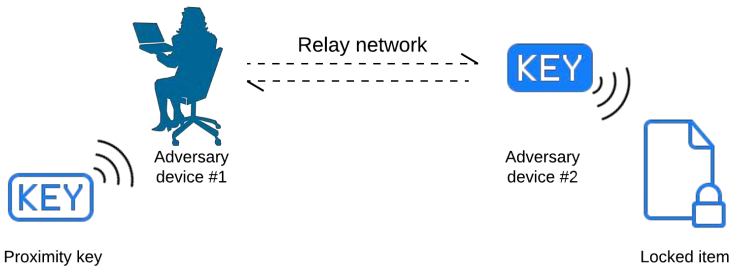

Figure 2.13 – Relay Attack

2.4.2 Active Attack

An active attack is an attempt to modify transmitted information from the system that is under attack. Its aim is to add, modify or even delete the message. An attacker can try to impersonate the victim in order to reach his goal such as having a full access to their personal information. Among the attacks that are considered active are desynchronization, reflection, man in the middle and denial of service attacks.

2.4.2.1 Desynchronization attack

In RFID, the desynchronization attack occurs when the adversary tries to disrupt the key updates between tags and reader resulting in the authentication key to be mismatched and to render the tag unusable. In this context, keys represent a set of preshared key shared between tags and the reader. Once the key is used, both tags and reader move to the next key in line. The attack tries to prevent the key from each side from being of the same sequence. Even though this attack does not add, modify nor delete any messages, the consequence is that the system will not be able to recognize the tag. Again, Safkhani et al. [56] is among researchers that is actively work in finding weakness in RFID Gen2 tags.

2.4.2.2 Man in the middle attack

The man-in-the-middle attack occurs when the adversary managed to be in between Alice and Bob conversation in real time. As illustrated in Figure 2.14,

the adversary can pose as Alice when communicating with Bob and act as Bob when communicating with Alice. However, the adversary is required to understand the message.

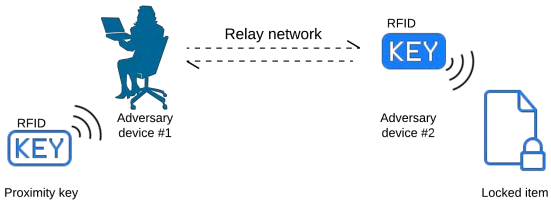

Figure 2.14 – Man-in-the-middle

However, due to its resources limitations, RFID has yet be considered fully secured [56]

2.4.3 Authentication

Many RFID privacy literatures focused on tag authentication protocols to prove that the EPC-C1G2 standard has a weak security by applying a cryptanalysis on a series of authentication protocol and come up with a new solution [57, 58, 59]. Some did not consider reader authentication [58] while some concentrated in timely mutual authentication [59]. Mutual authentication is considered the best way to authenticate a communication where both tags and reader are verified. Among the solutions proposed in improving security by offering mutual authentication is Chou in [60].

Low cost RFID tags come with limited resources where at most 10000 Gate Equivalent (GE) is allocated for security purposes [61, 62, 63]. The Gate Equivalent (GE) value is used as a common reference for the performance of different hardware architecture. GE relates to the area of silicon in μm^2 to form a RFID tag divided by the area of two-input NAND gates as described by Rolfes et al in [64]. Based on the calculation resources required, the attacks countermeasures can be divided into four categories:

- *Full-fledged* is the ability to perform one-way cryptography (such as hashing encryption), symmetric encryption (such as AES) or public key algorithm.
- *Simple* is the ability to calculate both random number function and hash function.
- *Lightweight* is the ability to formulate both PseudoRandom Number Generator (PRNG) and Cyclic Redundancy Code (CRC)
- *Ultra-lightweight* is the ability to perform bit-wise operation suc as XOR, AND and OR.

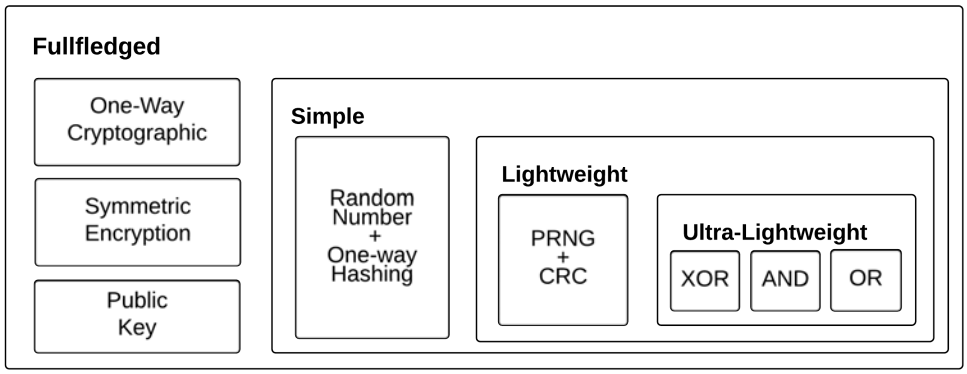

Figure 2.15 – RFID tag security classification

As mentioned in Figure 2.15, if the tag is capable of performing a full fledged cryptography, it could easily compute a random number, a hash function, CRC and bitwise operations. The same would go to the simple category where it could easily perform the CRC and bitwise operation and so forth.

To improve the security of passive RFID tag, Gen2V2 adds nine cryptographic encryption suites within its specification to allow authentication as an optional extension of ISO/IEC 18000 series. The full list of the possible implementation of crypto suite within the Gen2V2 passive RFID can be found in the ISO/IEC 29167-1 [65] which encompasses AES128 [66], PRESENT-80 [67], ECC-DH [68], Grain-128A [69], AES OFB [70], XOR [71], ECDSA-ECDH [72], cryptoGPS [73], RAMON [74]. It must be noted that a tag can use only one of the cryptographic suite that is selected during its manufacturing.

Four of the crypto suites will be described in the following section where

AES128 implementation has been chosen to represent the de facto standard in security. It has been selected among numerous proposals to the US government to replace its previous encryption method called DES that is dated from 1977. It is widely used by other well-known technologies for embedded connected devices like Bluetooth, Zigbee and WiFi. AES implementation prototype in RFID has been performed by Moradi et al. in [75] and Ertl et al. in [76], however, their prototypes are based on the C1G2. PRESENT-80 [77] is an example of a block cipher. It has been chosen for its similarity to AES but requires less resources (lightweight) thus suitable to most RFID. XOR on the other hand, is suitable for low cost passive tag due to its simplicity and finally, cryptoGPS is an example of an asymmetric cryptography that offers a highly secure authentication. The explanation of the cryptographic suites will be based on the improvement done in Gen2V2 as in Figure 2.16 where the CSI (Cryptographic Suites Indicator) represents the authentication identification.

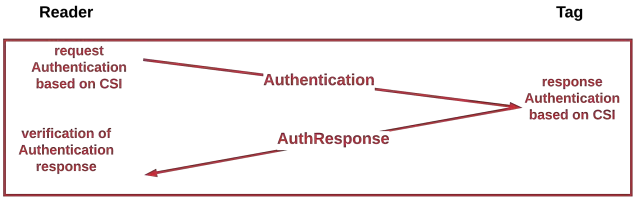

Figure 2.16 – Gen2V2 Improvement

2.4.4 Advanced Encryption Standard: AES128

AES128 [78] is a part of the Advanced Encryption Standard (AES) cryptographic algorithm defined in [79] that is a symmetrical block cipher. It uses a set of substitution and permutation of a fixed block of 128 bits.

To ensure that the tags are capable of performing the required calculation, the smallest size of possible key is selected among the 128, 192 and 256 bits key size/length.

Since RFID tag resources are limited, lower GE value is preferable. Fu et al.'s proposed an implementation of AES128 authentication in [80] and showed the

cost to be at 4952 GE, [63] at 3400GE and Moradi et al. in [75] at 2400 GE.

The input to be encrypted by the AES is arranged in a set of bytes as the basic unit of processing. It is then represented in a 4x4 matrix. This input will then be copied in a state array. All AES operations will be performed on the state array, the result will then be copied in the output array. (refer to Figure 2.17)

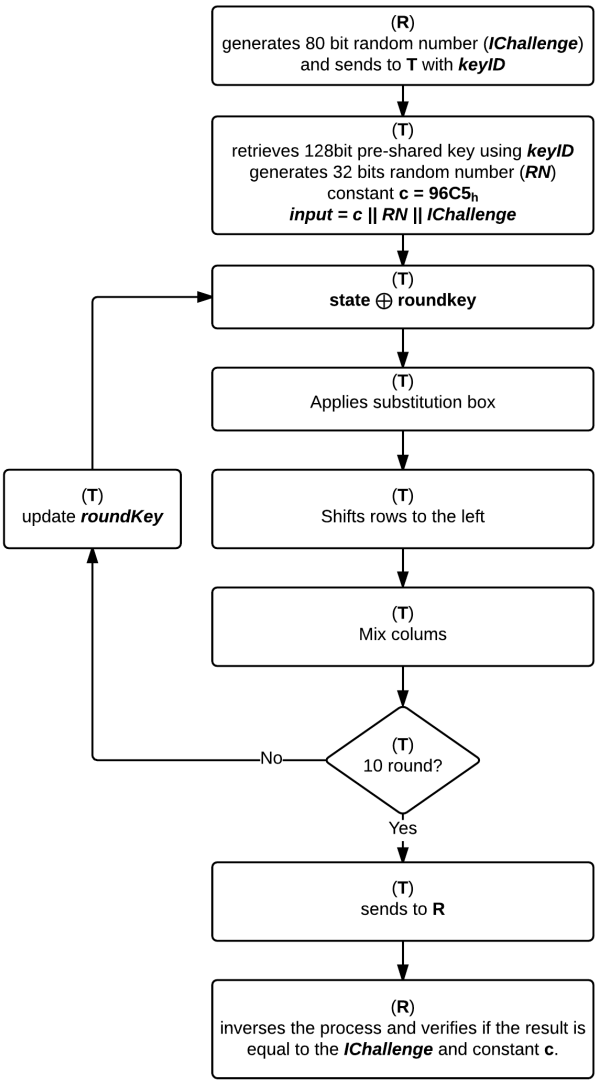

Figure 2.17 – Tag authentication using AES128

The tag authentication is performed based on a challenge and response ex-

change with a preshared key as described in the Gen2V2 improvement in Figure 2.16. The explanation of this section is based on the Figure 2.18.

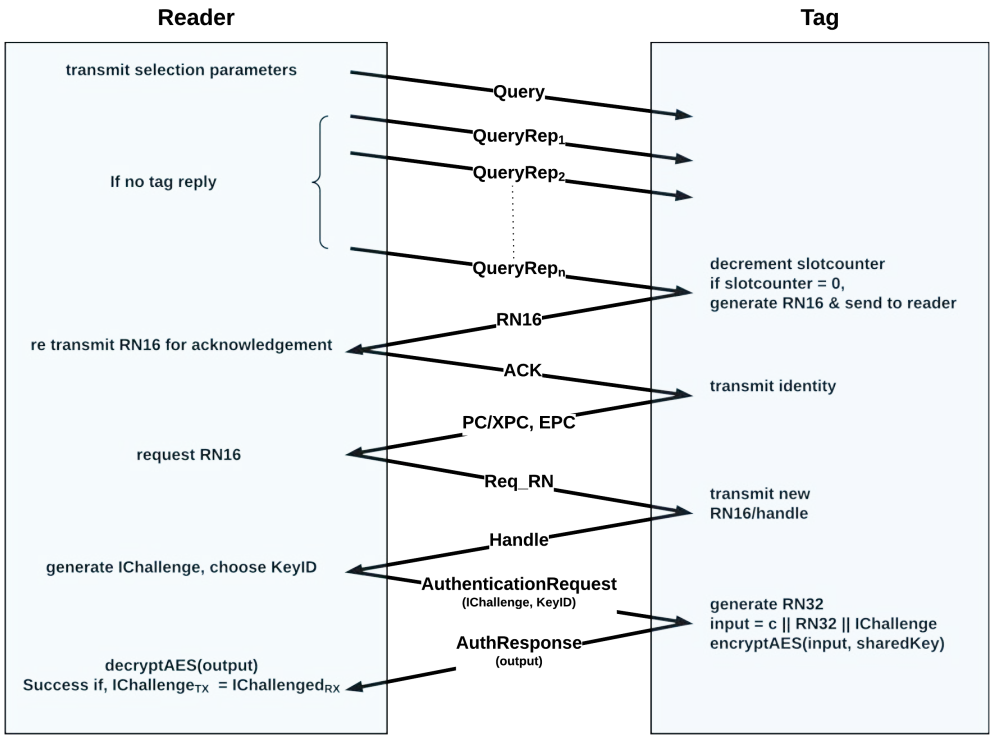

Figure 2.18 – Authentication protocol exchange between reader and tag for AES128 in Gen2V2

To begin, the reader generates and sends an 80 bits random number called '*IChallenge*' along with a reference *keyId* as an authentication request (refer to table 2.4).

The *keyId* is a preshared key identifier from a key table that is preloaded in the tag beforehand, either during fabrication or during the tag implementation within the system. This prevents any preshared key to be transmitted in an unencrypted form through the wireless channel.

	AuthMethod	CustomData	RFU	KeyId	IChallenge
bits	2	1	5	8	80

Table 2.4 – AES128 Authentication request format

Once the tag receives the authentication message request, (see section 2.4) it prefixes a 16 bits constant having a value of $96C5_h$ called '*c*', a 32 bits random number (RN) generated by the tag itself and the 80 bits *IChallenge* received. All together it forms the 128 bits input matrix. This input matrix is then copied to the state array and undergo a bitwise XOR operation with the first *roundKey*. This represents the first round of state array as mentioned above. The result will then go through a substitution box (refer to table 2.5) that replaces each byte with a substitute value. Each line of the matrix is then shifted to the left corresponding to the line index as described in table 2.6.

The state matrix then goes through a mix column process (refer to table 2.7) before going through the bitwise XOR again but with an updated key for the round. The process is repeated for 10 rounds.

The result is then concatenated to a 16 bits constant (C) and a 32 bits random number. The tag finally sends this response (Challenge) to the reader. The reader decrypts the response by inverting the process and retrieves both 'C' and 'Challenge'. The tag authentication is considered successful if both values are identical for the reader and the tag.

2.4.5 PRESENT-80

PRESENT is a lightweight symmetrical block cipher proposed by Bogdanov et al. in [77]. Its implementation requires only 1570 GE (Gate Equivalent). Gen2V2

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Table 2.5 – AES: Substitution Box

(a) before

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

(b) after

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

Table 2.6 – AES: Shifting columns to the left

(a) before

$S_{0,0}$	$S_{0,1}$	$S_{0,c}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,c}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,c}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,c}$	$S_{3,3}$

(b) after

$S_{0,0}$	$S_{0,1}$	$S'_{0,c}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S'_{1,c}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S'_{2,c}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S'_{3,c}$	$S_{3,3}$

Table 2.7 – AES: MixColumns

privileged the 80 bits preshared key as compared to the 128 bits preshared key due to the resource constraint. PRESENT-80 uses 64 bits data block with a 80 bits

preshared key as described in [67].

Once the RFID tag is identified, the reader is able to start an authentication session with it to further enhance the security. The chronogram in Figure 2.19 helps to highlight the communication exchanges. Figure 2.20 illustrates the overall process.



Figure 2.19 – PRESENT-80: Protocol exchange between reader and tag

As described in [77] and further explained in [67] the PRESENT-80 requires 31 rounds of substitution and permutation of the plaintext. It uses a 64 bits round key, with a 42 bits challenge. In every round, the tag performs an exclusive OR (XOR) between the round key and the received challenge.

The round key changes in every round. The first round key is the 64 most significant bits of the 80 bits preshared key. As described in [67];

$$presharedKey_1 = key_{79}key_{78}key_{77}...key_0 \tag{2.2}$$

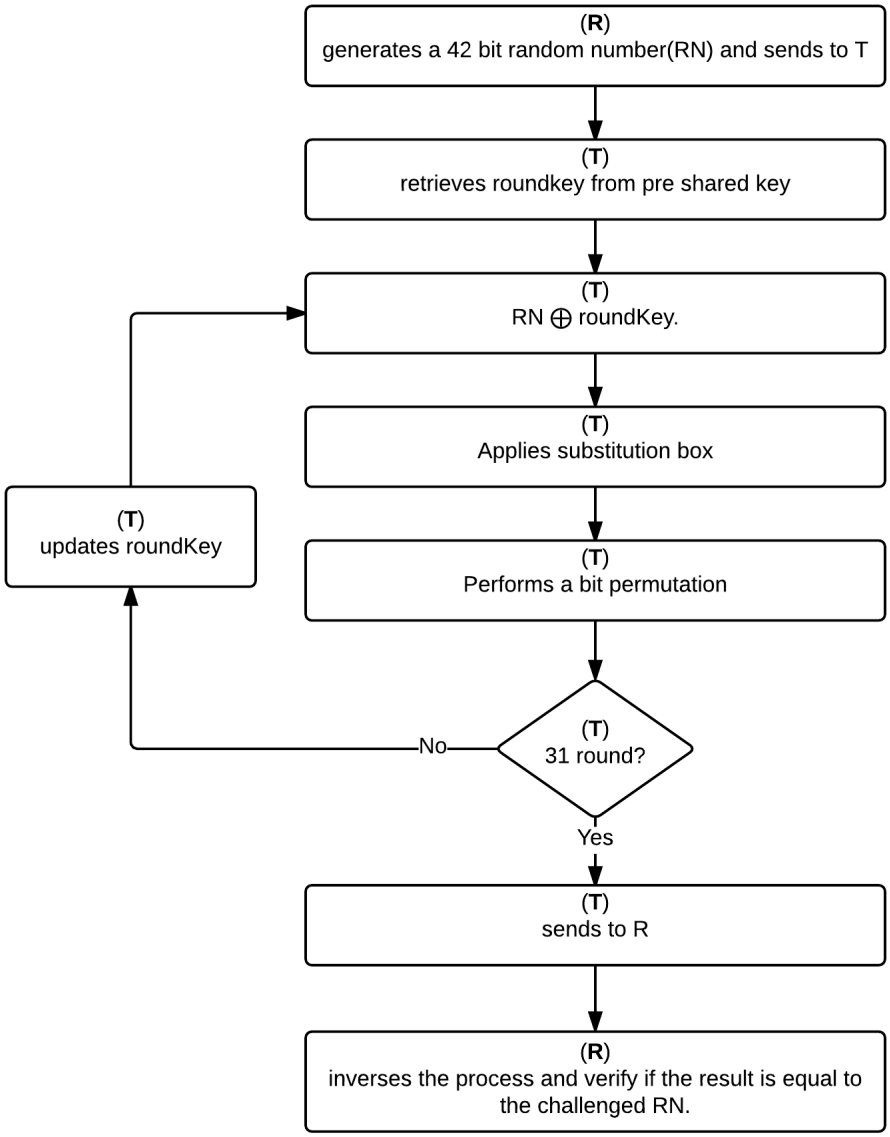

Figure 2.20 – Tag authentication using PRESENT80

$$roundKey_1 = key_{79}key_{78}key_{77}...key_{16} \tag{2.3}$$

To get the next round key, a 61 bit shift to the left is applied to the current preshared key and became the $presharedKey_2$ (cf Equation 2.4). The round key

became the Equation 2.5.

$$presharedKey_2 = key_{18}key_{17}key_{16}...key_{19} \tag{2.4}$$

$$roundKey_2 = key_{18}key_{17}key_{16}...key_{35} \tag{2.5}$$

The outcome is then passed through a substitution box (as in Table 2.8) and a bit permutation box (as in Table 2.9) as defined by the authors in [77]. Considering P(i) is the permutation box formula, it is calculated by adding the quotient of i when divided by four, plus the remainder or the division multiply by 16 (refer to Equation 2.6 deduced from table 2.9).

$$P(i) = \left\lfloor \frac{x}{4} \right\rfloor + (x \ mod \ 4) * 16 \tag{2.6}$$

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 2.8 – PRESENT-80 Substitution box

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(i)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Table 2.9 – PRESENT-80 permutation box

Finally, the result from the substitution and permutation is sent back to the reader as the authentication response. The reader inverses the process and verifies if the challenge in the tag response corresponds to the challenge value that has been previously sent.

2.4.6 XOR

As described in the chronogram in Figure 2.21, the crypto suite based on the exclusive OR (XOR) operation for tag authentication is implemented after the initial exchange in the inventory phase. It is simple to be implemented and does not require a lot of resources. The process depicted in Figure 2.22 requires only an addition and the XOR operation. To encrypt the plaintext message, the algorithm uses a preshared key called *PSK* and a constant value of 5555 5555 5555 5555h called '*On*'. The verification is based on the exchange value passed between the reader and tags. The values come from a XOR operation between the random number (RN), the constant '*On*' and the *PSK*.

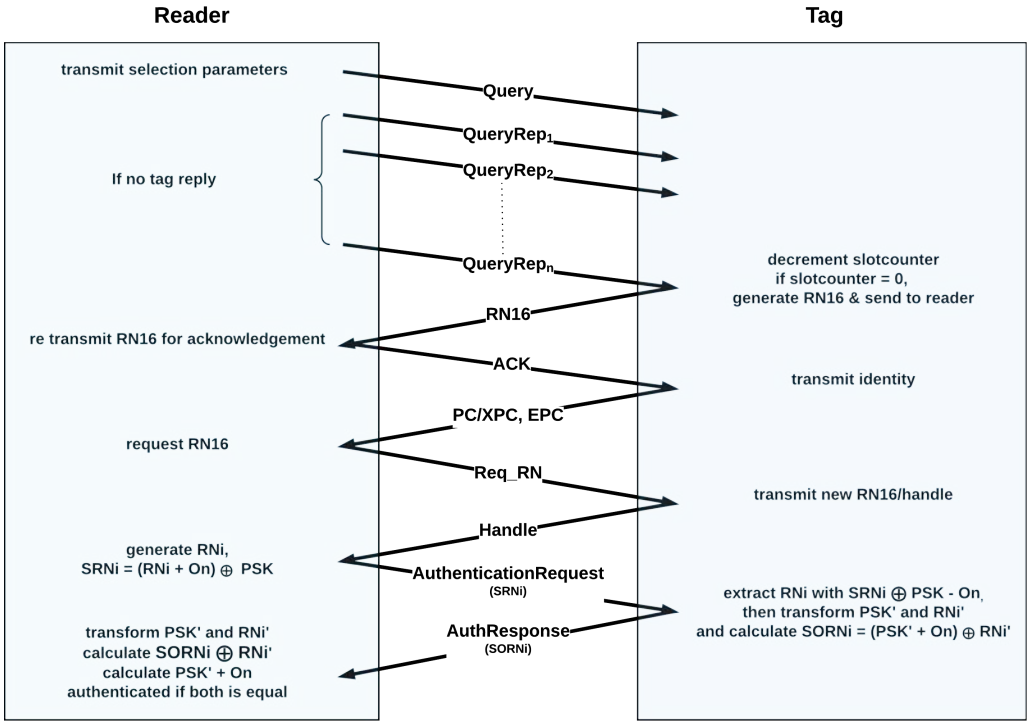

Figure 2.21 – XOR: Protocol exchange between reader and tag

The reader starts the authentication process by sending a *SRNi* value computed using a random number generated by the reader and the constant '*On*'. The *SRNi* calculation is represented in Equation 2.7.

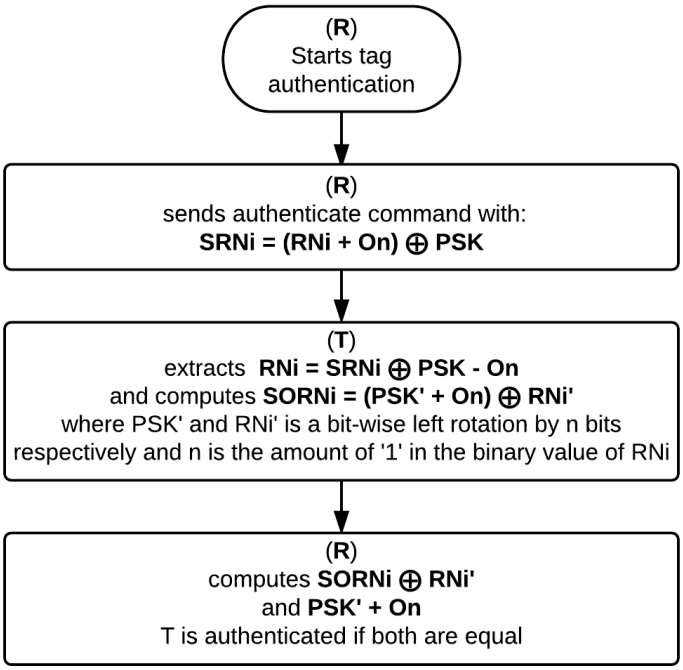

Figure 2.22 – Tag authentication using XOR

$$SRNi = (RNi + On) \bigoplus PSK \tag{2.7}$$

Upon reception of the challenge message, the tag performs a *XOR* operation with its preshared value, resulting in the *XOR* of the random number and the On value. To obtain the random number sent by the reader, the tag needs to remove the *On* number from the total (refer to Equation 2.8).

$$RNi = SRNi \bigoplus PSK - On \tag{2.8}$$

Once the random number from the reader is known, the tag computes the total summation of '1' in the binary value of the random number. As an example, a value of 13 in binary is 1101, therefore the total iteration of '1' is three. By using the total iteration value, it performs a bitwise rotation to the left on the random number and the preshared key in order to get both *RNi'* and *PSK'*.

With the help of these new values, the tag finally computes *SORNi* by performing a *XOR* operation between the total of the shifted preshared key with the *On* constant and the shifted random number (refer to Equation 2.9) and sends it back to the reader.

$$SORNi = (PSK' + On) \bigoplus RNi' \tag{2.9}$$

In order to authenticate the tag, the reader performs the bitwise rotation on both its random number and the preshared key to get the RNi' and PSK'. It performs a XOR operation between the received message and the RNi' (as in Equation 2.10). It also calculates the sum of PSK' with the constant value On (as in Equation 2.11).

$$SORNi \bigoplus RNi' \tag{2.10}$$

$$PSK' + On \tag{2.11}$$

The reader then compares results from the Equation 2.10 and the Equation 2.11. As a consequence, the tag is authenticated if the results are identical.

2.4.7 cryptoGPS

Named after the its inventors, Girault, Poupard and Stern, cryptoGPS is a lightweight asymmetric identification scheme based on an elliptic curve discrete logarithm problem (ECDLP).The prefix crypto is added to their acronym to avoid confusion from the Global Positioning System (GPS). Its implementation standard is defined in [73]. Prior to the standardisation, an example of the implementation is performed by Poschmann et al. in [81] which shows that the implementation requires between 2000 - 3000 GE. The cryptoGPS elliptic curve is represented in the Equation 2.12. A list of precomputed coupons is stored within the tag to minimize the calculation effort by the tag.

$$y^2 = x^3 + ax + b \tag{2.12}$$

To begin with, both reader and tags are required to refer to the same elliptic curve $\boldsymbol{E}$ with a field size of $\boldsymbol{q}$, a base point $\boldsymbol{P}$ and a multiplier $\boldsymbol{s}$. Any random point $\boldsymbol{V}$ on the curve $\boldsymbol{E}$ is equal to the multiple of base points $\boldsymbol{P}$ as presented in Equation 2.14.

$$V = -[s]P \tag{2.13}$$
$$= (x_v, y_v) \tag{2.14}$$

In the asymmetric cryptography, we consider $\boldsymbol{V}$ as the public key and $\boldsymbol{s}$ as the private key. Due to the complexity of its calculation, CryptoGPS uses preloaded coupons on the tags before using them. This is comparable to AES where it preloads its *keyID* beforehand as mentioned in section 2.4.4. These coupons consist of a set of precomputed data in a form of (r_i, X_i). The coupon is a one-off coupon that can only be used once. Figure 2.23 highlights the authentication process.

To start the authentication process, the reader sends an authentication request to the tag. Once the tag receives the request, it chooses a coupon X_i and sends it to the reader. When the reader receives X_i, it retrieves randomly a challenge $\boldsymbol{c}$ from its list of challenge and sends it to the tag. The tag computes and sends $\boldsymbol{y}$ according to Equation 2.15 where r_i is within the coupon selected, $\boldsymbol{s}$ is the private key and $\boldsymbol{c}$ is the challenge received. The protocol exchanged is presented in Figure 2.24

$$y = r_i + c * s \tag{2.15}$$

Upon reception of $\boldsymbol{y}$, the reader can deduce the r_i value according to Equation 2.16.

$$r_i' = y - c * s \tag{2.16}$$

With r_i the reader can then find X_i' and compares it to X_i. If they are identical, the tag is then authenticated.

Having presented the four main cryptographical suite algorithms used in the authentication of the Gen2V2 RFID tags, the following section will deal with the main mecanisms of localization that are employed in locating the RFID tags. The selected crypto suites will be implemented in the simulation and will then be

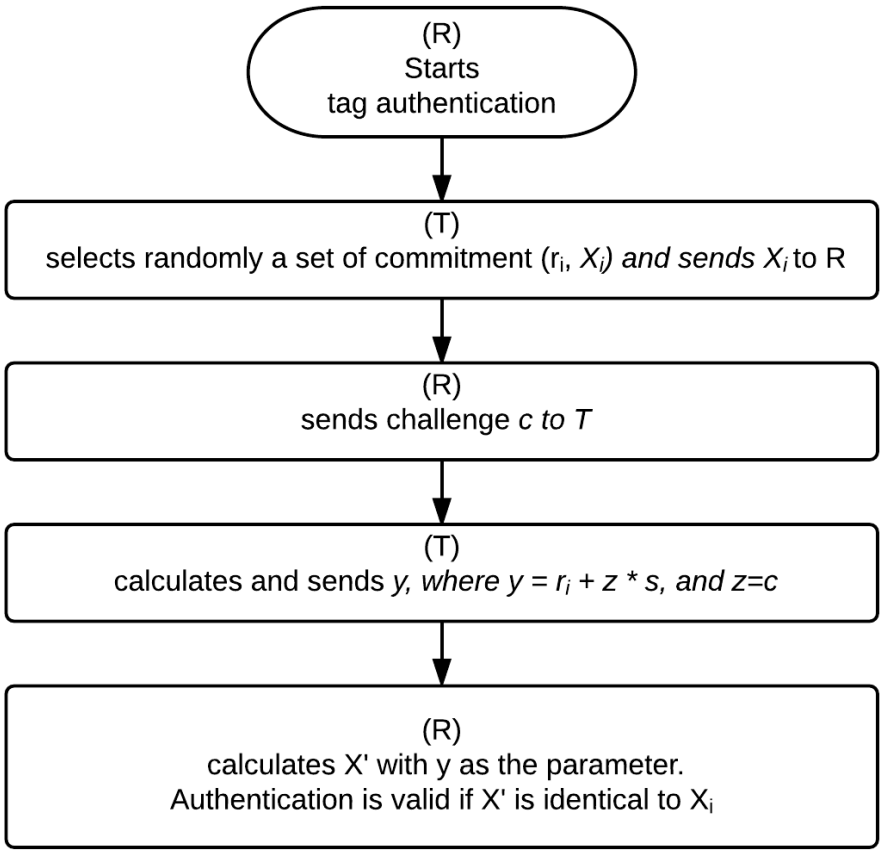

Figure 2.23 – CryptoGPS Commitment Challenge Response (CCR)

further evaluated in chapter 3.

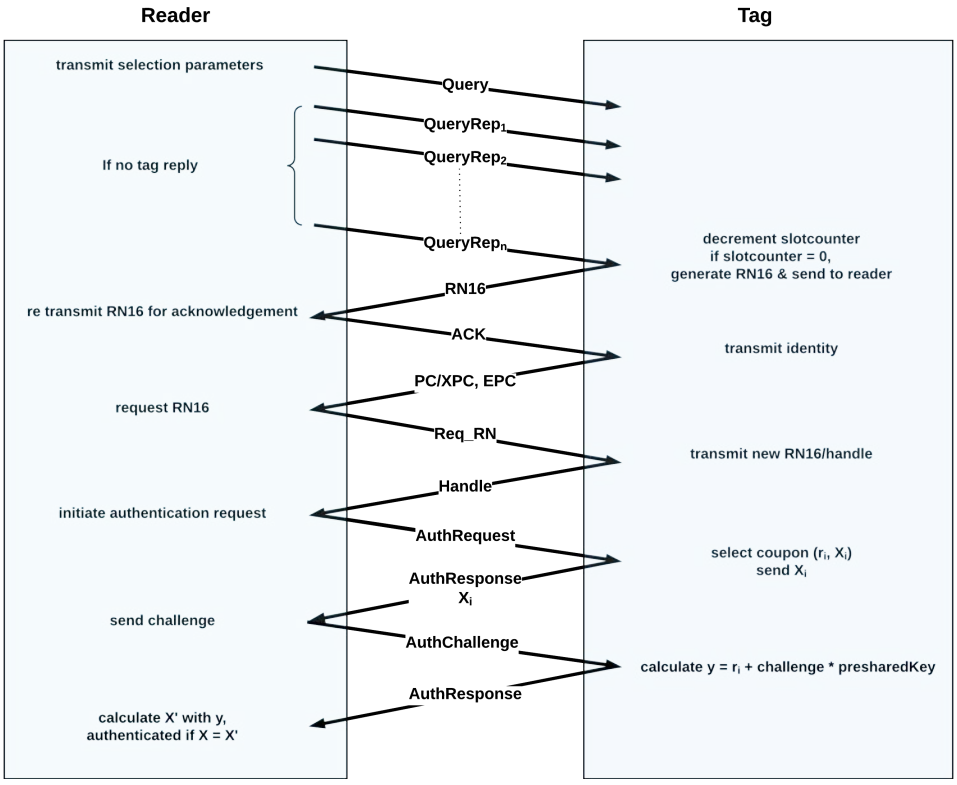

Figure 2.24 – cryptoGPS: Protocol exchange between reader and tag

2.5 2D Tag Localization

Tag localization is a research subject on its own. In this work we only focus in 2D localization. Numerous works have been done on different methods used to estimate the exact coordinates of a passive RFID tag. To name a few, Azzouzi et al. in [82] proposed the positioning of a tag based on the received signal using three antennas. The experiment requires a reference signal to be compared with. At the accuracy of 0.21 meter, it is vulnerable to multipath signal that can interfere in the calculation. Wang et al. in [83] on the other hand, offered an accuracy of 0.49 meter with an approach consisting of a mobile reader. The system estimates the distance based on the combination of the signal power and the angle of the signal received. Choi et al. in [62] proposed the use of the signal strength to estimate

the distance between a tag and a reader. The system designates several reference tags with known distances to help in estimation of the actual distance. The result of the signal from the tag to be positioned is then compared to the said reference. The error estimation of the system is at less than 0.21 meter. Recently, Zhao et al. in [84] proposed to group a set of tags based on their distance. However their precision is within 0.50 meter. Finally, Scherhaufl et al. in [85] demonstrated a 2D indoor localization based on the phase of the signal received with the help of reference tags. The error estimation of this implementation is at 0.01 meter.

As stated above, most localization techniques are based on physical characteristics of the signal travelling from the object to the receiver. Among the characteristics that are looked into are the different levels of the received signal strength, the time taken by the signal to travel from the source to the destination, the different angles of the received signal and the different phase of the received signal. Most of the localization methods are based on the comparison of the different values from different sources. The following section discussed the trilateration technique used to locate the object.

2.5.1 Trilateration

Trilateration is a concept of finding the position of an object based on three measurements [86, 87]. It calculates the intersection of three signal ranges centering at three different readers. To ease the presentation we will assume that the signal coverage can be depicted as a circle xxx if due to signal propagation in a real environment this range looks like a elipsoïde, The radius of the circle represents the distance of the tag from each reader. Therefore, before any trilateration calculation can be performed, the system requires that each reader provides its estimated value. Once ready, the reader sends to the system its coordinates and its distance from the tag as an update. From there, the system can calculate the estimated location of the tag.

The computed distance metrics by readers are based on various methods such the Time of Flight(ToF), the Received Signal Strength (RSS), the Angle of Arrival (AoA) and the Phase of Arrival (PoA). All methods will be presented in the following sections :

2.5.1.1 Roundtrip Time of Flight (RToF)

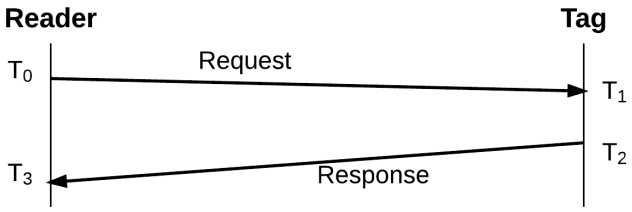

Figure 2.25 – Roundtrip Time of Flight

The Time of Flight (ToF), also known as Time of Arrival (ToA), refers to the time taken by the signal to travel from the source to the destination. As mentioned by Shen et al. in [88], it requires that the transmitter and the receiver are synchronized. Unfortunately, it is difficult to maintain the clock synchronization of a set of tags. However, since the reader is able to record the time when it sends a message and the time it receives the response, the Roundtrip Time of Flight (RToF) can be computed easily. It refers to the time taken by the signal to travel from the source to the destination and to return back to the source. ToA is then calculated by dividing by two the time taken to make the journey back and forth between the reader and the tag (refer Equation 2.17) assuming that the communication conditions are the same for both request and response.

$$ToA = \frac{RToF}{2} \tag{2.17}$$

To get the actual propagation time between the reader and the tag, we deduct the duration required to transfer both messages and divided the rest by two (refer Equation 2.20). The distance can be deduced by multiplying the *propagation time* (t_{Prop}) with the signal propagation rate (see Equation 2.21).

$$totalDuration = t_{Prop} + durationMsg1 + t_{Prop} + durationMsg2 \quad (2.18)$$

$$2 * t_{Prop} = totalDuration - durationMsg1 - durationMsg2 \quad (2.19)$$

$$t_{Prop} = \frac{totalDuration - durationMsg1 - durationMsg2}{2} \quad (2.20)$$

$$distance = t_{Prop} * propagationRate \quad (2.21)$$

2.5.1.2 Angle of arrival (AoA)

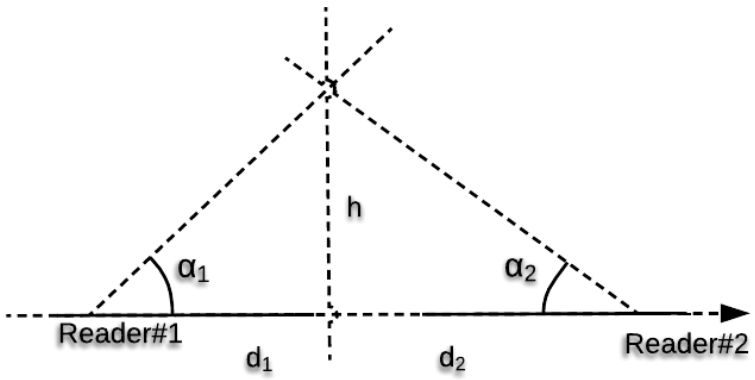

Figure 2.26 – Angle of Arrival

Angle of Arrival (AoA) refers to the angle of a signal from a source to arrive to the receiver/sensor. The angle is calculated based on a reference plane which is normally the horizon. Basic trigonometric definition gives;

$$tan(\alpha_1) = \frac{h}{d_1} \quad (2.22)$$

$$tan(\alpha_2) = \frac{h}{d_2} \quad (2.23)$$

$$d_1 + d_2 = \frac{h}{tan(\alpha_1)} + \frac{h}{tan(\alpha_2)} \tag{2.24}$$

$$d_1 + d_2 = \frac{h * tan(\alpha_2) + h * tan(\alpha_1)}{tan(\alpha_1) * tan(\alpha_2)} \tag{2.25}$$

$$d_1 + d_2 = \frac{h * \Big(tan(\alpha_2) + tan(\alpha_1)\Big)}{tan(\alpha_1) * tan(\alpha_2)} \tag{2.26}$$

$$h = \frac{(d_1 + d_2)(tan(\alpha_1) * tan(\alpha_2))}{tan(\alpha_2) + tan(\alpha_1)} \tag{2.27}$$

$$\tag{2.28}$$

once h is known, it is applied in Equation 2.22

$$d_1 = \frac{h}{tan(\alpha_1)} \tag{2.29}$$

Considering Reader 1 as the reference point, the tag coordinates can be deduced by:

$$T_{coord} = (x_{R_1} + d_1, y_{R_1} + h) \tag{2.30}$$

However, this method is not suitable for indoor purposes as the signal can be reflected by various obstacles. Further details on the advantage of using TDoA over AoA can be found in [89].

2.5.1.3 Received Signal Strength (RSS)

RSS estimates the distance based on the signal strength where the higher the signal, the closer the distance. However, the RSS alone can not guarantee the accuracy of the localization as other factors such as signal absorption, signal angle and signal reflection can impact the measured RSS. Alvarez Lopez et al. in [90] deployed a system with RSS with a combination with the AoA. Others like Choi et al. in [62] and Wang et al. in [83] are among the researchers who used RSS as the only method to locate a passive RFID object.

2.5.1.4 Phase of Arrival (PoA)

Phase of Arrival (PoA) estimates the length of multiple propagation paths by the backscattered tag signal to the receiver. To achieve this, Scherhaufl et al. in [85] used an antenna and series of passive tags. Hekimian Williams et al. in [91] added that the accuracy of PoA experiments is within milimeters.

2.5.2 Trilateration calculation

Once the distance estimation between each reader and the tag is known (refer to the following section), we can calculate the estimated coordinate by considering the reader 1 as the reference point. We have several known parameters such as all readers coordinates: (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) and the distance from reader to tag: r_1, r_2 and r_3.

As described in Figure 2.27, r_1 is the distance from tag to reader1, r_2 is the distance from tag to reader2, r_3 is the distance from tag to reader3. Several other constatation can be retreived within the same figure such as:

$$x_2 = x_1 - d \tag{2.31}$$

$$x_3 = x_1 - i \tag{2.32}$$

$$y_3 = y_1 - j \tag{2.33}$$

The following calculation will be done by considering x_1 = x and the solution of the intersection of the three circles is the estimated position of the tag.

$$(r_1)^2 = x^2 + y^2 + z^2 \tag{2.34}$$

$$(r_2)^2 = (x - d)^2 + y^2 + z^2 \tag{2.35}$$

$$(r_3)^2 = (x - i)^2 + (y - j)^2 + z^2 \tag{2.36}$$

To get the x coordinate, we subtract the Equation 2.34 from the Equation 2.35

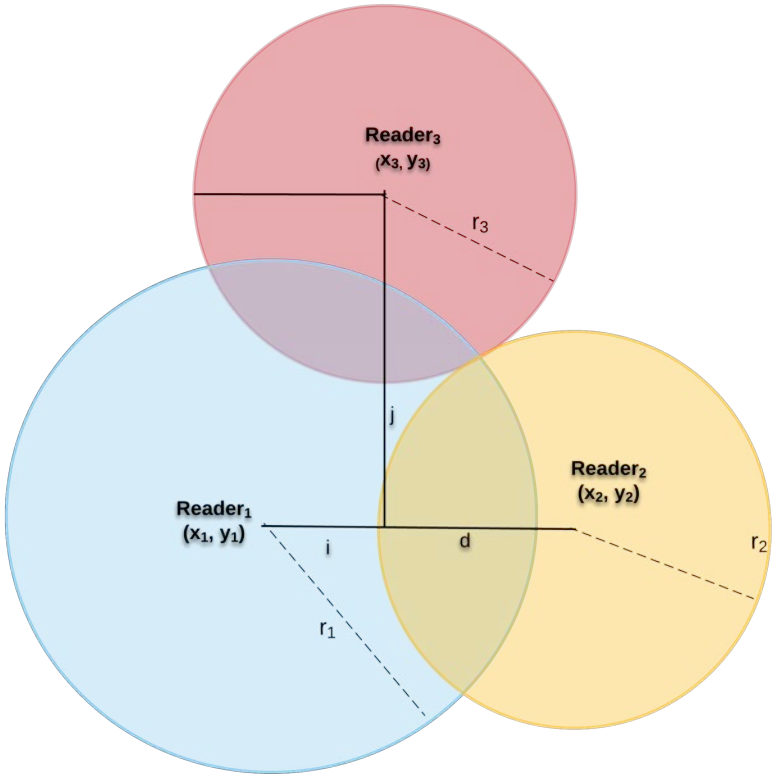

Figure 2.27 – Trilateration

$$(r_1)^2 - (r_2)^2 = x^2 - (x-d)^2 \tag{2.37}$$
$$(r_1)^2 - (r_2)^2 = x^2 - (x^2 - 2xd + d^2) \tag{2.38}$$
$$(r_1)^2 - (r_2)^2 = 2xd - d^2 \tag{2.39}$$

$$x = \frac{(r_1)^2 - (r_2)^2 + d^2}{2d} \tag{2.40}$$

x is known since the distance between the tag and different readers (r_1, r_2, r_3) and the distance between R_1 and R_2 (d) are known. To get the y value, we substitute

the Equation 2.36 with the Equation 2.34

$$(r_3)^2 - (r_1)^2 = (x-i)^2 + (y-j)^2 + z^2 - (x^2 + y^2 + z^2) \quad (2.41)$$

$$(r_3)^2 - (r_1)^2 = x^2 - 2ix + i^2 + y^2 - 2jy + j^2 + z^2 - x^2 - y^2 - z^2) \quad (2.42)$$

$$(r_3)^2 - (r_1)^2 = -2ix + i^2 - 2jy + j^2 \quad (2.43)$$

$$2jy = (r_1)^2 - (r_3)^2 + i^2 + j^2 - 2ix \quad (2.44)$$

$$y = \frac{(r_1)^2 - (r_3)^2 + i^2 + j^2 - 2ix}{2j} \quad (2.45)$$

Where i, the signed magnitude for x

$$i = e_x * (R_3 - R_1) \quad (2.46)$$

with the use of unit vector for x axis:

$$e_x = \frac{R_2 - R_1}{||R_2 - R_1||} \quad (2.47)$$

and j, the signed magnitude for y,

$$j = e_y * (R_3 - R_1) \quad (2.48)$$

and the unit vector for y axis.

$$e_y = \frac{R_3 - R_1 - ie_x}{||R_3 - R_1 - ie_x||} \quad (2.49)$$

We finally have the tag coordinates:

$$Tag_{coord} = R_1 + x_{e_x}x + y_{e_y}y \quad (2.50)$$

$$x_{Tag} = x_1 + x_{e_x}x + y_{e_y}x \quad (2.51)$$

$$y_{Tag} = y_1 + x_{e_x}y + y_{e_y}y \quad (2.52)$$

Ko [92], Fortin-Simard et al. [93] and Zhao et al. [94] are among other authors that work with the said method. In the next section, localization of objects and

the persons as well as the respect of privacy will be presented.

2.6 Privacy

Today's advanced technologies enable the collection of personal data into multiple databases. This can be done easily. Information such as name, date of birth, age and marital status are among the common ones but it does not just stop there as other personal data such as medical history and financial history are also easily accessible.

This section will discuss further on what is privacy, how private data are collected and how to manage the possibility of revealing a person's identity through multiple databases. Also discussed are the localization privacy with RFID tags, the threats and the definitions of privacy in the context of RFID.

The term privacy is used to represent the ability of a person to choose either to share or not to share his personal information such as health status, financial details, their whereabouts, interests, political affiliation, etc.

The individual should also be able to decide between which information and until what level of details he is willing to release and share with others. The individual should be able to share that he is in a shopping mall without the obligation to detail out the people he met, the shops he went to, the items he purchased and their price. He can merely choose to share that he went to the shopping mall for window shopping.

In the era of information technology, details such as name, gender and interest are the most common items collected through various media. The social media such as Facebook and Tweeter advocates the simplicity to identify a person. Some are willing to share their current location, mainly during their vacation, family trip or honeymoon. The motivation is essentially to share their happiness with their relatives or close friends. Some are willing to share the restaurant that they have visited. Some like to give feedbacks on the food they just ordered. However, the same person can also be reluctant to share the location he went to, to prevent any embarrassment, or whenever he needs to be left alone.

Most of the information gathered are not straight forward. Data are processed to find the association between the individual and the overall data collected. As

an example, the health status can be deduced by the type of medication taken by the individual or the visit frequency to a medical practitioner.

Not everybody is willing to share their health status with the public as it can be considered as very personal. The severity of the disease is not the measure either to share or not to share the information. Either if it is benign or serious, the individual should always have the control to decide whether to share or not his condition with anybody.

On the other hand, the association to a medical record can be done by detecting items within the same location as the individual. A group of drugs can identify a specific health problem. This can lead to a discrimination towards an individual from a specific service. Therefore to ensure the privacy of an individual, it is required to handle personal related data without the possibility to make a deduction towards the owner of the object. The ability to identify an object and an individual will open the possibility of profiling and tracking an individual. As a rule of thumb, an enforcement can be done by either to render the data to be anonymous [95, 96], or to change the identification of the object on every transaction (pseudonym) [97].

An example of possible data collection which is often overlooked by everyone; public transport companies usually store their customers' details and travelling logs to optimise their services; such as to either adding or reducing their fleet. On the other hand, collected data can create an opening in identifying to a certain extent, the workplace and the residence of an individual where his daily commute can indicate the stations served in the morning from his home and the reverse flow in the afternoon from his workplace.

Juels in [98] stated that two main concerns in privacy is the unauthorized tracking and inventorying. As an example, tracking could be done by associating the credit card with the item purchased and inventorying is the act of listing the items attached to a person such as member cards and loyalty cards. The author then mentioned that RFID tags are easy to duplicate as it is just strings of bits without any real access-control mechanisms. However, it limits the adversary to be physically close to a tag/reader. To enable privacy, the author listed several methods such as tag killing or tag sleeping that render the tag to be unusable. This method however, withdrawn the ability to identify a sold item from the

aftersales services. Another method described was the minimalism that releases different pseudonyms for every request. Therefore an unauthorized reader could not correlate the different pseudonyms with a single tag. To further enhance the protection, tags should limit their responses when queried hastily.

2.6.1 Localization Privacy with RFID tags

It is common nowadays to tag everyday items with RFID tags. With the help of a reader, one could identify, communicate, read/write and locate a tag. And data gathered from the tag could provide vital information of an individual.

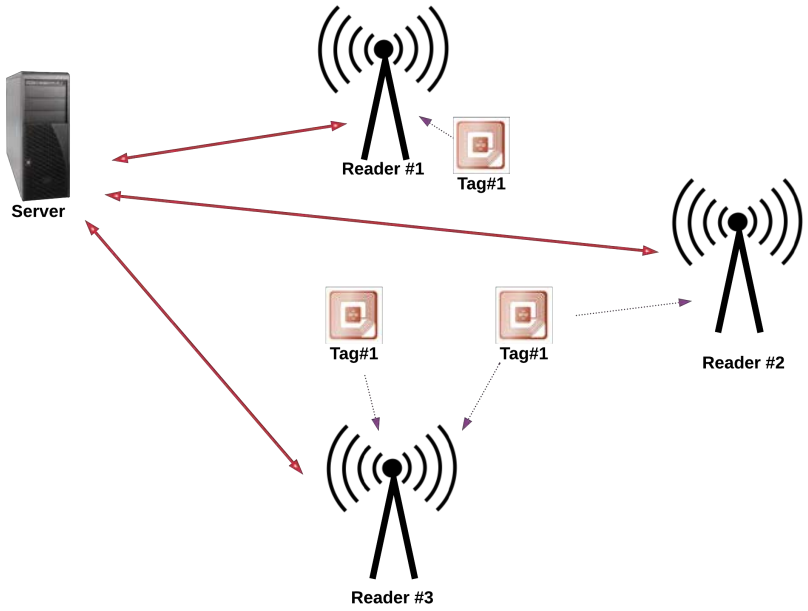

Figure 2.28 – Localization privacy topology

As an example, at home, a different group of items in a wardrobe could indicate the age range of a person, their specific interests in a brand of perfume, clothes and accessories. As illustrated in Figure 2.28, once a reader detects a tag, it relays the information to a server. The server serves to stores all tag information in its database. This information can lead to stereotyping a person. A free Internet connection provided by a shopping mall could help to locate a person in the mall.

With a set of free Internet access points, they could track the customer's whereabouts within their premise and therefore identify their interests. The duration of a person passing through the section could show their level of interest in certain things. This information could help the management of the mall to go about on how to arrange their goods. This, however, only applies to a device owned by customers which is equipped with a WiFi connection. On a bigger scale, every details gathered throughout the year could help to identify the person's residence, workplace, meeting locations, favourite restaurants, ideal routes, medical conditions, etc. This information is useful to improve specific services in the long run, but on the other hand, could also be used against the owner.

The scariest scenario is when a malicious person can continuously monitor individual's movement. It can lead to discrimination and an opening towards various crimes such as theft, blackmail, kidnapping or even murder. Therefore it is to the best of our interest to prevent this scenario from happening.

In the next subsection, the RFID localization privacy threat and ways to minimise the risk will be discussed.

2.6.2 Privacy Threat in RFID localization

RFID tag technology is vulnerable due to the inheritance of the wireless communication technologies' drawback. Any entity within the range of communication could capture information exchanged during the conversation. Non-protected communication could lead to clandestine inventorying, object tracking and up to identity stealing.

As anybody can hear every conversation within its range, it is possible to log the data exchange between the two speakers. The recorded data can then be compared with other related data that could reveal certain details. This situation is considered as a threat towards privacy. Such practice could disclose the following:

- Identity - By definition, every RFID will reply to a query request sent by a reader [47]. The default response could include the identification of the tag. If it is not well prepared and not encrypted, any entity within the range is capable of collecting the tag identifications.
- Location and time information - By default, there is no protection for the

communication medium. Therefore, any reader within the range could easily collect data with regards to the time and the position from the tag.

- Transaction History - Transaction history can give a trail of association between the owner and their sensitive data. This can reveal their whereabout within the system. Any entity can log details during a non-encrypted operation.

It is important to understand that a basic RFID tag does not protect the privacy of an individual. The use of RFID tags could expose specific details of a person without his knowledge. It is required to fulfill the following criteria to maintain the RFID tag privacy;

- anonymity - the ability of not being known, identified or tracked
- pseudonymity - the ability of not using the real name or identity
- unlinkability - the ability of not being able to specify the relation of two or more items
- observability - the ability of not being observed

All these criteria relate closely to the tag identity. If the identity is unknown, it could not be identified. Therefore it becomes anonymous and it is unlinkable to any other data. If it could not be linked, it could escape from being observed in the long run. However, is there any way to ensure that only the authorised person could identify a tag? The answer will be discussed in the following subsection.

2.6.3 RFID Privacy Definitions

Numerous researches discussed the formal RFID security and privacy model elaborately. Significant researches have been done on the existence of privacy within the RFID system [99]. Among topics discussed are the possible definition of a *strong privacy*. Juels and Weis in [99] define that a RFID system is considered private if no adversary has a non-negligible advantage in successfully guessing a specific tag identity. Vaudenay in [58] on the other hand, described that a strong privacy is not possible if the adversaries can corrupt any tags and read the return channel. Among the primary concern of a RFID privacy is on how to avoid the *traceability* of a tag [100]. However, Lu et al. in [101] highlight that a strong privacy have a scalability issue if the system is to be implemented in larger scale.

The authors then proposed a weaker definition to reduce the overhead and the delay of the implementation. It relies on the principle that a tag will produce a different output whenever it is interrogated by a legitimate reader in order to minimize the correlation between two sessions.

As mentioned previously, a RFID system requires a *tag* and a *reader*. And the definition of an *adversary* is required to address the malicious party.

- A tag (T) is an entity with limited storage resources and limited calculation performance. It has the possibility to provide secrets. It is equipped with a *session identifier* and is able to carry a cryptographic key [99]. The combination helps to increase the difficulty in guessing the secret key. On the other hand, it requires a particular intention to avoid corrupted tags [102].
- A reader (R) initiates a session and sends a challenge to a tag. Based on the response from the tag, it could then decide either to continue or to terminate the communication session. Most of the current authentication methods rely on this challenge-respond definition. Either it uses a pseudorandom generator, hashing function, symmetric cryptography, or asymmetric cryptography.
- An adversary definition varies a lot from one literature to another. Each tries to bring forward an issue that is not covered by the other. In general, an adversary can perform basic actions such as eavesdropping the communication channel. However, it can also perform advanced actions such as query inititation, message generation, send a challenge and response, data modification, query replay and set a secret key.
  A more elaborate definition of the formal model assumes the existence of different set of adversary that could perform actions such as monitoring all communication channels, corrupting tags and tracking tags within a limited period [58].

2.7 Conclusion

In this chapter, the general overview of IoT is discussed along with its application in AAL. Explanation on the RFID standard, classification and identification

is given. The RAIN RFID tag collision management is introduced to depicts the medium access control that is used in a multi user environment and that serves as a root for every communication including localization. The security in RFID which includes the passive and active attacks along with the authentication process are discussed. Apart from that, a presentation of the tag localization and privacy has also been done.

Having seen these, chapter 3 will give a clear insight of the work performed to model and implement a new RFID framework within the OMNET++ simulator as well as its anti-collision management, security features, localization and finally, the localization privacy.

3 Gen2V2 Framework in OMNET++

This chapter presents a newly created Gen2V2 framework within OMNET++. This framework serves to simulate the Gen2V2 Layer 2 exchanges that are not currently addressed in OMNET++. On top of that, an implementation of a new security module of several cryptographical suites defined in the protocol standard is proposed. Finally, a new module of tag localization is implemented. It will be a new localization privacy solutions. First, a presentation of the OMNET++ structure and items required to set up a project within OMNET++ will be discussed. The newly created framework will required a validity test to ensure that its functionalities correspond to the standard protocol. Therefore, the framework protocol validity is then checked through the anti collision management that is discussed in the previous chapter. This phase is critical to ensure that the results correspond to the theoretical values. Once validated, four algorithms presented in the previous chapter are then implemented within the framework to enhance its security especially for the authentication of the reader/tags. To further investigate the Gen2V2 characteristics, a radio medium is introduced within the protocol to simulate a wireless environment. The addition of a wireless environment within the framework enables the creation of an adversary entity that can passively eavesdrop any conversations on the shared medium. This adversary will be used to evaluate the security of the localization protocol.

3.1 OMNET++

At the beginning of this thesis, three years ago, none of the network simulators had a RFID model implemented, not even the RFID C1G2 standard. At

that point of time, OPNET [103], NS3 [104] and OMNET++ [105] were the best candidates among the existing simulators because they met all the main criteria needed for the automate or code modelization. Furthermore, they have the wireless communication features. OMNET++ has finally been selected for this work because of its modular framework which permits easier customization. On top of that, it has a powerful Graphical User Interface (GUI) which makes tracing and debugging tasks easier. Despite having the best GUI among the three, OPNET was not chosen because of it cost.

OMNET++ is a discrete event simulator. It is primarily designed to cater as a network simulator. However, its' modular approach enables other opportunities. The framework coding is done in C++, and it is free for non-commercial use.

OMNET++ offers a different framework that covers computer network from the underlying network protocol such as UDP, TCP, IP, IPv6, PPP, and Ethernet. It also includes an advanced system such as Wireless Sensor Network (WSN), Controller Area Network (CAN), vehicle network, cloud computing systems and satellite systems. However, there is no known framework that caters for RFID. Nevertheless Godor et al. works in [106] on Elliptic Curve Cryptography (ECC) for RFID have been successfully simulated in OMNET++.

3.2 OMNET++ structure

The advantage of OMNET++ is the possibility to design the framework in modular basis. Each module can be customized to match specific requirements. A particular protocol layer can be defined as a simple module (example in code 3.2).

In order to properly set up a project in OMNET++, at least a network definition and a simple module file are required. Other components that can be defined within a project are a compound module and a communication channel. To present further the structure, each item is explained in the following subsections.

3.2.1 Network definition files (NED)

A project in OMNET++ requires a network definition structure called NED (NEtwork Definition). This file defines the network structure with several elements such as parameters, gates, connections and submodules. It can be edited in a text format using any text editor or configured through the OMNET++ graphical user interface is in Figure 3.1.

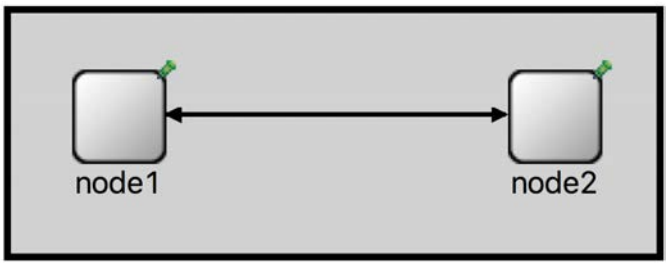

Figure 3.1 – OMNET++: network definition in graphical user interface (GUI)

In the code sample 3.1, a *sampleNetwork* is defined. The network consists of two nodes named *node1* and *node2* that want to communicate with each other. Both nodes are represented with submodules based on a simple module named *Node*, the bi-directional communication is enabled with gates in and out in both submodules.

```
package sampleNetwork;

network SampleNetwork {
submodules:
node1: Node;
node2: Node;

connections:
node1.out --> node2.in;
node1.in <-- node2.out;
}
```

Code 3.1 – network definition in text mode

3.2.2 Simple module

The most typical component in OMNET++ is called a *simple module* where basic behaviors are set. To communicate with other modules, it uses dedicated *gates* and a communication *channel* as depicted in Code 3.2 and Figure 3.2.

```
simple Node {
  gates:
        input in;
        output out;
        }
```

Code 3.2 – Node.ned

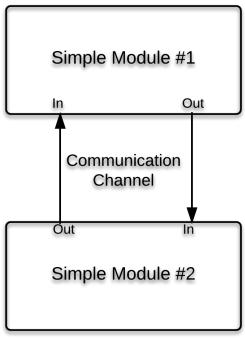

Figure 3.2 – Simple module

3.2.3 Compound module

A *compound module* defines the common parameters, the submodules, the input and output gates to the module and the communication channel parameters between each submodules (example in code 3.3). It is a combination of multiple "*simple modules*" such as described in Figure 3.3. It enables the creation of hierarchical layers of communication. Each object can have separate modules such as *identification*, *mobility*, *network layer*, etc. Each module can communicate with other modules by sending a message through the dedicated gates.

3.2.4 Communication channel

A *Communication channel* can be defined as a full duplex link or as a half duplex link. The advantage of the half duplex as in the code example 3.4 is that both channels can be set differently. The communication channel can represent various medium. It can be used to mimic the physical conditions of every communication technologies such as Bluetooth, Zigbee or WiFi by changing few parameters namely

```
module moduleCompound {
   parameters:

   gates:
      output   out;
      input    in;

   submodules:
      subModule1:      SimpleModule1;
      subModule2:      SimpleModule2;

   connections:
      subModule1.out --> subModule2.in;
      subModule1.in <-- subModule2.out;
}
```

Code 3.3 – Compound module

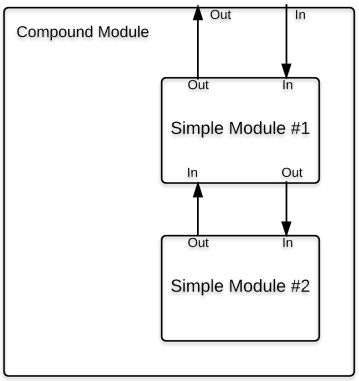

Figure 3.3 – Compound module

```
connections:
   node1.out --> {delay=10ms; ber=1e-8;} --> node2.in;
   node1.in <-- {delay=12ms; ber=1e-8;} <-- node2.out;
```

Code 3.4 – Basic communication channel example

the propagation delay, the data rate, the bit error rate (BER) and the transmission power.

3.2.5 OMNET++ coding

Once the network is defined, the protocol functionality is programmed in C++. As a discrete event simulator, OMNET++ reacts based on events triggered by the exchanged messages between modules or submodules. These messages pass through the input and output gates and can be retrieved using the *"handleMessage(msg)"* function. By means of this function, conditioning can be performed based on the message received.

3.2.6 OMNET++ troubleshooting

OMNET++ has the ability to record the program execution step by step. It generates a sequence chart throughout the program execution. The sequence chart as in Figure 3.4 can help in visualizing the exchanged messages sequences between

entities. All communications pass through the radio layer before being sent to their respective node to be processed further in time. In our example, a tag, a reader and an adversary are represented in two layers. At event #22, the reader[0] sends a *Query* request to tag[0] through its radio submodule. At event #23 its radio submodule forward the request to the tag[0] radio submodule. The request arrived at event #24. Noted that the same request is captured by the adversary radio submodule at even #25. After receiving the request at event #28, the nodeTag do not respond to the request. The sequence can help to identify if the node is not responding to conditionning of the message as per written in the program. In this case, it is due to the fact that the condition to respond is not met. Further detail on why it is not met will be discussed in the next section.

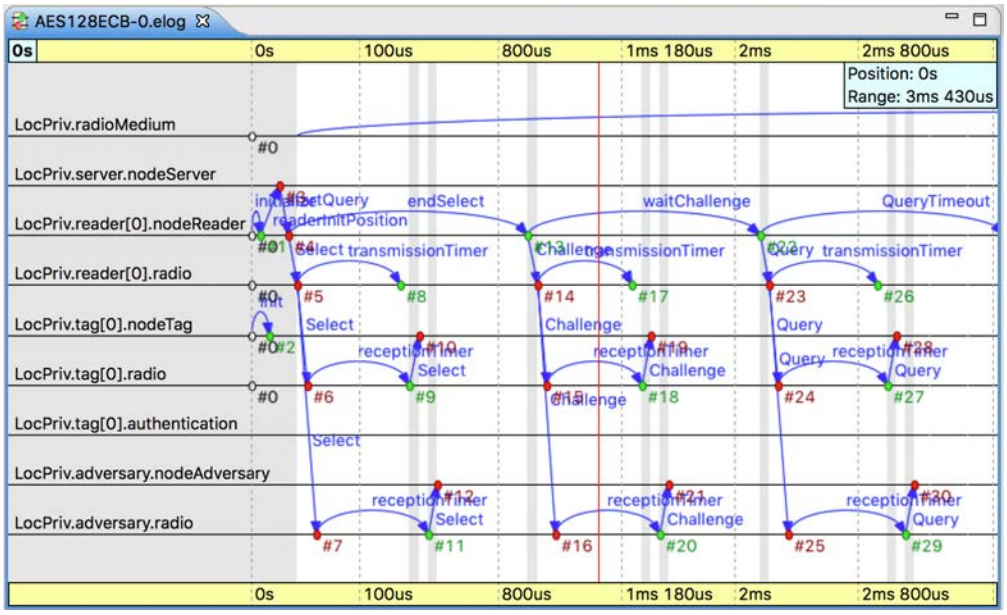

Figure 3.4 – OMNET++: Event Log

The troubleshooting of the protocol chronograms has been done based on the sequence chart in Figure 3.4 and the work is also presented and discussed in the next sections.

3.3 Gen2V2 framework

OMNET++ does not offer any RFID framework, let alone the Gen2V2. In order to study the passive RFID behaviour within OMNET++, the EPC Gen2V2 [47] specification is examined. The corresponding scenario depicted in Figure 3.5 and Figure 3.6 are then built within OMNET++. The implementation of both scenarios helps to differentiate the most efficient technique of the two. The initial Gen2V2 framework consists of creating two entities: a reader and a tag. Both required to be declared in a network definition file (explicitly *"Gen2V2.ned"* as depicted in code 3.5) to define the network between the two entities.

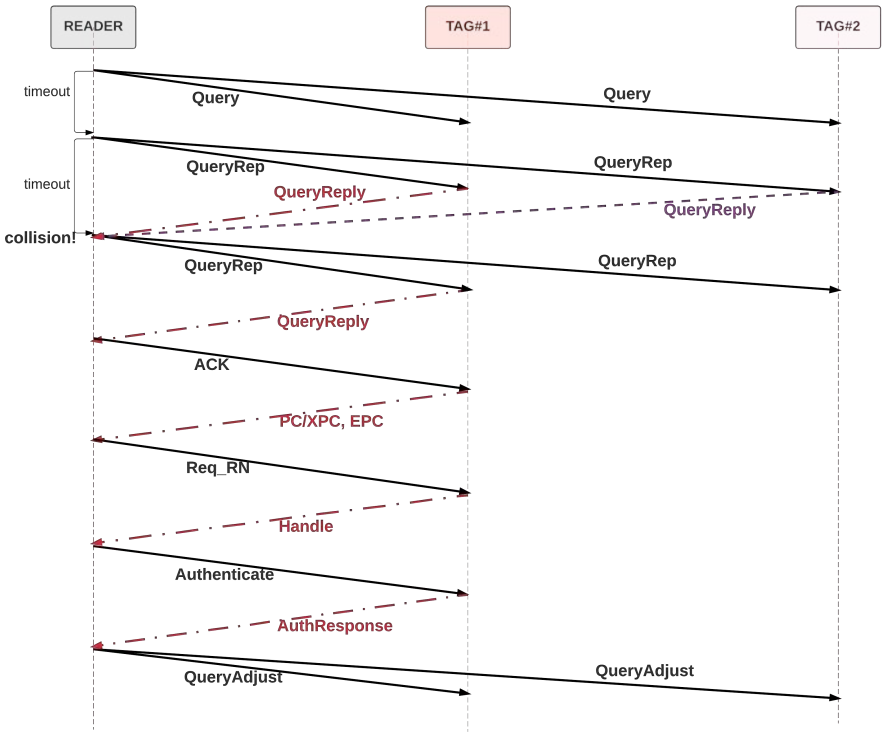

Figure 3.5 – Scenario 1: QueryAdjust at the end of the frame

The establishment of both modules *"Tag.cc"* and *"Reader.cc"* is then carried out in order to define their functionalities. Both are required to introduce a *"handleMessage()"* function in order to manipulate the received messages and to act

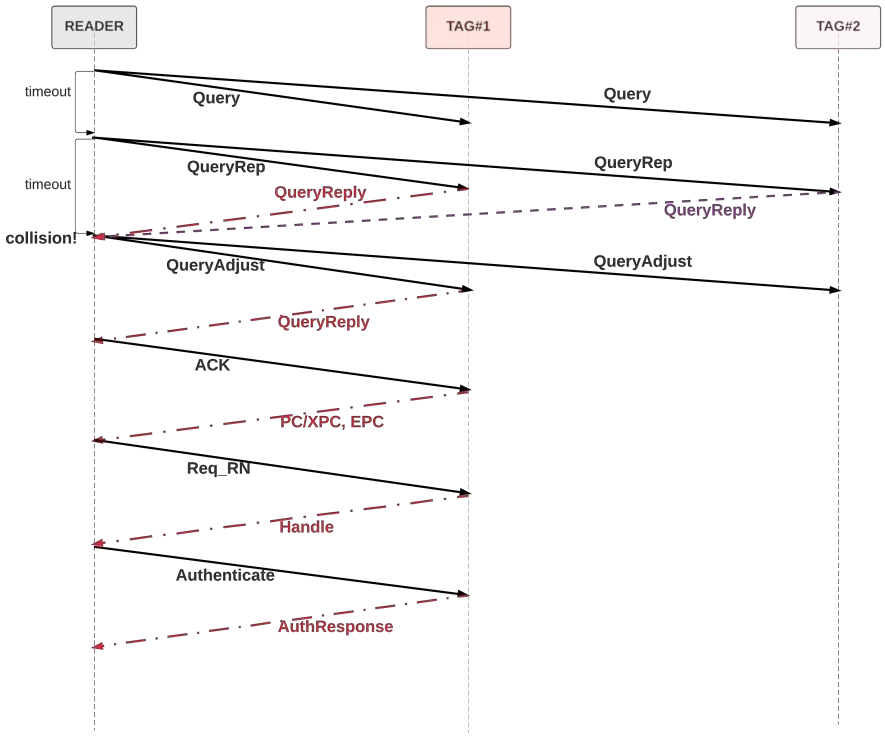

Figure 3.6 – Scenario2: QueryAdjust right after collision

accordingly. At this stage, the reader communicates directly with each tag through its input and output gate. As depicted in Figures 3.5 and 3.6, both tag and reader are needed to handle the exchanged messages. Figure 3.5 depicts the first scenario where a *QueryAdjust* is called at the end of a frame if any collision occurs during the session. On the other hand, the second scenario presented in Figure 3.6 called the *QueryAdjust* immediately after a collision occurs without waiting for the end of the session. The difference in terms of efficiency results between the two scenarios has been discussed in section 2.3.4.

At first, the reader sends a *Query* request in order to initiate a session as passive tags are unable to do so. It should be able to transmit the *QueryRep* if no tag is responding within the time limit or when there is a collision. At this stage, only the tag with a slot counter equals to zero will start transmitting the *QueryReply* message (Tag#1 in Figure 3.6). The *Acknowledgement* (ACK) is sent if the reader

received an answer from a tag. The random number request (Req_RN) is sent if the reader successfully received the tag identity (PC/XPC, EPC). If there is a collision that occurs within the frame, the *QueryAdjust* is sent.

```
network Gen2V2 {
parameter:
int numTags =  default (1);

submodules:
tag[numTags]:  Tag;
reader:        Reader;
}
```

Code 3.5 – Gen2V2.ned

On the other hand, the tag needs to manage the generation of a 16 bits random number to be sent to the reader as the first communication. It is done through the *QueryReply* process. Upon reception of ACK message from the reader, the tag will send its identity (PC/XPC, EPC) to the reader. Finally, the reader confirms that it receives the identity through a request, of another random number (Req_RN) from the tag. The tag will generate another 16 bits random number and send it back to the reader. This random number will be used as a reference for the following communication of the session.

3.3.1 Gen2V2 hierarchy

A new network definition file is redefined in order to ensure the possibility to easily improve the framework. In order to do so, submodules that characterize a protocol layer and an authentication layer (refer to code 3.6) are created.
It is then interpreted as the *NodeTag* and *NodeReader* that define the protocol layer and the *authenticationTag* and *authenticationReader* that serve as the authentication layer. The hierarchical method will render any modification to the current framework to be an easy task as it is treated in a modular manner. Any additional functions such as mobility can be added at this level in the future.

```
module moduleTag {
   parameters:
      @networkNode;

   gate:
      input in @directIn;

   submodules:
      nodeTag: NodeTag;
      authenticationTag:      AuthenticationTag;

   connection:
      nodeTag.toAuth --> authenticationTag.fromTag;
      authenticationTag.toTag --> nodeTag.fromAuth;
}
```

Code 3.6 – moduleTag.ned

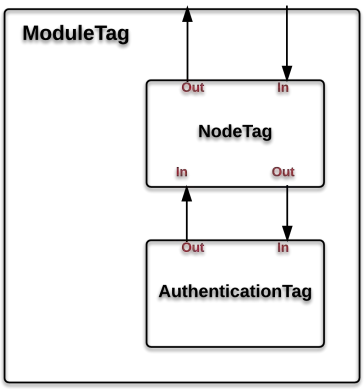

Figure 3.7 – ModuleTag Topology

```
simple nodeTag {
   parameters:

   gate:
      input in;
      output out;
}
```

Code 3.7 – nodeTag.ned

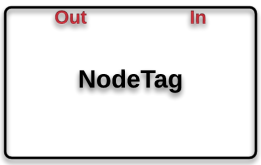

Figure 3.8 – NodeTag Topology

3.3.1.1 Module: ModuleTag

The objective of the tag's main module is to orchestrate the information between submodules and to define how they communicate. In the example given below (refer to Code 3.6 and Figure 3.7), the nodeTag is directly connected to the authenticationTag. Two communication channels are defined to establish the back and forth connection.
The main functionality of a tag is confined within the *nodeTag* submodule. All messages received by tag are evaluated and performed within this submodule's coding (refer to Code‘3.7 and Figure 3.8).

3.3.1.2 Submodule: authenticationTag

To complete the implementation, an authentication submodule is created and added to the framework. A network definition for the submodule is then defined based on AES128 (section 2.4.4), PRESENT80 (section 2.4.5), XOR (section 2.4.6) and cryptoGPS (section 2.4.7). The selected cryptographical suite is then implemented within the submodule coding and each of them is verified through their official test vectors [66, 67, 71, 73, 107]. The choice of cryptographical suite is then configured through a variable named *cryptosuiteID* that offers an option within the parameters segment (refer to Code 3.8).

```
simple AuthenticationTag {
   parameters:
      int cryptosuiteId:

   gates:
      input    fromTag;
      output   toTag;
}
```

Code 3.8 – authenticationTag.ned

```
void AuthenticationTag::handleMessage(cMessage *msg) {
  if (strcmp(msg->getName(), "AuthRequest") == 0) {
     if (cryptosuiteId = XOR) suiteXOR;
     else if (cryptosuiteId = PRESENT80) suitePRE80;.
     else if (cryptosuiteId = AES128) suiteAES128;
     else if (cryptosuiteId = cryptoGPS) suiteCryptoGPS;
     }
}
```

Code 3.9 – authenticationTag.cc

3.3.1.3 Submodule: Radio Medium

A shared communication medium is added to complete the simulated scenario. An open source model suite called the *"INET"* [108] offers a radio medium functionality within the OMNET++ simulator. It delimits the shared medium by supervising messages through radios and tracking the ongoing transmissions. The model defines the communication parameters such as the propagation rate and delay (refer to Code 3.10). At this stage, no external noise has been considered.

The addition of the shared medium submodule requires some modification within the framework. Various signals are needed to ensure its functionality. Each signal defines its operation state. The *reception state* informs reception availability, either it is buzy or ready to received any signal. The *signal transmission state* is used to inform that it is ready to transmit or that it is already buzy sending messages.

```
parameters:
@signal[receptionStateChanged];
@signal[transmissionStateChanged];
```

Code 3.10 – Parameter update for radio medium

3.3.1.4 Module: adversary

Once the communication between the reader and tags has been established, the framework becomes more elaborated with the addition of the authentication and the implementation of the radio medium. The adversary submodule is then added to complete the framework with the ability to eavesdrop communications through the shared medium. However, with the current implementation, man-in-the-middle attack can be added to the framework through this module.

3.4 Anti-collision management

In addition to the message administration, the reader handles collisions by detecting if there is more than one tag trying to send their response at the same time. As previously mentioned in section 2.3.4, the frame size is defined by a Q value , where 2^Q represents the number of slots within a frame. The association time is calculated from the first request sent by reader in the first slots until the last message received from the last tag in the last slot of the frame. The reader is required to wait for a certain period of time also known as *timeout* before sending a new request indicating the beginning of the next slot. Therefore, even if the slot is free, the reader still requires to allocate a certain amount of time to ensure that the slot is not in use. The overall number of collisions for different number of tags with different values of Q is represented in Figure 3.9. Note that the choice of

frame size depends on the number of tags. If the frame size is too low, the number of collision increases and a retransmission is required, resulting in an increase of the duration to associate the group of tags.

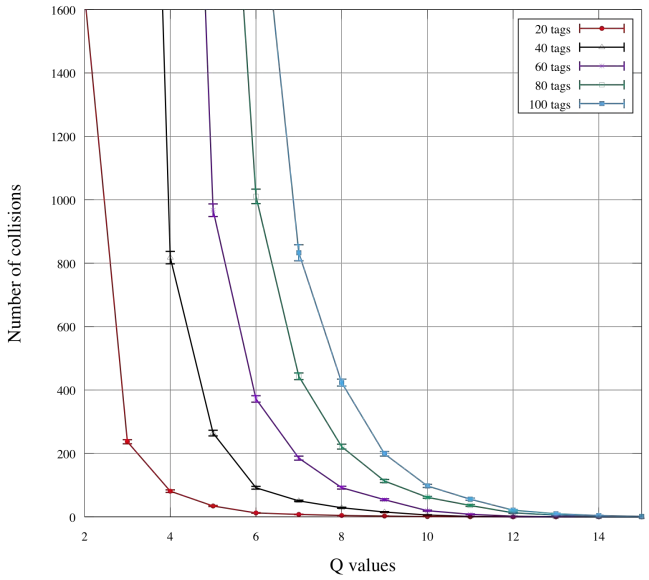

Figure 3.9 – Collisions vs Q values

A bigger frame size does reflect less collisions. However, it does not represent the best solution for the system as presented in Figure 3.10 where tag association duration keep increasing after a certain Q value. As an example, for 100 tags, the duration increases exponentially after Q is equal to 7. Therefore, even with 800 collisions as in Figure 3.9, Q=7 still represents the fastest time to interrogate 100 tags. This enforces the previous efficiency theoretical representation in Figure 3.12.

As described in Figure 3.11, if the reader is receiving a message, it is considered as busy and a collision is detected. The reader will then discard any incomplete message and will send a *QueryRep* to re-initiate the request. Otherwise, it will proceed to the next stage.

To validate the framework, a comparison of the efficiency result from the simulation and the Frame Slotted Aloha (FSA) theoretical value is performed (refer to section 2.3.4). The Figure 3.13 represents the channel utilization efficiency of 100 tags at different frame sizes (frame size is equal to 2^Q). Note that the simulated value of

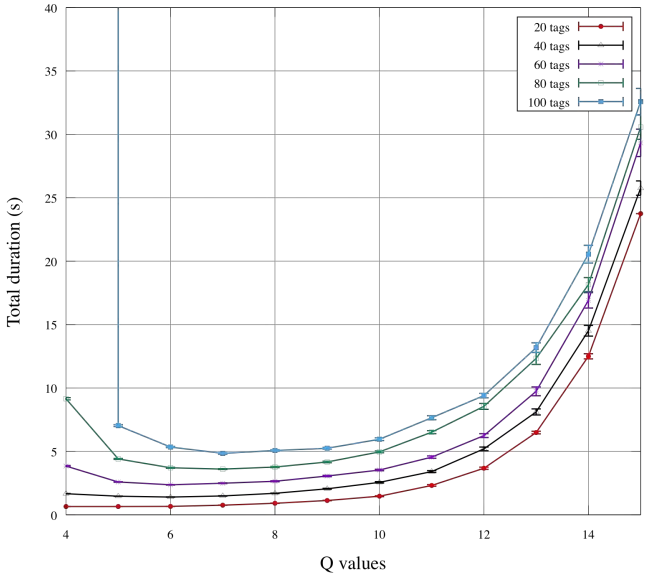

Figure 3.10 – Total duration of association

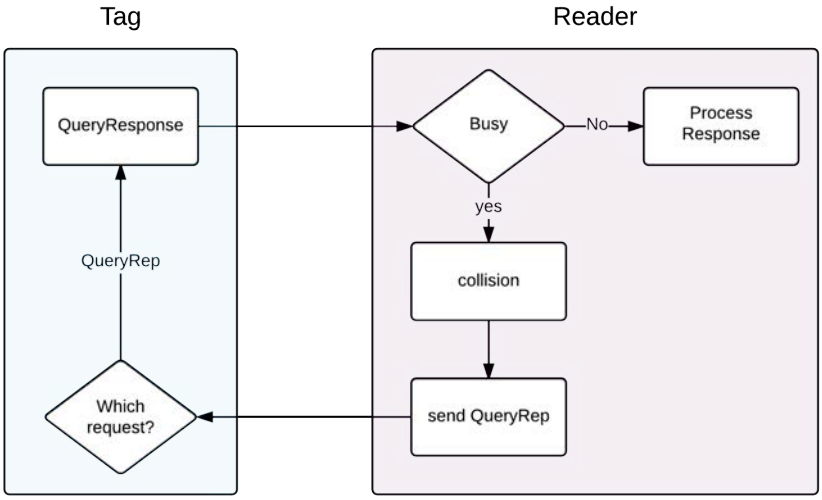

Figure 3.11 – Reader's collision management

the scenario 1 (in red triangle) represented in Figure 3.5 is similar to the theoretical FSA values (in black circle) thus validating our implementation. In addition, the simulation also gathers a second result from scenario 2 (in green square) as per Figure 3.6 where the reader restarts another frame immediately after a collision.

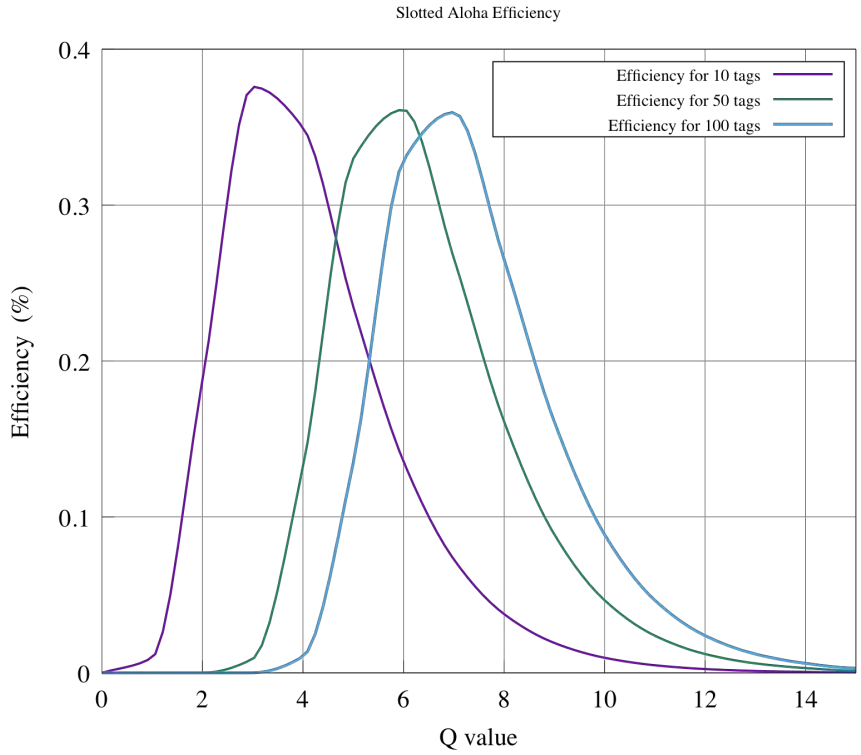

Figure 3.12 – Slotted Aloha Theoretical Efficiency

The result shows that scenario 2 requires a bigger frame to achieve the maximum efficiency therefore not matching the theoretical FSA value. In other words, it is not the best way to implement the protocol.
Once the framework is validated, the implementation of the four cryptographical suites can be made in the proposed Gen2V2 framework.

3.5 Cryptographic Suites within the framework

The major improvement of Gen2V2 from the previous passive RFID version is the implementation of nine cryptographical suites within the protocol. It requires both tag and reader to indicate which cryptographical suite to be used. A modification of the *tag* and the *reader* initial module within the framework is needed. A hierarchical component is required to address this changes. It reflects a new definition structure to cater this new functionality.

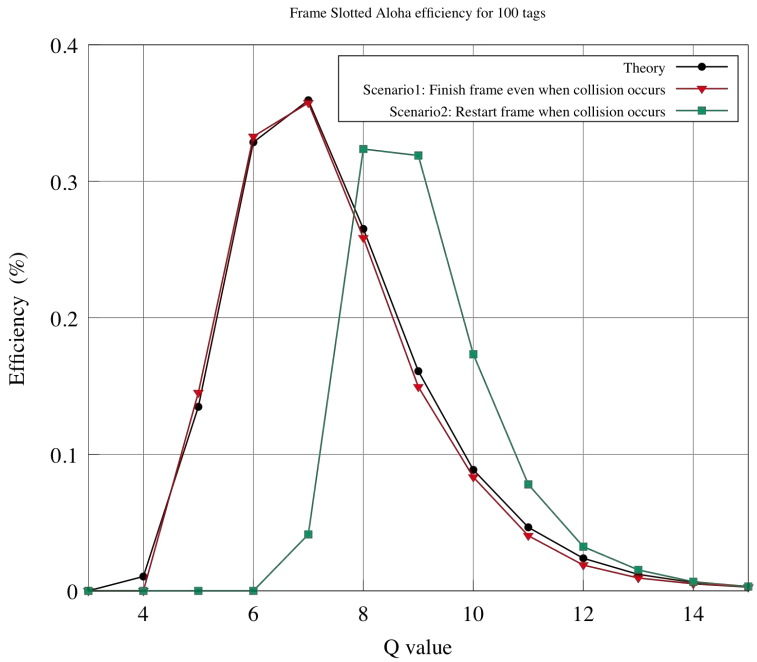

Figure 3.13 – Efficiency comparison with 100 tags

3.6 Cryptographical suites evaluation results

The framework helps to evaluate the impact of the authentication protocols response on the system time. The performance is evaluated based on the duration required to perform all message exchanges without considering the time to perform the authentication calculations. The evaluation includes all four encryptions suites presented in section 2.4. The curves in Figure 3.14 and Figure 3.15 illustrate the average time needed to perform the association of every tag using the cryptographical suites mentioned above and will be discussed further in the next subsection.

3.6.1 Evaluation parameters

Each simulation parameter is set within *omnetpp.ini* The 95% confidence interval is performed to validate the result where thirty rounds [109] of simulation with different seeds of random numbers are executed. The first line described the number

of the random seeds required. The seed is then applied to the *nodeTag* and the *nodeReader* respectively. To perform the simulation, a bitrate is set to simulate the transfer speed, the number of reader is set, the number of tags can also be defined.

3.6.2 Framework execution

The execution start time is recorded and used as the baseline. The execution finish time is also recorded in order to get the overall duration as in Figure 3.10. It reflects the duration required to perform all message exchanges.
A start time at the beginning of each cryptographical suite is also registered along with the end time. The difference of the two enables the calculation of the authentication duration as depicted in Figure 3.14 and Figure 3.15.

3.6.3 Simulation results

In order to validate our results, the performance of the tag association without any authentication is used as a baseline. The execution duration to associate all tags through different cryptographical suite is then recorded and compared to the baseline. Figure 3.14 and Figure 3.15 depict the result of the authentication simulation where each curve represents the duration required to finish interrogating 20 tags and 100 tags. Note that both figures have similar pattern as Figure 3.10 where the duration increases with the size of the frame.
The additional duration observed is due to the authentication and is inline with the amount of data exchanged between the tag and the reader during the authentication process (refer to Table 3.1).

	PRESENT80	XOR	AES128	cryptoGPS
R to T (bits)	112	139	160	72
T to R (bits)	121	121	185	465
Total	233	260	345	537

Table 3.1 – Bit exchange between tag and readers

As expected, the authentication takes an additional time to be performed. At first, PRESENT80 seems to be the best solution as it impacts the less the association

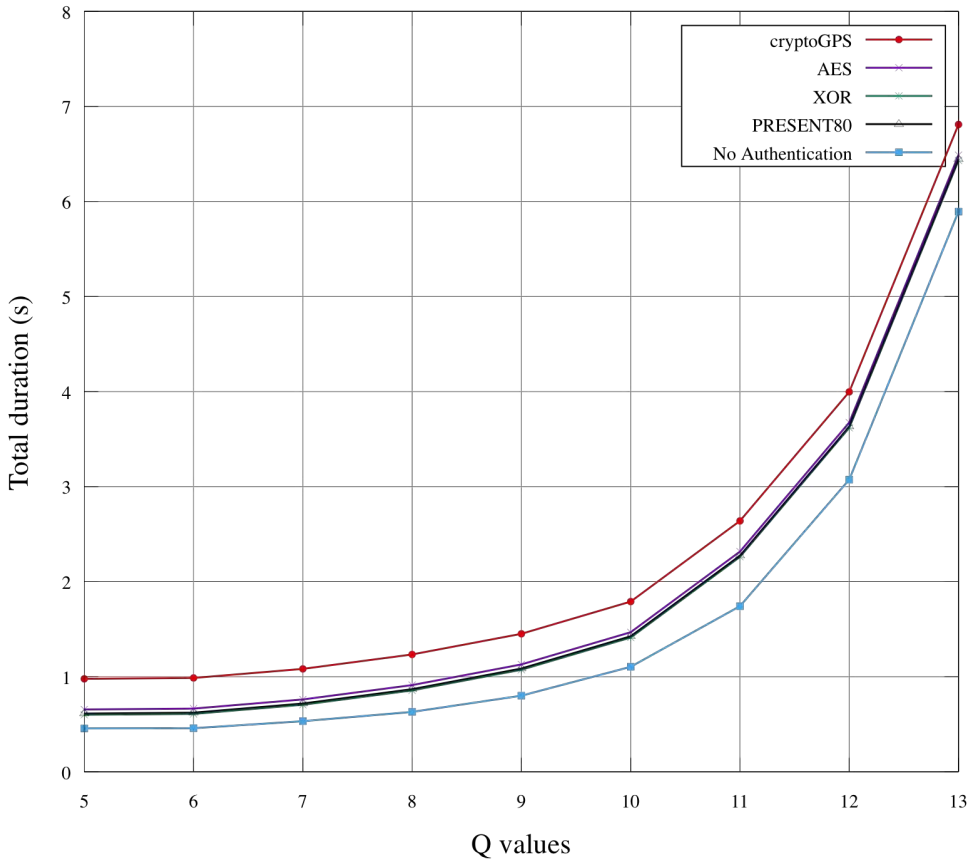

Figure 3.14 – Authentication duration for 20 tags

time. But even with an additional time cost cryptoGPS is still a relevant candidate as it relies on an asymmetric algorithm which is known to be more secure than symmetric one, where secret key is shared between the two entities. Furthermore, cryptoGPS authenticates both the reader and the tag while others only perform the tag authentication.

In the next section, the RFID localization will be further explained and elaborated. The section will cover from the implementation of the RFID up to the results gathered from the simulation.

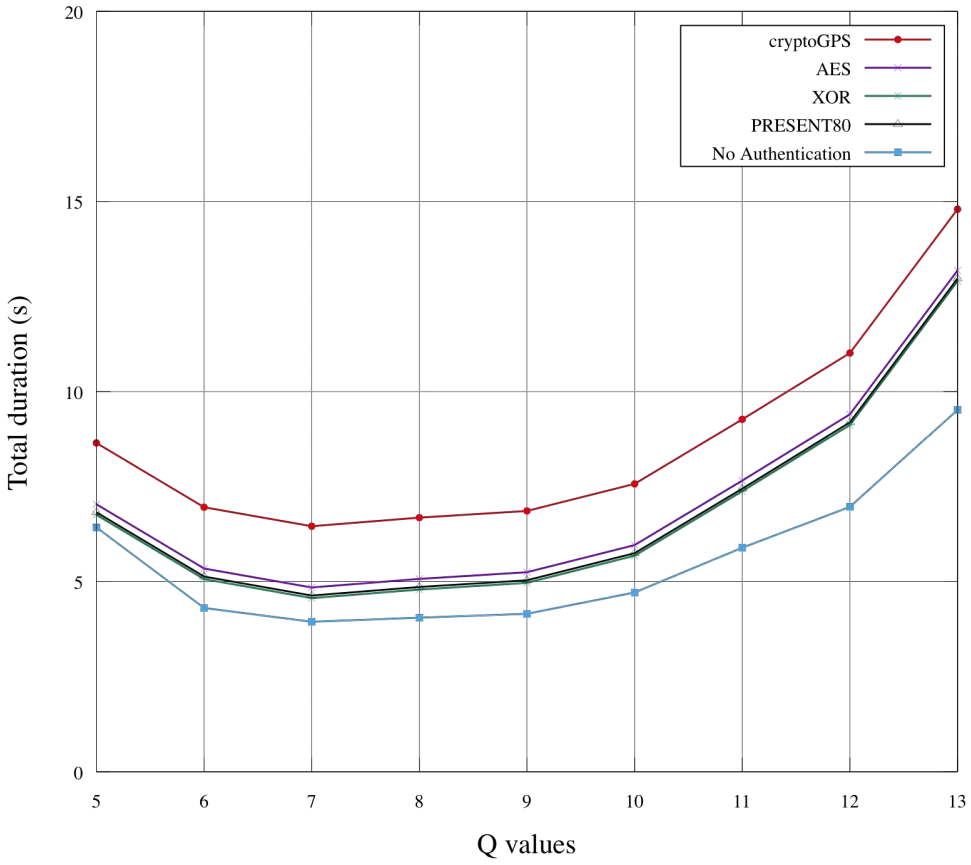

Figure 3.15 – Authentication duration for 100 tags

3.7 RFID localization

A trilateration method is a suitable solution to perform localization of a RFID tag as discussed in section 2.5. It requires three readings from three different readers that are at known positions and are assumed to remain still. All readers are required to report their distance to the tag to localize. As readers do not have any intelligence, it is therefore a necessity to have a central entity to gather these measurements and to perform the localization. A server module is then created for this purpose. It has the task to coordinate the query requests from all readers to avoid unnessary collisions and to collect all the feedbacks. No communication error is considered between the server and the reader. The Figure 3.16 depicts the implementation used in this work in order to locate a tag. The server serves

to calculate the location of a tag based on the distance feedback from the three different readers. Noted that the medium implemented at present is considered as perfect and without any interference. The following section will introduce the server module in detail.

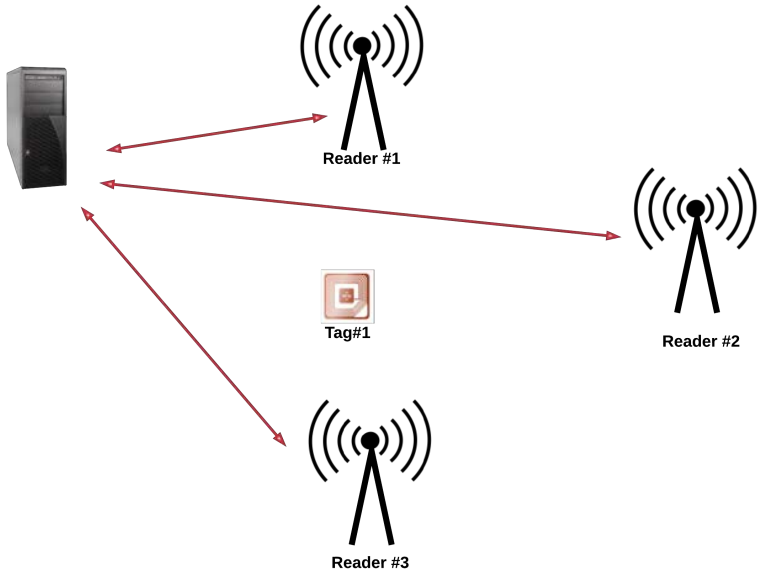

Figure 3.16 – Localization Topology

3.7.1 Module: Server

The server coordinates the communication initiation by the readers towards RFID tags. It has the possibility of requesting a reader to collect information from the tags. The information are updated regularly by the readers through dedicated gates. Code 3.11 helps to understand how to automate and connect multiple gates definition without the need to set the gate explicitly. First, the number of readers is defined in *"parameters"* segment. The creation of the same number of input and output gates is defined in the *"gates"* segment. In the segment *"connections"*, the link betwwen the server and all readers are configured through a loop of a number of readers. Noted that communications between the server and readers are performed through a wired network that is assumed to be secured.

```
module ModuleServer {
        parameters:
                int numReaders = default(1);

        gates:
                input fromReader[numReaders];
                output toReader[numReaders];

        submodules:
                nodeServer: NodeServer;
                localization: Localization;

        connections:
                for i=0..numReaders-1 {
                        fromReader[i] --> nodeServer.fromReader[i];
                        toReader[i] <-- nodeServer.toReader[i];
                }
                nodeServer.toLocalization --> localization.fromLocalization;
                nodeServer.fromLocalization <-- localization.toLocalization;
}
```

Code 3.11 – moduleServer.ned

3.7.2 Submodule: localization

The localization submodule is added to the server module to benefit its ability to gather information from various readers one by one to avoid possible collisions. If only one reader exists, the position of the tag is estimated on a circle around the reader with a radius of the gathered distance. Having two readers give the opportunity to have two possible coodinates on the intersection of the two circles. The ideal case is when there are three circles (as in Figure 2.27) that enable the system to perform the trilateration calculation as described in Section 2.5 and illustrated in Figure 3.16. At this stage, no external noise is taken into consideration within the radio medium. Therefore the communication signals are not modified in any way. Thus the three circles will intersect with each other.
There are three different approaches in the implementation of the localization submodule. The first and the third scenario are the continuation of the validated framework. The second requires a major change in the coordination of how the reader associate with a tag Therefore, the RFID standard validity is unknown for this second scenario, hence not implemented in the current framework.
The summary of all three scenarios are presented within Figure 3.17 where at the end of each scenario, the server is able to gather information as in Table 3.2.

	$Reader_n$	$Reader_2$	$Reader_n$
Tag_1	$distance_{r_{1t1}}$	$distance_{r_{2t2}}$	$distance_{rn_{tn}}$
Tag_2	$distance_{r_{1t2}}$	$distance_{r_{2t2}}$	$distance_{rn_{t2}}$
	▪	▪	▪
Tag_n	$distance_{r_{1tn}}$	$distance_{r_{2tn}}$	$distance_{r_{ntn}}$

Table 3.2 – Tag distance from readers

Basically, *scenario 1* and *scenario 2* require the server to wait for all readers to finish locating all tags before it is able to calculate the location. This is due to the fact that the reader is coordinated consecutively to associate all tags, while the rest of the readers remain inactive. In *scenario 3*, the server receives the distance updates from all readers eventhough they are not the active one that interrogates the tag. All inactive readers within the communication range that receive the communication from the tag should now send a feedback to the server. This passive detection is depicted as dotted squares in figire 3.17. Therefore, the server is able to interprete the tag position much earlier in this scenario comparing to the other two. In this scenario, reader#2 and reader#3 are not required to interrogate the tag in order to estimate their distance. All simulations are performed with the optimum Q value obtained in Section 2.3.4.

3.7.2.1 Scenario 1: Wait for all tags

The first scenario localize a tag after all readers have completed the interrogation of all tags. Therefore, to be able to locate a tag, the server is required to wait for all tags to be detected by all readers. This specific operation requires the sum of time needed to detect all tags in all readers which can be presented as

$$LocatizationTime = \sum_{j=1}^{m} \sum_{i=1}^{n} r_j t_i \tag{3.1}$$

where m is refering to the number reader, n is refering to the number of tags and t_i is the time taken to associate a tag. The detail of the process of reader1 interrogating two tags is depicted in Figure 3.18. First, the server initiates a *startQuery* that indicates reader1 to start interrogating the tags. Reader1 will

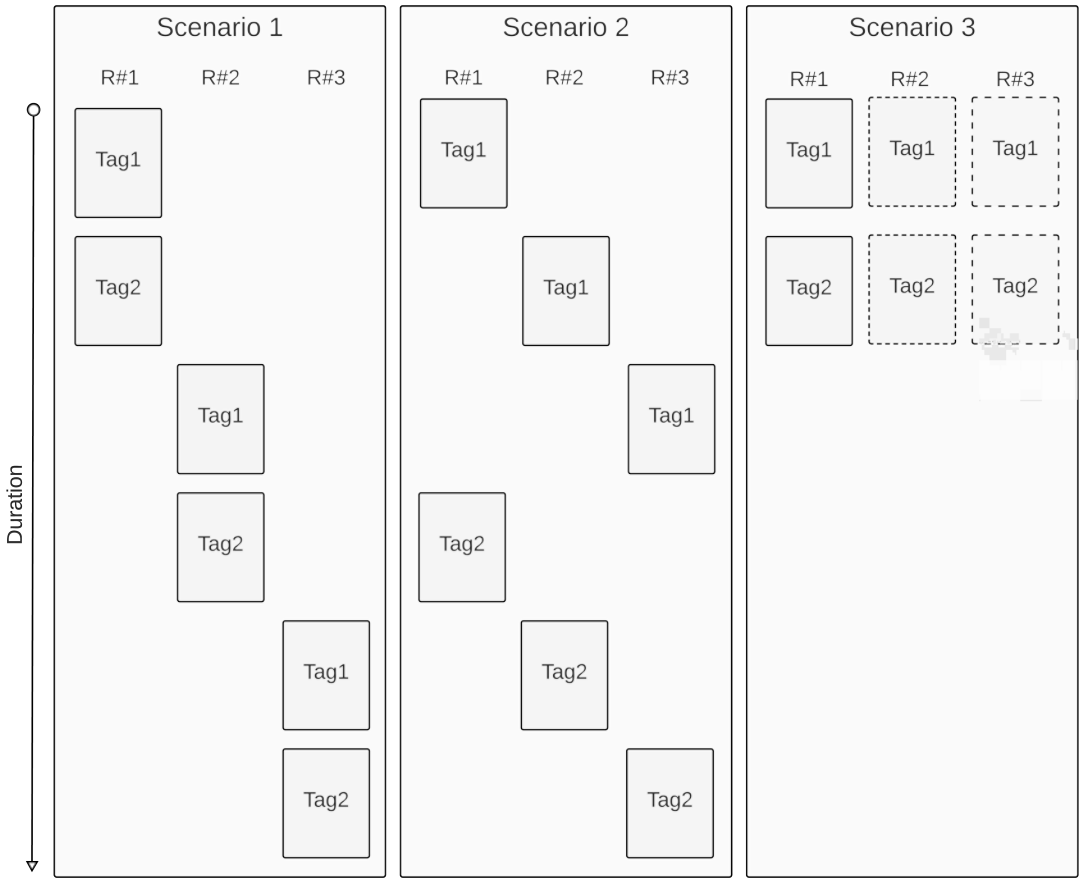

Figure 3.17 – Scenario summary

then proceed to interrogate all tags within its range by following the FSA principle as discussed in Section 3.3 before sending a notification to the server stating that it has associated all tags. The server will repeat the process with all readers until it receives feedbacks of the corresponding distances between every tags and every readers as depicted in Figure 3.19. The server then compile all results in the localization calculation.

3.7.2.2 Scenario 2: Tag by tag

In the second scenario, the server requests a reader to interrogate every tag one by one. This implementation is however not included within the framework since it is not scalable. It does not comply with the current standard that associates

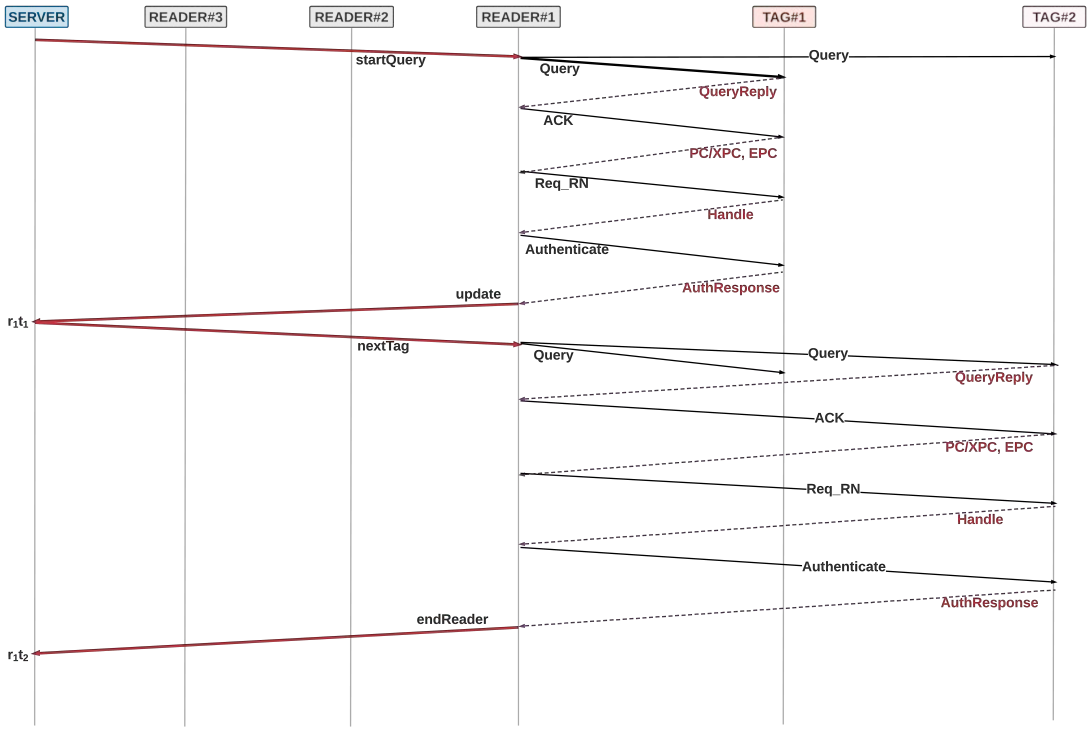

Figure 3.18 – Scenario 1: Reader1

all tags within its range before proceeding to the following reader. It also requires a radical change in the current framework. In scenario 1, the server initiates a reader to start sending query to the tags and the rest of the process is done by the reader. If the second scenario is to be implemented, the reader needs to be reconfigured to only forward all the query requests when it is told to do so and the server is required to manage the slot counter of each readers. As a consequence, a bigger number of readers creates a bottleneck to the system due to excessive communication between the server and the readers. The time taken to locate a tag is reduced to:

$$LocalizationTime = \sum_{i=1}^{m} t_i \tag{3.2}$$

However as depicted in Figure 3.17 the total duration to localize the same group of tags remains the same as the first scenario since all readers are required to interrogate the tag one by one with all tags in the group (refer to Equation 3.1). Note that in overall, only tag sequence is changed. The duration required to locate

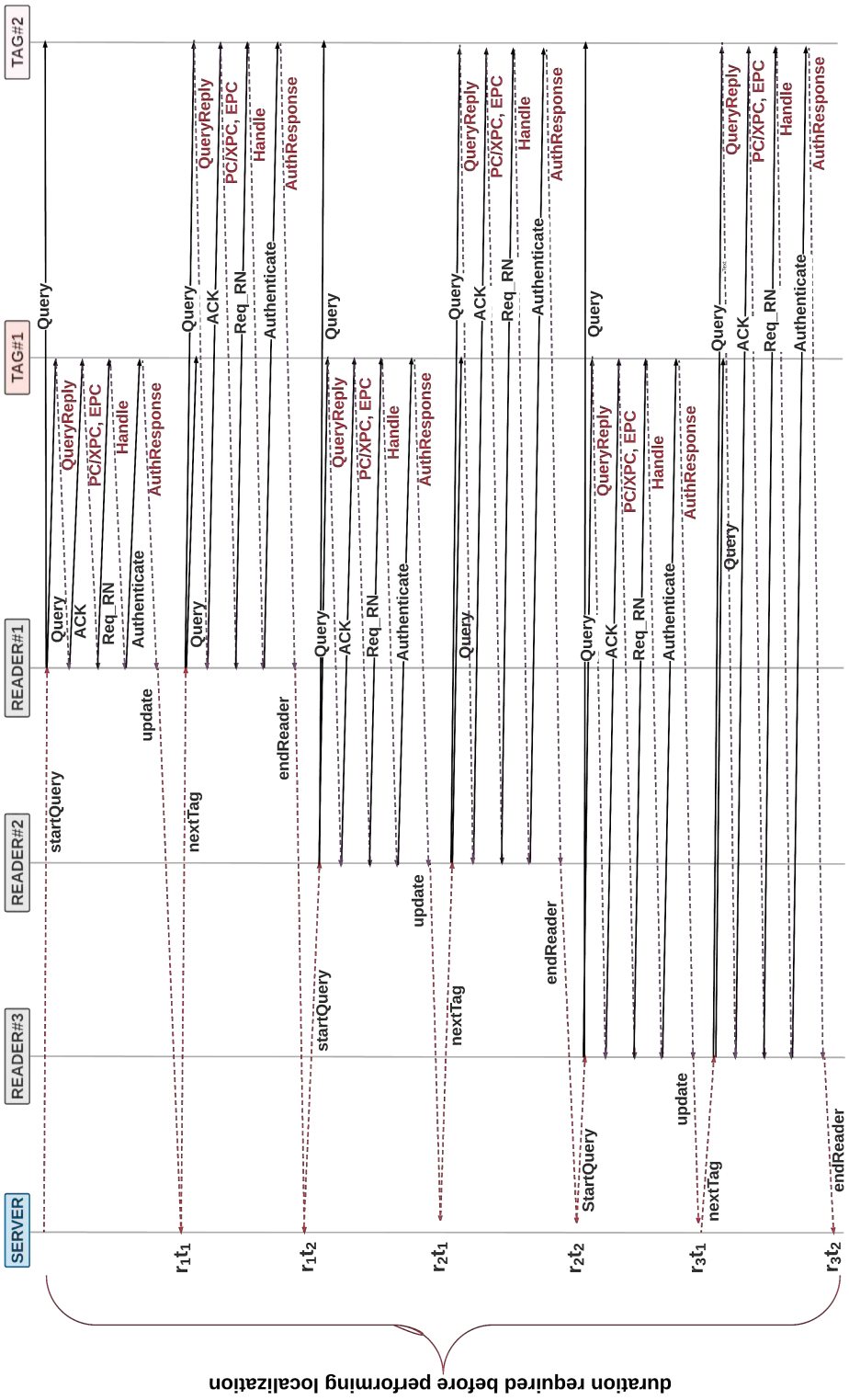

Figure 3.19 – Scenario 1: Wait for all tags to be detected by all readers

still remain the same. Therefore no further investigation will be proceeded.
As mentioned in Figure 3.20, the server can perform the localization calculation once all the readers have updated their distance from a specific tag. Opposing to the previous scenario, the time taken to locate a tag does not require the server to wait for the discovery of the total number of tags. However, the total duration to locate a set of n tags in scenario 1 and scenario 2, requires the same amount of time as illustrated in Figure 3.17.

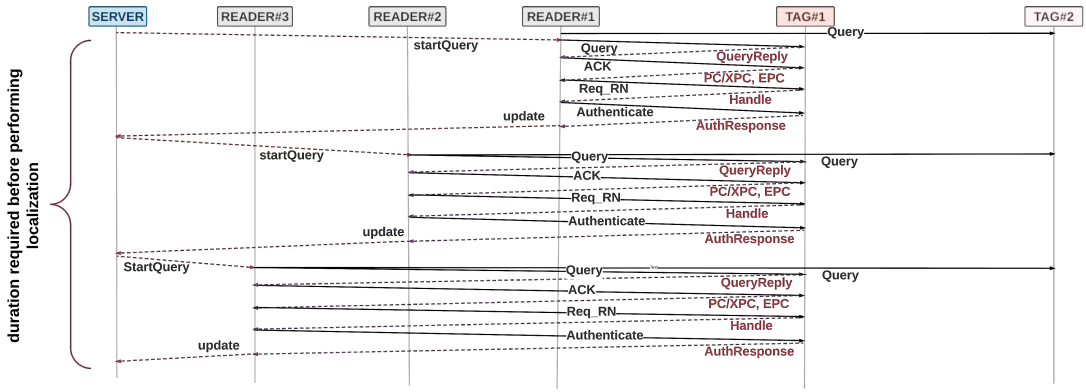

Figure 3.20 – Scenario 2: Tag by tag

3.7.2.3 Scenario 3: Realtime update

The third method is a variation of the first scenario where readers are in charge of all requests and slot counters (refer to Section 3.3). In addition, it uses every messages exchanged in order to determine the distance between the reader and the tag as described in Figure 3.21. The server initiates the tag interrogation sequence and receives timely feedbacks from each reader for every messages send by tags. The server will then calculate the time difference between feedback to indentify the RToF (refer to section 2.5.1.1) and to deduce the ToA by subtracting the messages and its overhead from RToF. This methodology reduces the time required to localize a tag to a strict minimum. The server can start calculating the localization with the first query response from the tag. This solution is the most efficient of all three specified in this section. As described in previous scenario, if the duration to interrogate a tag is equal to t_{tag}, the time needed to localize a tag should be less than t_{tag}.

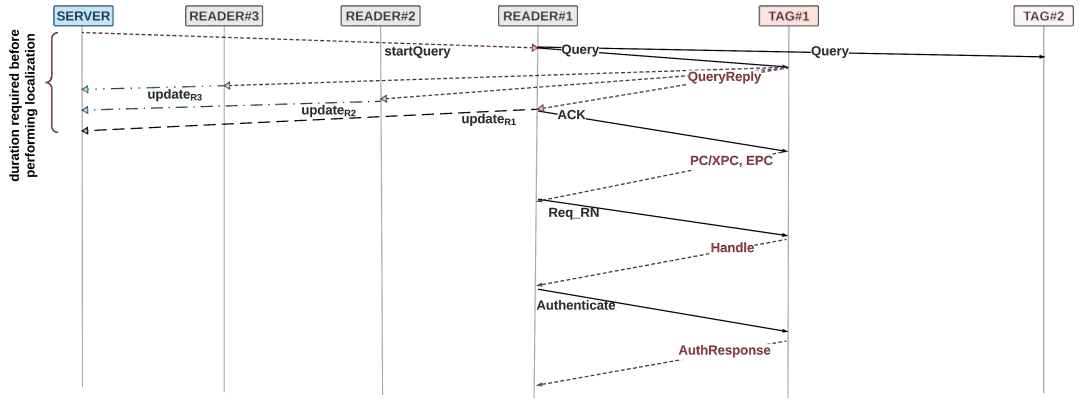

Figure 3.21 – Scenario 3: All readers update tag location actively

3.7.2.4 Localization results

The results gathered from simulations presented in the Figure 3.22 confirm the affirmation stated in Section 3.7.2.3 that scenario 3 is the best scenario among the three propositions. A sample of 10 to 100 tags has been chosen to identify the divergence of the simulations. The most optimum frame size is used for each number of tags. As an example, for 100 tags, the best value for scenario 1 is at almost 5 (the same value found in Figure 3.15) and at almost 15 for scenario 3. It is observed that the improvement performed by the scenario 3 over the scenario 1 tripled. This is due to the fact that in scenario 1, all readers are required to interrogate all tags as compared to the scenario 3 where only one reader actively interrogates the tag to gather related information for localization calculation. The rest of the readers are only required to update the server when they received the messages transmitted by the tag and the distance between the reader and the tag is calculated by the server accordingly before proceeding to localization calculation. The scenario 2, on the other hand, will produce the same result as scenario 1 as the server still requires all readers to interrogate all tags even though the sequencing is different.

Localization is subject to multiple security issues, among which is the privacy violation. Indeed, the tag identity communication within Gen2V2 protocol exchanges is vulnerable to eavesdropping. Therefore the identity is easily captured during the communication. Thus, the importance to carry out an improvement to the

protocol to hide it. In the next section, we will address this issue.

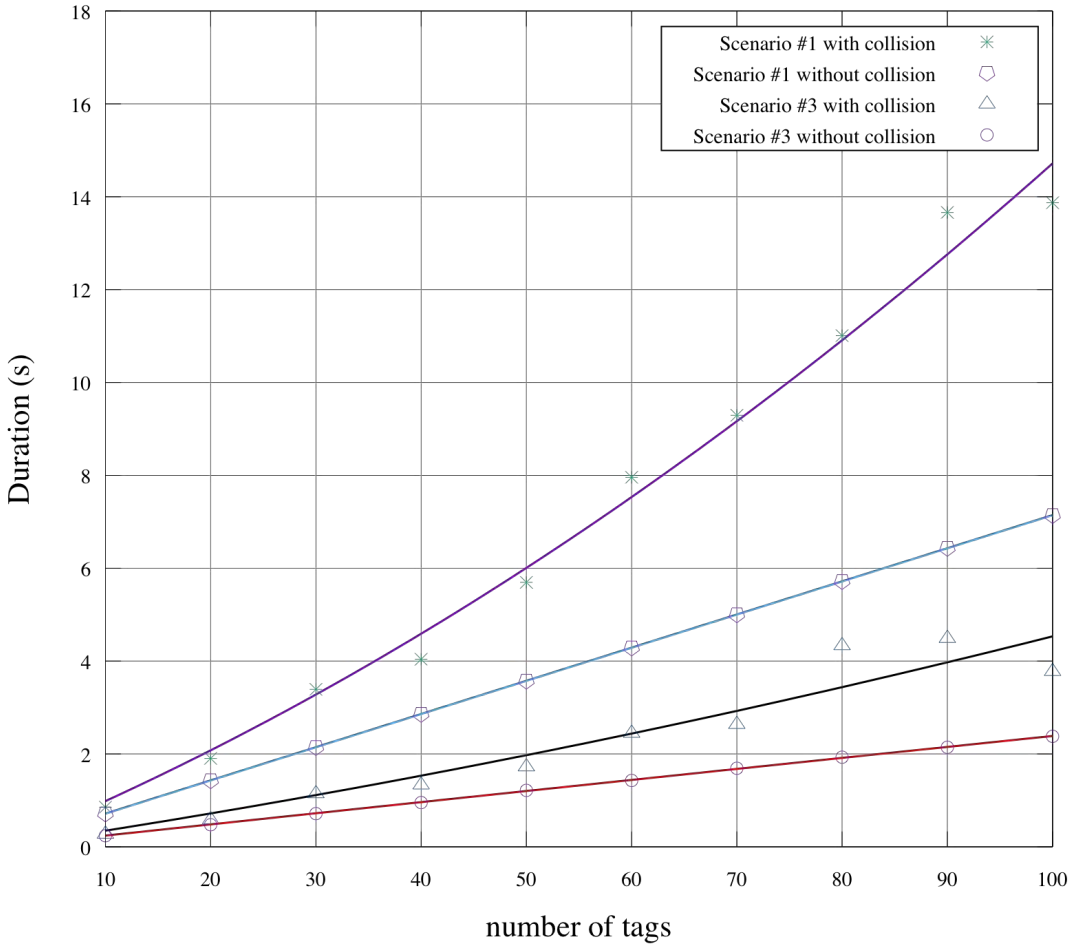

Figure 3.22 – Localization duration

3.8 RFID tag privacy

By default, RFID communications are not secure. The conversation is transparent to anybody within the communication range. In Gen2V2 [47] protocol, when a reader sends a query to a tag, the tag will respond with a freshly generated RN16. The reader will receive the tag identification by returning the RN16 back to the tag. Therefore, any reader could collect this information without any difficulty. This could leave a trace of tag identification along with its movement.

The Gen2V2 protocol standard introduced an optional command called "untraceable". It helps to hide some details of the tag identity. Yet, it requires prior authentication process to secure the tag. This authentication in itself is optional. Consequently, a tag with or without authentication has already exposed its identity. Hence, it is vulnerable to traceability attack.

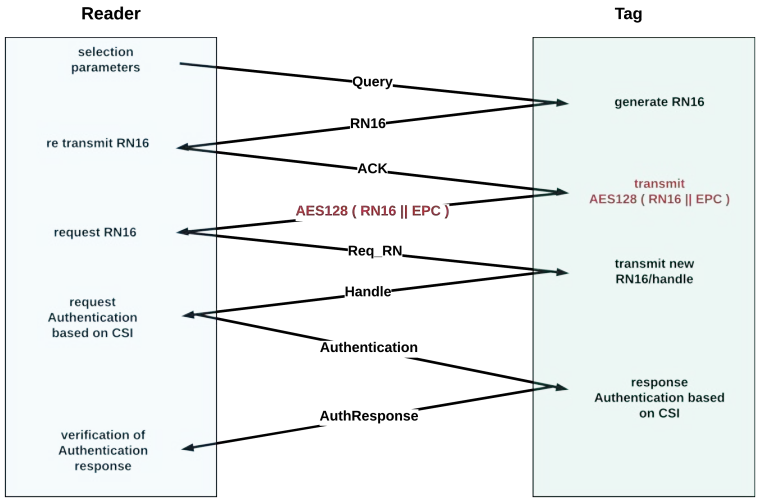

Figure 3.23 – Best case scenario: Communication exchange in Gen2V2 protocol

In this work, we proposed to anonymize the tag identity by introducing AES128 encryption as described in Section 2.4.4 into the identification process. The idea is that, when a tag sends its identity to a reader, every entity within the communication range can *hear* it, therefore an encryption of the identity can hide its real value. AES128 is just an example to enable a prove of concept of the idea. However, the encryption results produce the same output if the input is the same. As a result if an adversary wanted to located a tag, it can refer to a series of tags having the same encrypted identity. Hence, eventhough the real identity is not revealed, the tag location can be deduced by performing any localization method described in Section 2.5 . In order to overcome this problem, the proposed work applies a XOR operation between the real identity with the random number produced previously during the *QueryResponse* operation. The result of the XOR operation is then introduced to the AES128 encryption and is later sent to the reader. The reader will then send the ciphertext to the server along with the other

parameters.The server will then be able to decrypt the ciphertext given by the reader using the shared key and the given random number.
Another concept is by using a set of pseudonym. A pseudonym concept is when an object has several identifications. The authorized entity should have the list of the alias (either precalculated or not). Without the list, the unauthorised party would have difficulties to trace the object. The idea is to use several secret keys along with the tag identification. This is rather different than using a separate identification for the same tag such as in [110]. However, it requires the server to store a list of hashing codes in its database. The downside of the protocol proposed is the system demands more time to identify a tag. This can affect the scalability of the system as it requires a significant overhead as described by Alomair et al. in [59].

3.9 Localization privacy

At this point, the framework is implemented, tested and able to localize tags. The localization depends on the signal received and the identification of the object. The main idea to maintain privacy is to prevent the tag from simply giving away its identification to any reader, either it is authorized or not. One of the implemented cryptographical suites has been chosen to hide the identification by encrypting the EPC within the limit of the standard. The proof of concept of the proposed solution involves the utilisation of AES128 to encrypt the identification in order to make it more difficult for the reader to identify the tag. The AES128 has been chosen due to its popularity among ubiquitous systems. However, its encrypted output is not varying if the input is fixed (in this case the identification). Therefore, the same outcome is expected if no modification is done to the input. In order to get a different result with the same identification, an exclusive OR is performed to the identification (EPC) using the random number (RN16) used in the first tag reply as shown below.

$$input = RN16 \oplus EPC \tag{3.3}$$

$$output = encryptAES128(input, presharedKey) \tag{3.4}$$

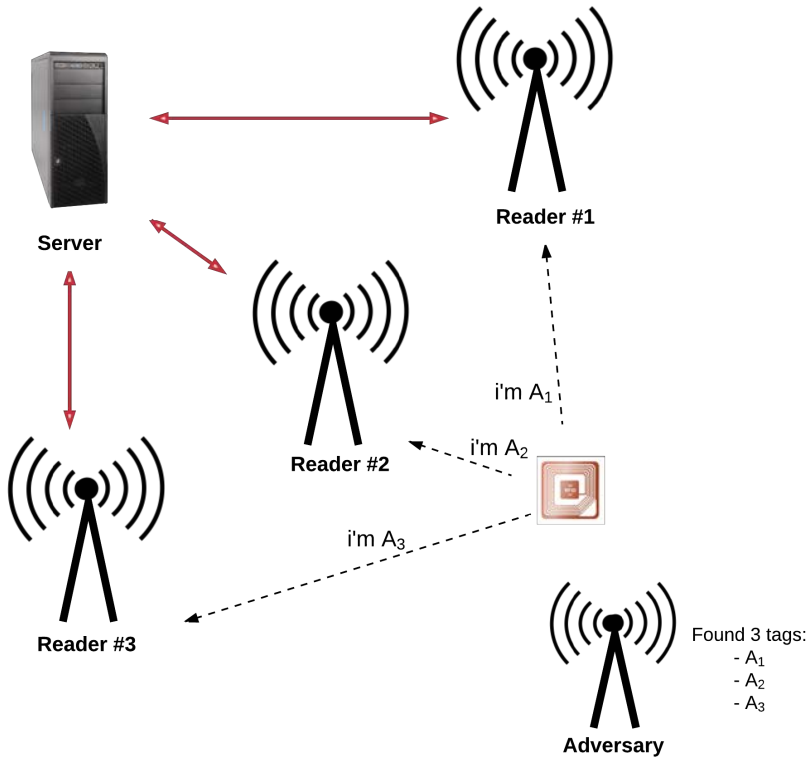

Figure 3.24 – Localization Privacy Topology

By performing this, every request for a tag identification will result in a completely different identification. Thus, as illustrated in Figure 3.24, the adversary can only detect that there are several tags around him without knowing their true identity nor to the fact that they represent only one tag. On top of that, if there is a set of readers to identify the tag, they will not be able to refer to a specific tag due to the different identities provided by the same tag, hence rending the localization by more than one reader to be impossible.
Within the authorized system, the server decrypts the encrypted identification using AES128 with the pre-shared key. An exclusive OR is then performed on the result with the random number given in order to get the identification.

$$output = decryptAES(input, presharedKey) \tag{3.5}$$

$$EPC = RN16 \oplus output \tag{3.6}$$

3.10 Conclusion

In this chapter a new Gen2V2 framework is built within the OMNET++ simulator. Every details of the framework implementation is presented. First, is the implementation of FSA protocol to simulate the anti-collision management. Its performance is observed, a comparison between implementations of the frame is also performed and compared against the theoretical values. In addition, the implementation of four cryptographical suites is done to evaluate and measure their impact on the authentication process. The communication overhead performance are also evaluated. Prior to that, the cryptographical suites have been verified through a series of known test vectors to ensure the confirmity of the implemented algorithm. Finally three possible scenarios of the RFID localization are proposed and compared. The framework is thus ready to be used as a platform to investigate the localization privacy. The identity manipulation within the implemented protocol helps to increase privacy in the localization. Moreover, it reduces the precision by reducing the ability to triangulate the object by more than one reader. Up until the manuscript is written, the implemented framework represents over 7000 lines of codes and keeps increasing. The codes are available at *https://github.com/Ahmad2015/Secure_RAIN_RFID-*.

4 Conclusion and Perspectives

4.1 Conclusion

The Ambient Assisted Living provides numerous opportunities in bringing comfort to an elderly person. It helps them to be less dependant to other people and delays or even ceases the needs for some of them to go to a retirement home. However, the uncertainty of the security and privacy of the underlying technology hinders them from adopting the solution. Therefore, some improvements within the area is needed in order to reassure new/potential adopters.
The goal of this work is to provide a new method to improve privacy during the localization process. The method proposed proves that by sending a different identification to each communication session, it will render the localization of an object to be imprecise. As noted previously, a reader can sense the presence of a tag whenever the tag is within its range. Therefore, it can deduce that the tag is nearby. However, with the presence of hundreds of tags within its surrounding at most time, it is nearly impossible to detect any specific tag among them.
In order to prove that the proposed method can enchance the privacy during the passive tag localization, a new Gen2V2 framework has been modeled within OMNET++ simulator. The newly created framework validation proves that its communication efficiency is in concordance with the theoretical value of the Frame Slotted Aloha protocol implemented within the Gen2V2 tag standard.
With the help of a radio medium framework already implemented within the OMNET++, the Gen2V2 framework is able to simulate the wireless communication channel where any forms of communication can be heard by anybody within range. This functionality enables the simulation of request broadcasts by the reader and

the response backscattered by tags. It also enables the implementation of an adversary within the framework where every conversation is recorded.
The implementation of the four cryptographical suites within the framework demonstrates the possibility to increase the security at a small cost. Each cryptographical suites is validated by its known test vectors. It is implemented through a separate module that can be used or reused by any other modules. By taking the advantage of the existing cryptographical suites, an additional procedure used to hide the real identity of a tag during the communication also proves that the localization privacy can be improved without major modification to the current RFID tag protocol.

4.2 Prespectives

4.2.1 Short term perspectives

The newly developped framework within OMNET++ is limited to only four cryptographical suites among nine available for the Gen2V2 tags. Therefore to fully compare all cryptographical suites proposed within the standard, the implementation of remaining cryptographical suites is required. This will enable the investigation of different matrix such as the amount of data exchanged or the total duration to finish the reader/tag association. An addition of other cryptographical suites can also help to decide the best option to hide the tag identity.
The current Gen2V2 framework localizes a tag based on the Time of Arrival (ToF). As it is not the only way to locate a tag, an implementation of other methods can be carried out in the near future. This can help in investigating other options to ensure the localization is permissible to the authorized parties only. Among other methods used to locate a tag that can be looked into are the use of the signal strength, the angle of arrival or a hybrid of two or more methods. The mobility module has been implemented within the framework, however, it is set to be static. A localization privacy of a mobile tag can be interesting to investigate.

4.2.2 Long term perspectives

Although the localization privacy is tightly related to the AAL domain as it is specifically associated to human lives, it can also serve other close related domains such as eMedicine and eHealth or to the IoT itself in general.
There are numerous areas that require improvements due to the RFID tag limitations. The IoT implementations are in a rapid expansion, however, that the future of localization privacy within IoT is a necessity in order to ensure the security and privacy of the users are not neglected.

Appendix

Omnetpp.ini

```
[General]
num-rngs = 2
**.nodeReader.rng-0 = 0
**.nodeTag.rng-0 = 1
seed-0-mt = ${ seed0 = 74593..171163 step 3330 }
seed-1-mt = ${ seed1 = 100235..228995 step 4440 ! seed0 }
**.headerBitLength = 1b
**.bitrate = 40kbps
**.numReaders = 1
**.numTags = ${ ntag=20..100 step 20 }
**.rQ = ${ Q = 3..15 step 1}
[Config NoAuth]
**.CryptoSuite = 499
[Config PRESENT80]
**.CryptoSuite = 402
[Config XOR]
**.CryptoSuite = 406
[Config CRYPTOGPS]
**.CryptoSuite = 408
[Config AES128]
**.CryptoSuite = 400
```

Code 1 – Simulation parameters in omnetpp.ini

Test vector PRESENT-80

Plaintext	Key	Ciphertext
00000000h || 00000000h	00000000h || 00000000h || 0000h	5579C138h 7B228445h
00000001h || 00000001h	00000000h || 00000000h || 0000h	086FC044h 9733895Bh
00000001h || 00000001h	00000000h || 00000000h || 0001h	65249D8Fh 0626D7FDh
FFFFFFFFh || FFFFFFFFh	00000000h || 00000000h || 0000h	A112FFC7h 2F68417Bh
00000000h || 00000000h	FFFFFFFFh || FFFFFFFFh || FFFFh	E72C46C0h F5945049h
FFFFFFFFh || FFFFFFFFh	FFFFFFFFh || FFFFFFFFh || FFFFh	3333DCD3h 213210D2h

Test vector cryptoGPS

curve P-19
$E : Y^2 = X^3 - 3X + b \ \ overF_q$
q = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF
b = 64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1

Base point P over E.
P = (x_P,y_P)
= (188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012,
07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811)

n is the order of point P.
n = FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831
The bit length of the cryptoGPS private key is $\sigma = |n| = 192$ bits.

Private key
s = 4F1DF03A A32DCA02 652E83E7 E5FF5259 D61F5563 B3A0FA10

Public point
V = –[s]P
= (x_V,y_V)
= (D753BF14 9529BC23 B1850A37 57C4D34A 0D686A95 C3B03855,
1656B8CB 2896BFD4 BC8F94A8 F3708741 B954CC44 4FC3951A)

Step a
r is a fresh string of random bits
r = 05E8B1 E1121B08 FB9A0F58 FC1E932F 9CEFE94D 629BC223 40B5F04B

554DCD2B C812A76D 98F8BA3E
[r]P = (DAD48D02 4B83E223 4C0F5FFF B51C15B7 1D52CF92 B35358CF, FFE42756 843D0DF8 F3166971 E8AF6E22 6FD381B0 A816720F)

Step b
X = 04 DAD48D02 4B83E223 4C0F5FFF B51C15B7 1D52CF92 B35358CF FFE42756 843D0DF8 F3166971 E8AF6E22 6FD381B0 A816720F

Step c, d
Verifier's challenge:
c = 2D F0F5B4F2

Step e, f
z = 2D F0F5B4F
y = 5E8B1 E1121B08 FB9A0F67 2ED9CE48 044BD618 3242087C ADDDA392 F2CA1F36 FDD94248 E8485D5E

Step g
Verification:
X* = 04 DAD48D02 4B83E223 4C0F5FFF B51C15B7 1D52CF92 B35358CF FFE42756 843D0DF8 F3166971 E8AF6E22 6FD381B0 A816720F
Authentication is valid.

AES Test vector

PLAINTEXT: 00112233445566778899aabbccddeeff
KEY: 000102030405060708090a0b0c0d0e0f

round[0].input 00112233445566778899aabbccddeeff
round[0].k_sch 000102030405060708090a0b0c0d0e0f
round[1].start 00102030405060708090a0b0c0d0e0f0
round[1].s_box 63cab7040953d051cd60e0e7ba70e18c
round[1].s_row 6353e08c0960e104cd70b751bacad0e7
round[1].m_col 5f72641557f5bc92f7be3b291db9f91a
round[1].k_sch d6aa74fdd2af72fadaa678f1d6ab76fe
round[2].start 89d810e8855ace682d1843d8cb128fe4
round[2].s_box a761ca9b97be8b45d8ad1a611fc97369
round[2].s_row a7be1a6997ad739bd8c9ca451f618b61

round[2].m_col ff87968431d86a51645151fa773ad009
round[2].k_sch b692cf0b643dbdf1be9bc5006830b3fe
round[3].start 4915598f55e5d7a0daca94fa1f0a63f7
round[3].s_box 3b59cb73fcd90ee05774222dc067fb68
round[3].s_row 3bd92268fc74fb735767cbe0c0590e2d
round[3].m_col 4c9c1e66f771f0762c3f868e534df256
round[3].k_sch b6ff744ed2c2c9bf6c590cbf0469bf41
round[4].start fa636a2825b339c940668a3157244d17
round[4].s_box 2dfb02343f6d12dd09337ec75b36e3f0
round[4].s_row 2d6d7ef03f33e334093602dd5bfb12c7
round[4].m_col 6385b79ffc538df997be478e7547d691
round[4].k_sch 47f7f7bc95353e03f96c32bcfd058dfd
round[5].start 247240236966b3fa6ed2753288425b6c
round[5].s_box 36400926f9336d2d9fb59d23c42c3950
round[5].s_row 36339d50f9b539269f2c092dc4406d23
round[5].m_col f4bcd45432e554d075f1d6c51dd03b3c
round[5].k_sch 3caaa3e8a99f9deb50f3af57adf622aa
round[6].start c81677bc9b7ac93b25027992b0261996
round[6].s_box e847f56514dadde23f77b64fe7f7d490
round[6].s_row e8dab6901477d4653ff7f5e2e747dd4f
round[6].m_col 9816ee7400f87f556b2c049c8e5ad036
round[6].k_sch 5e390f7df7a69296a7553dc10aa31f6b
round[7].start c62fe109f75eedc3cc79395d84f9cf5d
round[7].s_box b415f8016858552e4bb6124c5f998a4c
round[7].s_row b458124c68b68a014b99f82e5f15554c
round[7].m_col c57e1c159a9bd286f05f4be098c63439
round[7].k_sch 14f9701ae35fe28c440adf4d4ea9c026
round[8].start d1876c0f79c4300ab45594add66ff41f
round[8].s_box 3e175076b61c04678dfc2295f6a8bfc0
round[8].s_row 3e1c22c0b6fcbf768da85067f6170495
round[8].m_col baa03de7a1f9b56ed5512cba5f414d23
round[8].k_sch 47438735a41c65b9e016baf4aebf7ad2
round[9].start fde3bad205e5d0d73547964ef1fe37f1
round[9].s_box 5411f4b56bd9700e96a0902fa1bb9aa1
round[9].s_row 54d990a16ba09ab596bbf40ea111702f
round[9].m_col e9f74eec023020f61bf2ccf2353c21c7
round[9].k_sch 549932d1f08557681093ed9cbe2c974e
round[10].start bd6e7c3df2b5779e0b61216e8b10b689
round[10].s_box 7a9f102789d5f50b2beffd9f3dca4ea7

round[10].s_row 7ad5fda789ef4e272bca100b3d9ff59f
round[10].k_sch 13111d7fe3944a17f307a78b4d2b30c5
round[10].output 69c4e0d86a7b0430d8cdb78070b4c55a

XOR Test vector

Tag authentication

The following example uses a 64-bit Key and a 64-bit random number.

PSK d4f625e4 122688af

RNi 1ba58677 7e45a0e7

SRNi a40cfe28 c1bc7d93

SORNi 204bb61f 654744d0

Publications

Khalid, A., Conchon, E. and Peyrard, F. (2016). **"Evaluation of RAIN RFID authentication schemes",** *In 2016 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications*, SSIC 2016 - Proceedings. http://doi.org/10.1109/SSIC.2016.7571807

Bibliography

[1] *ISO 11784: Radiofrequency identification of animals - Code structure*, 1996.

[2] *ISO 11785: Radiofrequency identification of animals - Technical concept*, 1996.

[3] *ISO 14223-1: Radiofrequency identification of animals — Advanced transponders - Air Interface*, 2011.

[4] *ISO/IEC 14443-2: Identification - Contactless integrated circuit cards - Proximity cards - Radio frequency power and signal interface*, 2017.

[5] Apple, "Apple Pay," last accessed 16-August-2017, https://www.apple.com/apple-pay/.

[6] Google, "Android Pay," last accessed 16-August-2017, https://www.android.com/pay/.

[7] Samsung, "Samsung Pay," last accessed 16-August-2017, http://www.samsung.com/us/support/owners/app/samsung-pay.

[8] Orange.fr, "Orange Cash," last accessed 16-August-2017, http://orangecash.orange.fr/decouvrir.

[9] D. Hellström and M. Wiberg, "Improving Inventory Accuracy Using RFID Technology: A Case Study," *Assembly Automation*, vol. 30, no. 4, pp. 345–351, 2010.

[10] T. Fan, F. Tao, S. Deng, and S. Li, "Impact of RFID technology on supply chain decisions with inventory inaccuracies," *International Journal of Production Economics*, vol. 159, pp. 117–125, 2015.

[11] S. Piramuthu, S. Wochner, and M. Grunow, "Should retail stores also RFID-tag 'cheap' items?" *European Journal of Operational Research*, vol. 233, no. 1, pp. 281–291, 2014.

[12] E. Cho, M. Mohammadifar, and S. Choi, "A self-powered sensor patch for glucose monitoring in sweat," in *Proceedings of the IEEE International Conference on Micro Electro Mechanical Systems (MEMS)*, 2017, pp. 366–369.

[13] S. Manzari, C. Occhiuzzi, and G. Marrocco, "Feasibility of body-centric systems using passive textile RFID tags," *IEEE Antennas and Propagation Magazine*, vol. 54, no. 4, pp. 49–62, 2012.

[14] A. J. Jara, M. a. Zamora, and A. F. Skarmeta, "Drug identification and interaction checker based on IoT to minimize adverse drug reactions and improve drug compliance," *Personal and Ubiquitous Computing*, vol. 18, no. 1, pp. 5–17, oct 2012. [Online]. Available: http://link.springer.com/10.1007/s00779-012-0622-2

[15] R. Radziszewski, H. Kenfack Ngankam, H. Pigot, V. Grégoire, D. Lorrain, and S. Giroux, "Designing Calm and Non-intrusive Ambient Assisted Living System for Monitoring Nighttime Wanderings," *International Journal on Perceptive and Cognitive Computing*, vol. 1, no. 1, pp. 114–129, 2016. [Online]. Available: http://www.emeraldinsight.com/doi/10.1108/IJPCC-02-2017-0015

[16] R. Radziszewski, H. Ngankam, H. Pigot, V. Grégoire, D. Lorrain, and S. Giroux, "An ambient assisted living nighttime wandering system for elderly," in *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services - iiWAS '16*, 2016, pp. 368–374. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3011141.3011171

[17] F. Bergeron, K. Bouchard, S. Gaboury, S. Giroux, and B. Bouchard, "Indoor Positioning System for Smart Homes Based on Decision Trees and Passive RFID," in *Proceedings of the 20th Pacific Asia Conference on Knowledge Discovery and Data Mining (PAKDD) 2016*, 2016, pp. 42–53. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-31750-2_4

[18] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, oct 2010. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128610001568

[19] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," 2014.

[20] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, Sep. 2013. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0167739X13000241

[21] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, apr 2014. [Online]. Available: http://link.springer.com/10.1007/s10796-014-9492-7

[22] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, sep 2012. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1570870512000674

[23] A. Whitmore, A. Agarwal, and L. Xu, "The Internet of Things: A survey of topics and trends," *Information Systems Frontiers*, mar 2014. [Online]. Available: http://link.springer.com/10.1007/s10796-014-9489-2

[24] A. S. Khalid, E. Conchon, and F. Peyrard, "Evaluation of RAIN RFID authentication schemes," in *2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*, July 2016, pp. 1–8.

[25] GS1, last accessed 27-April-2015, UHF Air Interface Protocol Standard. [Online]. Available: http://www.gs1.org/epcrfid/epc-rfid-uhf-air-interface-protocol/2-0-1

[26] T. INSTRUMENT, last accessed 14-August-2017, ISO/NFC Standards and Specifications Overview. [Online]. Available: http://e2e.ti.com/cfs-file/

___key/communityserver-discussions-components-files/667/2072.ISO_5F00_NFC-Standards-and-Specifications-Overview_5F00_2014.pdf

[27] *IEEE 802.11: IEEE Standard for Information technology —Telecommunications and information exchange between systems Local and metropolitan area networks — Specific requirements - Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications*, 2016.

[28] ANT+, "What is ANT+," last accessed 16-August-2017, https://www.thisisant.com/consumer/ant-101/what-is-ant/.

[29] Bluetooth, "Bluetooth Specifications," last accessed 16-August-2017, https://www.bluetooth.com/specifications/protocol-specifications.

[30] *IEEE Standard for Low-Rate Wireless Networks*, 2015.

[31] Z. Alliance, "Zwave Alliance," last accessed 16-August-2017, http://z-wavealliance.org/z-wave_alliance_member_companies/.

[32] D. C. Wyld, *RFID: The Right Frequency for Government*. IBM Center for the Business of Government Washington, 2005.

[33] "CNRFID - French National RFID center," Accessed: 2017-07-27, http://www.centrenational-rfid.com/features-of-rfid-tags-article-19-gb-ruid-202.html.

[34] "GS1 standards organisation," Accessed: 2017-07-27, https://www.gs1.org.

[35] "ISO International Organization for Standardization," Accessed: 2017-07-27, https://www.iso.org/home.html.

[36] *ISO/IEC 18000-1: Information technology — Radio frequency identification for item management - Reference architecture and definition of parameters to be standardized.*

[37] *ISO/IEC 18000-2: Information technology — Radio frequency identification for item management - Parameters for air interface communications below 135 kHz.*

[38] *ISO/IEC 18000-3: Information technology — Radio frequency identification for item management - Parameters for air interface communications at 13,56 MHz.*

[39] *ISO/IEC 18000-6: Information technology — Radio frequency identification for item management - Parameters for air interface communications at 860 MHz to 960 MHz*, 2015.

[40] *ISO/IEC 18000-4: Information technology — Radio frequency identification for item management - Parameters for air interface communications at 2,45 GHz*, 2015.

[41] "GS1 UHF regulations," Accessed: 2017-07-27, https://www.gs1.org/docs/epc/uhf_regulations.pdf.

[42] *ISO/IEC15693-2: Identification - Contactless integrated circuit cards - Vicinity cards - Air interface and initialization*, 2006.

[43] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice.* Newton, MA, USA: Newnes, 2007.

[44] "RAIN RFID," Accessed: 2017-09-18, http://rainrfid.org/.

[45] *ISO/IEC 18000-63: Information technology — Radio frequency identification for item management - Part 63: Parameters for air interface communications at 860 MHz to 960 MHz type C.*

[46] "GS1 EPCglobal," Accessed: 2017-07-27, https://www.gs1.org/epcglobal.

[47] *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID - Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz Version 2.0.1 Ratified*, 2015.

[48] H. Vogt, "Efficient Object Identification with Passive RFID Tags," *Pervasive Computing*, pp. 98—-113, 2002. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.17.6871{&}rep=rep1{&}type=pdf

[49] S. R. Lee, S. D. Joo, and C. W. Lee, "An enhanced dynamic framed slotted ALOHA algorithm for RFID tag identification," *MobiQuitous 2005: Second Annual International Conference on Mobile and Ubiquitous Systems - Networking and Services*, no. Mic, pp. 166–172, 2005.

[50] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, fifth edition ed. Prentice Hall, 2011.

[51] "GS1 EPC/RFID standard," Accessed: 2017-07-28, https://www.gs1.org/epc-rfid.

[52] G. P. Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens," in *Journal of Computer Security*, vol. 19, no. 2, 2011, pp. 259–288.

[53] R. Silberschneider, T. Korak, and M. Hutter, "Access without permission: A practical rfid relay attack," 2014.

[54] L. Sportiello and A. Ciardulli, *Long Distance Relay Attack*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 69–85. [Online]. Available: https://doi.org/10.1007/978-3-642-41332-2_5

[55] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," *Network and Distributed System Security Symposium*, pp. 431–439, 2011. [Online]. Available: http://eprint.iacr.org/2010/332

[56] M. Safkhani, N. Bagheri, P. Peris-Lopez, A. Mitrokotsa, and J. C. Hernandez-Castro, "Weaknesses in another Gen2-based RFID authentication protocol," *2012 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, pp. 80–84, nov 2012. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6404572

[57] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador, and J. C. A. Van Der Lubbe, "Cryptanalysis of an EPC Class-1 Generation-2 standard compliant authentication protocol," *Engineering Applications of Artificial Intelligence*, 2011.

[58] S. Vaudenay, "On Privacy Models for RFID," in *Advances in Cryptology – ASIACRYPT 2007*. Springer Berlin Heidelberg, 2007, pp. 68–87.

[59] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Scalable RFID Systems: A Privacy-Preserving Protocol with Constant-Time Identification," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1536–1550, Aug 2012.

[60] J.-S. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, dec 2013. [Online]. Available: http://link.springer.com/10.1007/s11227-013-1073-x

[61] M. O'Neill, "Low-Cost SHA-1 Hash Function Architecture for RFID Tags," in *Conference on RFID Security*, 2008. [Online]. Available: http://rfidsec2013.iaik.tugraz.at/RFIDSec08/Papers/Publication/04-ONeill-LowCostSHA-1-Paper.pdf

[62] J. S. Choi, H. Lee, R. Elmasri, and D. W. Engels, "Localization Systems using Passive UHF RFID," in *International Joint Conference on INC, IMS and IDC*. IEEE Computer Society, 2009, pp. 1727–1732.

[63] M. Feldhofer and J. Wolkerstorfer, "Strong Crypto for RFID Tags – A Comparison of Low-Power Hardware Implementations," *Circuits and Systems*, pp. 1839–1842, 2007.

[64] C. Rolfes, A. Poschmann, G. Leander, and C. Paar, "Security for 1000 Gate Equivalents," 2005.

[65] *ISO/IEC 29167-1: Information technology — Automatic identification and data capture techniques - Security services for RFID air interfaces*, 2015.

[66] *ISO/IEC 29167-10: Information technology — Automatic identification and data capture techniques - Crypto suite AES-128 security services for air interface communications*, 2014.

[67] *ISO/IEC 29167-11: Information technology — Automatic identification and data capture techniques - Air interface for security services crypto suite PRESENT-80*, 2014.

[68] *ISO/IEC 29167-12: Information technology — Automatic identification and data capture techniques - Crypto suite ECC-DH security services for air interface communications*, 2014.

[69] *ISO/IEC 29167-13: Information technology — Automatic identification and data capture techniques -Part 13: Crypto suite Grain-128A security services for air interface communications*, 2015.

[70] *ISO/IEC 29167-14: Information technology — Automatic identification and data capture techniques - Air interface for security services cryptographic suite AES OFB*, 2014.

[71] *ISO/IEC 29167-15: Information technology — Automatic identification and data capture techniques - Air Interface for security services crypto suite XOR*, 2014.

[72] *ISO/IEC 29167-16: Information technology — Automatic identification and data capture techniques - Air interface for security services crypto suite ECDSA-ECDH*, 2014.

[73] *ISO/IEC 29167-17: Information technology — Automatic identification and data capture techniques - Crypto suite cryptoGPS security services for air interface communications*, 2015.

[74] *ISO/IEC 29167-19: Information technology — Automatic identification and data capture techniques - Part 19: Crypto suite RAMON security services for air interface communications*, 2016.

[75] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A very compact and a threshold implementation of AES," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6632 LNCS, pp. 69–88, 2011.

[76] J. Ertl, T. Plos, M. Feldhofer, N. Felber, and L. Henzen, "A security-enhanced uhf rfid tag chip," in *2013 Euromicro Conference on Digital System Design*, Sept 2013, pp. 705–712.

[77] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT : An Ultra-Lightweight Block Cipher," *Springer Berlin Heidelberg*, pp. 450–466, 2007.

[78] *ISO/IEC 18033-3: Information technology — Security techniques - Encryption algorithms - Block ciphers*, 2010.

[79] National Institute of Standards and Technology, *FIPS PUB 197: ADVANCED ENCRYPTION STANDARD (AES)*. pub-NIST, 2001. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[80] L. Fu, X. Shen, L. Zhu, and J. Wang, "A low-cost UHF RFID tag chip with AES cryptography engine," *Security and Communication Networks*, 2014.

[81] A. Poschmann, M. Robshaw, F. Vater, and C. Paar, "Lightweight cryptography and RFID: Tackling the hidden overheads," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5984 LNCS, 2010, pp. 129–145.

[82] S. Azzouzi, M. Cremer, U. Dettmar, R. Kronberger, and T. Knie, "New measurement results for the localization of UHF RFID transponders using an angle of arrival (AoA) approach," in *2011 IEEE International Conference on RFID*, April 2011, pp. 91–97.

[83] C. Wang, L. Xie, and S. Lu, "Search for a Needle in a Haystack : an RFID-based Approach for Efficiently Locating Objects," in *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*, April 2014, pp. 2144–2149.

[84] Y. Zhao, K. Liu, Y. Ma, Z. Gao, Y. Zang, and J. Teng, "Similarity analysis-based indoor localization algorithm with backscatter information of passive uhf rfid tags," *IEEE Sensors Journal*, vol. 17, no. 1, pp. 185–193, Jan 2017.

[85] M. Scherhaufl, M. Pichler, and A. Stelzer, "UHF RFID Localization Based on Phase Evaluation of Passive Tag Arrays," *Instrumentation and Measurement, IEEE Transactions on*, vol. 64, no. 4, pp. 913–922, April 2015.

[86] "GEOCACHING- trilateration," Last accessed: 2017-08-04, https://www.geocaching.com/geocache/GC3RVE3_triangulation-calculation?guid=da6a4e5b-9406-444f-9df3-9dd8d0fdc5e6.

[87] "Positioning and Trilateration," last access August 2017, http://www.alanzucconi.com/2017/03/13/positioning-and-trilateration/#part2.

[88] J. Shen, A. F. Molisch, and J. Salmi, "Accurate passive location estimation using TOA measurements," *IEEE Transactions on Wireless Communications*, vol. 11, no. 6, pp. 2182–2192, 2012.

[89] International Telecommunication Union, "Comparison of time-difference-of-arrival and angle-of-arrival methods of signal geolocation SM Series," Tech. Rep., 2014.

[90] Y. Álvarez López, M. E. de Cos Gómez, and F. Las-Heras Andrés, "A received signal strength RFID-based indoor location system," *Sensors and Actuators, A: Physical*, vol. 255, pp. 118–133, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.sna.2017.01.007

[91] C. Hekimian-Williams, B. Grant, X. Liu, Z. Zhang, and P. Kumar, "Accurate localization of RFID tags using phase difference," in *RFID 2010: International IEEE Conference on RFID*, 2010.

[92] C.-H. Ko, "RFID 3D location sensing algorithms," *Automation in Construction*, vol. 19, no. 5, pp. 588–595, aug 2010. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0926580510000300

[93] D. Fortin-Simard, K. Bouchard, S. Gaboury, B. Bouchard, and A. Bouzouane, "Accurate passive RFID localization system for smart homes," *Proceedings - 2012 IEEE 3rd International Conference on Networked Embedded Systems for Every Application, NESEA 2012*, pp. 1–8, dec 2012. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6474010

[94] Y. Zhao and J. R. Smith, "A battery-free RFID-based indoor acoustic localization platform," *IEEE International Conference on RFID*, pp. 110–117, 2013.

[95] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving iot target-driven applications," *Computers & Security*, vol. 37, pp. 111 – 123, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404813000904

[96] M. Chen, S. Chen, and Y. Fang, "Lightweight Anonymous Authentication Protocols for RFID Systems," *IEEE/ACM Transactions on Networking*, vol. PP, no. 99, pp. 1–14, 2017.

[97] B. Song and C. J. Mitchell, "Scalable RFID security protocols supporting tag ownership transfer," *Computer Communications*, vol. 34, no. 4, pp. 556 – 566, 2011, special issue: Building Secure Parallel and Distributed Networks and Systems. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366410001027

[98] A. Juels, "RFID security and privacy: A research survey," pp. 381–394, 2006.

[99] A. Juels and S. A. Weis, "Defining Strong Privacy for RFID," in *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, March 2007, pp. 342–347.

[100] G. Avoine, "Adversarial model for radio frequency identification." *IACR Cryptology ePrint Archive*, vol. 2005, p. 49, 2005.

[101] L. Lu, Y. Liu, and X.-Y. Li, "Refresh: Weak Privacy Model for RFID Systems," *2010 Proceedings IEEE INFOCOM*, pp. 1–9, mar 2010. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5462153

[102] G. Avoine, I. Coisel, and T. Martin, *Time Measurement Threatens Privacy-Friendly RFID Authentication Protocols*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 138–157. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-16822-2_13

[103] "Opnet," https://www.riverbed.com/fr/products/steelcentral/opnet.html?redirect=opnet.

[104] "Ns3," https://www.nsnam.org.

[105] "OMNET++," last access August 2017, https://omnetpp.org.

[106] G. Gódor, N. Giczi, and S. Imre, "Elliptic curve cryptography based mutual authentication protocol for low computational capacity rfid systems - performance analysis by simulations," in *2010 IEEE International Conference on Wireless Communications, Networking and Information Security*, June 2010, pp. 650–657.

[107] "Test vector AES," http://csrc.nist.gov/groups/STM/cavp/block-ciphers.html#aes.

[108] "INET," last access July 2017, https://inet.omnetpp.org.

[109] T. P. S. University, "Confidence Intervals and the Central Limit Theorem," last accessed 16-August-2017, https://onlinecourses.science.psu.edu/stat506/node/8.

[110] H. M. Sun and W. C. Ting, "A Gen2-Based RFID Authentication Protocol for Security and Privacy," *IEEE Transactions on Mobile Computing*, vol. 8, no. 8, pp. 1052–1062, Aug 2009.

Résumé

Internet des objets (IoT) est actuellement à notre portée. De nombreux domaines ont bénéficié de cette technologie. Cela va d'une application simple, comme l'identification d'un objet jusqu'à la gestion d'un système plus complexe. L'identification par radiofréquence (RFID) est l'une des technologies qui a une part importante dans l'IoT aujourd'hui. C'est une technologie embarquée, peu onéreuse et qui ne nécessite aucune source d'alimentation supplémentaire dans le cas de tag passif. Avec sa fonctionnalité omniprésente, cette technologie permet d'identifier un objet dans une zone spécifique. L'Assistance et l'Autonomie des personnes à Domicile (AAL) est l'un des nombreux domaines qui bénéficient de l'IoT. Il vise à aider les personnes âgées dans leurs routines quotidiennes en fournissant de nouveaux services d'assistance dans les maisons intelligentes (smart home). La présence de RFID dans une maison intelligente est d'une grande aide pour une personne âgée et/ou déficiente, par exemple, pour l'aider à trouver un objet dans son environnement quotidien.
Cependant, parmi tous les avantages qu'apporte l'IoT dans notre vie quotidienne certains peuvent s'avérer de réels inconvénients en particulier la localisation et le respect de la vie privée. En effet, pour pouvoir aider les personnes âgées à localiser un objet, le système nécessite certaines données relatives au positionnement de cet objet, tout au moins son identification. Étant donné que la couverture de l'étiquette RFID passive est très faible, une fois sa présence détectée, il est difficile de la masquer. La capacité de cette technologie à localiser des objets donne l'occasion à une tierce personne de profiter du système.
Parallèlement au besoin persistant et constant de confidentialité par les utilisateurs, l'objectif de cette thèse consiste à améliorer la confidentialité dans la localisation d'un objet grâce à un nouveau protocole basé sur la deuxième génération de RFID passive. Le protocole proposé doit pouvoir empêcher un objet d'être identifié et localisé par des parties non autorisées ou par un lecteur malveillant. La première contribution de ce travail est l'évaluation de la gestion anti-collision RFID. Elle est réalisée par la création d'un modèle OMNET++, construit sur la

base de la dernière norme RFID développée par GS1 et adaptée par ISO / IEC appelé Gen2V2 (RFID classe 2 Génération 2 Version 2). Les étiquettes (tag) RFID passives conforment à Gen2V2 communiquent dans la bande de fréquence UHF (900MHZ) avec des portées de plusieurs dizaines de mètres. La norme Gen2V2 propose une liste de suites cryptographiques qui peuvent être utilisées comme méthodes pour authentifier une étiquette et un lecteur. Cette nouvelle génération d'étiquettes est soutenue par une alliance de fabricants appelée RAIN (RAdio frequency IdentifatioN) qui favorise l'adoption du Gen2V2. Nous évaluons dans cette thèse les performances globales du protocole anti-collision et nous comparons ensuite quatre de ces suites cryptographiques, à savoir PRESENT80, XOR, AES128 et cryptoGPS pour garantir l'authentification lecteur/tag. Parmi les performances évaluées dans ce modèle, nous nous sommes intéressé au nombre de collisions et à la durée requise pour interroger un groupe d'étiquettes. Nous avons intégré la fonctionnalité de localisation dans le modèle en s'appuyant sur les messages échangés avant l'authentification, ce qui peut conduire à une localisation malveillante d'un objet. Pour augmenter la confidentialité de la localisation au sein des applications AAL, nous proposons donc une deuxième contribution qui est une nouvelle méthode de localisation basée sur les échanges standard Gen2V2 en anonymisant l'identité de l'étiquette.

Mots clés : Internet des Objects, AAL, RFID, Authentication, Localisation, Vie Privée

Abstract

Internet of things (IoT) is currently on our doorsteps. Numerous domains have benefited from this technology. It ranges from a simple application such as identifying an object up to handling a more complex system. The Radio Frequency IDentification (RFID) is one of the enabling technologies that drive the IoT to its position today. It is small, cheap and does not require any additional power sources. Along with its ubiquitous functionality, this technology enables the positioning of an object within a specific area. Ambient Assisted Living (AAL) is one of the many domains that benefit from the IoT. It aims at assisting elderly people in their daily routines by providing new assistive services in smart homes for instance. RFIDs in a smart home come as a great help to an elderly person, for example, to find an object that they misplaced. However, even with all its benefits in simplifying our lives, it is unfortunately double-edged where the advantage that it brings to an object could in turn go against itself. Indeed to be able to help the older adults to locate an object, the system requires certain data in relation to the positioning of the object and its identification. As the passive RFID tag coverage is very small, once its presence is detected, it is difficult to hide it. The ability of this technology in localizing objects gives an opportunity to a third person to take an advantage of the system.

In parallel with the persistent and constant need of privacy and secrecy by the users, the objective of this thesis consists of improving the privacy in localizing an object through a new protocol based on the latest version of the RFID second generation passive tag. The proposed protocol must be able to prevent an object from being identified and located by unauthorized parties or a malicious reader. The first contribution of this work is the assessment of the RFID anti collision management. It is performed through the creation of an OMNET++ framework, modelled and built based on the latest RFID standard developed by GS1 and incorporated by ISO/IEC called Gen2V2 (RFID class 2 Generation 2 Version 2). It is a passive RFID tag that does not require any internal power sources to operate. It communicates using the UHF frequency. The Gen2V2 standard provides

a list of cryptographical suites that can be used as a method to authenticate a tag and a reader. This new generation of tags is supported by an alliance of manufacturers called RAIN (RAdio frequency IdentificatioN) that promotes the adoption of the Gen2V2. The anti collision management overall performance is then compared with its theoretical value and four of its cryptographical suites namely PRESENT80, XOR, AES128 and cryptoGPS. Among the performances evaluated within the framework is the number of collisions and the duration required to interrogate a group of tags. Note that an addition of a localization functionality within the framework reveals that exchanged messages through wireless channel prior to the authentication can lead to a malicious localization of an object. To increase the localization privacy within AAL application, we propose therefore a second contribution which is a new localization method that is based on the current Gen2V2 standard exchanges by anonymizing the tag identity.

Keywords: Internet of Things, Ambient Assisted Living, Radio Frequency Identification (RFID), Authentication, Localization, Privacy