MULTICAST GROUP KEY MANAGEMENT ON THE INTERNET OF MEDICAL THINGS USING ZERO KNOWLEDGE PROTOCOL

BY

CHONG WEI FENG

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfillment of the requirements

for the degree of

BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) COMMUNICATIONS AND NETWORKING

Faculty of Information and Communication Technology

(Kampar Campus)

JAN 2022

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: MULTICAST GROUP KEY MANAGEMENT ON THE INTERNET OF MEDICAL THINGS USING ZERO KNOWLEDGE PROTOCOL

Academic Session: JAN 2022

I CHONG WEI FENG
(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

(Author's signature) (Supervisor's signature)

Address:
3, PSRN BERCHAM TIMUR 5,
TAMAN BERCHAM BARU,
31400 IPOH, PERAK.

Vasaki Ponnusamy
Supervisor's name

Date: 20/04/2022

Date: 21/4/22

Universiti Tunku Abdul Rahman			
Form Title : **Sample of Submission Sheet for FYP/Dissertation/Thesis**			
Form Number: **FM-IAD-004**	Rev No.: **0**	Effective Date: **21 JUNE 2011**	Page No.: **1 of 1**

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TUNKU ABDUL RAHMAN

Date: 20/04/2022

SUBMISSION OF FINAL YEAR PROJECT /DISSERTATION/THESIS

It is hereby certified that ***CHONG WEI FENG*** (ID No: ***18ACB02120***) has completed this final year project entitled "***MULTICAST GROUP KEY MANAGEMENT ON THE INTERNET OF MEDICAL THINGS USING ZERO KNOWLEDGE PROTOCOL***" under the supervision of **TS. DR. VASAKI A/P PONNUSAMY** (Supervisor) from the Department of Computer and Communication Technology, Faculty of Information and Communication Technology.

I understand that University will upload softcopy of my final year project in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

____

(*CHONG WEI FENG*)

*Delete whichever not applicable

DECLARATION OF ORIGINALITY

I declare that this report entitled "**MULTICAST GROUP KEY MANAGEMENT ON THE INTERNET OF MEDICAL THINGS USING ZERO KNOWLEDGE PROTOCOL**" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : ______________________

Name : CHONG WEI FENG

Date : 20/04/2022

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to Dr. Vasaki Ponnusamy as my supervisor for providing me a golden opportunity to do this project and her encouragement and guidance throughout the project. I had learnt a lot of new knowledge while completing this project from her advice and suggestions given.

I would also like to extend my special thanks of gratitude to all lecturers and tutors in UTAR who taught me before as well as current semester. Various knowledges from different aspects are required to accomplish this project. By attending their classes and the wonderful lectures, I am prepared to utilise all knowledges gained in this work.

Not to forget my supportive family in giving me a chance to pursue my bachelor's degree which allow me to expose to more experience. Also, my friends who directly or indirectly assisted me by providing ideas really do help in my project.

ABSTRACT

As the world moving into industrial revolution 4.0 era, many industries as well as residential areas are adopting Internet of Things (IoT) for its convenience. Healthcare sectors such as hospitals and clinics nowadays are transitioning from traditional devices to IoT devices, where Internet of Medical Things (IoMT) are born. These devices enable real-time monitoring and minimise the need of medical professionals for non-severe situations. Thus, hospital personnel and patients' sensitive data will be transmitted through the Internet which supposedly need to be handle in care. However, due to the insufficient security measure, cybercriminals utilise the loopholes and perform cyberattacks for various purposed, which in worse case may lead to life-threatening events. Hence, authentication remains the key requirement in this matter. Group Key Management had been a popular topic to be discovered in order to maintain the truthfulness of the IoT environment. Unfortunately, the exchange of the group keys among IoT nodes in current group key management protocols can be easily intrude by third-party through Man-in-the-Middle attacks. To overcome the problems, zero knowledge protocol that meet 3 properties, completeness, soundness, and zero-knowledge, is proposed in this project. CupCarbon IoT 5.0 is used as the simulation tool to perform modelling and performance study. This report provides a real-life situation where sensor nodes in an IoT network will choose a leader node to establish the key distribution using zero-knowledge before the nodes are recognised as a network. After the performance study of this project, the group key distribution scheme is proven to be secured whereby the key is distributed successfully without transmitting the actual key. This greatly mitigate the chance of MITM is occur in the multicast group. In addition, when an unknown node joined the multicast group, the node will not receive the identical group key of the group, thus it will not be authenticated and banned from communicating within the multicast group.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AKMS	Area Key Management Server
CRT	Chinese Remainder Theorem
DBGK	Decentralised Batch-based Group Key Management Protocol
DG	Data Group
ECDH	Elliptic Curve Diffie Hellman
ECQV	Elliptic Curve Qu-Vanstone
GC	Group Controller
GKM	Group Key Management
GWD	Gateway Node
IoMT	Internet of Medical Things
IoT	Internet of Things
IP	Internet Protocol
KDC	Key Distribution Centre
KGC	Key Generation Centre
KMP	Key Management Protocol
LKH	Logical Key Hierarchy
MBS	Multicast Broadcast Group
MGKM	Multiple Group Key Management
MITM	Man-In-The-Middle
MKE	Master Key Encryption
MKE-MGKM	Master-Key-Encryption-based Multiple Group Key Management
SG	Service Group

SKDC	Sub Key Distribution Centre
SN	Sensor Node
SSH	Secure Socket Shell
TCP	Transmission Control Protocol
TEK	Traffic Encryption Key
UD	User

Chapter 1

Introduction

The Internet of Things (IoT) is referred to a network of “things” that can communicate with each other using TCP/IP, where the “things” are physical objects such as sensors, vehicles, smart phones, home appliance, etc., connected and sharing information [11, 22]. IoT employed the concept of hyper-connectivity, whereby individuals and organisations could be connected effortlessly regardless of the remote distance [26]. The IoT is not new to the world, and people adopting it not only for industrial purposes, but also used in smart houses, smart cities, or smart agricultures.

As the world is moving towards the Industrial Revolution 4.0 era, healthcare industry also gradually adopting IoT, and the Internet of Medical Things (IoMT) was born because of this. IoMT enables for real-time remote monitoring and telemedicine services, especially in this pandemic where the entire world is currently dealing with the rapid expansion of COVID-19. IoMT assists in minimising the needs of medical professionals for non-severe situations and focusing on more serious ones, when social distancing becomes a concern [25]. The architecture proposed by Al-Odat et. al. [2] is an example of IoMT. In their proposed scheme, diabetic patients could receive prescribed insulin doses through an infusion pump which connected to a microcontroller via a serial connection. The SSH protocol is used to establish a secure connection between the microcontroller and the cloud, and the SHA-256 mechanism is used to authenticate data flow between the cloud and the microcontroller. Authorized remote parties such as medical and research institutes, can access the stored health records and monitor the patients’ vital signs. Also, approved physician has the authority to regulate the infusion pump remotely [2].

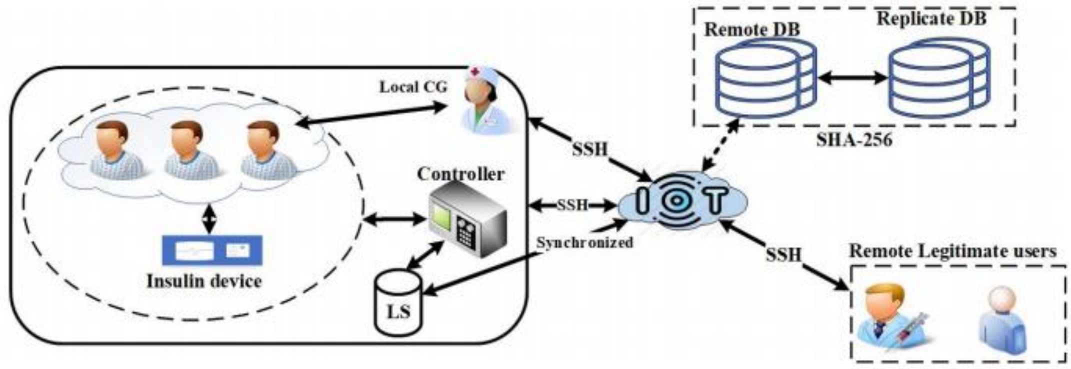


Figure 1.1. General architecture of IoT insulin device. Adapted [reprinted] from "A Reliable IoT-Based Embedded Health Care System for Diabetic Patients" by Al-Odat, Z. A., Srinivasan, S. K., Al-Qtiemat, E. M. and Shuja, S., 2019, https://arxiv.org/pdf/1908.06086.pdf

However, cyberattacks are focusing on a variety of industries, including the medical field. Cyber criminals are targeting medical devices such as pacemakers as well as medical institutions like hospitals and clinics. These flaws could lead to the leakage of patient data, or even worse, a life-threatening catastrophe [4].

Beavers & Pournouri [4] had collected a dataset from Open-Source Intelligence (OSINT) of year 2013 to 2016 on the trend of cyberattacks to healthcare field. The report shows that there has been an increase in the number of cyber-attacks during the timeline. From 2013 to 2015, there are 11, 30 and 33 cases reported respectively in each year, whereas there is a slightly drop in 2016 which is 19 cases, but there could be more than what had been reported.

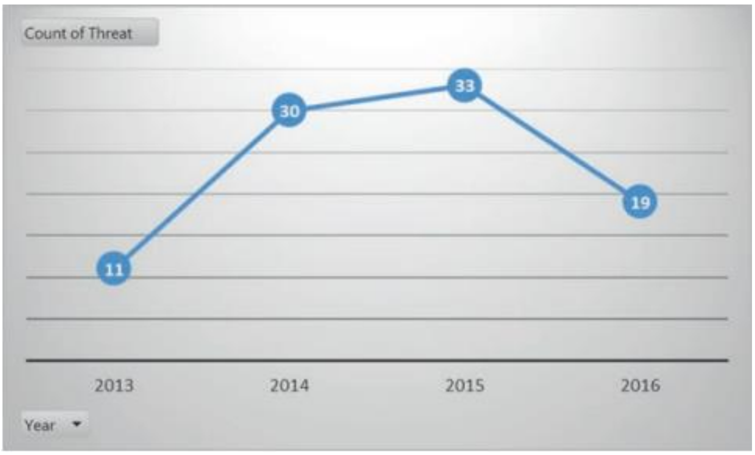


Figure 1.2. Cyber Attack trend from 2013 to 2016. Adapted [reprinted] from "Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions" by Beavers J., and Pournouri S., 2019, *Springer*, https://doi.org/10.1007/978-3-030-11289-9_11

Among these 93 reported cases, the most common cyberattack is account hijacking which holds 27% of the overall reported attacks, while the second most common is malware attack which occupies 24%. Account hijacking refers to an individual's email account, computer account, or any other account connected with a computing device or service is taken or hijacked by a hacker, while malware attacks are a sort of computer programme that infects and harms a legitimate user's computer in a variety of ways, for instance, virus, worms, and trojans. On the other hand, unknown attacks are becoming more common, indicating that either they were not adequately reported in the news or that cyber professionals were unable to identify the type of attack.

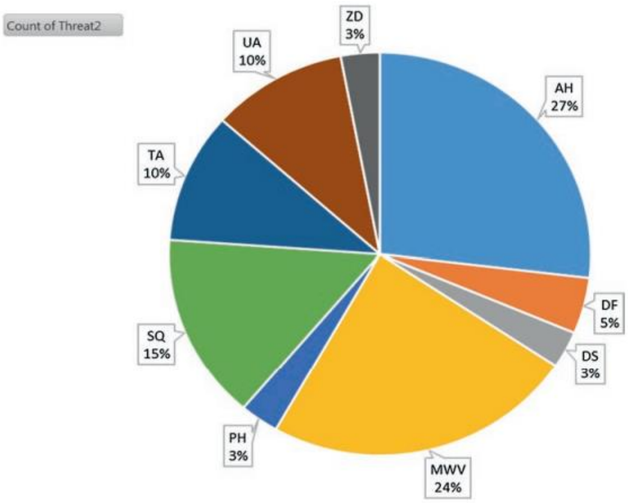


Figure 1.3. Type of attack to healthcare institutions. Adapted [reprinted] from "Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions" by Beavers J., and Pournouri S., 2019, *Springer*, https://doi.org/10.1007/978-3-030-11289-9_11

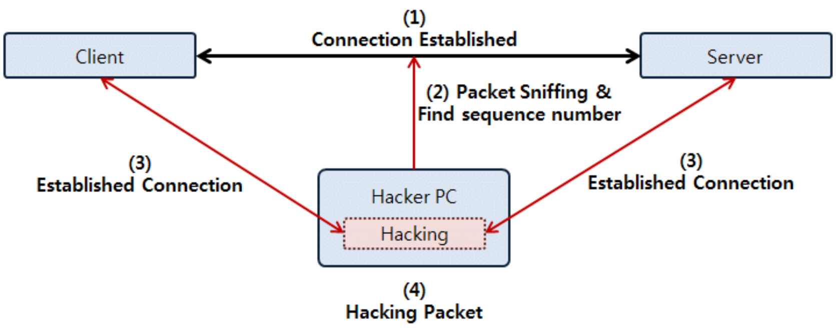


Figure 1.4. Example of account hijacking using session hijack. Adapted [reprinted] from "Comparative Analysis of Cyber Security Attacks in Virtual Organizations with their Mitigation Plans" by Saeed, K., Khalil, W., Ahmed, S., Hassan, F., Naeem, M. and Yousaf, M., 2020.

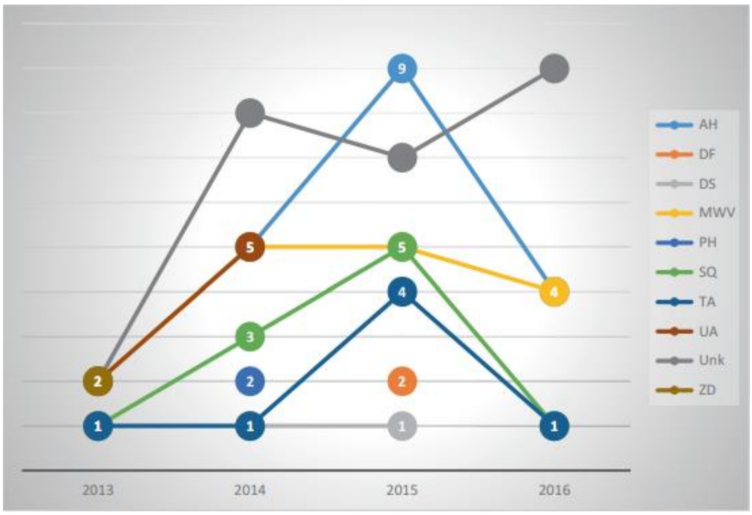


Figure 1.5. Type of Attack trends from 2013 to 2016. Adapted [reprinted] from "Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions" by Beavers J., and Pournouri S., 2019, *Springer*, https://doi.org/10.1007/978-3-030-11289-9_11

According to the report discussed, trends of unknown attacks are increasing and intrusions without authority are happening, due to that, intruders could join the multicast group (collection of all IoT medical devices of a same group) without authorised users' intention and perform eavesdropping within the group. Technologies are improving as the time goes, meanwhile attackers may develop different ways to perform cyberattacks. Nevertheless, attackers could compromise the integrity of users' data by performing jamming and spoofing attack, and various kind of unauthorised access [26]. Hence, authentication remains the key requirement for IoT by which the truthfulness of devices joining an IoT network is utmost important [9]. Thus, to safeguard authorised users' privacy and data, authentication scheme in IoMT is significant to prevent various type of illegitimate access. Many researchers are focusing on improving Group Key Management (GKM) to secure the group communication. Group keys are shared among the group members and needed to be secure and fresh so that only authorised members have the key. Message sent must be encrypted by the group key before sending to guarantee its integrity and confidentiality. On the other hand, GKM must be able to adapt with the scalability and the dynamic environment of the network, whereby users could subscribe and unsubscribe at any time. Therefore, GKM operation has to be performed to ensure the forward secrecy, backward secrecy, collusion freedom and group confidentiality. Thus, a proper and secure GKM and authentication mechanism are important to safeguard the communications within the multicast group [19].

Zero Knowledge Proof method can be proposed as a solution to the IoT technology. It is a powerful cryptographic solution for authentication problem and could proof the authenticity of legitimate users without revealing any easily computable information [5]. As compared to key sharing method, since information exchange in zero knowledge proof is not computable, thus there is no useful information that middlemen can sniff for the propose of intruding into the group or having any intention. For zero knowledge proof to work, there will be a Prover and a Verifier. The Verifier should provide an instance of a problem to the Prover, then the Prover must respond with a verifiable answer. To be more secure and obtained confidentiality, normally the Verifier would verify through repeated iterations [6].

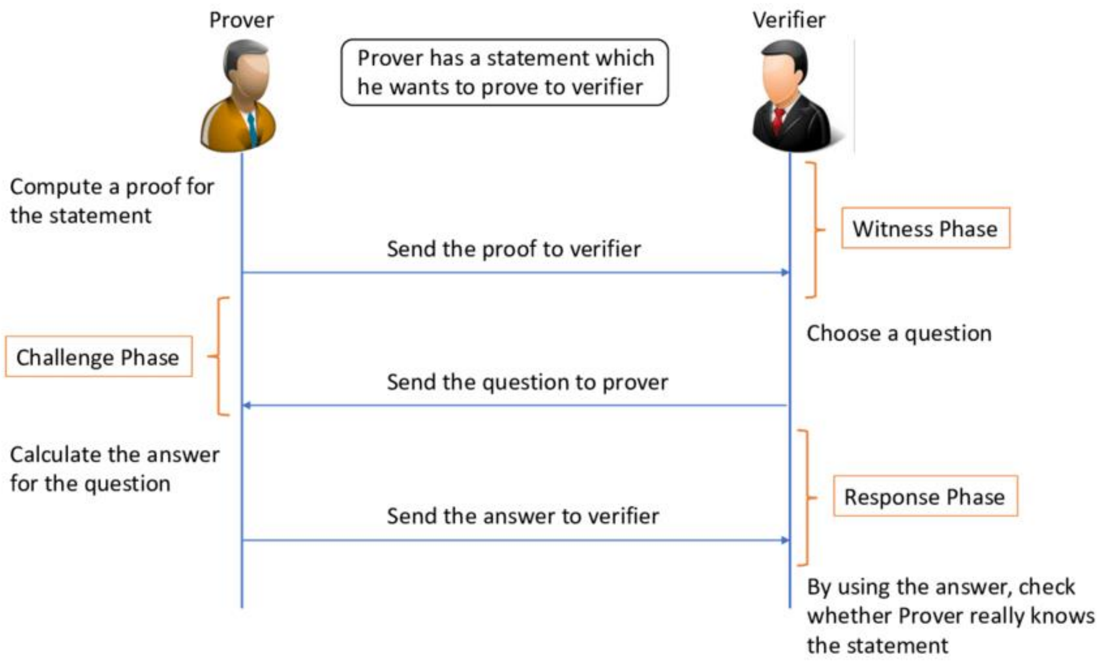


Figure 1.6. An interactive zero-knowledge protocol. Adapted [reprinted] from “SoK of Used Cryptography in Blockchain” by Raikwar, M., Gligoroski, D. and Kralevska, K., 2019, *IEEE Access, 7, 148550 – 148575.*

1.1 Problem Statement and Motivation

In IoT environment, access of users to the multicast group could be carried out using encryption techniques by shared keys. The purpose of these shared keys is to encrypt the communications between the users and to prevent unauthorised access. These shared keys are called group keys. Encryption of the communication within the multicast group uses symmetric encryption algorithm, and the group key exchange process is essential for the encryption process. Thus, group key management plays an important role to ensure the distribution of keys is secure.

But attackers might make use of unsecured medium to interrupt the group key exchanging process and break the cryptographic algorithm for own beneficial purposes. Also, they might pretend to be legitimate users to enter the multicast group to perform further actions. Especially in IoMT environment, the data transmitted between medical devices must be secure to avoid any kind of threats occurs. Other than data leakage, more serious cases would happen such as session hijacking where attackers control the devices and put the patients in danger. There could be revenge purposes that would cause life-threatening catastrophe which we do not want it to happen. Therefore, current group key management and authentication mechanism are not able to completely secure the multicast group from illegal access and ensure the secrecy of the group keys. A new solution is needed to be proposed to solve the above problems.

Zero knowledge protocol is suitable in this situation and there is no existing zero knowledge protocol in GKM scheme. Most existing GKM schemes adopt public-key cryptography such as SSH to maintain the authenticity of the data but unfortunately the keys can easily be stolen and cracked. Zero knowledge protocol enables the identification and verification process to happen without exchanging any keys, but only verification and proving algorithm are needed. This algorithm does not provide any information that is computable. It only required a Prover and Verifier in the process. Verifier will provide a question to the Prover, while the Prover needs to reply with a verifiable answer to proof that he/she had the key generated by legitimate centre.

The following research questions need to be addressed:

Question 1: How to develop a key distribution scheme for authentication purpose without revealing the actual key information in the IoMT?

Question 2: How to authenticate devices in the multicast group using Zero Knowledge Protocol?

1.2 Objectives

The main goal of this project is to add to the body of knowledge regarding the development of group key management protocols that can be used in IoMT group applications. It is important for IoMT applications to have strong security mechanisms built-in to ensure patients are in safe environment. The following objectives must be met to establish a group key management protocol for IoMT.

1. **To enhance the authentication process with existing GKM schemes.**
    1.1. To design a novel Zero Knowledge Protocol as an extra level to authenticate users within a multicast group.
2. **To authenticate devices within a multicast group without revealing actual key information.**
    2.1. To ensure the zero knowledge properties (completeness, soundness, zero-knowledge) in the authentication process.

1.3 Project Scope and Direction

This project is aimed to propose a novel authentication scheme using Zero Knowledge Protocol in IoT medical devices, more precisely, IoMT. There are variety of Group Key Management scheme being proposed and in use but still not able to ensure the authenticity of the multicast group devices due to computable information is transmitted during authentication process. A method that can identify every node within the multicast group without exchanging computable information is needed to enhance the security. Hence, Zero Knowledge Protocol is introduced in this project.

The IoT environment is huge, including tens of hundreds of devices connected. But in this project, we reduce the number of devices to eases the implementation and analysis process. On the other hand, existing GKM scheme is utilised together with the Zero Knowledge Protocol as second level authentication, thus the scope of this project is to strengthen the authentication process in a small scale IoT environment using Zero Knowledge Protocol. Moreover, this project focuses security issues on IoT medical devices as a subset of the huge IoT topic.

It is expected that there is no chance for intruders to join the multicast group without being authorised. Also, cyberattacks such as collusion attacks will be prevented. Hence, users' information will be secured and not leaked. The result will be tested using CupCarbon IoT 5.0 as a simulation tool.

1.4 Contributions

Due to the rapid growth of IoT Technology, security is also needed to be enhanced periodically to make sure that users' data is protected. In this project, the main contribution is to decrease possibility of the security attacks such as collusion attacks and other MITM attacks in IoT environment, specifically healthcare sector, as Zero Knowledge Protocol does not require communication in exchange of computable information. Thus, patients would be protected from data breach or any life-threatening events. On the other hand, the protocol can apply in any IoT areas, so users would trust the technology as the confidentiality of their data is ensured and the cyberworld is secured. In addition, this project is unique since most of the existing schemes are only using one way authentication while it provides two level where the Zero Knowledge Protocol is employed together with the existing GKM scheme to further improves the authentication process in IoT multicast group communication. Moreover, Zero Knowledge Protocol have not been used in existing GKM schemes.

1.5 Report Organization

This report is organised into 6 chapters: Chapter 1 Introduction, Chapter 2 Literature Review, Chapter 3 System Model, Chapter 4 System Design, Chapter 5 Experiment/Simulation, Chapter 6 System Evaluation and Discussion, and Chapter 7 Conclusion. The first chapter is the introduction of this project which includes project background, problem statement and motivation, project scope, project objectives, project contribution, and report organisation. The second chapter is the literature review having done by researchers on several existing group key management protocols and the implementation of zero knowledge protocol. The third chapter is focusing on the project methodology and how is the project be done. The fourth chapter is discussing the overall system design of this project. The fifth chapter is regarding the details on how to proof the proposed protocol using a simulation tool. Furthermore, the sixth chapter reports the outcome of the simulation and the efficiency of the proposed protocol. The last chapter is to conclude the project and come up with recommendation for future work.

Chapter 2

Literature Review

2.1 Summary of Existing Key Management Scheme

Various types of key management scheme had been proposed by many researchers. All to them have their respective pros and cons. Table 2.1 represents the overview of previous proposed solutions.

Table 2.1. A summary table of security & key management related work.

No.	Paper Title	Advantage(s)	Disadvantage(s)	Characteristic(s)
1.	Two-factor mutual authentication with key agreement in wireless sensor networks [29].	Computational costs for gateway and sensor nodes are in acceptable range.	Depends on user-supplied information	Mutual authentication scheme is introduced in which a user and an object agree on a session key. For gateway entry, traditional password authentication is used, with a secret created and stored on various devices within the system.
2.	Chaotic maps-based password-authenticated key agreement using smart cards [13].	can withstand a series of attacks while still meeting critical security requirements. Computational cost is acceptable.	user anonymity is not preserved, and double secret keys are inefficient.	A novel password-authenticated key agreement protocol is proposed based on chaotic maps.

3.	Key Management for Multiple Multicast Groups in Wireless Networks [21].	In the rekeying process, dramatically reduce storage and communication overheads.	Did not consider dynamic device groups.	Propose MKE-MGKM Scheme that uses master keys and slave keys.
4.	A Decentralized Batch-Based Group Key Management Protocol for Mobile Internet of Things (DBGK) [1].	Both backward and forward secrecy is guaranteed without making any assumptions about the moving member validity in the source field.	Did not consider that multiple users can join at the same time.	Adopt decentralised architecture to avoid single point of failure issues. Time-driven approach is used with a group key for each time slot or interval.
5.	A novel batch-based group key management protocol applied to the Internet of Things [30].	The number of exchanged messages needed for managing group member changes and rekeying is reduced by dividing time into intervals.	Did not consider that multiple users can join at the same time.	Time is partitioned into fixed-length intervals to minimise membership shift overhead. Rekeying acts are handled based on time intervals.
6.	Key Management in Internet of Things via Kronecker Product [28].	The computation cost and storage cost are reduced. Does not require communication during the computation of the pairwise key.	The key update when users or devices join and leave the system was not taken into account to maintain forward and backward secrecy.	Kronecker product is introduced in the scheme to decrease data stored in nodes, efficient pairwise key computation and exclude the need of communication

				during computation of keys.
7.	A Computation-Efficient Group Key Distribution Protocol Based on a New Secret Sharing Scheme [15].	It lowers the cost of computation for group members during the rekeying process. A simple and efficient key-numbering system was discovered.	Did not consider dynamic device groups.	The logical key hierarchy (LKH) tree structure is used to implement a simple and efficient key-numbering system. An enhanced secret sharing scheme has been proposed to develop better encryption and decryption algorithms.
8.	Authenticated Group Key Transfer Protocol Based on Secret Sharing [14].	The group key distribution is information technically safe in terms of confidentiality.	In large groups, the computational cost is immense.	An authenticated group key transfer protocol (AGKTP) was proposed on the basis of a secret-sharing scheme. It safeguards sensitive group information that is broadcast to all group members by KGC.
9.	Group Key Management based on (2,2) Secret Sharing [32].	The number of rekeying messages is reduced to only one.	In large commutation groups, it results in a substantial	A group-key management scheme based on (2, 2) secret sharing is proposed.

		The size of multicast messages is smaller, and there is less key storage demand and processing overhead.	increase in computing costs.	After receiving the GKD’s multicast rekeying message, each member will create a group key on their own.
10.	Key Management Protocol with Implicit Certificates for IoT systems [24].	It provides reliable key negotiation, lightweight node authentication, fast re-keying, and effective security against relay attacks all at the same time.	Asymmetric encryption methods are used, which are not suitable for use on resource constrained IoT devices.	KMP that is incorporated at layer-2 of the protocol stack is proposed and aims to save as much airtime as possible by using the ECQV technique.

As refer to Table 2.1, most of the researchers are focusing on proposing a suitable key management scheme that is able to maintain the confidentiality of the communication within a multicast group, at the same time, reduce the computational cost and storage due to limited resources in IoT. Forward and backward secrecy protection is essential to prevent any data leak. To achieve this, rekeying process is a must by renewing the group key after a member joins or leave the multicast group. Some of the rekeying process require high computational cost which lower down the performance of overall key management. Also, some of the proposed solution still required user-supplied information in order to establish the communication. Thus, a new protocol is needed to enhance the existing key management scheme. This project report is continued with the elaboration of the related works and the methodology used in each of them.

2.1.1 Existing Key Management Scheme

Vaidya et. al. [29] proposed a mutual authentication scheme in which a user and an object agree on a session key. For gateway access, traditional password authentication has been used, with a secret created and stored on various devices within the system. These devices are assigned to fulfil the users' requests. During the login process, a smart card was added to allow the device to determine if the request was completed within an appropriate timeframe for the session key to be generated. At the stage of transferring credentials to devices inside the network, most of the techniques listed above depend on user-supplied information. The protocol's basic concept is that a user receives a smart card from GWN during the registration process, and that during the login-authentication phase, the user can log in to the sensor or GWN and access data using the user's password and smart card. Figure 2.1 and Figure 2.2 depict the phases flow of the scheme.

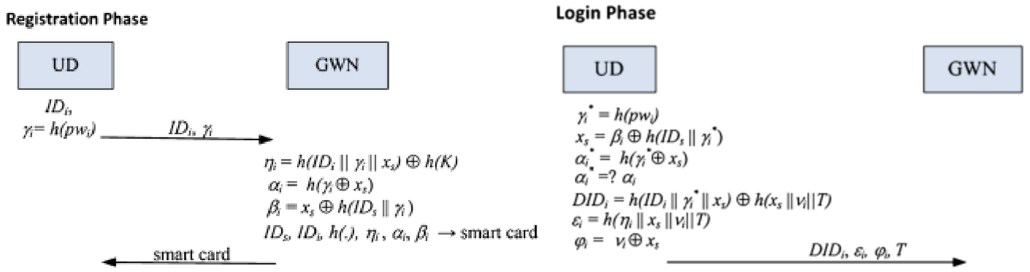


Figure 2.1. Registration and login phase flow of the mutual authentication scheme. Adapted [reprinted] from "Two-factor mutual authentication with key agreement in wireless sensor networks" by Vaidya, B., Makrakis, D., and Mouftah, H., 2012, *Security and Communication Networks, 9(2), 171–183.* Copyright 2012 by "John Wiley & Sons; Ltd".

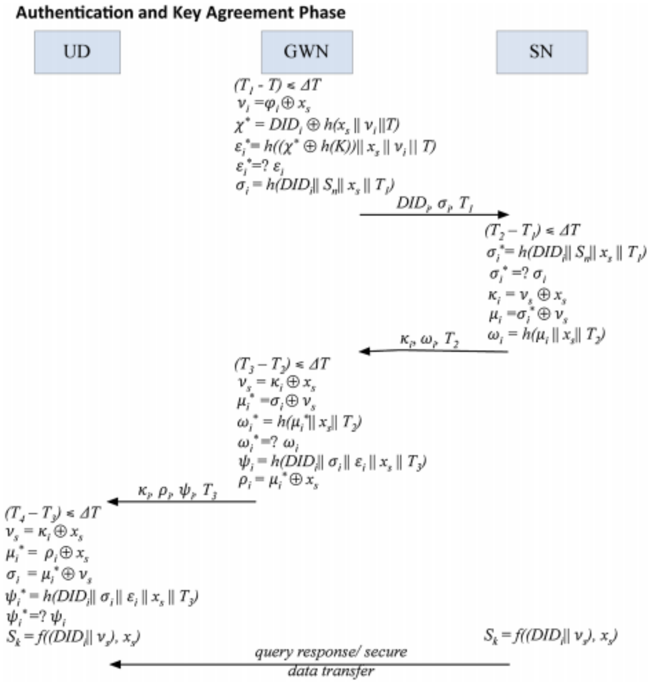


Figure 2.2. Authentication and key agreement phase flow of the mutual authentication scheme. Adapted [reprinted] from "Two-factor mutual authentication with key agreement in wireless sensor networks" by Vaidya, B., Makrakis, D., and Mouftah, H., 2012, *Security and Communication Networks, 9(2), 171–183.* Copyright 2012 by "John Wiley & Sons; Ltd".

A novel password-authenticated key agreement protocol is proposed by Guo & Chang [13] based on chaotic maps. This scheme consists of 4 phases namely the Parameter generation phase, the Registration phase the Authentication phase and the Password change phase. First, parameters such as a public key scheme based on Chebyshev chaotic maps, a one-way hash function and a symmetric key cryptosystem will be chosen by the server. Then, user with identity ID will select a password and random number to register to the server. The process proceeds by a mutual authentication and establish an agreed-upon session key used in the communication. If user intends to modify his/her password, a series of computational process will be followed. Figure 2.3 and Figure 2.4 shows the registration phase and authentication phase of the scheme, respectively. Hence, user anonymity is not preserved, and double secret keys are inefficient as it requires user-supplied information as the scheme proposed by Vaidya et. al. [29].

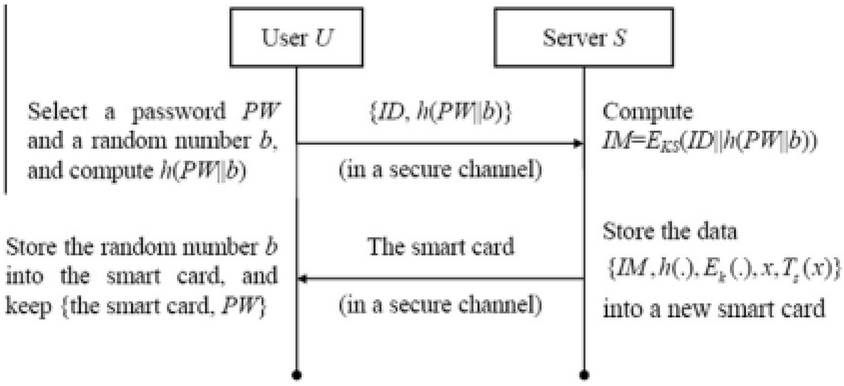


Figure 2.3. Registration phase of the key agreement protocol based on chaotic maps. Adapted [reprinted] from "Chaotic maps-based password-authenticated key agreement using smart cards" by Guo, C., and Chang, C. C., 2013, *Communications in Nonlinear Science and Numerical Simulation, 18(6), 1433–1440.* Copyright 2012 by "Elsevier B.V.".

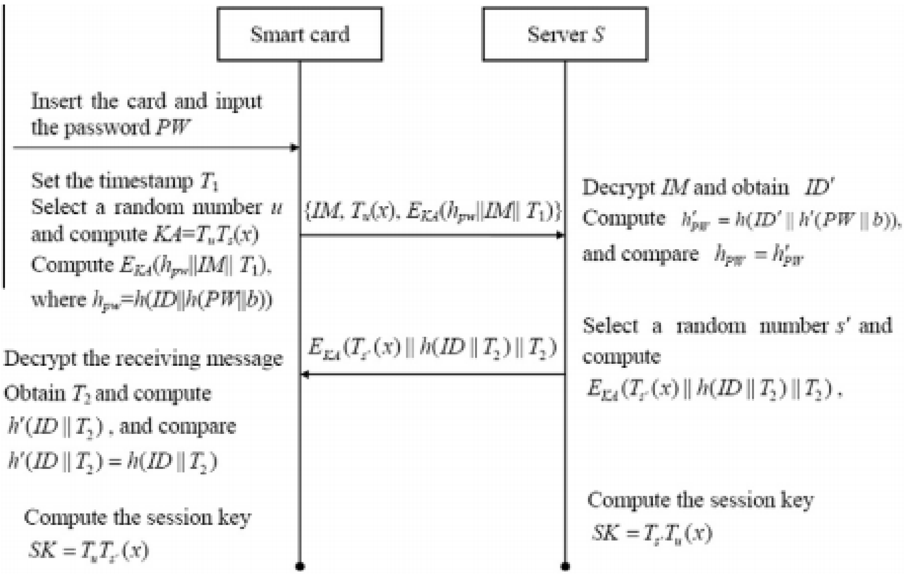


Figure 2.4. Authentication phase of the key agreement protocol based on chaotic maps. Adapted [reprinted] from "Chaotic maps-based password-authenticated key agreement using smart cards" by Guo, C., and Chang, C. C., 2013, *Communications in Nonlinear Science and Numerical Simulation, 18(6), 1433–1440.* Copyright 2012 by "Elsevier B.V.".

Park et. al. [21] proposed MKE-MGKM scheme that uses master keys and slave keys. In this proposed scheme, two types of user groups are defined as Data Group (DG) and Service Group (SG), where DG refers to all users who subscribe to MBS while SG refers to the set of users who subscribe to the same set of MBSs. A user may be a member of one or more DGs, but only one SG at a time. Thus, it does not consider dynamic device groups. The procedure of this scheme begins with an initial step whereby a master key and slave keys will be generated. Then, SG key tree is constructed based on the number of SG. Finally, the initial step ends with the MKE-key graph construction to distribute corresponding TEKs to users in each SG. However, users may unsubscribe from one SG and switch to another SG, so rekeying process is needed to maintain the forward secrecy. The process starts with revoking the old keys and create new a master key, then broadcast the new TEK that is encrypted with it. Figure 2.5 and Figure 2.6 describe the MKE-based key graph after initial set up and after the rekeying process.

Capability Matrix

Service Group	MBS / User	1	2	3
SG1	user1	1	1	1
	user2	1	1	1
	user3	1	1	1
	user4	1	1	1
SG2	user5	1	1	0
	user6	1	1	0
	user7	1	1	0
	user8	1	1	0
SG3	user9	1	0	1
	user10	1	0	1
	user11	1	0	1
	user12	1	0	1
SG4	user13	1	0	0
	user14	1	0	0
SG5	user15	0	1	0
	user16	0	1	0

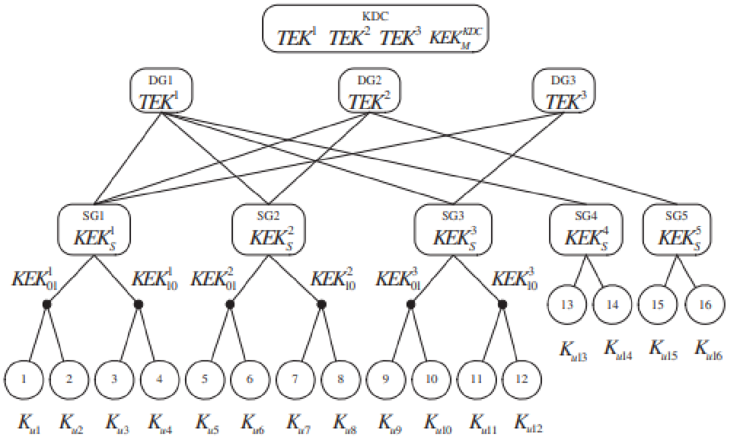


Figure 2.5. MKE-based key graph after initial set up. Adapted [reprinted] from “Key Management for Multiple Multicast Groups in Wireless Networks.” by Park, M. H., Park, Y. H., Jeong, H. Y., and Seo, S. W., 2013, *IEEE Transactions on Mobile Computing, 12(9), 1712–1723.* Copyright 2012 by “IEEE”.

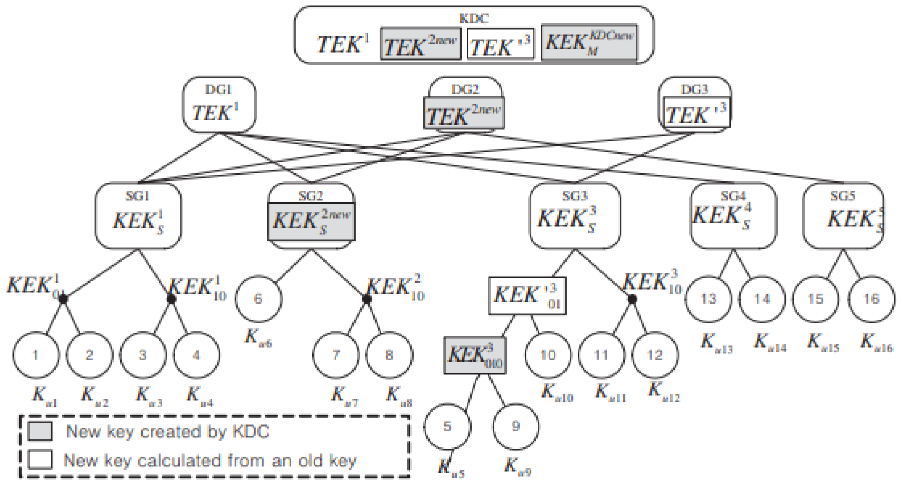


Figure 2.6. MKE-based key graph after rekeying process. Adapted [reprinted] from “Key Management for Multiple Multicast Groups in Wireless Networks.” by Park, M. H., Park, Y. H., Jeong, H. Y., and Seo, S. W., 2013, *IEEE Transactions on Mobile Computing, 12(9), 1712–1723.* Copyright 2012 by “IEEE”.

To adapt to the scalable condition of the IoT and the limited power and computational capabilities, Abdmeziem et. al. [1] had proposed a decentralised batch based GKM. In this scheme, time is divided into intervals and keys are used in each time slot. Moreover, the decentralised architecture reduces the chance of a single point of failure issues. Its network model is divided into multiple areas whereby each of them are managed by an AKMS. The purpose of the AKMS is to establish TEK and distribute to the users of the specific area. On the other hand, another server called GKMS is responsible to manage all AKMSs and set security policy for the overall group. Meanwhile, an Active Object List (AOL) is maintained by the AKMS to stores the delivered credentials to the objects for each time slot. However, the proposed scheme does not consider multiple users may join the group at the same time. Figure 2.7 illustrate the decentralised architecture and Figure 2.8 shows the DBGK signalling flow.

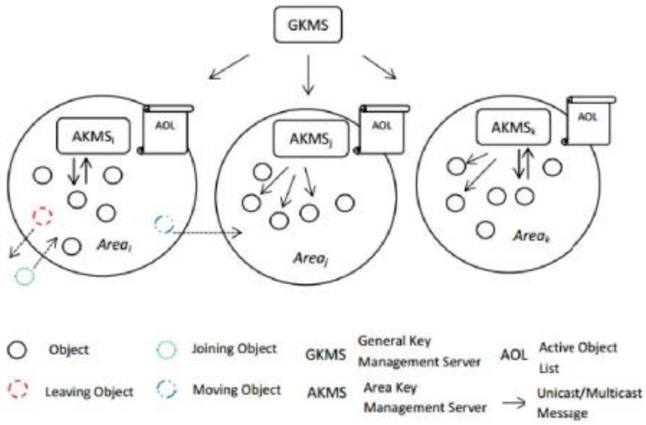


Figure 2.7. DBGK network model: a decentralized architecture based on an independent group key per area. Adapted [reprinted] from "A Decentralized Batch-Based Group Key Management Protocol for Mobile Internet of Things (DBGK)" by Abdmeziem, M. R., Tandjaoui, D., and Romdhani, I., 2015, *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.* Copyright 2015 by "IEEE".

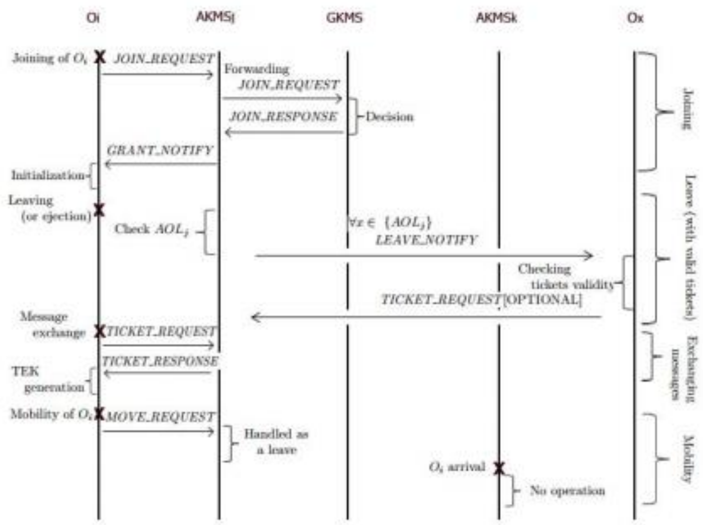


Figure 2.8. DBGK signalling flow. Adapted [reprinted] from "A Decentralized Batch-Based Group Key Management Protocol for Mobile Internet of Things (DBGK)" by Abdmeziem, M. R., Tandjaoui, D., and Romdhani, I., 2015, *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing.* Copyright 2015 by "IEEE".

Veltri et. al. [30] also propose a batch-based group key management protocol to be applied in IoT. In this scheme, similar to the previous scheme stated in this project report, the time is partitioned into fixed-length intervals to minimise membership shift overhead and each time slots are given a different group key. Meanwhile rekeying acts are handled based on time intervals. Users intended to join the group have to wait until the next slots to reduce the cost of rekeying. On the other hand, this scheme considers two types of leave strategies, pre-determined leave events and unpredictable leave events. Rekeying process only happens in the stime slots where the new join and leave events occur. The limitation of this scheme is that the subscription of multiple users at the same time is not considered. Figure 2.9 shows the deriving process and Figure 2.10 explains how to achieve backward and forward secrecy by transmitting the smallest set of values x that span the subscription duration of a member.

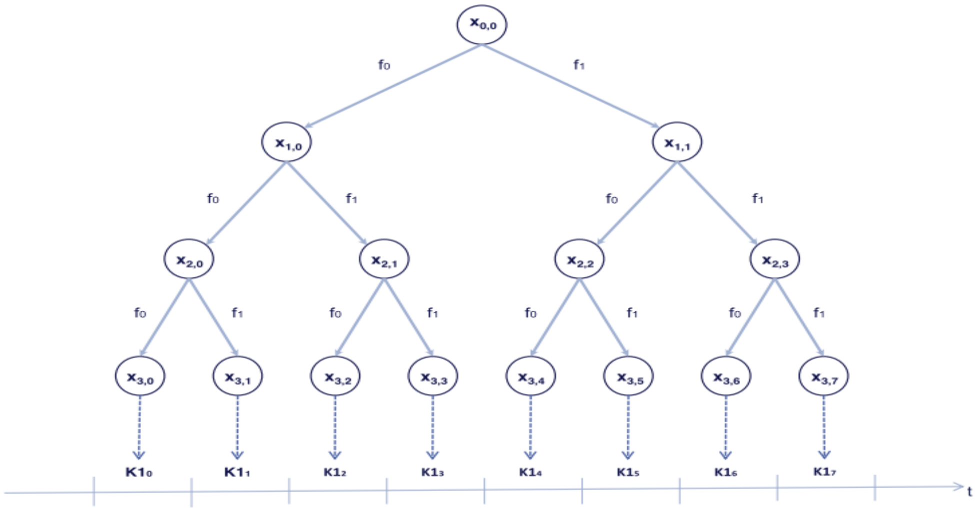


Figure 2.9. Deriving all K1 subkeys by applying functions f_0 and f_1. Adapted [reprinted] from "A novel batch-based group key management protocol applied to the Internet of Things" by Veltri, L., Cirani, S., Busanelli, S., and Ferrari, G., 2013, *Ad Hoc Networks, 11(8), 2724–2737*. Copyright 2013 by "Elsevier B.V.".

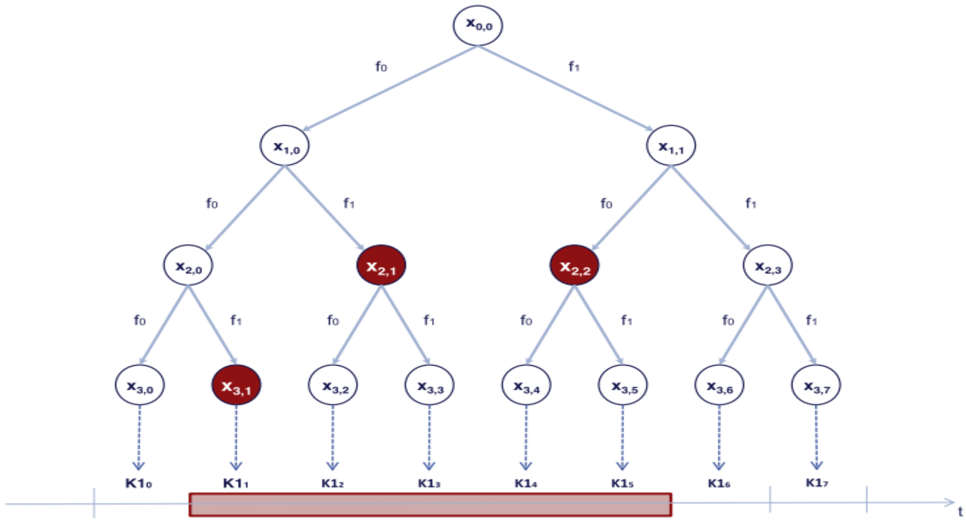


Figure 2.10. Achieving backward and forward secrecy. Adapted [reprinted] from "A novel batch-based group key management protocol applied to the Internet of Things" by Veltri, L., Cirani, S., Busanelli, S., and Ferrari, G., 2013, *Ad Hoc Networks, 11(8), 2724–2737*. Copyright 2013 by "Elsevier B.V.".

Tsai et. al. [28] proposed a key management scheme using on Kronecker Product. Kronecker Product is denoted by ⊗ and it is an operation that produces a block matrix from two matrices of any dimension. This scheme is composed of 4 steps, first, apply Kronecker Product, second, apply matrix decomposition, third, assign data to sensor nodes, and forth, communication between sensor nodes. The advantage side of this scheme is that the computation cost and storage cost can be reduced, and it does not require communication during the computation of the pairwise key. However, the key update when users or devices join and leave the system was not taken into account to maintain forward and backward secrecy. The following steps demonstrates the process of this scheme proposed by the authors.

1. Kronecker Product

   Assume $A = B \bullet D = \begin{bmatrix} 2 & 25 \\ 25 & 105 \end{bmatrix}$

   $G = C \bullet F = \begin{bmatrix} 292 & 134 \\ 134 & 30 \end{bmatrix}$

$$A \otimes G = K : \begin{bmatrix} 5 & 25 \\ 25 & 105 \end{bmatrix} \bigotimes \begin{bmatrix} 292 & 134 \\ 134 & 30 \end{bmatrix}$$

$$= \begin{bmatrix} 5 \times 292 & 5 \times 134 & 25 \times 292 & 25 \times 134 \\ 5 \times 134 & 5 \times 30 & 25 \times 134 & 25 \times 30 \\ 25 \times 292 & 25 \times 134 & 105 \times 292 & 105 \times 134 \\ 25 \times 134 & 25 \times 30 & 105 \times 134 & 105 \times 30 \end{bmatrix}$$

2. Matrix decomposition

   A can be decomposed into B • D, while G can be decomposed into C • F

$$B{\cdot}D \otimes C{\cdot}F = K : \begin{bmatrix} 3 & 4 \\ 11 & 18 \end{bmatrix} \cdot \begin{bmatrix} -1 & 3 \\ 2 & 4 \end{bmatrix} \bigotimes \begin{bmatrix} 10 & 42 \\ -4 & 25 \end{bmatrix} \cdot \begin{bmatrix} 4 & 5 \\ 6 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 5 \times 292 & 5 \times 134 & 25 \times 292 & 25 \times 134 \\ 5 \times 134 & 5 \times 30 & 25 \times 134 & 25 \times 30 \\ 25 \times 292 & 25 \times 134 & 105 \times 292 & 105 \times 134 \\ 25 \times 134 & 25 \times 30 & 105 \times 134 & 105 \times 30 \end{bmatrix}$$

=

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cc} \quad\quad\quad 1 \quad\quad\quad & \quad\quad\quad 2 \quad\quad\quad \end{array} \\ \begin{bmatrix} B_{1,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,1} & B_{1,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,2} \\ B_{1,-} \cdot D_{-,1} \times C_{2,-} \cdot F_{-,1} & B_{1,-} \cdot D_{-,1} \times C_{2,-} \cdot F_{-,2} \\ B_{2,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,1} & B_{2,-} \cdot D_{-,1} \times C_{1,-} \cdot F_{-,2} \\ B_{2,-} \cdot D_{-,1} \times C_{2,-} \cdot F_{-,1} & B_{2,-} \cdot D_{-,1} \times C_{2,-} \cdot F_{-,2} \end{bmatrix} \end{array}$$

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cc} \quad\quad\quad 3 \quad\quad\quad & \quad\quad\quad 4 \quad\quad\quad \end{array} \\ \begin{bmatrix} B_{1,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,1} & B_{1,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,2} \\ B_{1,-} \cdot D_{-,2} \times C_{2,-} \cdot F_{-,1} & B_{1,-} \cdot D_{-,2} \times C_{2,-} \cdot F_{-,2} \\ B_{2,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,1} & B_{2,-} \cdot D_{-,2} \times C_{1,-} \cdot F_{-,2} \\ B_{2,-} \cdot D_{-,2} \times C_{2,-} \cdot F_{-,1} & B_{2,-} \cdot D_{-,2} \times C_{2,-} \cdot F_{-,2} \end{bmatrix} \end{array}$$

3. Assign data to sensor nodes

   B and C is then assigned to each sensor node accordingly, for example,

   sensor node #1 keeps ($B_{1,-}$), ($C_{1,-}$), which is [3 4], [10 42].

   sensor node #2 keeps ($B_{1,-}$), ($C_{2,-}$), which is [3 4], [-4 25].

   sensor node #3 keeps ($B_{2,-}$), ($C_{1,-}$), which is [11 18], [10 42].

   sensor node #4 keeps ($B_{2,-}$), ($C_{2,-}$), which is [11 18], [-4 25].

4. Communication of sensor nodes

   When 2 sensor nodes intend to communicate, they only need to compute the indexes of matrix D and F's column vectors and perform simple vector multiplication. Figure 2.11 demonstrates how Node #1 and Node #3 generate pairwise to communicate. Each pair of nodes that are going to transmit data will retrieve the same key. It is clearly shown that no information is being exchange during the process.

Node #1	Node #3
1. Computes index number [3/√4] = 2 and 3 % √4 = 1	2. Computes index number [1/√4] = 1 and 1 % √4 = 1
3. Calculates $(B_{1,-} \bullet D_{-,2}) \times (C_{1,-} \bullet F_{-,1})$ where $D_{-,2}$ and $F_{-,1}$ are form of the computed index number. $(3 \quad 4) \bullet \binom{3}{4} \times (10 \quad 42) \bullet \binom{4}{6}$ $= 25 \times 292$ $= 7300$	4. Calculates $(B_{2,-} \bullet D_{-,1}) \times (C_{1,-} \bullet F_{-,1})$ where $D_{-,1}$ and $F_{-,1}$ are form of the computed index number. $(11 \quad 18) \bullet \binom{-1}{2} \times (10 \quad 42) \bullet \binom{4}{6}$ $= 25 \times 292$ $= 7300$

Figure 2.11. Key generation process. Adapted [reprinted] from “Key Management in Internet of Things via Kronecker Product” by Tsai, I. C., Yu, C. M., Yokota, H., and Kuo, S. Y., 2017, *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC).* Copyright 2017 by “IEEE”.

Jiao et. al. [15] had proposed a computation-efficient group-key distribution protocol based on a new secret-sharing scheme to solve the problem of insufficient computation resource of mobile terminals in the key distribution mechanism, based on the LKH scheme. In this scheme, GC is responsible for the overall group key distribution using secret-sharing scheme in the network model. The depth of the key tree equals the number of polynomials to be built by GC, and the degree of the polynomials equals the degree of the key tree. If the composition of a group changes in the LKH system, all members who are still in the group must update all keys on their key paths. Decryption operations must be performed many times in the case of a large contact group. Thus, it will increase the overall time and resource required. Another secret-sharing scheme is suggested, in which the secret distributor calculates the corresponding polynomial before all authorised members' secret shares are determined, allowing any authorised member to access the secret. However, this proposed scheme does not actually consider the dynamic device group whereby there are possibilities that one user would join multiple groups. Figure 2.12 shows the key tree update process provided by the authors.

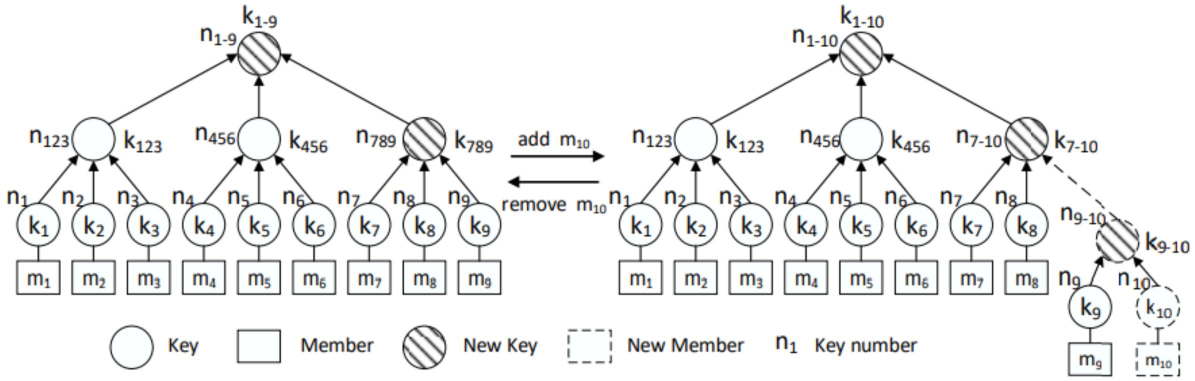


Figure 2.12. Key tree update process. Adapted [reprinted] from "A Computation-Efficient Group Key Distribution Protocol Based on a New Secret Sharing Scheme." by Jiao, R., Ouyang, H., Lin, Y., Luo, Y., Li, G., Jiang, Z., and Zheng, Q., 2019, *Information, 10(5), 175.* Copyright 2019 by the authors.

Harn and Lin [14] suggested an authenticated group key transfer protocol (AGKTP) based on a secret-sharing scheme in which members share a secret with GC when they join a group for the first time. To subscribe to the group key transfer service and create a secret with KGC, each user must first register at KGC. As a result, a safe channel is needed to share this secret with each user at first. Then, in a broadcast channel, KGC can transport the group key and communicate with all group members. Moreover, no computational assumption is required for the group key to transfer to each group member. The group key is authenticated by sending a single authentication message to all members of the group. Also, KGC broadcasts the rekeying message to all group members, and only approved group members can recover the group key during the rekeying process. Due to this, Jiao et. al. [15] claimed that the number of group members equals the degree of polynomials in this scheme, so the computational cost in large groups is immense. Figure 2.13 demonstrates the group key transfer protocol for this scheme.

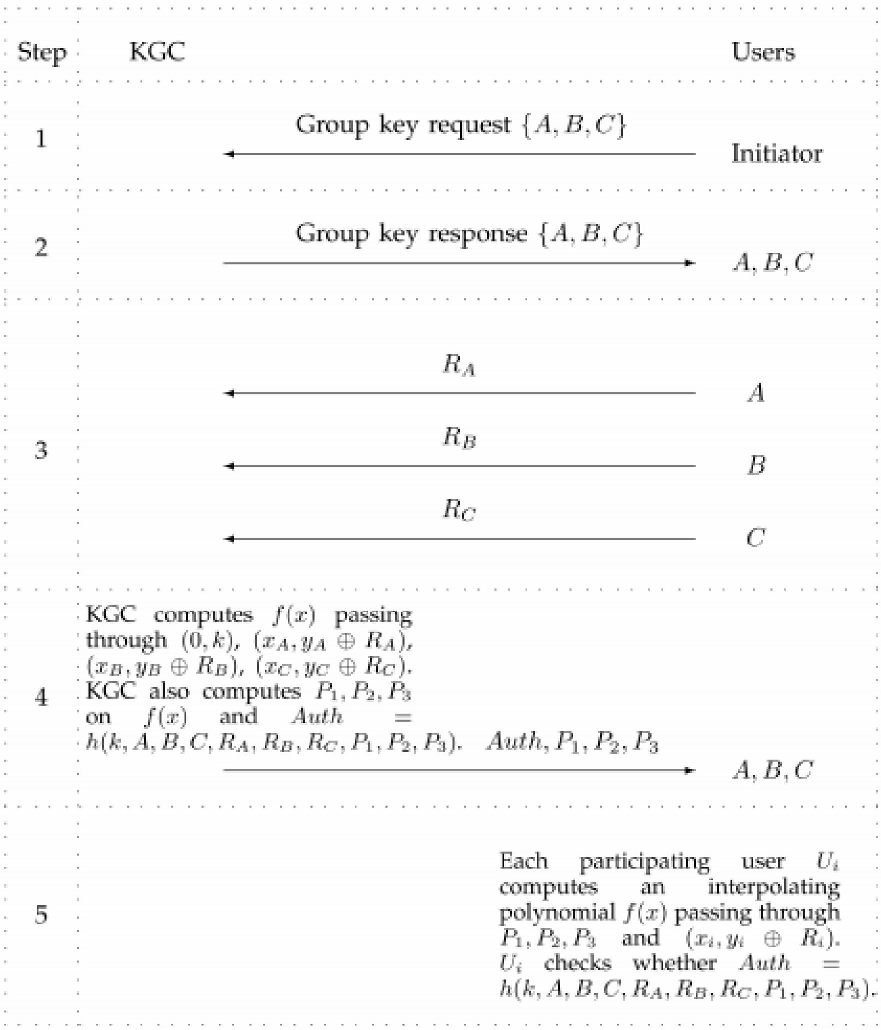


Figure 2.13. Group key transfer protocol. Adapted [reprinted] from "Authenticated Group Key Transfer Protocol Based on Secret Sharing" by Harn, L., and Lin, C., 2010, *IEEE Transactions on Computers, 59(6), 842–846.* Copyright 2010 by "IEEE".

Wuu et. al. [32] outlined a secure authenticated group key management scheme based on (2, 2) secret sharing technology that does not require the maintenance of a key tree and the number of rekeying messages is reduced to only one. After receiving the GKD's multicast rekeying message, each member will create a group key on their own. Thus, no message is needed to be sent out. Each member and the GKD will perform implicit mutual authentication during the self-generation of group key operation. Therefore, the size of multicast messages is smaller, and there is less key storage demand and processing overhead. However, in large commutation groups, the number of polynomials to create is equal to the number of members, resulting in high computation costs. The proposed scheme composed of four processes, which are system initialisation, group creation, member join and member leave. In the initial stage, GKD will declare a prime number, one-way hash function and a symmetric encryption algorithm. Then, user should register to the GKD in order to retrieve the pre-shared key. The process is followed by group creation by Group Initiator, eventually members can join the group by sending request message to the GKD. After a member left the group, group key will be renewed by the GKD. Figure 2.14 to Figure 2.16 illustrate the process of user registration, group creation and member joining.

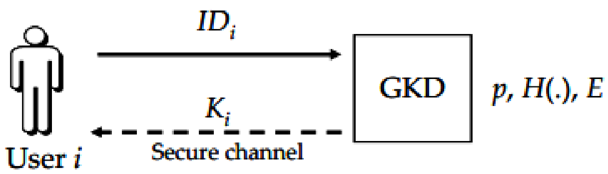


Figure 2.14. User registration process. Adapted [reprinted] from "Group Key Management based on (2,2) Secret Sharing" by Wuu, L.C., Hung, C. H. and Kuo, W. C., 2014, *KSII Transactions on Internet and Information Systems. 8. 1144-1156.* Copyright 2014 by "KSII".

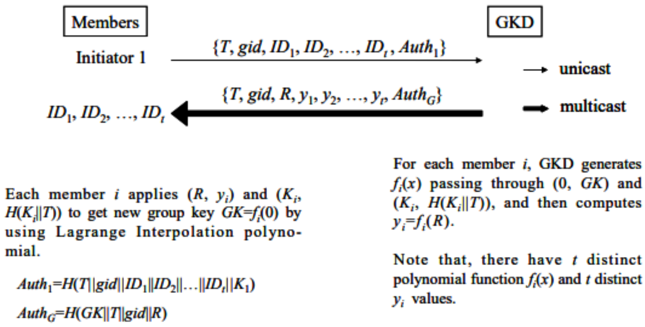


Figure 2.15. Group creation process. Adapted [reprinted] from "Group Key Management based on (2,2) Secret Sharing" by Wuu, L.C., Hung, C. H. and Kuo, W. C., 2014, *KSII Transactions on Internet and Information Systems. 8. 1144-1156.* Copyright 2014 by "KSII".

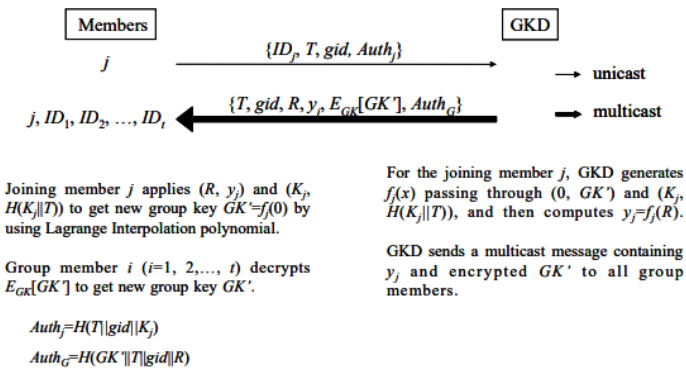


Figure 2.16. Member joining. Adapted [reprinted] from "Group Key Management based on (2,2) Secret Sharing" by Wuu, L.C., Hung, C. H. and Kuo, W. C., 2014, *KSII Transactions on Internet and Information Systems. 8. 1144-1156.* Copyright 2014 by "KSII".

Sciancalepore et. al. (2015) proposed a Key Management Protocol which makes use of commonly used Elliptic Curve Cryptography constructions, such as the Elliptic Curve "Fixed"

Diffie Hellman (ECDH) key exchange and Elliptic Curve Qu-Vanstone (ECQV) implicit certificates. This scheme is incorporated at layer-2 of the protocol stack based on the IEEE 802.15.4 technology and aims to save as much airtime as possible by using the ECQV technique. Although it provides reliable key negotiation, lightweight node authentication, fast re-keying, and effective security against relay attacks all at the same time, but asymmetric encryption methods are used in this scheme, which are not suitable for use on resource constrained IoT devices. The process of this proposed scheme begin with Node A sends the first letter to Node B, which includes a nonce and an implicit certificate. Then, Node B will compute the shared secret by evaluating the remote device's public key, follow by sending the first message with its implicit certificate. Similarly, Node A will then compute the shared secret. After that, both nodes will create a Pre-Link Key by a Key Derivation Function and authentication process will occur. Figure 2.17 demonstrates the process in diagram form.

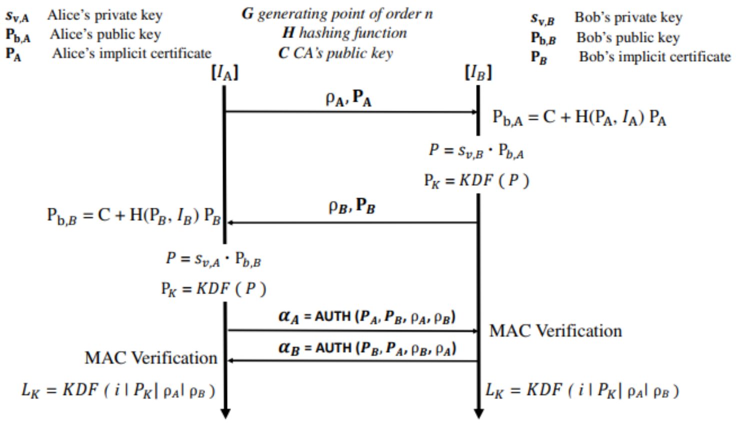


Figure 2.17. Key negotiation protocol. Adapted [reprinted] from "Key Management Protocol with Implicit Certificates for IoT systems" by Sciancalepore, S., Capossele, A., Piro, G., Boggia, G., and Bianchi, G., 2015, *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems - IoT-Sys '15.* Copyright 2015 by "ACM"

Kung et. al. [18] proposed a lightweight two-tier GKM architecture for dynamic IoT environment called GroupIT. In this architecture, upper and lower tiers are liable for key management between groups and within groups, respectively, where it is preventing unauthorised users from joining the groups. Moreover, devices and users are separated into groups, namely device group and user group. Each group executes its own GKM scheme to handle key updates when there are membership changes within the group and each device in the same group has its own device key based on shared TEK in the group, thus other devices are not able to retrieve data from one another without authorisation. The upper tier of GroupIT is needed to prevent unnecessary communication overhead during the updates of multiple user groups in KDC. In their proposed work, the GKM scheme has two levels chosen from existing GKM methods, so that collusion attack can be avoided. The GKM scheme adopts LKH and CRT in this work.

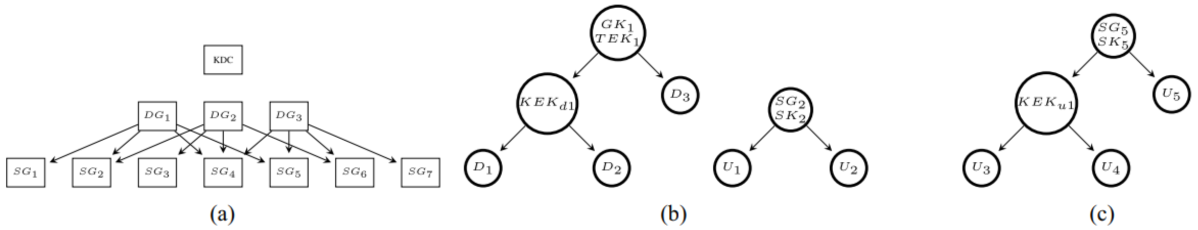


Figure 2.18. Initial structure overview

(a) Three device groups and seven user groups. Structure inside (b) DG_1, SG_2, and (c) SG_5. Adapted [reprinted] from “GROUPIT: Lightweight Group Key Management for Dynamic IoT Environments.” by Kung, Y. H and Hsiao, H. C., 2018, *IEEE Internet of Things Journal, 5(6).* Copyright 2018 by “IEEE”.

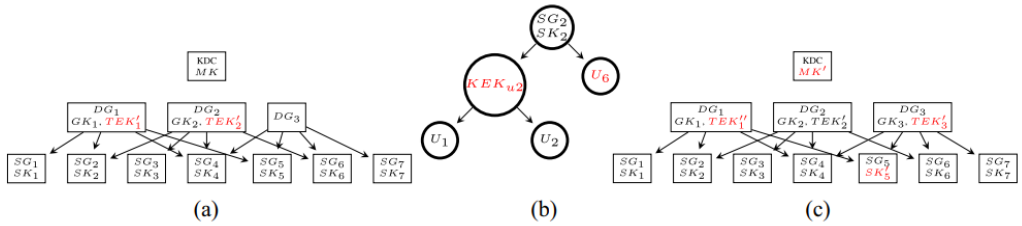


Figure 2.19. Example of structure update for user join/leave events

(a) Structure when U_6 joins. (b) Structure inside SG_2 when U_6 joins.

(c) Structure when U_4 leaves. (d) Structure inside SG_5 when U_4 leaves.

Adapted [reprinted] from “GROUPIT: Lightweight Group Key Management for Dynamic IoT Environments.” by Kung, Y. H and Hsiao, H. C., 2018, *IEEE Internet of Things Journal, 5(6).* Copyright 2018 by “IEEE”.

According to Dammak et. al. [8], current access control systems predominantly concentrate on centralised models, which fail to resolve the scalability challenge raised by the large scale of IoT devices and the increasing number of subscribers. Existing GKM schemes only use dependent symmetric group keys for subgroup communication, which is inefficient for subscribers with highly dynamic behaviour. Hence, Decentralised Lightweight Group Key Management architecture for Access Control (DLGKM-AC) is proposed to build an effective and adaptable process for securing content delivery to qualifying subscribers. In addition, a master token management protocol for key dissemination is also introduced. In this scheme, a hierarchical architecture made up of a Key Distribution Centre (KDC) and several Sub Key Distribution Centres (SKDC) is introduced to mitigate alleviate the single point of failure issue. The jobs for KDC and SKDCs are to manage device group and user group, respectively.

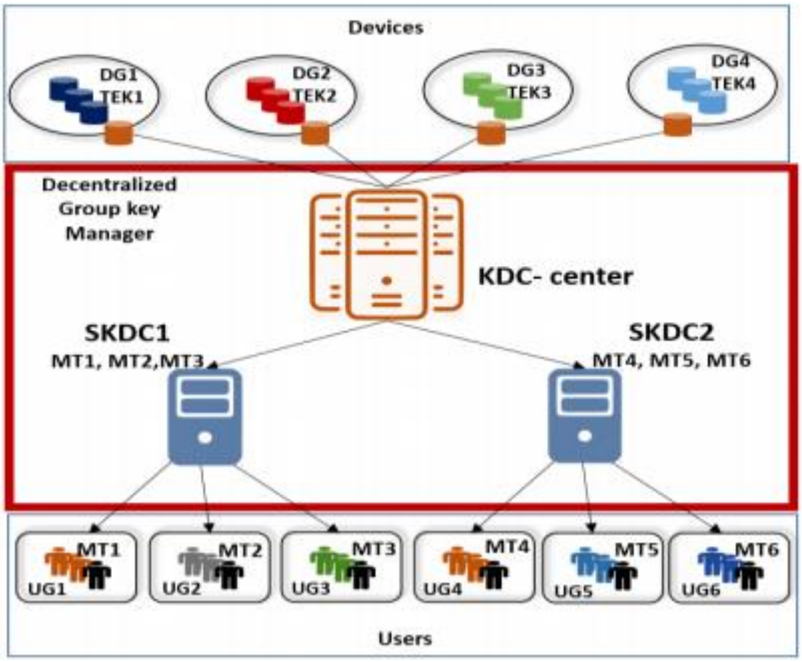


Figure 2.20. Proposed system model for DLGKM-AC. Adapted [reprinted] from "Decentralized Lightweight Group Key Management for Dynamic Access Control in IoT Environments" by Dammak, M., Senouci, S. M., Messous, M. A., Elhdhili, M. H. and Gransart, C., 2020, *IEEE Transactions on Network and Service Management, 17(3).* Copyright 2020 by "IEEE".

2.2 Zero Knowledge Protocol

According to Gaba et. al. [10], due to various resource-constrained nodes involved, securing IoT is difficult. The developer and administrator cannot apply elaborate security mechanisms because of the limited resources available on IoT nodes. Despite greatest attempts to build suitable security measures, the incidence of cyber-attacks on healthcare organisations has increased dramatically. The impacted people were stranded for more than 40 days after a cyber assault on the University of Vermont Health Network in 2020. Due to the failure of over 5000 computers, nearly 300 people were laid off for several days. According to experts, the cyber-attack resulted in a daily revenue loss of 1.5 million dollars and additional expenses. The proposed scheme contains 3 phases.

Phase 1: User and user device registration phase.

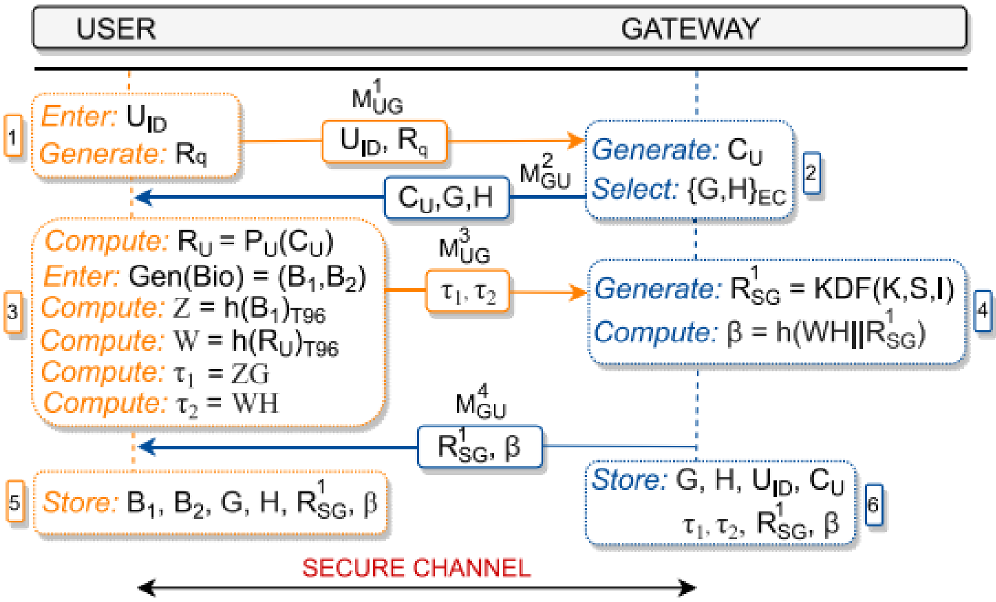


Figure 2.21. User and user device registration phase. Adapted [reprinted] from “Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare” by Gaba, G., S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M. and Alazab, M., 2022, *Sustainable Cities and Society, 20.* Copyright 2022 by “Elsevier Ltd.”.

Phase 2: IoT sensor node registration phase

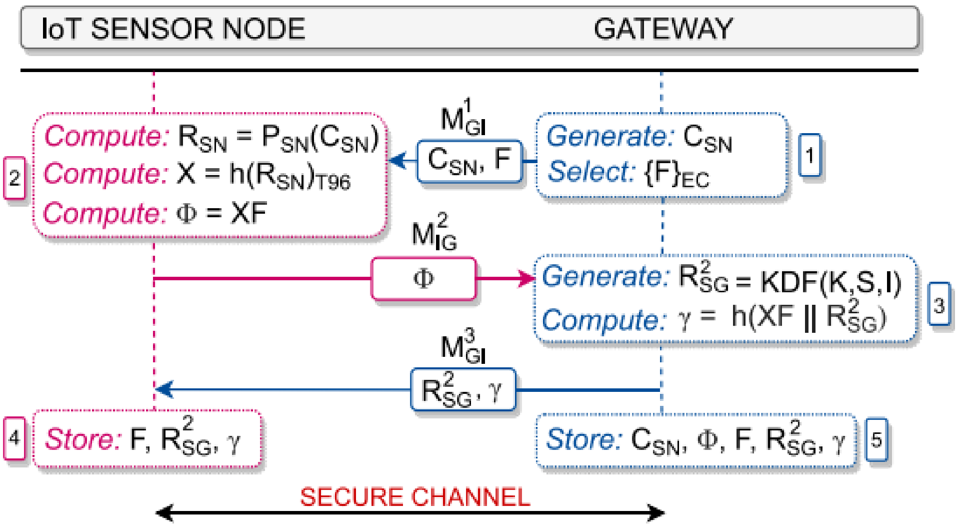


Figure 2.22. IoT sensor node registration phase. Adapted [reprinted] from “Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare” by Gaba, G., S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M. and Alazab, M., 2022, *Sustainable Cities and Society, 20.* Copyright 2022 by “Elsevier Ltd.”.

Phase 3: Mutual authentication and key agreement phase

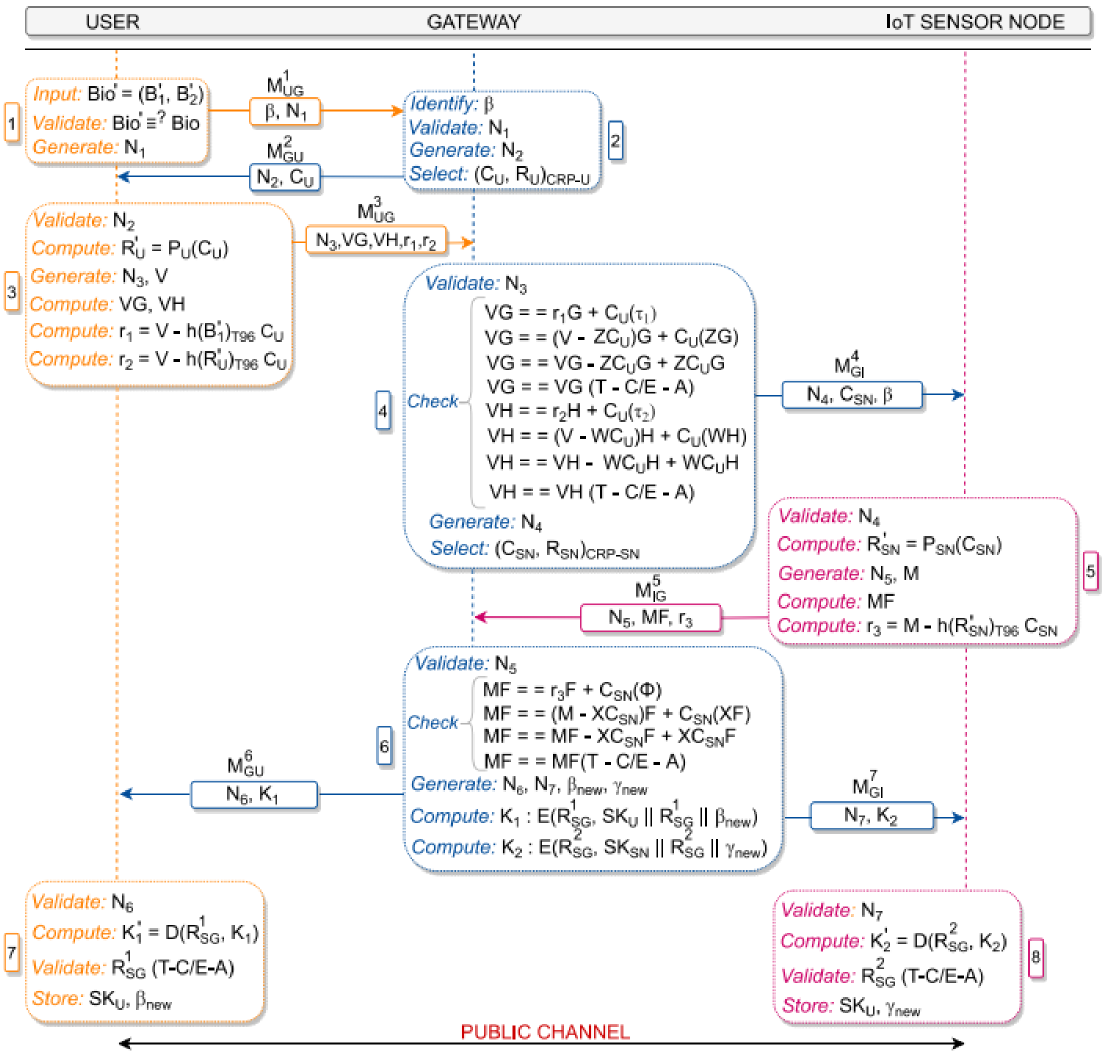


Figure 2.23. Mutual authentication and key agreement phase. Adapted [reprinted] from "Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare" by Gaba, G., S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M. and Alazab, M., 2022, *Sustainable Cities and Society, 20.* Copyright 2022 by "Elsevier Ltd.".

Chapter 3
System Model

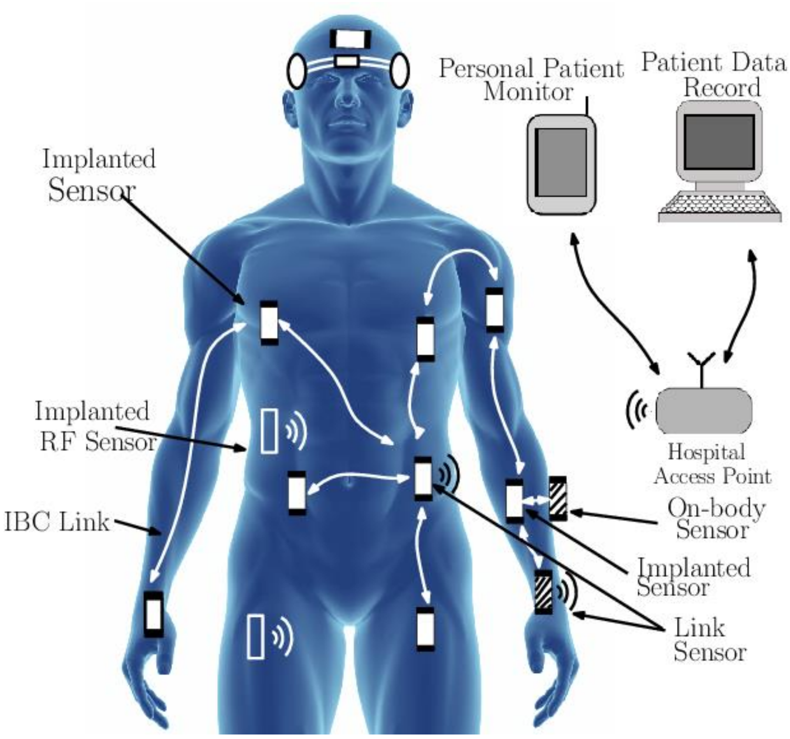


Figure 3.1. An example of communication in IoT wearable medical devices. Adapted [reprinted] from 'A Review of Implant Communication Technology in WBAN: Progresses and Challenges' by Teshome, A., Kibret, B. and Lai, D., 2018, *IEEE Reviews in Biomedical Engineering*. Copyright 2018 by "IEEE".

Figure 3.1 shows an example of IoMT where sensor nodes are implanted into patients' body for monitoring purposes. These sensor nodes are interconnected among each other to ensure the correctness of the function performed. For instance, glucose sensor and insulin pump work together to the deliverable of insulin is accurate to balance the glucose level of a patient. Thus, if the data that indicates the value of glucose is being tempered, the incorrect amount of insulin released would harm the patient. Moreover, the implanted sensors are as well transmit data to device outside the body such as smart bands or smartphones for visualised monitoring [27]. As these data are being transmitted, it is crucial that to maintain their confidential and minimise the risk from data leak. As a result, a leader node should be elected among all nodes to manage the group key generation and distribution for the authentication process.

3.1 Methodology

This project will be carried out by combination of analytical, theoretical, and experimental research. The overall project workflow is represented in Figure 3.2.

Analytical

An understanding of the literature on multicast group key management and determines the existing problems. It also consists of studies on security attacks that the applications may subjected to and the best model to avoid it.

Theoretical

Develop and design a novel group key management scheme to ensure the authenticity within the multicast group which fulfil the completeness and soundness of zero knowledge.

Experimental

Set up a simulation using simulation tool on multicast group. Analysis on security, complexity, and perform performance study of the proposed scheme.

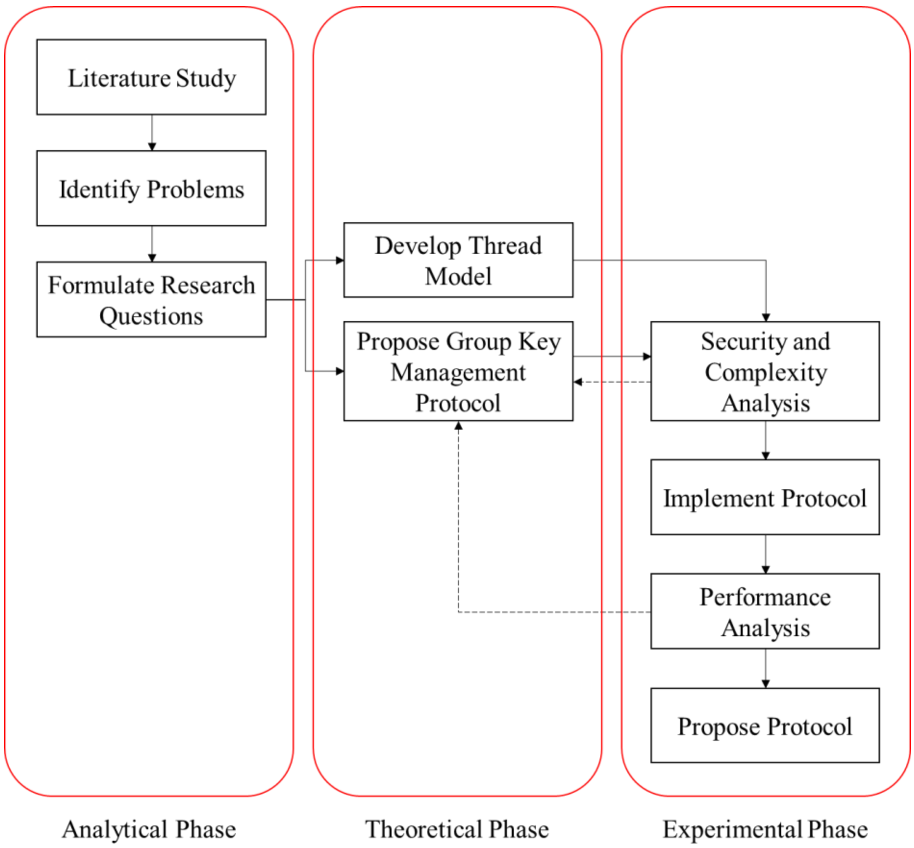


Figure 3.2. Project workflow.

The project begins with performing a literature study in the IoT multicast group management in understanding the behaviour within a group such as multicast routing and group key management. The process will continue with formulating the problem statements and research questions that this project is intended to solve.

Furthermore, a simulation of the multicast group membership management and routing will be developed. At the same time, the algorithm of proposed zero knowledge protocol will be drafted based on the problems defined.

The drafted protocol will then be validated until it satisfies the security and complexity criteria. After that, the evaluated protocol can be implemented into the simulation and perform a performance analysis using the output data from the simulation tools. If the analysis results do not meet the requirements, the protocol will be refined again until it achieves the objective of this project.

3.2 Simulation Tool

In this project, the performance study will be done using CupCarbon Iot 5.0 as the simulation tool. CupCarbon is a simulator for Smart Cities and the Internet of Things Wireless Sensor Network (SCI-WSN). Its goal is to create environmental scenarios such as fires, gas, mobiles, and more within educational and scientific initiatives by designing, visualising, debugging, and validating distributed algorithms for monitoring, environmental data gathering, and so on. It can not only assist scientists in graphically explaining the fundamental ideas of sensor networks and how they work, but it can also assist them in testing their wireless topologies, protocols, and so on.

Utilizing the OpenStreetMap (OSM) framework to place sensors directly on the map, networks may be planned and prototyped using an ergonomic and easy-to-use interface. It comes with a script called SenScript that lets you programme and customise each sensor node separately. It is also feasible to produce codes for hardware platforms such as Arduino/XBee with this script. CupCarbon does not yet fully implement this feature, but it does allow for the generation of codes for simple networks and algorithms. CupCarbon simulation is based on the nodes' application layer. Thus, it is a great complement to other simulators. Due to the complicated nature of urban networks, which must combine other sophisticated and resource-intensive information such as buildings, roads, mobility, signals, etc., it does not emulate all protocol levels.

CupCarbon's current version allows users to dynamically configure nodes in order to split nodes into separate networks or join other networks, a task that is based on network addresses and channel. As a function of the simulated time, the energy consumption could be estimated and displayed. This enables the structure, practicality, and realistic implementation of a network to be clarified prior to its actual deployment.

3.3 Implementation Issues and Challenges

CupCarbon programmes nodes using SenScript that is having different syntax as any other programming languages. There is no complete manual on SenScript tutorial, and it finds hard to understand and explore the usage of pre-defined functions. Moreover, although it allows user-defined function, but no clear procedure in the ways of calling the function. Thus, different tasks are not able to define in separate blocks which then causes logic error to be happened easily within the script. The algorithms in this project are programmed in separate individual scripts to minimise the possible error to occur.

3.4 Project Timeline

FYP 1

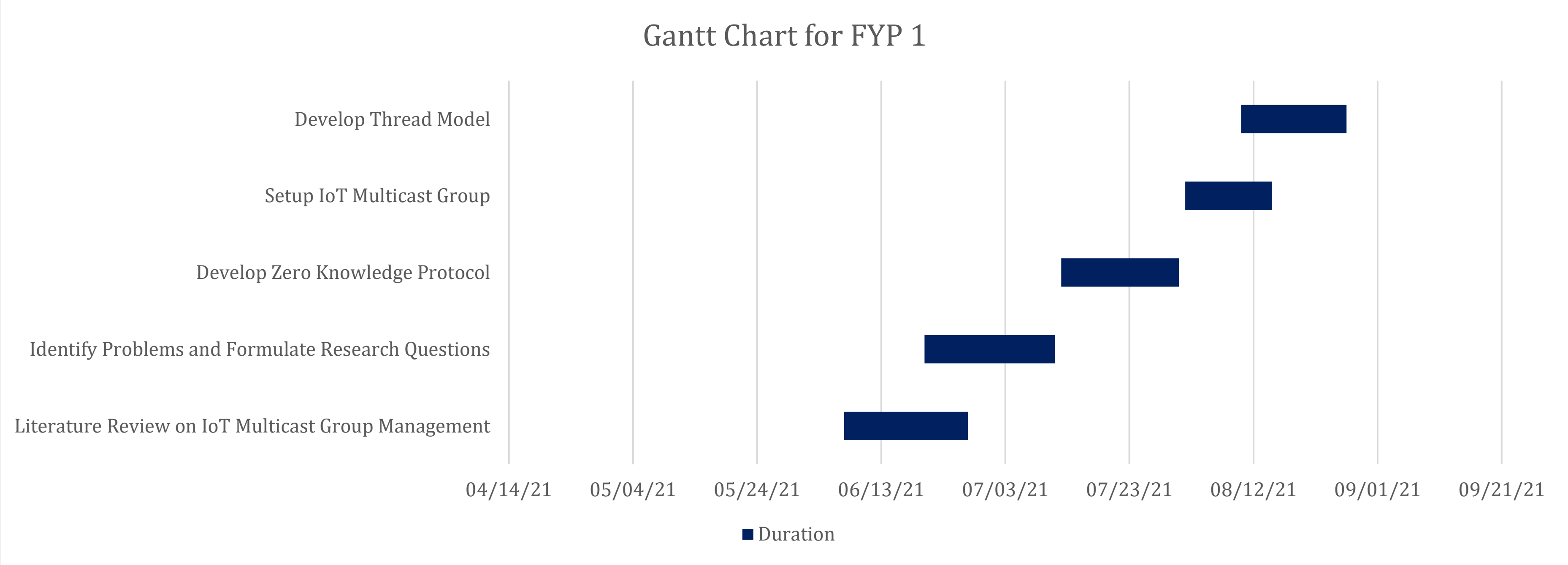


Figure 3.3. Gantt Chart for FYP1.

The project begins with a 20-day literature study on IoT Multicast Group Management to understand on how current group key management works. At the same time, the problem statement and research question will be formulated. After understanding the problems, 19 days are to be spent to develop a Zero Knowledge Protocol to enhance the current group key management. Approximately 27 days will be spent on setting up an IoT multicast group using simulation tool and develop a thread model to be studied.

FYP 2

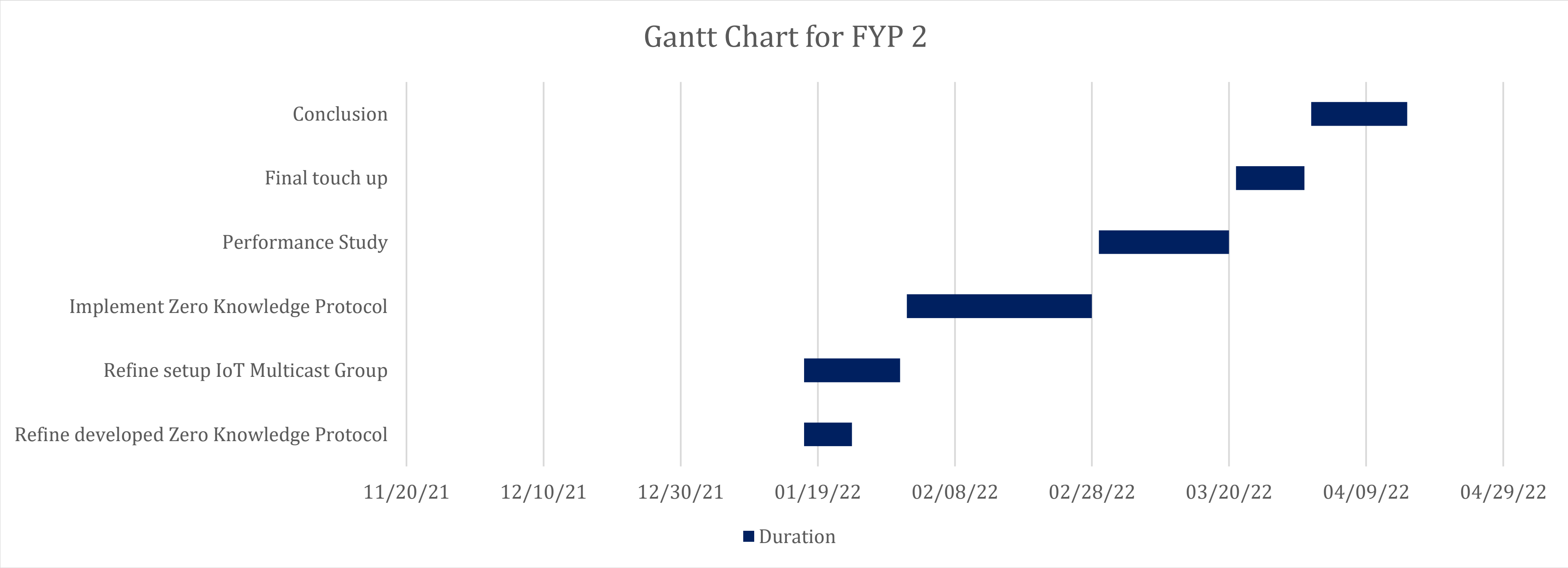


Figure 3.4. Gantt Chart for FYP2.

Before the project to be continued, the developed protocol and set up IoT multicast group are to be refined in 2 weeks. Then, apply the developed Zero Knowledge Protocol into the simulation. The performance of the protocol will be studied after completion of the simulation. To further validate the project, 10 days of final touch up will be done. Finally conclude the overall project.

Chapter 4

System Design

4.1 System Block Diagram

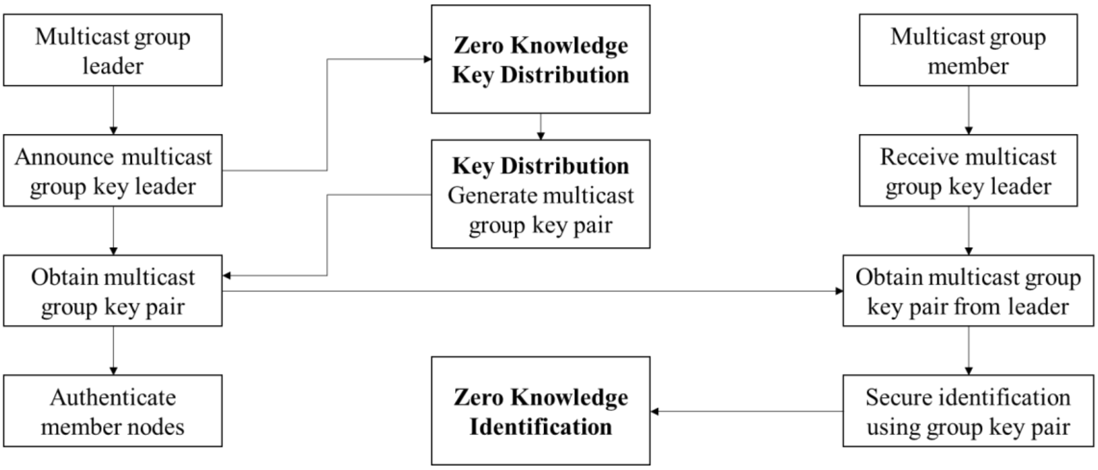


Figure 4.1. Flow of multicast network deployment.

The multicast nodes will select a multicast group leader and the rest will be the multicast group members. Once the multicast group leader is identified, the leader will announce to all the members within the multicast group, then generate group key pair and distribute through zero knowledge. After all members received the key, the members can start communicating with each other, while the leader are responsible in authenticating the member nodes using zero knowledge identification.

4.2 Pseudocode

The proposed system is combination of 3 algorithms / method: Leader Node Election, Group Key Distribution and Zero Knowledge Identification. Each algorithm is tested in the simulation as seamless as in the reality. The pseudocode and flowchart of the algorithms are included in this section, which show their process in a sequence and clear manner. Table 4.1 lists the functions of the algorithms, as well as the descriptions.

Table 4.1. Functions of the algorithms.

Function	**Description**
getID( )	returns the node identifier.
rand(*a*)	Initialise random number *a*.
pow(*a*, *b*)	*a* to the power of *b*.
root(*a*, *b*)	b^{th} root of *a*.
read( )	waiting for receipt of messages. If there is no received message, then the execution will continue and go to the next instruction.
receive( )	Wait until receiving data in the buffer. This is a blocking function, if there is not data in the buffer then it remains blocked on this instruction.
send(*a*, *)	Sends broadcast message *a* to neighbour sensors.
send(*a*, *, *b*)	Sends broadcast message *a* to neighbour sensors except node having identifier *b*.

4.2.1 Leader Node Election

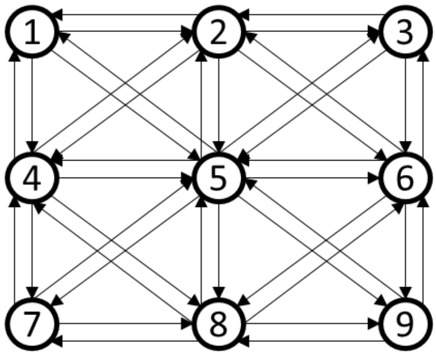


Figure 4.2. Leader Node Election Illustration.

```
Input: id
Output: leader
id = getID()
leader = true
rp = read()
if(rp == null) then
        send(id+"#"+id, *)
else
        rid = rp.rid
        v = rp.v
        if(id>rid) then
                leader = true
        else
                leader = false
        end if
        send(rid+"#"+id, *, v)
end if
```

Figure 4.3. Leader Node Election Algorithm.

First and foremost, all nodes within a multicast group should perform an election to identify a leader node to manage the key distribution. Other nodes which were not elected will be the member nodes. Leader node election algorithm proposed by Kadjouh et. al. [16, 17] adopts node identifier as comparison to elect a leader node. The selection of node identifier is due to its uniqueness among all nodes as each node has distinct identifier.

Refer to Figure 4.2 and Figure 4.3, all nodes will get its node identifier and set itself as a leader in the beginning. Then, the nodes will start receiving message from their neighbour nodes. If no message is received, the node will initiate its identifier to its neighbour nodes. Otherwise, the nodes get the data in the message (received identifier). If the node's identifier is greater than the received identifier, the node will remain as a leader, else resign as a leader. Finally, it routes the received identifier to its neighbour nodes without sending back from where it received the message. Figure 4.4 and Figure 4.5 shows the flowchart and the source code of the algorithm, respectively.

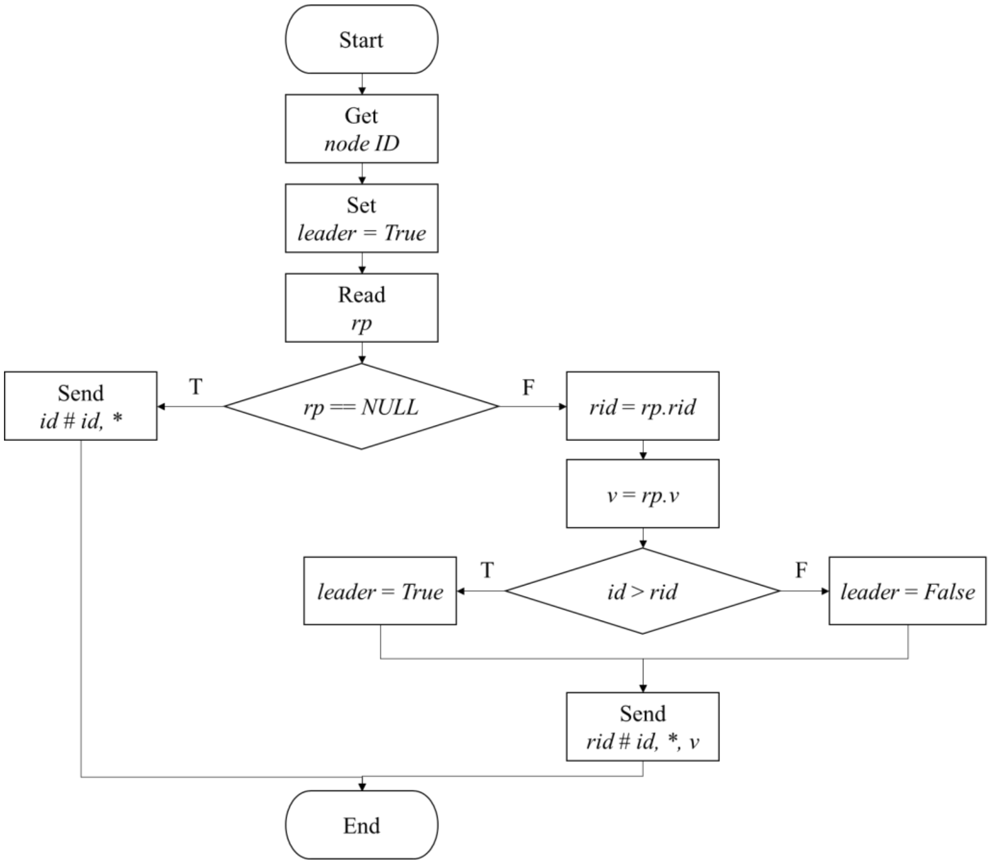


Figure 4.4. Flowchart for Leader Node Election Algorithm.

```
atget id id
set leader 1

loop
read rp
if(rp=="")
        data p id id
        send p
else
        rdata rp rid v
        print rid
        if(id>rid)
                if(leader==0)
                        mark 0
                else
                        mark 1
                end
        else
                set leader 0
                mark 0
        end
        data fwd rid id
        send fwd * v
end
delay 1000
```

Figure 4.5. Source code of Leader Node Election Algorithm in SenScript.

4.2.2 Group Key Distribution without Zero Knowledge Protocol

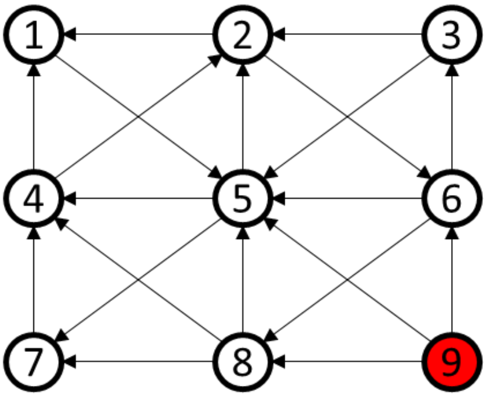


Figure 4.6. Group Key Distribution Illustration.

```
Input: x
Output: key
id = getID()
key = NULL
if(leader == true) then
      rand(x)
      send(x+"#"+id, *)
else
      rp = receive()
      rid = rp.rid
      y = rp.y
      send(y+"#"+id, *, rid)
      key = y
end if
```

Figure 4.7. Group Key Distribution Algorithm.

The elected leader node would bear the responsibility to manage the group key and the distribution of the keys. Figure 4.6 and Figure 4.7 defines the algorithm for the key distribution. Initially, all nodes will get its node identifier and set the key into null, which represent that there is no key at first. Then, if the node is the leader, it will generate a random number as the group key and distribute to it neighbour nodes. The member nodes will receive the message and read the data. The key received will be stored into the key variable and also send to the following nodes. At the end, all nodes should be able to receive the same group key. Figure 4.8 and Figure 4.9 shows the flowchart and the source code of the algorithm, respectively.

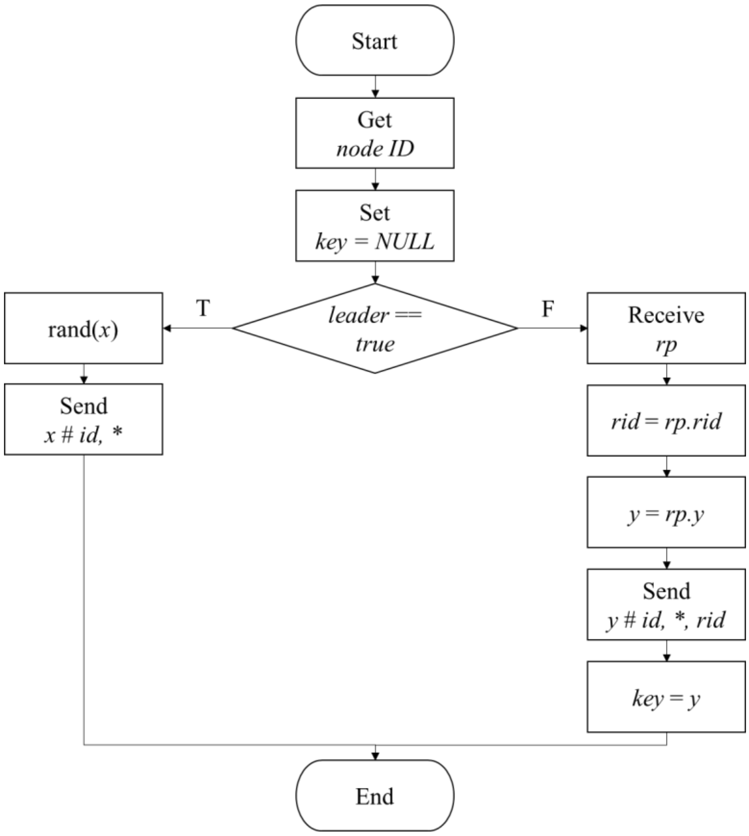


Figure 4.8. Flowchart for Group Key Distribution Algorithm.

```
atget id id
set key ''

loop
if(id==32)
        rand x
        data p x id
        print x
        send p
        stop
else
        receive rp
        rdata rp y rid
        data q y id
        send q * rid
        set key y
        print y
        stop
delay 1000
```

Figure 4.9. Source code of Group Key Distribution Algorithm in SenScript.

4.2.3 Group Key Distribution with Zero Knowledge Protocol

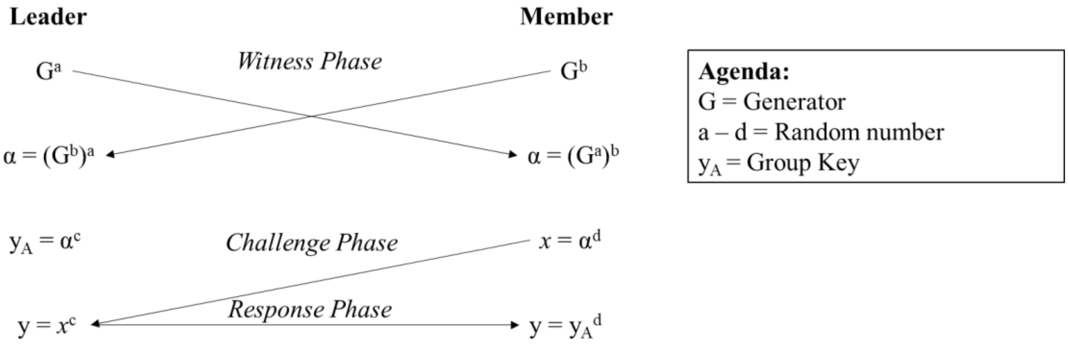


Figure 4.10. Zero Knowledge Protocol Illustration.

```
Input: g, a, b, c, d
Output: ya
g = 6
if(leader == true) then
    rand(a)
    ga = pow(g, a)
    send(ga, *)
    r1 = receive()
    rgen_b = r1.rgen_b
    ka = pow(rgen_b, a)
    rand(c)
    ya = pow(ka, c)
    r2 = receive()
    rx = r2.rx
    y = pow(rx, c)
    send(y, *)
else
    rand(b)
    gb = pow(g, b)
    r1 = receive()
    rgen_a = r1.rgen_a
    send(gb, *)
    kb = pow(rgen_a, b)
    rand(d)
    x = pow(kb, d)
    send(x, *)
    r2 = receive()
    ry = r2.ry
    ya = root(ry, d)
```

Figure 4.11. Group Key Distribution using Zero Knowledge Protocol.

In the proposed system, the leader node is responsible in distributing the group key to all member nodes without revealing the actual key. As refer to Figure 4.10 and Figure 4.11, expect each node will receive the same *g* value after registering to a group. Leader and members will generate a value using generator and a random number, *a* and *b*, then send to each other. The value is then used to compute α, which will be the same result in both sides. After that, the leader node will generate the group key (y_A) using α and a random number, *c*, meanwhile member nodes will generate a “question” to challenge the leader node. The question is generate using α and a random number, *d*. Leader then sends back the “answer” that is generate using the received "question" and *c*. Eventually, the member nodes receive the group key from the provided "answer". Figure 4.12 shows the flowchart for the proposed system.

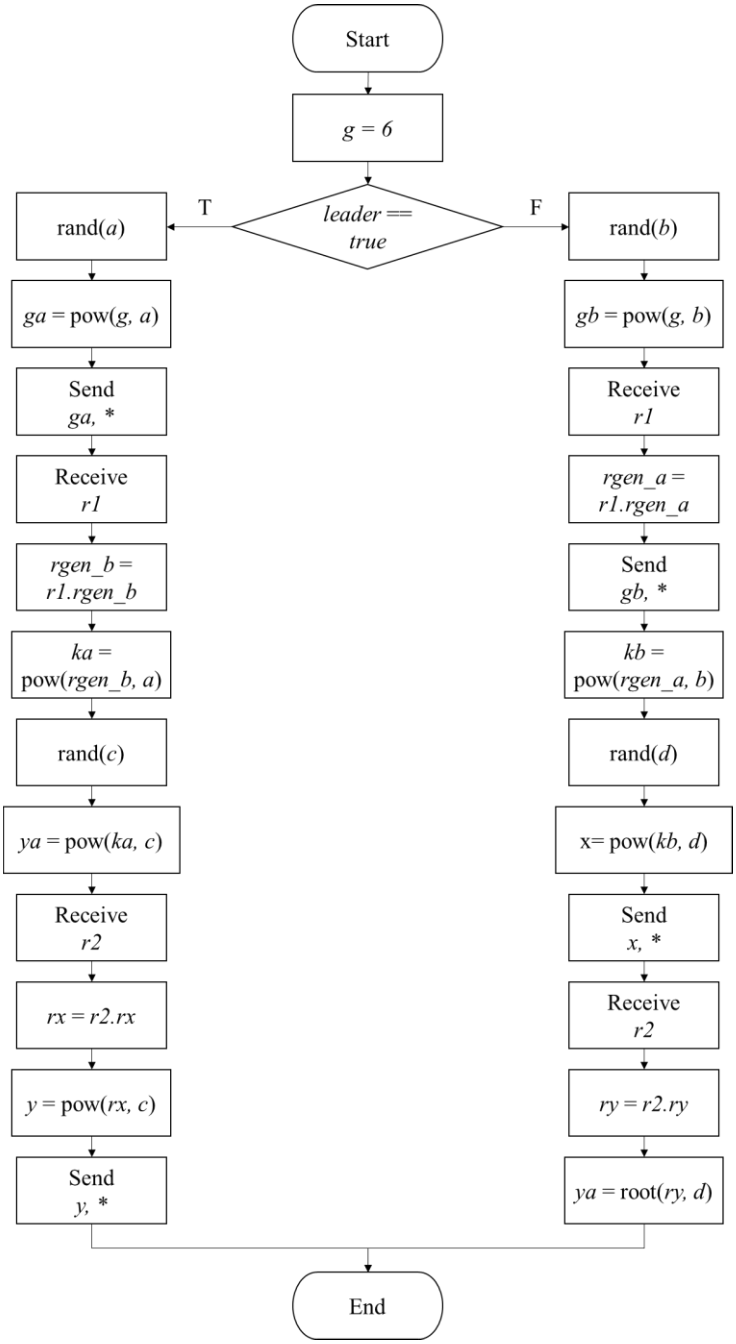


Figure 4.12. Flowchart for Group Key Distribution using Zero Knowledge Protocol.

Chapter 5

Experiment/Simulation

5.1 Simulation Setup

This section will introduce the steps to setup the simulation tool that is used in this project.

1. Download the CupCarbon U-One from http://www.cupcarbon.com/download.html

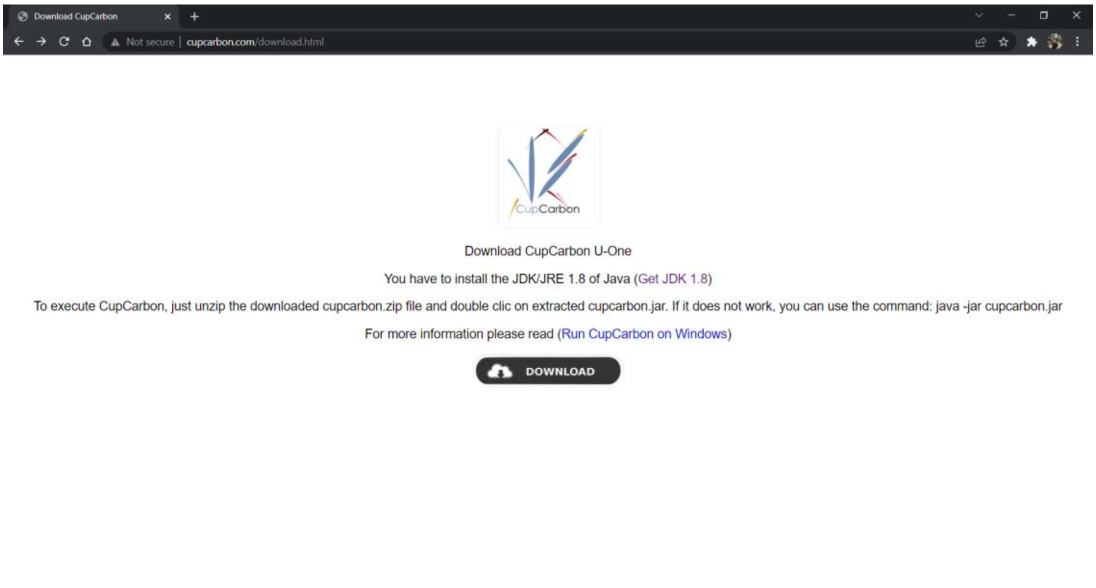


Figure 5.1. CupCarbon download page.

2. Download and install the JDK/JRE 1.8 of Java from https://www.oracle.com/fr/java/technologies/javase/javase8-archive-downloads.html

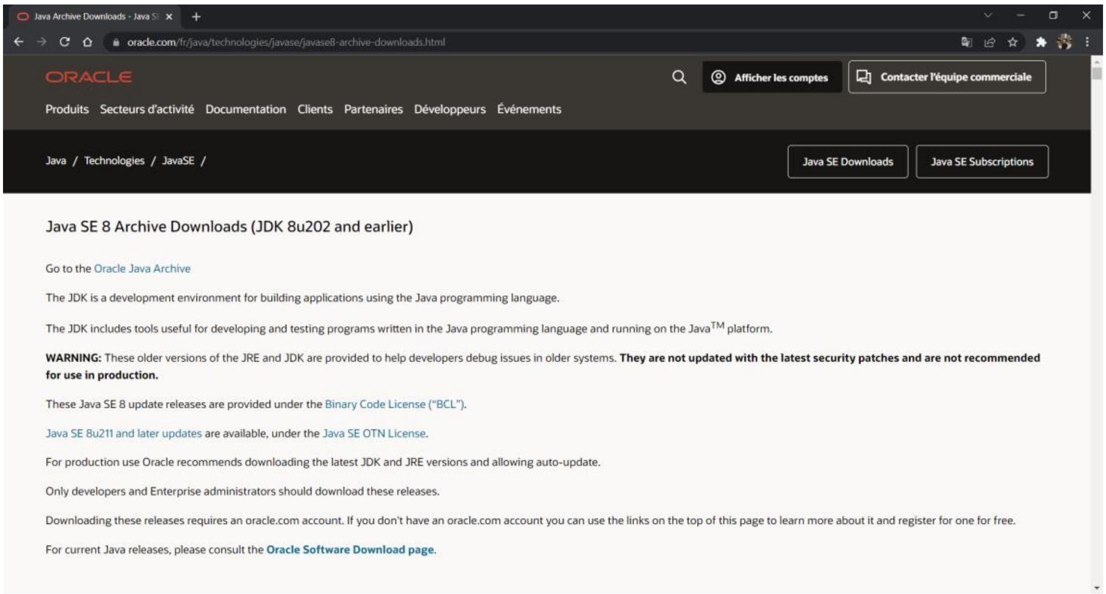


Figure 5.2. JDK/JRE 1.8 download page.

3. Unzip the CupCarbon zip folder.

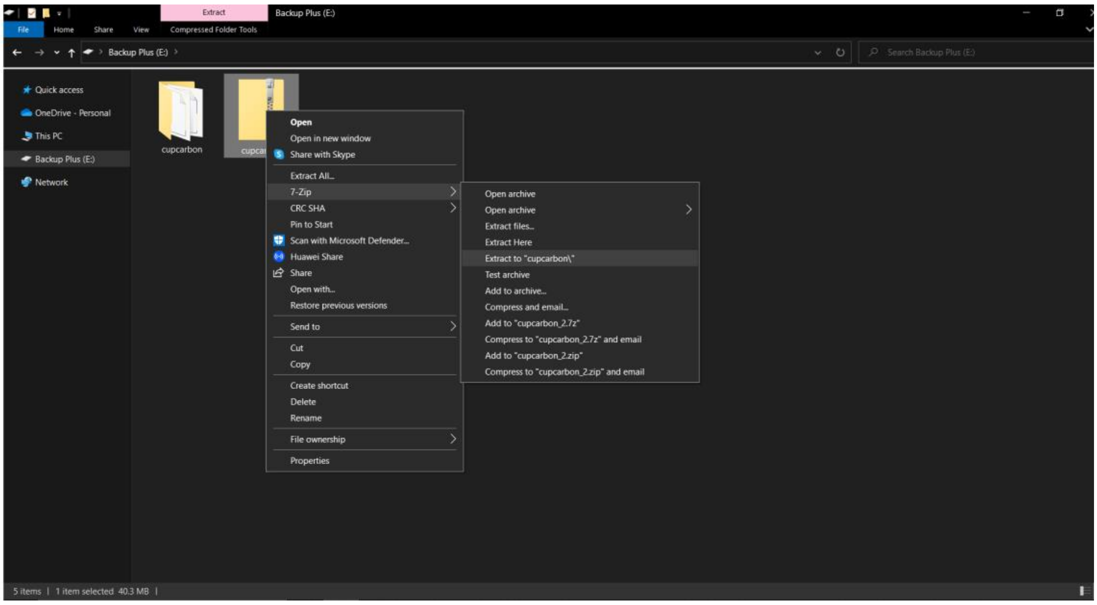


Figure 5.3. Unzip the CupCarbon zip folder.

4. Open command prompt and change to the cupcarbon directory.

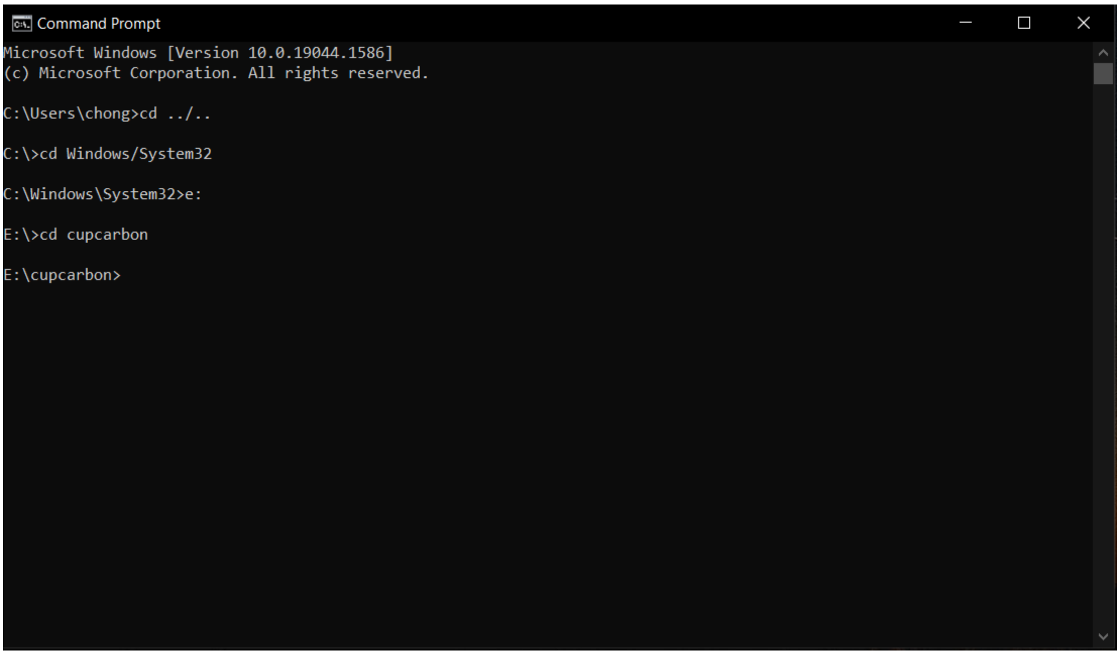


Figure 5.4. Change directory in command prompt.

5. Use the following command to execute the program.

   java -jar cupcarbon.jar

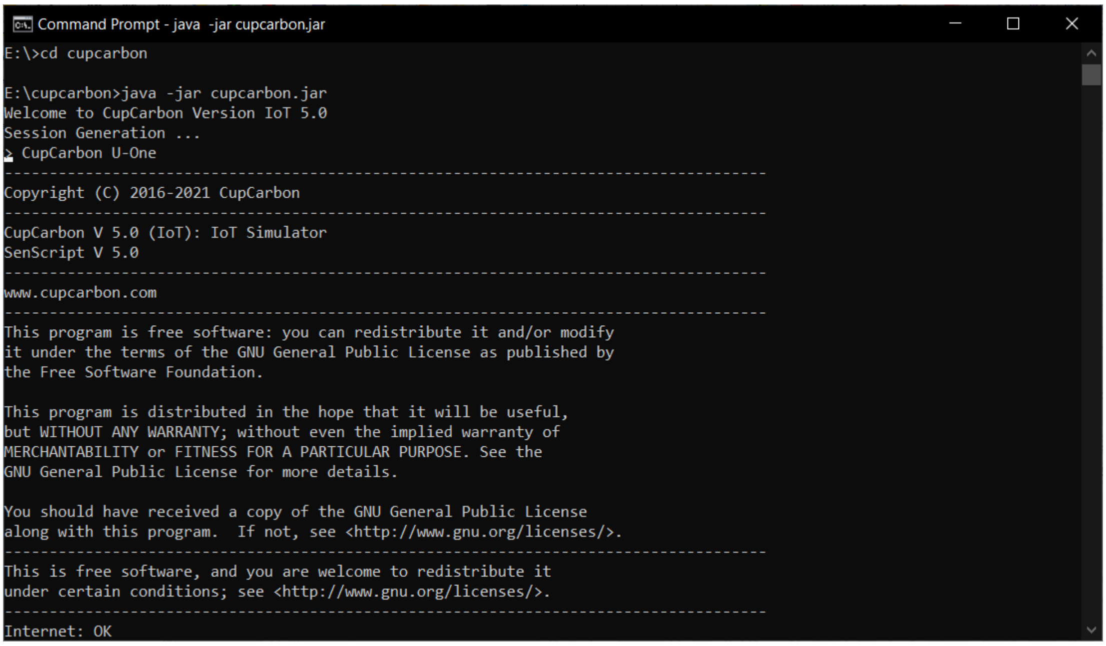


Figure 5.5. Execute CupCarbon.

6. The simulation tool is ready to use.

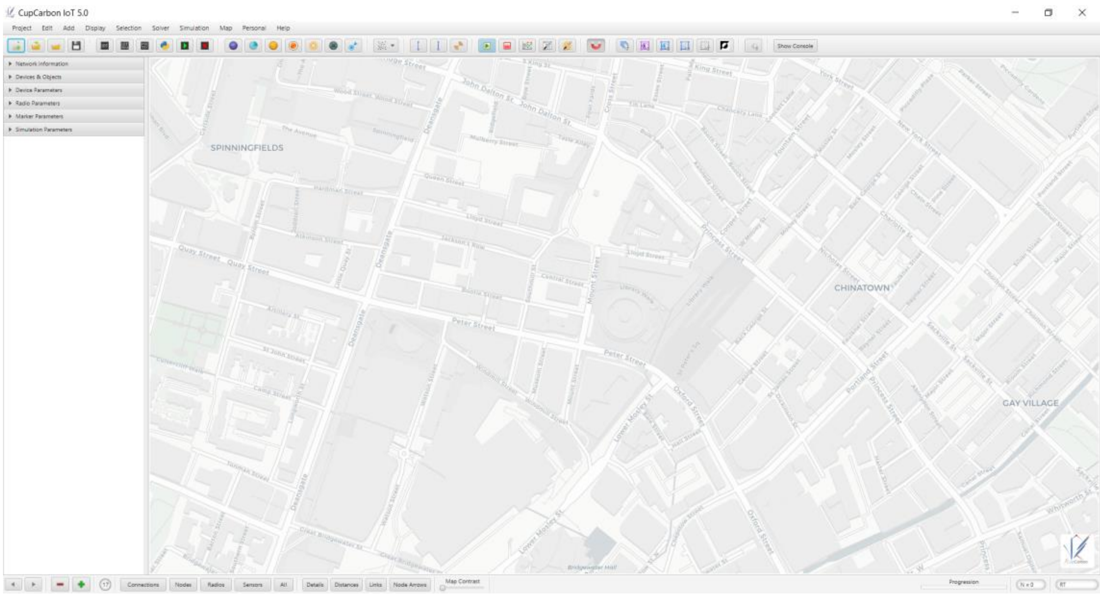


Figure 5.6. CupCarbon simulation tool.

Chapter 6

System Evaluation and Discussion

6.1 System Testing and Performance Metrics

6.1.1 Performance Study of Leader Node Election

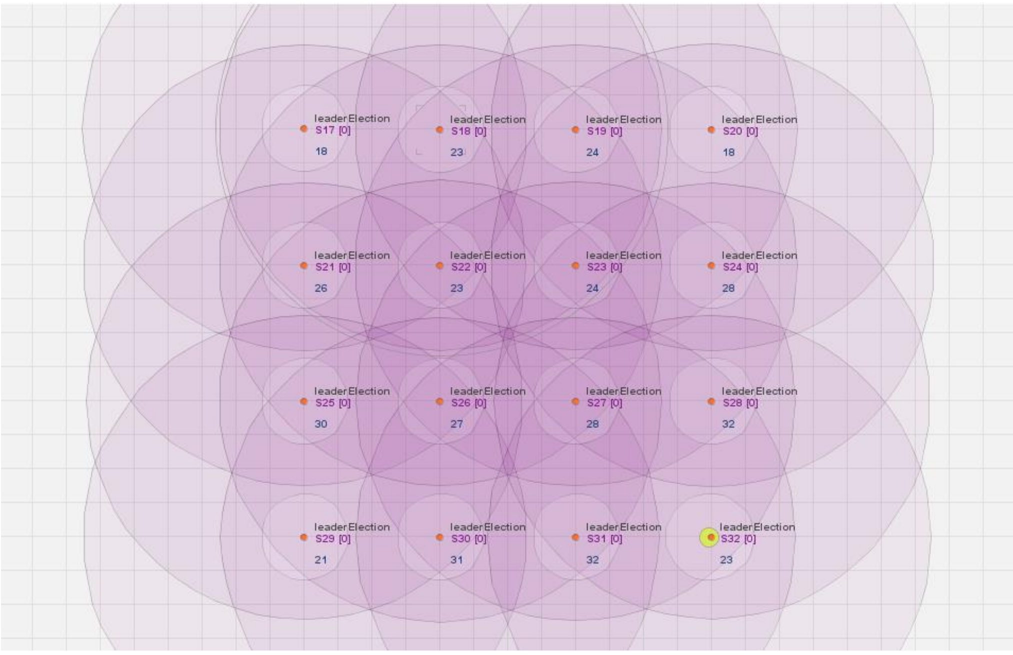


Figure 6.1. IoT simulation model in sequence.

Figure 6.2. Performance of Leader Node Election in sequential order nodes.

When the nodes are arranged in sequence according to their identifier, the leader node election requires 6.0267 seconds to elect a leader node. In the meantime, 520 messages are being transmitted.

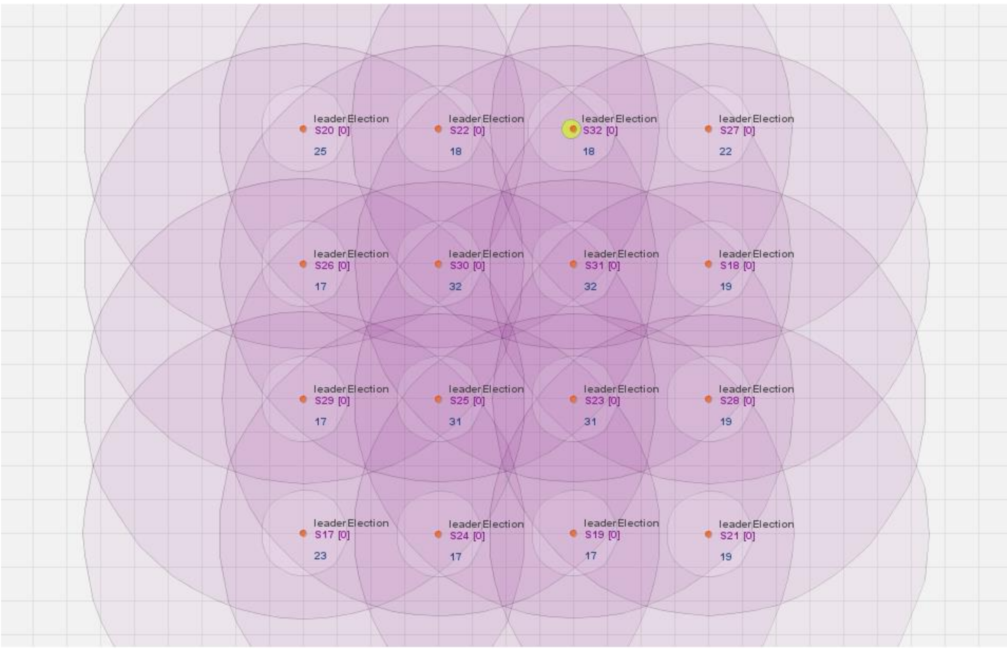


Figure 6.3. IoT simulation model in random.

Figure 6.4. Performance of Leader Node Election in random order nodes.

On the other hand, when the nodes are arranged in random according to their identifier, the leader node election requires 9.0267 seconds to elect a leader node. In the meantime, 772 messages are being transmitted.

Table 6.1. Comparison on the leader node election performance in different nodes ordering.

Order	Sequential	Random
Time spent (s)	6.0267	9.0267
Sent messages	96	144
Received messages	424	628
Total sent and received messages	520	772

From the results, the leader node election demands for longer time in random ordered model as compared to the sequential ordered model. This is due to the time taken for each node to receive to identifier greater than itself. When nodes are arranged randomly, there will be chances that node with greater identifier are in few hops away from the one with smaller identifier. Thus, nodes with smaller identifier that have yet to receive message from those greater than itself would assume to be the leader. Furthermore, the election will be conducted concurrently that may cause one node to receive multiple messages at once, therefore race condition might occur which obstruct the message passing and further delay the time spent.

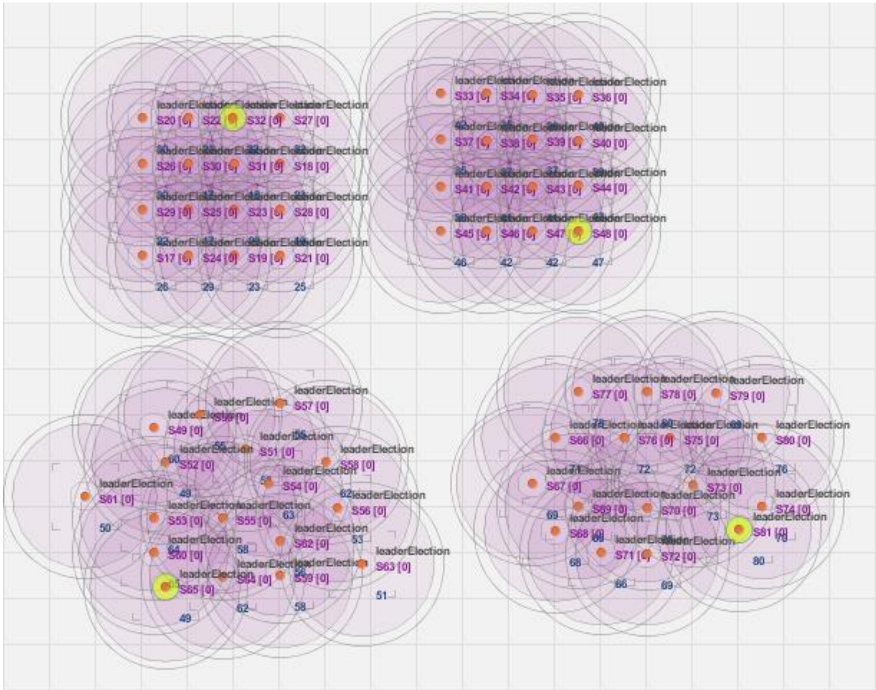


Figure 6.5. Leader node election in four different multicast group.

Figure 6.5 proved that the leader node election algorithm is capable in different type of architecture. Full and partial mesh topologies are tested in sequential and random nodes ordering. Yellow light marks the leader node.

6.1.2 Performance Study of Group Key Distribution Algorithm without Zero Knowledge Protocol

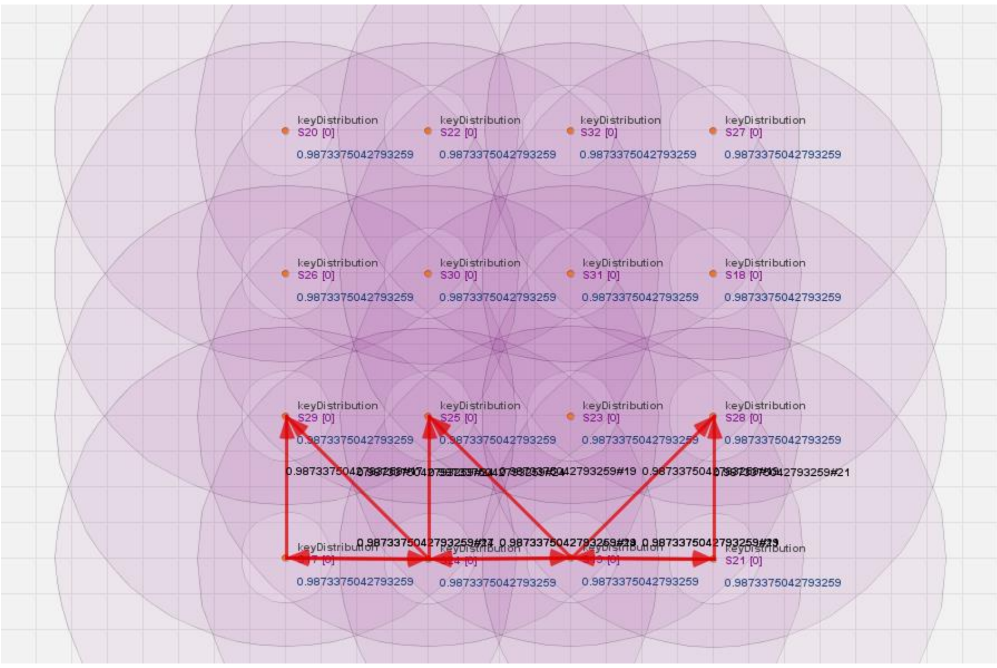


Figure 6.6. Group Key Distribution.

Mobility: false
Generate Restul File: false
Initialization ...
End of Initialization.
Start Simulation ...
Infinite Times!

End of Simulation.
2.379 sec
Time: 0.1264 s
Number of SENT messages: 16.0 [336.0]
Number of RECEIVED messages: 69.0 [1449.0]
Number of SENT & RECEIVED messages: 85.0 [1785.0]
Number of ACK messages: 0.0 [0.0]
Number of LOST messages: 0.0 [0.0]
Number of Marked Sensors: 0

Figure 6.7. Performance of Group Key Distribution.

Assuming node 32 is the leader node in this simulation, it will initiate the group key by generating a random number. The group key will then route and stored in each member node. The Group Key Distribution only requires 0.1264 seconds within a 16 nodes model. If any unknown node joins the multicast group, the node will also receive the key easily. Thus, an effective security protocol is essential to mitigate the issue. The proposed protocol is suggested to avoid such issue occur.

6.1.3 Performance Study of Group Key Distribution Algorithm with Zero Knowledge Protocol

All random numbers in the simulation are hardcoded into constant number for better testing on the accuracy. The values are as below:

g = 6,

a = 3,

b = 2,

c = 3,

d = 2.

Figure 6.8 shows the expected value for each phase.

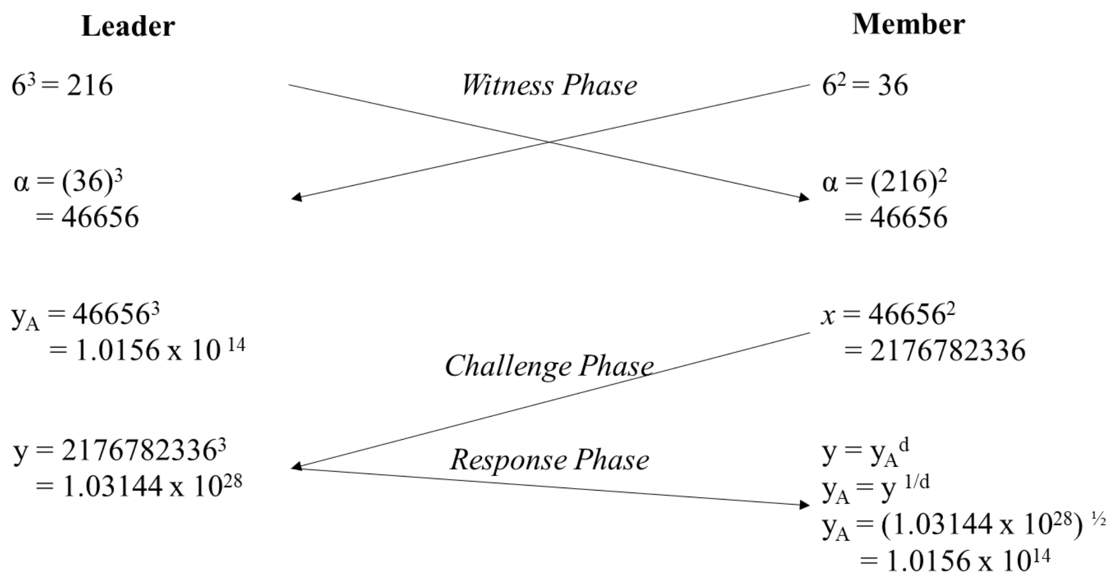


Figure 6.8. Expected output for the proposed protocol.

From Figure 6.8, it is clearly shown that the leader does not transmit the actual group key for communication, but the member is convinced that the node is the leader, which fulfilled the **zero-knowledge** property of zero knowledge protocol. At the end of the algorithm, member nodes would determine the group key, meaning that they are truly belong to the network group, that achieve the **completeness** property. If there is an unknown source pretends to be the leader and trying to take control of the group, it may not have the *g* value that is identical to that group, thus, the challenge would not be successful and inconvincible. As a result, the member will not consider that node to be true, and this concludes the **soundness** property. In contrast, if any of the member nodes do not belong to the group, the *g* value is not corresponded to the group's *g* value, hence, they have no authorisation to send or receive data within the group. Figure 6.9 to Figure 6.13 demonstrate the flow in simulation form.

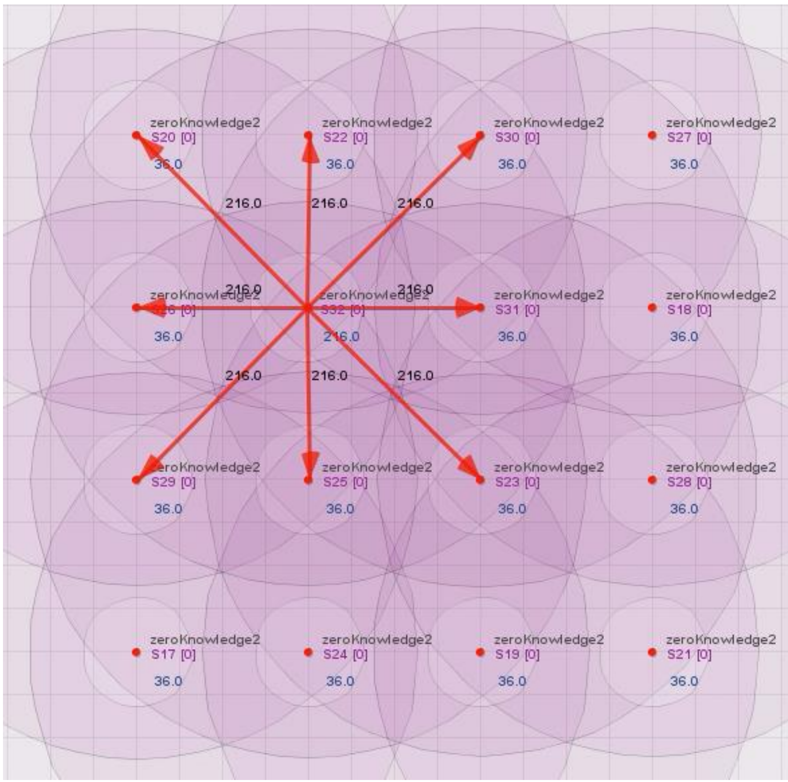


Figure 6.9. Witness Phase 1 (Leader node to Member nodes).

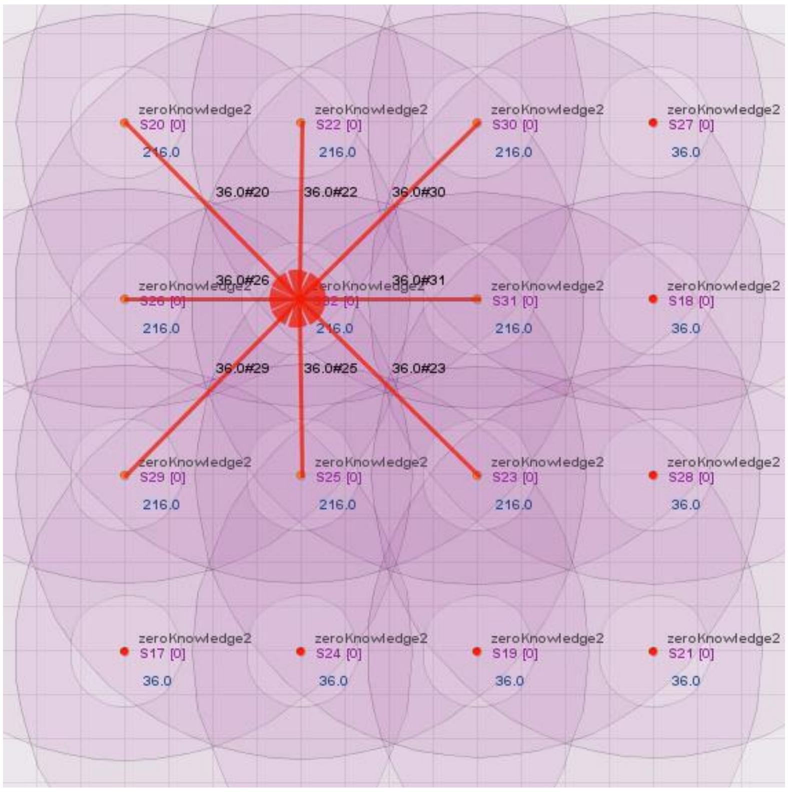


Figure 6.10. Witness Phase 2 (Member nodes to Leader node).

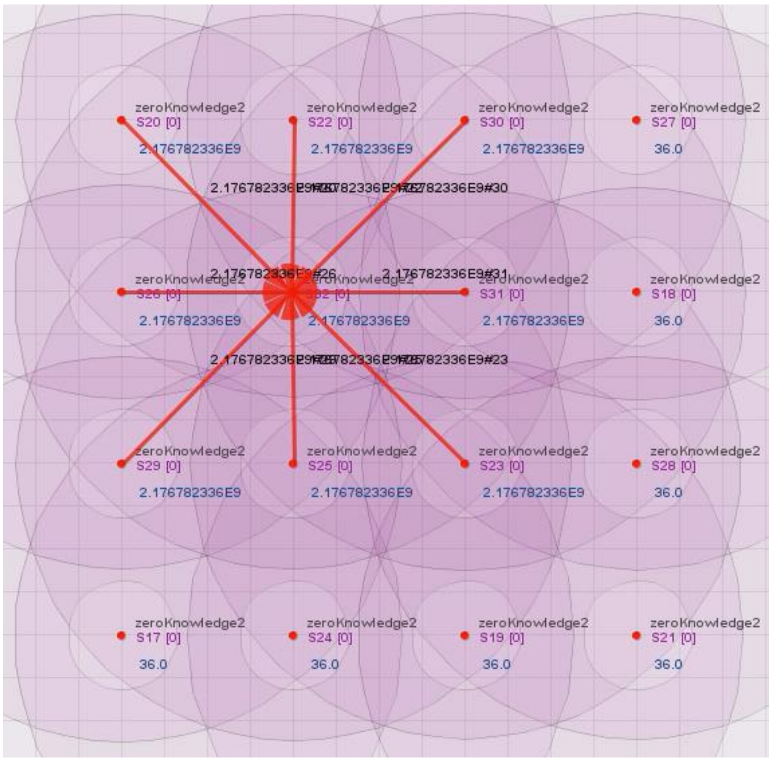


Figure 6.11. Challenge Phase.

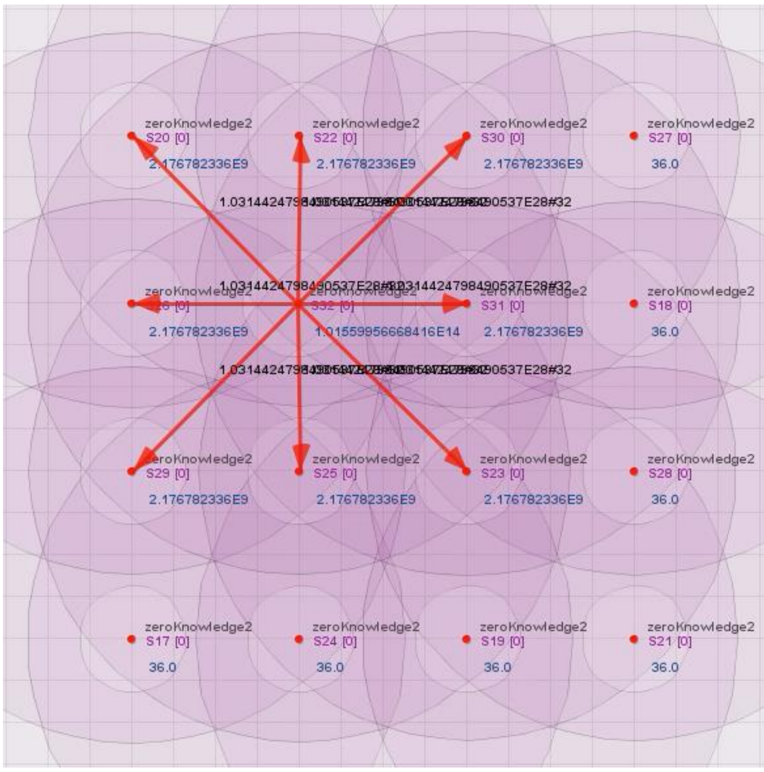


Figure 6.12. Response Phase.

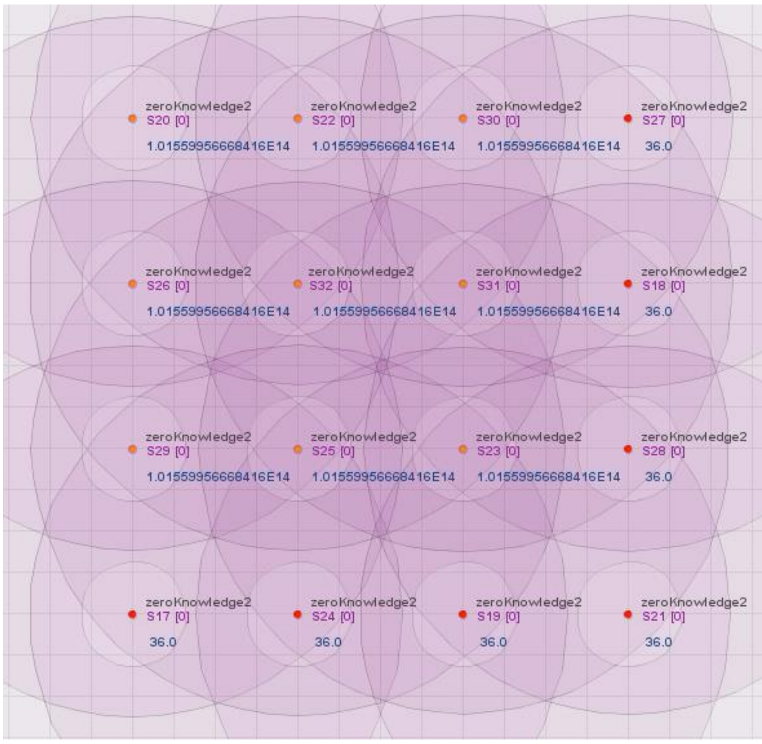


Figure 6.13. Key determined by the member nodes without receiving the actual key.

In essence, the leader node sent g^a (216) to the member nodes (Figure 6.9) and then the member nodes sent g^b (36) to the leader node (Figure 6.10). After that, all nodes computed α, and y_A in leader node and x in member nodes. Later, the member nodes sent x to the leader node (Figure 6.11). After the computation of y, the leader node sent y to the member nodes (Figure 6.12). Finally, the member nodes compute y_A value and are authenticated.

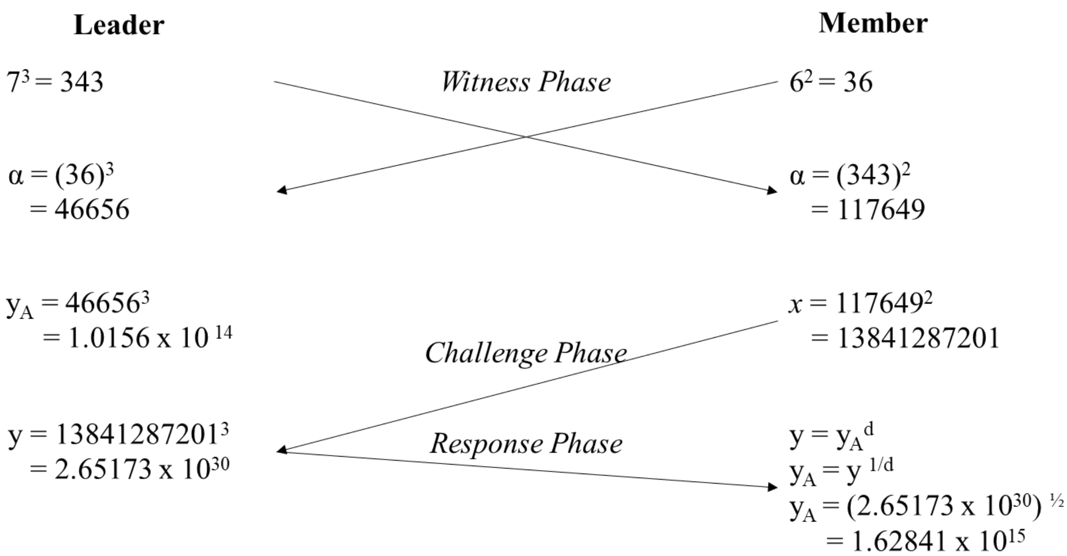


Figure 6.14. The expected output when the leader node does not belong to the group.

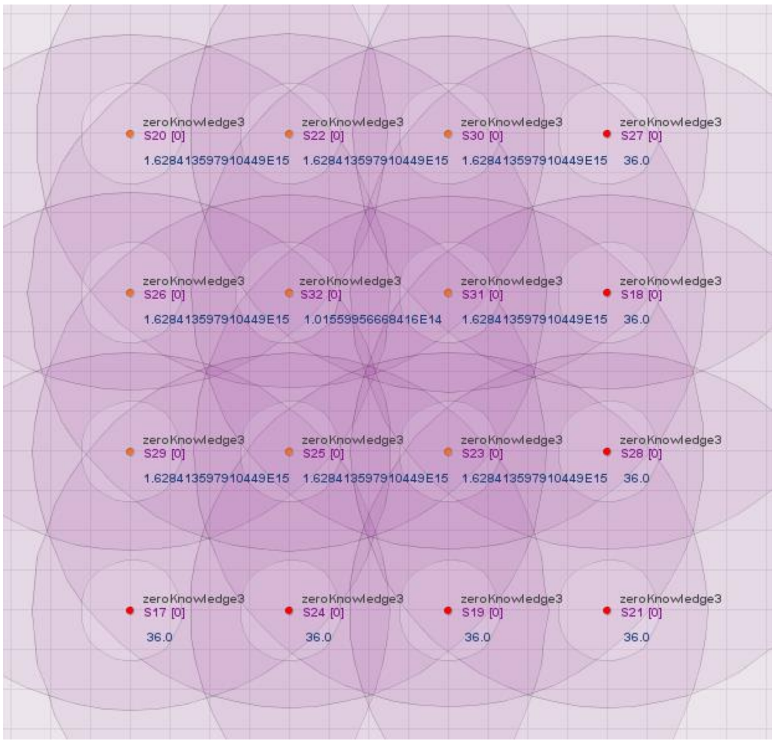


Figure 6.15. The result when the leader node does not belong to the group.

To prove that the group is not authenticated, the g in the leader node is set to 7, while the member nodes remain 6. It is obviously that the y_A value computed in the leader node and the y_A value determined in the member nodes are not similar. As a result, the key of the nodes within the multicast group is not identical, thus the communication with the unknown node is invalid.

Chapter 7
Conclusion and Recommendation

7.1 Conclusion

Internet of Medical Things (IoMT) benefits the healthcare sector that provides real-time remote monitoring and telemedicine services. As the non-severe medical cases can be monitored remotely, shortage of professionals could be solved and give more attention to those serious cases. However, the process involves transmitting sensitive information of the patients that might be sniffed by unauthorised personnel. Even worse, the attacker might modify the information that would lead to life threatening crisis. To prevent these consequences, group key management and authentication mechanism is needed in an Internet of Things (IoT) environment to make sure all joined nodes are authenticated. But there are still loopholes whereby attackers mimic to be a legitimate user and enter the multicast group. Thus, zero knowledge protocol is proposed to be implemented as another layer of security on the current group key management and authentication mechanism.

In this project, a node is selected as a leader that will be in-charge of the group key distribution which pass down the group key to all other nodes (member nodes). This process is done with the integration of zero knowledge protocol. A success zero knowledge protocol must fulfil 3 properties: completeness, soundness, and zero-knowledge. The proposed protocol in this project meets all the properties and enables the group key distribution to be achieved without revealing the actual key. The theory is proven using CupCarbon IoT 5.0 as a simulation tool. On the other hand, it is also proven that the communication with an unknown node in the multicast group is invalid.

7.2 Recommendation

The project successfully proven that the zero knowledge protocol provides another layer of security where the actual key is not being transmit. However, there are still rooms to improve for better convincement on the effectiveness of the group key management using zero knowledge protocol. In this project, only adjacent nodes of the leader node are transmitting data due to the lack of feature in the simulation tool. The group key distribution should involve all nodes within the multicast group, thus proper routing algorithm must be configured. Moreover, it is an adding advantage if the nodes are proven communicating using the group key determined to have better persuasion. Furthermore, thread model could improve by adapting the real behaviour of an actual attacker, so that the protocol can be proven secure not only theoretically, but also practically. All in all, the outcome of the proposed protocol is sufficient to verify its effectuality.

REFERENCES

[1] Abdmeziem, M. R., Tandjaoui, D., and Romdhani, I., "A Decentralized Batch-Based Group Key Management Protocol for Mobile Internet of Things (DBGK)," *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015. doi: 10.1109/cit/iucc/dasc/picom.2015.166

[2] Al-Odat, Z. A., Srinivasan, S. K., Al-Qtiemat, E. M. and Shuja, S., "A reliable IoT-based embedded health care system for diabetic patients," 2019. Available: https://doi.org/10.48550/arXiv.1908.06086

[3] Avinashiappan, A. and Mayilsamy, B., "Internet of Medical Things: Security Threats, Security Challenges, and Potential Solutions," in *Internet of Medical Things*, Hemanth, D. J., Anitha, J. and Tsihrintzis, G. A., Eds., Springer, Cham, pp. 1 – 16, 2021. doi: 10.1007/978-3-030-63937-2_1

[4] Beavers J., and Pournouri S., "Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions" in *Blockchain and Clinical Trial. Advanced Sciences and Technologies for Security Applications*, Jahankhani H., Kendzierskyj S., Jamal A., Epiphaniou G., and Al-Khateeb H., Eds., Springer, Cham, pp. 249 – 267, 2019. Available: https://doi.org/10.1007/978-3-030-11289-9_11

[5] Beydemir, A. and Soğukpinar, İ., "Lightweight zero knowledge authentication for Internet of things," *2017 International Conference on Computer Science and Engineering (UBMK)*, Antalya, pp. 360 – 365, 2017. doi: 10.1109/UBMK.2017.8093410

[6] Cheu, R., Yang, P., Lin, A., and Jaffe, A., "NARWHAL An implementation of Zero knowledge Authentication," Massachvsetts Institvte of Technology. [Online]. 2014. Available: https://docplayer.net/22360163-Narwhal-massachvsetts-institvte-of-technology-an-implementation-of-zero-knowledge-authentication-authors-ryan-cheu.html

[7] Dammak, M., Boudia, O. R. M., Messous, M. A., Senouci, S. M. and Gransart, C., "Token-Based Lightweight Authentication to Secure IoT Networks," 2019. doi: 10.1109/CCNC.2019.8651825

[8] Dammak, M., Senouci, S. M., Messous, M. A., Elhdhili, M. H. and Gransart, C., "Decentralized Lightweight Group Key Management for Dynamic Access Control in

IoT Environments," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, 2020. doi: 10.1109/TNSM.2020.3002957

[9] El-hajj, M., Fadlallah, A., Chamoun, M. and Serhrouchni, A., "A Survey of Internet of Things (IoT) Authentication Schemes," *Sensors*, vol. 19, no. 5, 2019. doi: 10.3390/s19051141.

[10] Gaba, G., S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M. and Alazab, M., "Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare," *Sustainable Cities and Society*, vol. 20, 2022. doi: 10.1016/j.scs.2022.103766

[11] Giusto, D., Iera, A., Morabito, G. and Atzori, L. (Eds.), "The Internet of Things," 2010, doi: 10.1007/978-1-4419-1674-7

[12] Grammatikis,P. I. R., Sarigiannidis, P. G. and Moscholios, I. D., "Securing the Internet of Things: Challenges, threats, and solutions," *Internet of Things*, vol. 5, 2019. doi: 10.1016/j.iot.2018.11.003

[13] Guo, C., and Chang, C. C., "Chaotic maps-based password-authenticated key agreement using smart cards," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 6, pp. 1433 – 1440, 2013. doi: 10.1016/j.cnsns.2012.09.032

[14] Harn, L., & Lin, C., "Authenticated Group Key Transfer Protocol Based on Secret Sharing," *IEEE Transactions on Computers*, vol. 59, no. 6, pp. 842 – 846, 2010. doi:10.1109/tc.2010.40

[15] Jiao, R., Ouyang, H., Lin, Y., Luo, Y., Li, G., Jiang, Z., and Zheng, Q., "A Computation-Efficient Group Key Distribution Protocol Based on a New Secret Sharing Scheme," *Information*, vol. 10, no. 5, p. 175, 2019. doi:10.3390/info10050175

[16] Kadjouh, N., Bounceur, A., Bezoui, M., Khanouche, M. E., Euler, R., Hammoudeh, M., … Al-Turjman, F., "A Dominating Tree Based Leader Election Algorithm for Smart Cities IoT Infrastructure," *Mobile Networks and Applications*, 2020. Available: https://doi.org/10.1007/s11036-020-01599-z

[17] Kadjouh, N., Bounceur, A., Tari, A., Lagadec, L., Euler, R., & Bezoui, M., "A New Leader Election Algorithm based on the WBS Algorithm Dedicated to Smart-cities," *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems - ICFNDS '19*, 2019. Available: https://doi.org/10.1145/3341325.3342014

[18] Kung, Y. H and Hsiao, H. C., "GROUPIT: Lightweight Group Key Management for Dynamic IoT Environments," *IEEE Internet of Things Journal*, vol. 5, no. 6, 2018. doi: 10.1109/JIOT.2018.2840321

[19] Mridula, R. D. and Rajesh, S., "Group Key Management Techniques," *Global Journal of Computer Science and Technology Network, Web & Security*, vol. 13, no. 11, 2013. Available: https://globaljournals.org/GJCST_Volume13/4-Group-Key-Management-Techniques.pdf

[20] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., and Lymberopoulos, D., "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," *Transactions on Emerging Telecommunications Technologies*, 2020. doi: 10.1002/ett.4049.

[21] Park, M. H., Park, Y. H., Jeong, H. Y., and Seo, S. W., "Key Management for Multiple Multicast Groups in Wireless Networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1712 – 1723, 2013. doi: 10.1109/tmc.2012.135

[22] Patel, K., Patel, S., Scholar, P. and Salazar, C., "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, 2016. doi: 10.4010/2016.1482.

[23] Raikwar, M., Gligoroski, D., & Kralevska, K., "SoK of Used Cryptography in Blockchain," *IEEE Access*, vol. 7, pp. 148550 – 148575, 2019. doi: 10.1109/ACCESS.2019.2946983

[24] Sciancalepore, S., Capossele, A., Piro, G., Boggia, G., and Bianchi, G., "Key Management Protocol with Implicit Certificates for IoT systems," *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems - IoT-Sys '15*, 2015. doi: 10.1145/2753476.2753477

[25] Siddiqui, M. F., "IoMT Potential Impact in COVID-19: Combating a Pandemic with Innovation," in *Computational Intelligence Methods in COVID-19: Surveillance, Prevention, Prediction and Diagnosis. Studies in Computational Intelligence*, Raza, K., Ed., Singapore: Springer, vol. 923, pp. 349 – 361, 2021. Available: https://doi.org/10.1007/978-981-15-8534-0_18

[26] Tawalbeh, L., Muheidat, F., Tawalbeh, M. and Quwaider, M., "IoT Privacy and Security: Challenges and Solutions," *Applied Science*, vol. 10, no. 12, 2020. doi:10.3390/app10124102

[27] Teshome, A., Kibret, B. and Lai, D., "A Review of Implant Communication Technology in WBAN : Progresses and Challenges," *IEEE Reviews in Biomedical Engineering*, 2018. doi: 10.1109/RBME.2018.2848228

[28] Tsai, I. C., Yu, C. M., Yokota, H., and Kuo, S. Y., "Key Management in Internet of Things via Kronecker Product," *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*, 2017. doi: 10.1109/prdc.2017.25

[29] Vaidya, B., Makrakis, D., and Mouftah, H., "Two-factor mutual authentication with key agreement in wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 2, pp. 171–183, 2012. doi: 10.1002/sec.517

[30] Veltri, L., Cirani, S., Busanelli, S., and Ferrari, G., "A novel batch-based group key management protocol applied to the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2724–2737, 2013. doi: 10.1016/j.adhoc.2013.05.009

[31] Wazid, M., Das, A. K., Shetty, S., Rodrigues, J. J. P. C. and Park, Y. H., "LDAKM-EIoT: Lightweight Device Authentication and Key Management Mechanism for Edge-Based IoT Deployment," *Sensor*, vol. 19, no. 24, 2019. doi: 10.3390/s19245539

[32] Wuu, L.C., Hung, C. H. and Kuo, W. C., "Group Key Management based on (2,2) Secret Sharing," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 3, pp. 1144-1156, 2014. doi: 10.3837/tiis.2014.03.025

[33] Yaacoub, J.–P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R. and Chehab, A., "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, pp. 581 – 606, 2020. doi: 10.1016/j.future.2019.12.028

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: T3Y3	**Study week no.: 2**
Student Name & ID: Chong Wei Feng (1802120)	
Supervisor: Ts. Dr. Vasaki a/p Punnusamy	
Project Title: Multicast Group Key Management on the Internet of Medical Things using Zero Knowledge Protocol	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Review on project proposal.
- Review on previous proposed protocol.
- Research more on zero knowledge protocol.

2. WORK TO BE DONE

- Continue to research on related protocol.
- Refine previous proposed protocol.
- Setup IoT multicast group.
- Implement the zero-knowledge protocol into the simulation.

3. PROBLEMS ENCOUNTERED

- Previous protocol may encounter MITM attack.
- Lack of literature review on zero knowledge protocol.

4. SELF EVALUATION OF THE PROGRESS

- Need to come up with refined zero knowledge protocol that is secured.
- Actively consult supervisor.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: T3Y3	**Study week no.: 4**
Student Name & ID: Chong Wei Feng (1802120)	
Supervisor: Ts. Dr. Vasaki a/p Punnusamy	
Project Title: Multicast Group Key Management on the Internet of Medical Things using Zero Knowledge Protocol	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Research on several papers related to zero knowledge protocol.
- Came up a prototype of refined zero knowledge protocol (on a piece of paper).

2. WORK TO BE DONE

- Test the refined protocol.
- Implement the refined protocol into the simulation.

3. PROBLEMS ENCOUNTERED

- To ensure the zero knowledge is as secure as possible.

4. SELF EVALUATION OF THE PROGRESS

- Find more sources to have better improvement in zero knowledge protocol.
- Actively consult supervisor.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: T3Y3	**Study week no.: 6**
Student Name & ID: Chong Wei Feng (1802120)	
Supervisor: Ts. Dr. Vasaki a/p Punnusamy	
Project Title: Multicast Group Key Management on the Internet of Medical Things using Zero Knowledge Protocol	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Complete a draft of the refined zero knowledge protocol.
- Tested theoretically and assumed expected output.
- Starting to code into the simulation tool.

2. WORK TO BE DONE

- Complete the implementation in the simulation.
- Performance study.

3. PROBLEMS ENCOUNTERED

- SenScript used in CupCarbon has limited documentation.
- Less knowledge on the operation of the simulation tool.

4. SELF EVALUATION OF THE PROGRESS

- The simulation testing is still in progress
- Actively consult supervisor.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: T3Y3	**Study week no.: 8**
Student Name & ID: Chong Wei Feng (1802120)	
Supervisor: Ts. Dr. Vasaki a/p Punnusamy	
Project Title: Multicast Group Key Management on the Internet of Medical Things using Zero Knowledge Protocol	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Completed the implementation of zero knowledge protocol into the simulation.

2. WORK TO BE DONE

- Performance study.
- Test using thread model.

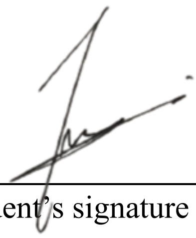
3. PROBLEMS ENCOUNTERED

- CupCarbon is lacking proper documentation.
- Routing cannot performed in the simulation.
- Only adjacent nodes around leader node can interact with leader node.
- Error when generating random numbers.

4. SELF EVALUATION OF THE PROGRESS

- Try to find out a solution for the problems encountered.
- Actively consult supervisor.

Supervisor's signature



Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: T3Y3	**Study week no.: 10**
Student Name & ID: Chong Wei Feng (1802120)	
Supervisor: Ts. Dr. Vasaki a/p Punnusamy	
Project Title: Multicast Group Key Management on the Internet of Medical Things using Zero Knowledge Protocol	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Performance study on the proposed zero knowledge protocol.

2. WORK TO BE DONE

- Final touch up.
- Complete the report.
- Conclude the project.

3. PROBLEMS ENCOUNTERED

- The issue due to the lack of documentation of the simulation tool cannot be solved.

4. SELF EVALUATION OF THE PROGRESS

- Although facing few problems, but the zero-knowledge protocol is implemented successfully.
- Actively consult supervisor.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: T3Y3	**Study week no.: 12**
Student Name & ID: Chong Wei Feng (1802120)	
Supervisor: Ts. Dr. Vasaki a/p Punnusamy	
Project Title: Multicast Group Key Management on the Internet of Medical Things using Zero Knowledge Protocol	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

- Final touch up.
- Completed report.
- Project is concluded.

2. WORK TO BE DONE

- Submit report.

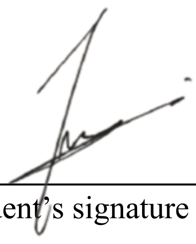
3. PROBLEMS ENCOUNTERED

- The issue due to the lack of documentation of the simulation tool cannot be solved.

4. SELF EVALUATION OF THE PROGRESS

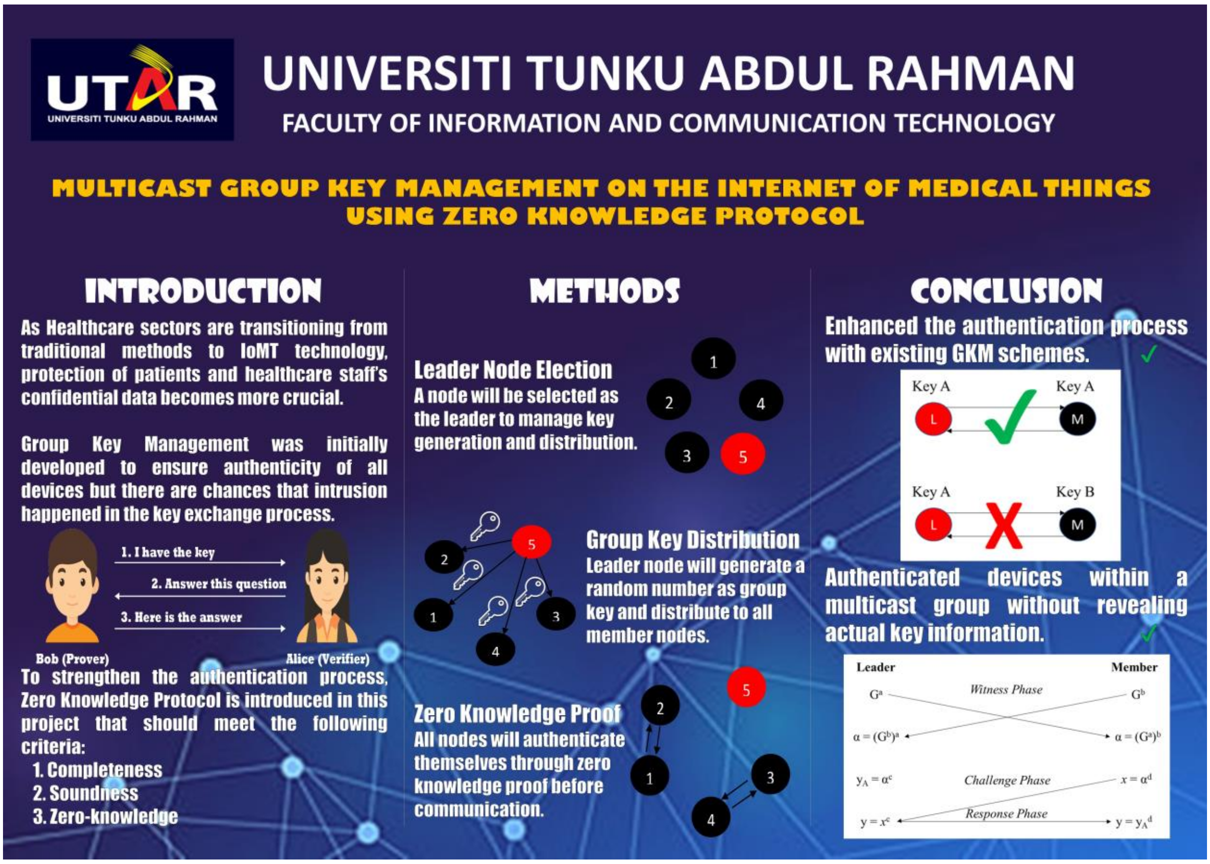
- Although facing few problems, but the zero-knowledge protocol is implemented successfully and perfectly tested.
- Actively consult supervisor.
- Seek comments from supervisor.

Supervisor's signature



Student's signature

POSTER


UNIVERSITI TUNKU ABDUL RAHMAN
FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
MULTICAST GROUP KEY MANAGEMENT ON THE INTERNET OF MEDICAL THINGS USING ZERO KNOWLEDGE PROTOCOL
INTRODUCTION
As Healthcare sectors are transitioning from traditional methods to IoMT technology, protection of patients and healthcare staff's confidential data becomes more crucial.
Group Key Management was initially developed to ensure authenticity of all devices but there are chances that intrusion happened in the key exchange process.
1. I have the key
2. Answer this question
3. Here is the answer
Bob (Prover)
Alice (Verifier)
To strengthen the authentication process, Zero Knowledge Protocol is introduced in this project that should meet the following criteria:
1. Completeness
2. Soundness
3. Zero-knowledge
METHODS
Leader Node Election
A node will be selected as the leader to manage key generation and distribution.
Group Key Distribution
Leader node will generate a random number as group key and distribute to all member nodes.
Zero Knowledge Proof
All nodes will authenticate themselves through zero knowledge proof before communication.
CONCLUSION
Enhanced the authentication process with existing GKM schemes.
Key A
Key A
Key A
Key B
Authenticated devices within a multicast group without revealing actual key information.
Leader
Member
Witness Phase
Challenge Phase
Response Phase

PLAGIARISM CHECK RESULT

Document Viewer

Turnitin Originality Report

Processed on: 20-Apr-2022 11:27 +08
ID: 1815107960
Word Count: 9892
Submitted: 1

Multicast Group Key Management on the Interne... By Chong Wei Feng

Similarity Index	Similarity by Source	
19%	Internet Sources:	13%
	Publications:	15%
	Student Papers:	N/A

include quoted include bibliography exclude small matches mode: quickview (classic) report Change mode print download

2% match (Internet from 14-Mar-2020)
https://www.mdpi.com/2078-2489/10/5/175/html

1% match (Internet from 05-May-2020)
https://www.csie.ntu.edu.tw/~hchsiao/pub/2018_IEEE_IOTJ.pdf

1% match (Internet from 19-Nov-2020)
http://www.cupcarbon.com

1% match (Internet from 10-Nov-2021)
https://fict.utar.edu.my/documents/FYP/FYP2_template/FYP2_Report_Template_IA.docx

1% match (publications)
"Future Internet Technologies and Trends", Springer Science and Business Media LLC, 2018

1% match ()
Walshe, M, Epiphaniou, G, Al-Khateeb, H, Hammoudeh, M, Katos, V, Dehghantanha, A. "Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments", 'Elsevier BV', 2019

1% match (Internet from 01-Apr-2022)
https://hal.archives-ouvertes.fr/hal-02965346/document

1% match (publications)
Savio Sciancalepore, Angelo Capossele, Giuseppe Piro, Gennaro Boggia, Giuseppe Bianchi. "Key Management Protocol with Implicit Certificates for IoT systems", Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems - IoT-Sys '15, 2015

1% match (publications)
Min-Ho Park, Young-Hoon Park, Han-You Jeong, Seung-Woo Seo. "Key Management for Multiple Multicast Groups in Wireless Networks", IEEE Transactions on Mobile Computing, 2013

1% match (publications)
Harn, Lien, and Changlu Lin. "Authenticated Group Key Transfer Protocol Based on Secret Sharing", IEEE Transactions on Computers, 2010.

1% match (publications)
Mohammed Riyadh Abdmeziem, Djamel Tandjaoui, Imed Romdhani. "A Decentralized Batch-Based Group Key Management Protocol for Mobile Internet of Things (DBGK)", 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015

<1% match (Internet from 10-Nov-2021)
https://fict.utar.edu.my/documents/FYP/FYP2_template/FYP2_Report_Template_CN.docx

<1% match (Internet from 10-Nov-2021)
https://fict.utar.edu.my/documents/FYP/FYP_guidelines/FYP2_Guidelines.docx

<1% match (Internet from 27-Oct-2020)
https://link.springer.com/chapter/10.1007%2F978-3-030-11289-9_11

<1% match (Internet from 31-Jan-2020)
https://link.springer.com/content/pdf/10.1007%2Fs11277-017-4912-x.pdf

<1% match (Internet from 27-Mar-2020)
https://link.springer.com/chapter/10.1007%2F978-3-319-45741-3_18

<1% match (Internet from 10-Sep-2020)
https://link.springer.com/chapter/10.1007%2F978-3-030-40305-8_19

<1% match (Internet from 24-Jan-2022)
https://lib.hcmut.edu.vn/uploads/files/A%20novel%20batch-based%20group%20key%20management%20protocol%20applied.pdf

<1% match (publications)
I-Chen Tsai, Chia-Mu Yu, Haruo Yokota, Sy-Yen Kuo. "Key Management in Internet of Things via Kronecker Product", 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), 2017

<1% match (Internet from 20-Feb-2022)
http://koreascience.or.kr

<1% match (publications)
Cheng Guo, Chin-Chen Chang. "Chaotic maps-based password-authenticated key agreement using smart cards", Communications in Nonlinear Science and Numerical Simulation, 2013

<1% match (Internet from 26-Feb-2019)
https://onlinelibrary.wiley.com/doi/full/10.1002/sec.517

<1% match (publications)

Runhai Jiao, Hong Ouyang, Yukun Lin, Yaoming Luo, Gang Li, Zaiyu Jiang, Qian Zheng. "A Computation-Efficient Group Key Distribution Protocol Based on a New Secret Sharing Scheme", Information, 2019

<1% match (publications)
Gurjot Singh Gaba, Mustapha Hedabou, Pardeep Kumar, An Braeken, Madhusanka Liyanage, Mamoun Alazab. "Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare", Sustainable Cities and Society, 2022

<1% match (Internet from 23-Sep-2019)
http://www.iariajournals.org

<1% match (publications)
"Advances on Broad-Band Wireless Computing, Communication and Applications", Springer Science and Business Media LLC, 2017

<1% match (publications)
Hongfeng Zhu. "Flexible and Password-Authenticated Key Agreement Scheme Based on Chaotic Maps for Multiple Servers to Server Architecture", Wireless Personal Communications, 2015

<1% match (publications)
Srinivas, Jangirala, Sourav Mukhopadhyay, and Dheerendra Mishra. "Secure and Efficient User Authentication Scheme for Multi-gateway Wireless Sensor Networks", Ad Hoc Networks, 2016.

<1% match (Internet from 28-Nov-2020)
http://eprints.utar.edu.my

<1% match (Internet from 17-Apr-2022)
https://www.deepdyve.com/lp/wiley/a-chaotic-map-based-anonymous-multi-server-authenticated-key-agreement-i5mYKwyGyr

<1% match (publications)
Yi-Hsuan Kung, Hsu-Chun Hsiao. "GROUPIT: Lightweight Group Key Management for Dynamic IoT Environments", IEEE Internet of Things Journal, 2018

<1% match (publications)
"Intelligent Computing Theories and Application", Springer Science and Business Media LLC, 2020

<1% match (Internet from 11-Feb-2022)
https://ouci.dntb.gov.ua/works/4gWrZym4/

<1% match (publications)
Ching-Fang Hsu, Lein Harn. "Lightweight Group Key Distribution Schemes Based on Pre-Shared Pairwise Keys", IET Communications, 2020

<1% match (publications)
Mehdi Gheisari, Guojun Wang, Md Zakirul Alam Bhuiyan, Wei Zhang. "MAPP: A Modular Arithmetic Algorithm for Privacy Preserving in IoT", 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), 2017

<1% match (publications)
Sarra Naoui, Mohamed Elhoucine Elhdhili, Leila Azouz Saidane. "Trusted Third Party Based Key Management for Enhancing LoRaWAN Security", 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), 2017

<1% match (publications)
"Blockchain and Clinical Trial", Springer Science and Business Media LLC, 2019

<1% match (publications)
Lecture Notes in Computer Science, 2013.

<1% match (publications)
Ruti Gafni, Tal Pavel. "Cyberattacks against the health-care sectors during the COVID-19 pandemic", Information & Computer Security, 2021

<1% match ()
Machado, Diogo Moreira Cabral. "People counting system using existing surveillance video camera", Instituto Politécnico do Porto. Instituto Superior de Engenharia do Porto, 2011

<1% match (publications)
"Quality, Reliability, Security and Robustness in Heterogeneous Networks", Springer Science and Business Media LLC, 2013

<1% match (publications)
Ling Xiong, Daiyuan Peng, Tu Peng, Hongbin Liang, Zhicai Liu. "A Lightweight Anonymous Authentication Protocol with Perfect Forward Secrecy for Wireless Sensor Networks", Sensors, 2017

<1% match (Internet from 11-Dec-2019)
https://acadpubl.eu/hub/2018-118-21/articles/21a/51.pdf

<1% match (Internet from 16-Jan-2022)
http://umpir.ump.edu.my

<1% match (publications)
"Body Area Networks: Smart IoT and Big Data for Intelligent Health Management", Springer Science and Business Media LLC, 2019

<1% match (publications)
"Mobile, Secure, and Programmable Networking", Springer Science and Business Media LLC, 2019

<1% match (publications)
"Tree Based Key Management Schemes", Secure Group Communications over Data Networks, 2005

<1% match (publications)
Ahcène Bounceur, Madani Bezoui, Loic Lagadec, Reinhardt Euler, Laouid Abdelkader, Mohammad Hammoudeh. "Chapter 5 DoTRo: A New Dominating Tree Routing Algorithm for Efficient and Fault-Tolerant Leader Election in WSNs and IoT Networks", Springer Science and Business Media LLC, 2019

<1% match (publications)
Cheng Guo. "An authenticated group key distribution protocol based on the generalized Chinese remainder theorem : AN AUTHENTICATED GROUP KEY DISTRIBUTION PROTOCOL BASED ON THE GCRT", International Journal of Communication Systems, 03/2012

PLAGIARISM CHECK RESULT

<1% match (publications)
Lee, Tian-Fu. "Enhancing the security of password authenticated key agreement protocols based on chaotic maps", Information Sciences, 2015.

<1% match (publications)
Samia Belattaf, Mohamed Mohammedi, Mawloud Omar, Rachida Aoudjit. "Reliable and Adaptive Distributed Public-Key Management Infrastructure for the Internet of Things", Wireless Personal Communications, 2021

<1% match (Internet from 01-Jan-2022)
https://research-portal.uws.ac.uk/en/publications/video-quality-in-5g-networks-context-aware-qoe-management-in-the-

<1% match ()
Karanjeet Choudhary, Gurjot Singh Gaba, Ismail Butun, Pardeep Kumar. "MAKE-IT—A Lightweight Mutual Authentication and Key Exchange Protocol for Industrial Internet of Things", Sensors (Basel, Switzerland)

<1% match (publications)
"Algorithms and Architectures for Parallel Processing", Springer Science and Business Media LLC, 2015

<1% match (publications)
Ahcène Bounceur, Madani Bezoui, Umber Noreen, Reinhardt Euler, Farid Lalem, Mohammad Hammoudeh, Sohail Jabbar. "Chapter 1 LOGO: A New Distributed Leader Election Algorithm in WSNs with Low Energy Consumption", Springer Science and Business Media LLC, 2018

<1% match (publications)
Baasantsetseg Bold, Young Hoon Park. "Optimising group key management for frequent-membership-change environment in VANET", International Journal of Internet Technology and Secured Transactions, 2020

<1% match (publications)
Hongfeng Zhu. "Cryptanalysis and Improvement of a Mobile Dynamic ID Authenticated Key Agreement Scheme Based on Chaotic Maps", Wireless Personal Communications, 2015

<1% match (publications)
Park, Min-Ho, Young-Hoon Park, Han-You Jeong, and Seung-Woo Seo. "Secure Multiple Multicast Services in Wireless Networks", IEEE Transactions on Mobile Computing, 2012.

<1% match (publications)
S K Hafizul Islam. "Comments on ID-Based Client Authentication with Key Agreement Protocol on ECC for Mobile Client-Server Environment", Communications in Computer and Information Science, 2011

<1% match (Internet from 18-Jul-2021)
https://eudl.eu/pdf/10.1007/978-3-319-78816-6_22

<1% match (Internet from 02-Mar-2022)
https://m.hausarbeiten.de/document/214039

<1% match ()
Asimakopoulou, Eleni, Chotzoglou, Konstantinos, Kolaitis, Dionysios, Zhang, Jianping, Delichatsios, Michael A. "Numerical investigation of externally venting flame characteristics in a corridor-façade configuration", 2019

<1% match (Internet from 08-Oct-2020)
https://worldwidescience.org/topicpages/a/authenticated+key+agreement.html

<1% match (publications)
"New Trends in Computer Technologies and Applications", Springer Science and Business Media LLC, 2019

<1% match (publications)
Hongxiang Gu, Miodrag Potkonjak. "Efficient and Secure Group Key Management in IoT using Multistage Interconnected PUF", Proceedings of the International Symposium on Low Power Electronics and Design - ISLPED '18, 2018

<1% match (publications)
Maissa Dammak, Sidi Mohammed Senouci, Mohamed Ayoub Messous, Mohamed Houcine Elhdhili, Christophe Gransart. "Decentralized Lightweight Group Key Management for Dynamic Access Control in IoT Environments", IEEE Transactions on Network and Service Management, 2020

<1% match (publications)
Nam, Junghyun, Kim-Kwang Raymond Choo, Sangchul Han, Moonseong Kim, Juryon Paik, and Dongho Won. "Efficient and Anonymous Two-Factor User Authentication in Wireless Sensor Networks: Achieving User Anonymity with Lightweight Sensor Computation", PLoS ONE, 2015.

<1% match (publications)
Krishna C.J.. "Key Transfer Protocol Based on Secret Sharing Using Initiator", 2012 International Conference on Advances in Computing and Communications, 2012

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	CHONG WEI FENG
ID Number(s)	1802120
Programme / Course	CN
Title of Final Year Project	MULTICAST GROUP KEY MANAGEMENT ON THE INTERNET OF MEDICAL THINGS USING ZERO KNOWLEDGE PROTOCOL

Similarity	**Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)**
Overall similarity index: 19 **%** **Similarity by source** Internet Sources: 13 % Publications: 15 % Student Papers: N/A %	Checked and verified
Number of individual sources listed of more than 3% similarity: 0	Checked and verified
Parameters of originality required and limits approved by UTAR are as Follows: **(i) Overall similarity index is 20% and below, and** **(ii) Matching of individual sources listed must be less than 3% each, and** **(iii) Matching texts in continuous block must not exceed 8 words** ***Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.***	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

Signature of Supervisor

Name: Vasaki Ponnusamy

Date: 21/4/22

Signature of Co-Supervisor

Name: ______________

Date: ______________

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY
(KAMPAR CAMPUS)

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	1802120
Student Name	CHONG WEI FENG
Supervisor Name	TS. DR. VASAKI A/P PUNNUSAMY

TICK (√)	**DOCUMENT ITEMS** Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
N/A	Front Plastic Cover (for hardcopy)
√	Title Page
√	Signed Report Status Declaration Form
√	Signed FYP Thesis Submission Form
√	Signed form of the Declaration of Originality
√	Acknowledgement
√	Abstract
√	Table of Contents
√	List of Figures (if applicable)
√	List of Tables (if applicable)
N/A	List of Symbols (if applicable)
√	List of Abbreviations (if applicable)
√	Chapters / Content
√	Bibliography (or References)
√	All references in bibliography are cited in the thesis, especially in the chapter of literature review
N/A	Appendices (if applicable)
√	Weekly Log
√	Poster
√	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)
√	I agree 5 marks will be deducted due to incorrect format, declare wrongly the ticked of these items, and/or any dispute happening for these items in this report.

*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report.

____
(Signature of Student)
Date: 20/04/2022