YOKOHAMA NATIONAL UNIVERSITY

DOCTOR THESIS

Hierarchical secret sharing and UWB wireless localization technologies and applications of their integrated technologies
階層型秘密分散と超広帯域無線測位の技術およびその統合技術の応用

A thesis submitted in partial fulfilment of the requirements for the award of
DOCTOR *in*
Electronic Network Engineering and Security

in the

Department of Mathematics, Physics, Electrical and Computer Engineering
Graduate School of Engineering Science

July , 2021

Declaration of Authorship

I, Ngye ANTOINETTE AGWA
ンギェアントイネッテアグァ
Student No: 18QC597, declare that this thesis titled, “Hierarchical secret sharing and UWB wireless localization technologies and applications of their integrated technologies
(階層型秘密分散と超広帯域無線測位の技術およびその統合技術の応用) and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

YOKOHAMA NATIONAL UNIVERSITY

Abstract

A thesis submitted in partial fulfilment of the requirements for the award of DOCTOR in Electronic Network Engineering and Security

in the Department of Mathematics, Physics, Electrical and Computer Engineering
Graduate School of Engineering Science

Hierarchical secret sharing and UWB wireless **localization technologies and applications of their integrated technologies**
階層型秘密分散と超広帯域無線測位の技術およびその統合技術の応用

by
Ngye ANTOINETTE AGWA
ンギェアントイネッテアグァ
Student No: 18QC597

The Internet of Things (IoT) is growing to an indispensable part of our daily lives, facilitating various emerging applications and services. Firstly, the limited data storage and processing capacity have exposed them to untold risks with many consequences. Cryptography protocols use for authentication overworked this device which makes them vulnerable to attacks. Secondly, At the physical layer, IoT devices are exposed to re-lay/replay attacks. Lastly, accurate localization of these devices is a potential problem for identification and authentication.

In this thesis, individual and integrated technologies of the Global Navigation Satellite System (GNSS) and Ultra-Wide Band (UWB) radio system are proposed as optimum solutions for accurate localization, followed by outsourcing hierarchical threshold secret sharing used to overcome limited data storage and processing capacity in IoT devices. Next, I use the Time of Flight (ToF) as the positioning technique between GNSS such as GPS（**Global Positioning System**）and UWB radio system. In other words, GNSS/UWB ToF to determine user position, which is an enhancement to the ambiguities in an international standard such as IEEE802.15.4z-2020. Finally, two use cases were presented as examples of integrated technology of GNSS/UWB and outsourcing hierarchical secret sharing. The most vital advantage of this thesis lies in improving system security and localization while minimizing communication costs and resource consumption. Performance of the proposed systems are analyzed. Computer simulation shows an overall effect on how the proposer enhances system security and equally enhances the positioning accuracy.

Acknowledgements

This masters thesis summarizes the research work that I have done in the Department of Mathematics, Physics, Electrical and Computer Engineering at the Graduate School of Engineering Science, Yokohama National University from October 2018 until March 2021. I will like to express my sincere thanks to the following organizations, individuals, and groups. Please note that order does not necessarily signify importance.

- Global Doctoral Program for Academic Career Support (GDACS), Japan Student Services Organization -(JASSO), Otsuka Toshimi Scholarship Foundation and people of Japan for the award of these scholarships that made it possible for me to come to Japan for graduate study.

- Prof. Ryuji Kohno and Prof. Chika Sugimoto, whom, despite my zero experience in research, granted me the opportunity to join their laboratories. Their practical supervision and patient support throughout this research has opened up a promising career path for me.

- Besides my academic advisors, I would like to thank my thesis committee: Prof. Ochiai, Prof. Hamagami, and Prof. Shima, for their insightful encouragement and comments, but also for the tricky question which incented me to stretch my research from various perspectives. Not forgetting my counselor, Dr. Takumi Kobayashi, who has always been there to guide me both academically and morally.

- My family back home who have supported me all through this endeavour.

- To my late Parents, Mr. and Mis Fon Joseph Ngye, for their immense sacrifice that made me the man I am today. May their souls RIP.

- Also, I will like to sincerely thank my colleagues especially the Cameroonians in Fujimota lab and Kohno lab for their patience in guiding me during this program.

- To all the members of Kohno lab for the family spirit that drives us to success.

- To my lovely husband, Nyambuh Etienne, who has been a constant source of support and encouragement during the challenges of graduate school and life. I am truly thankful for having you in my life.

- To the Almighty Creator of all things that are both tangible and intangible!

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview of Technologies

Ultra-wideband (UWB) is one of the wireless communication technologies that use radio waves as Wi-Fi and Bluetooth. UWB uses radio waves to permit devices to talk to each other. UWB transmits signals across short distances and accurately determines user location by measuring how long the radio pulse travels between devices. It also uses a broader frequency range between 3.1 and 10.6 GHz. UWB enables many new services for enterprises and consumers, such as accurate indoor location and positioning, precise analytics in real-time, and providing context-aware information.

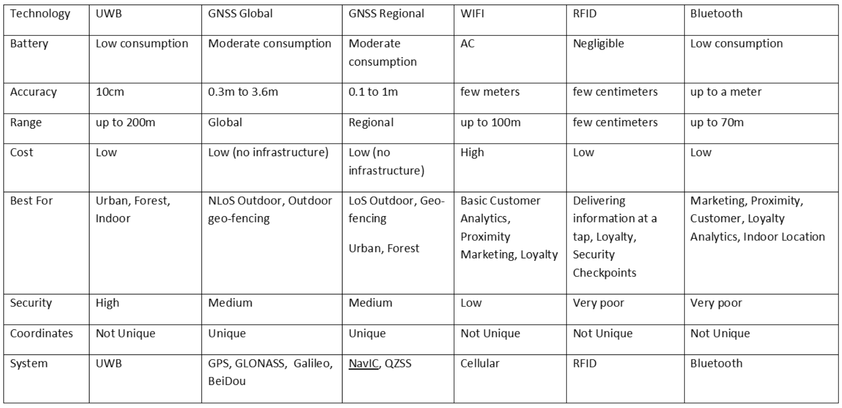
A UWB transmitter transmits billions of radio pulses over the broad spectrum frequency, and a UWB receiver then converts the pulses into data. Like bats use echolocation to sense their surroundings, UWB pulses are used to sense distances between two communication devices. UWB achieves high accuracy because it sends up to 1 billion pulses per second (about 1 per nanosecond). The shorter the period of the impulse, the more accurate the distance measurement will be. Generally speaking, UWB has four essential uses:

1. Determining a position (location)
2. Monitoring the movement of a person or object (tracking)
3. Moving from one place to another (navigation)
4. Creating a map of an area (mapping)

To the best of my knowledge, there is no unique solution to achieve all the above mention four points. This thesis aims to propose a solution that can securely perform all UWB use cases.

1.1.1 Determining a Position (Location)

A Positioning system is a method used to determine the position of an object in space. In most outdoor applications, satellite technology such as Global Navigation Satellite System (GNSS) provides users with precise location measurements. Similar range-only localization systems in densely cluttered environments generally lack reliability and accuracy due, notably, to line-of-sight (LOS) blockage, dense multipath, and excess propagation delays within materials. In particular, the range between transmitters and a receiver is often positively biased. Moreover, the ranging quality degrades with distance, and the geometric arrangement of the beacons also influences the localization accuracy. In the literature, many proposals have been made to improve localization accuracy in



Technology	UWB	GNSS Global	GNSS Regional	WIFI	RFID	Bluetooth
Battery	Low consumption	Moderate consumption	Moderate consumption	AC	Negligible	Low consumption
Accuracy	10cm	0.3m to 3.6m	0.1 to 1m	few meters	few centimeters	up to a meter
Range	up to 200m	Global	Regional	up to 100m	few centimeters	up to 70m
Cost	Low	Low (no infrastructure)	Low (no infrastructure)	High	Low	Low
Best For	Urban, Forest, Indoor	NLoS Outdoor, Outdoor geo-fencing	LoS Outdoor, Geo-fencing Urban, Forest	Basic Customer Analytics, Proximity Marketing, Loyalty	Delivering information at a tap, Loyalty, Security Checkpoints	Marketing, Proximity, Customer, Loyalty Analytics, Indoor Location
Security	High	Medium	Medium	Low	Very poor	Very poor
Coordinates	Not Unique	Unique	Unique	Not Unique	Not Unique	Not Unique
System	UWB	GPS, GLONASS, Galileo, BeiDou	NavIC, QZSS	Cellular	RFID	Bluetooth

FIGURE 1.1: Comparison of UWB technology to different wireless technologies

such environments. In [1] the fundamental limit of localization accuracy for a UWB system operating in such settings was derived by the author. More comparative analyses between UWB and other wireless technologies are presented in Table 1.1. However, the inability of UWB to make precise time measurements, global coverage, and uniquely identify the coordinate (longitude/latitude) of each point makes it not suitable for geo-localization compared to satellite technology. Therefore, to obtain secure ranging and unique location information, UWB needs to be combined with GNSS. Another problem faced by UWB is its inability to prevent the relay/replay attack at the physical layer.

1.1.2 Digital Land Point collection using Geo-fencing Technology (mapping)

Consider an application where digital certificate content is stored in the cloud; it becomes necessary to prevent the digital certificate from being falsified. Therefore, the most promising measure for ownership protection is to discourage people from faking ownership rights. One way to deter falsification is to make it detectable and highly punishable by law. If a person is accused of falsification by the owner, then the problem of ownership dispute arises. Considering such scenarios, previous proposals to resolve ownership right focus on resolving disputes using the watermark buyer-seller protocol. [2]–[7] Another way is to use the deduplication protocol proposed in literature [8]–[12]. The decision made by a verifier (a judge, for example) after comparing numerous claims of ownership rights results from an ownership dispute. Generally, this result may not determine the rightful owners in a situation where the rightful owner is not participating in the dispute. In addition, only a single claim of ownership is often faced by one and has to adapt to its rightfulness. An important example is the acquisition of a digital land certificate. Suppose a Fraudster obtains a digital copy, claims to be the rightful owner, and starts selling it to another person without proof of ownership. An honest buyer purchasing the land will get into trouble when the rightful owner later detects the (Unpremeditated) used. In such a condition, proof of ownership is required.

On the other hand, it guarantees the buyer that he obtain the right of possession of the land parcel. On the one hand, it makes the unauthorized selling or ownership transfer right (gift or acquisition) very difficult since honest buyers request ownership proof from the seller. Therefore, the ownership proof should be transferable. The new buyer (Lala) can show another buyer (Titi) how Lala took good care of acquiring the property.

All landowners must register with the appropriate authority, who will issue a land certificate in return. One might think that it is insignificant to achieve proof of ownership when a registration center is involved. Nevertheless, the critical point is that ownership right refers not only to registered land but also to all related lands which have not been registered. To prevent land dispute: a rightful owner of a land certificate should perform ownership proof on the land parcel. Furthermore, multiple registrations of the same land parcel have to be avoided by the appropriate authority. Otherwise, a falsifier may gradually modify a land certificate and register it under another name and hence be able to perform a fake ownership proof.

1.2 Motivation of This Thesis

1.2.1 Automatic data collection and management

With the fast development of computer science and technologies, embedded devices, such as mobile phones, computers are widely used in our daily life because they are small in size, portable and lightweight. Mobile Geographic Information System (MGIS), which combines the advantages of being the primary data process for mobile devices and analysis performance of desktop GIS [13], are more prevalent in outdoor data collections. Using MGIS, combined with desktop GIS environment and measuring equipment, makes data collection more accurate and efficient [14].

Existing mobile GIS solutions have many limitations. For example, using a large-scale wireless network can infer high costs in wireless communications [15]. The instability of mobile devices network makes data transmission unstable. In addition, memory capacity in a mobile device is far less than that of a cloud computer, and its computing ability is minimal. Many researchers on digital land collection and management focus on new technologies to improve localization accuracy and data transfer methods from survey devices to PCs.

To use the advantages of MGIS while avoiding their shortcomings in field data collection, processing, and storage. I proposed a geo-fence digital-point collection technique with automatic data transfer to the cloud as shown in Figure 1.2. Also, a novel proximity, distance, and secure localization scheme based on user location and outsource hierarchical threshold secret sharing scheme (Figure 1.3) is proposed to allow many people involved in land management. The above method is an innovation to the traditional data collection techniques presented in the literature.

1.2.2 Poor localization and multipart in environments with poor satellite visibility

In dense urban, mountain, forest, and indoor environments, precise positioning has always been a more challenging problem for many reasons: the GNSS signal is not strong enough to penetrate most materials. As soon as an object hides the GNSS satellite from the target's view, the signal is corrupted, limiting GNSS's usefulness to open environments and limiting its performance in the mountains, dense urban, and forest environments, as retaining a lock on the GNSS signals becomes very difficult. GNSS typically becomes almost useless in such challenging environments. However, there is an increasing need for precise localization in cluttered environments, in addition to open spaces. For example, in a land survey and keyless entry system, accurate localization of digital

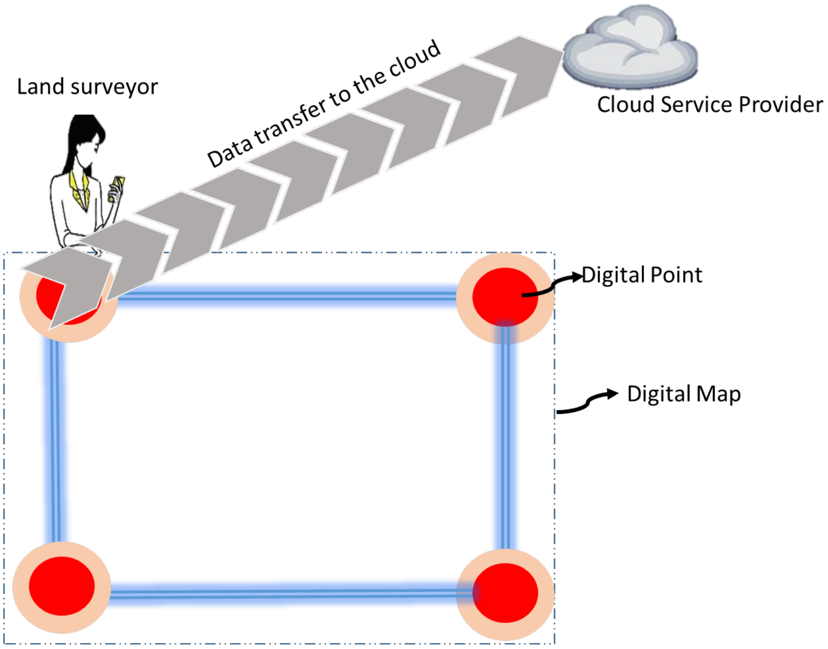


FIGURE 1.2: Automatic Data Management and Transfer to the Cloud

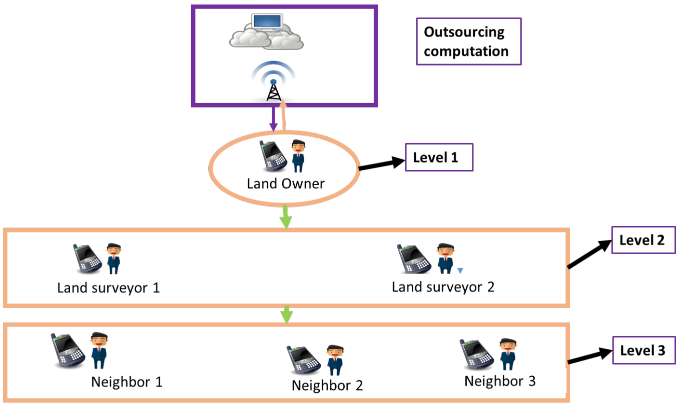


FIGURE 1.3: Hierarchical Outsource Threshold Multi level-secret sharing scheme

land points is an emerging need, "blue force tracking" that knows where friendly force, is of great significance, must especially in urban scenarios. A promising solution to minimize the multipath effect and increase position accuracy is radio signals like UWB technology because UWB ranging has several characteristics, which give them superiority over GNSS signals in low to limited signal environments. UWB is characterized by: sufficient time resolution ability, high-speed data transmission, accurate position estimation, low power transceiver designs, and robust performance in dense multipath environments that enable the GNSS navigation system, such as for land survey boost its operational environment. Furthermore, UWB ranging provides the capability to augment GNSS through high accuracy ranges. UWB information is transmitted through a series of baseband pulses instead of the modulated sinusoidal carrier in an impulse signal. On the other hand, multi-carrier UWB signals use a set of sub-carriers. Each of these sub-carriers must not interfere with one another and should overlap. The ability of multi-carrier UWB signals to minimize interference with bands used by different systems sharing the spectrum is advantageous [16]. UWB gives significant advantages in numerous applications, including industrial RF monitoring systems, high-speed LAN, Unmanned Aerial Vehicle (UAV), Intrusion Detection Radars, and Unmanned Ground Vehicle (UGV) precise positioning, Tactical Handheld Radios, and more. Other additional advantages of UWB include;

- With power spread over huge bandwidth, frequency selective fading from multipath/materials is mitigated [17]
- Ranging – very fine precision distance and range resolution.
- Low energy density gives less interference to closer systems and minimal RF health hazards.
- Minimal multipath cancellation effects

Multipath nullification happens when a multipath signal arrives at the anchor node partially or totally out of phase with the direct signal. It causes a reduced amplitude response. With a short period of signal pulses, direct signals will arrive before indirect signals. As a result, they are less multipath cancellation effects with UWB signals. UWB, like GNSS technology, is still subject to physics laws for radio frequency signals such as trade-off versus bandwidth. Another issue with UWB is its ranging accuracy. In addition, UWB provides reliable and precise results regarding relative positioning concerning a local frame, at the cost of covering the working area with expensive antennas, thereby limiting UWB technology only to a relatively small extent outdoor and applicable indoor. On the other hand, GNSS is a cheap technology that offers an adequately accurate localization outdoor worldwide, in terms of a global frame (longitude, altitude, latitude). Using UWB to increase GNSS enlarges navigating and positioning in areas where GNSS typical falters; this is mostly indoors or in hostile signal environments. Because both systems are harmonious, integrating these sensors for precise positioning draws benefits from both types of sensors while reducing their drawbacks. Previous sensor fusion proposed that a particle filter can combine GPS/UWB for and out/indoor scenarios, but there were no descriptions on anchor node placement. Besides, GPS provides low accuracy when compared to GNSS technology [18]. [19] equally shown that they were improvement in combining UWB and GPS. However, precision is also a function of the UWB beacon's location; besides, the estimation was slightly sensitive to the location's initial guess. Finally, [20] uses a single UWB range to increase GPS in hostile

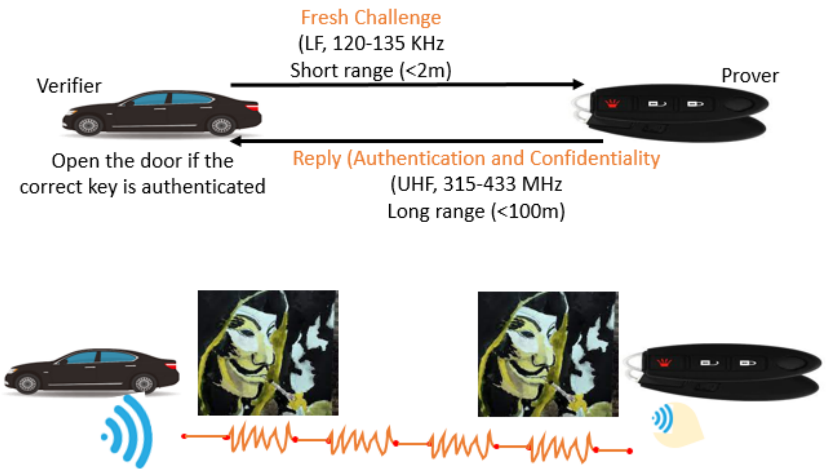


FIGURE 1.4: Conventional Relay Attack Model

environments. The analysis shows a rapid convergence of the Kalman filter positioning and a reduction in Dilution of Precision (DOP) values with the UWB range's augmentation.

1.2.3 Physical Layer Attacks

Two devices (prover and verifier) play a classical challenge-response protocol with some unexpected challenges and replies that are authenticated and confidential. The attacker is essentially just relaying the messages between the two locations. They are no notion of distance or time in this protocol, so it is vulnerable to attacks. The main reason for the vulnerability is because users do not interact with the system as shown in figure 1.4. IR-UWB ranging systems depend on ToF for distance measurement. ToF positioning systems are naturally secure against relay attacks. A relay helps the attacker to enlarge the communication range, which increases the ToF. Another type of attack is the Cicada attack which the receiver can prevent by limiting the search window. Thus the only threat to be addressed is the ED/LC attack [21], [22]. Clulow et al. [21] show that a system depending on longer symbols is inherently exposed to ED/LC attacks. Short symbol length was proposed as the only way to prevent B/LC attacks. Tippenhauer et al. [23] propose a system for processing short symbols. To reduce symbol length, they designate energy within a time frame as fast as feasible, which gives a limited chance for the system to be attacked. Conventional ED/LC attacks provide the decision between security or longer distance. A single narrow pulse 1-2ns with short symbols can be considered secure against ED/LC attacks which is the basis for secure ranging. The 802.15.4f extended and long-range rely on more pulses per bit. But, the long symbol length and anticipated symbol structures make it vulnerable to ED/LC attacks. Nevertheless, They are limited to the fact that many participant can not participate in the protocol. Therefore, it is important to proposed new methods to prevent the physical layer from these attacks and also provide a possibility for many users to participant in the proof system. Privacy-Preservation Contact Tracing Attack is one of the most recent physical layer attacks proposed by Google and Apple where mobile phones are in the system transmitting information to locate another mobile phone jointly. So, attackers can easily relay/replay such identity information being transmitted.

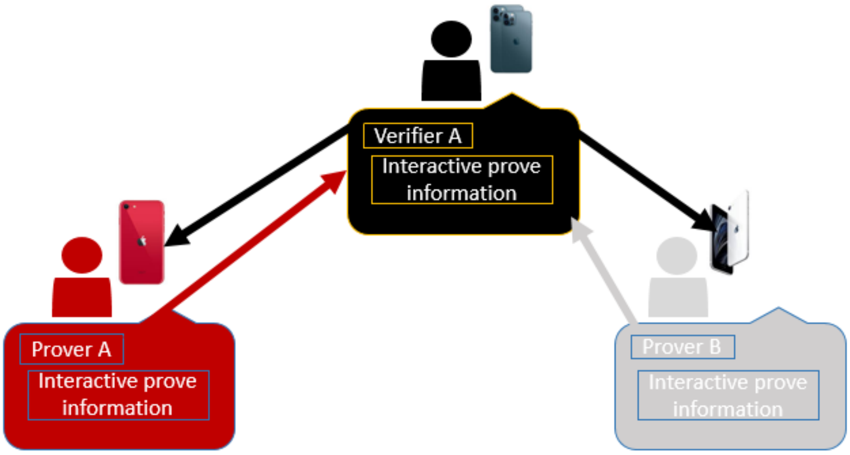

Verifier A
Interactive prove information
Prover A
Interactive prove information
Prover B
Interactive prove information

FIGURE 1.5: Wormhole Privacy-Preservation Contact Tracing Attack

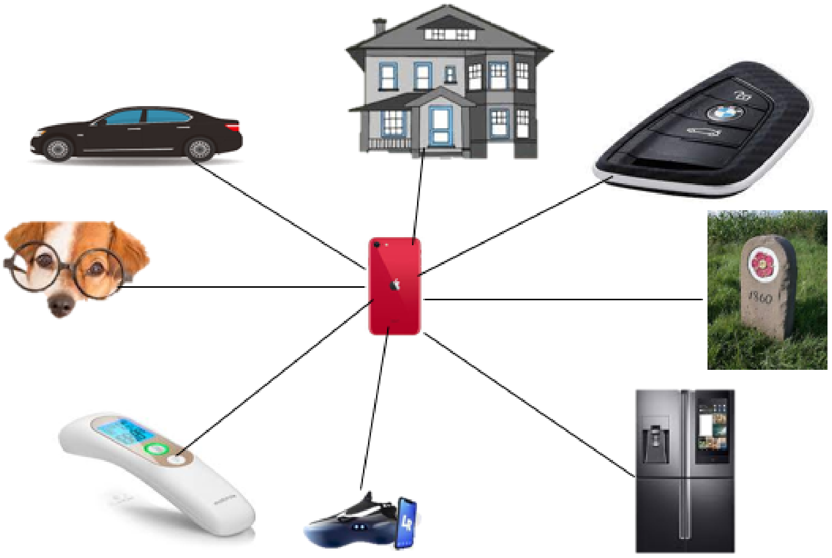


FIGURE 1.6: Secure Ranging System

1.3 Organisation of This Thesis

This thesis is organized as follows:

- In chapter II, related works to this thesis are presented.
- In chapter III the GNSS/UWB integration positioning method is presented.
- In chapter IV Outsource hierarchical threshold secret sharing is presented, the case study of land survey.

- In chapter V Advance GNSS/UWB security enhancement scheme to prevent relay attack to keyless entry system is presented.
- Conclusion and future works are presented in chapter VI.

1.4 Originality of This Thesis

GNSS has been proven to be a promising solution for geo-localization in the literature. However, its inability to perform accurate localization in deplorable signal conditions limits its performance. To overcome GNNS limitations, many researchers have different solutions in the literature, yet the accuracy is not good enough. In this section, I use CRLB to prove the significance of combining UWB and GNSS to achieve precise localization in deplorable signal conditions.

The Cramer-Reo lower bound (CRLB)

The bound CRLB [24] is used in this paper as a statistical measure to analyses the impact of combining GNSS with UWB for accurate ranging. In [24], the swap of any unbiased estimator is as large as the inverse of the Fisher data. The CRLB is a benchmark for comparison with any unbiased estimator. In positioning ranging, CRLB provides a method to estimate the theoretical most reliable performance of an estimator. In order to distinguish the characteristics of a signal that decreases the CRLB, consider the following two received signals $x^G(t) = s^G\left(t; \{b_k^G\}\right) + w^G(t)$ and $x^U(t) = s^U\left(t; \{b_k^U\}\right) + w^U(t)$ obtained as the signal sum of $x^{GU}\left(t; \{b_k\}\right)$ in function of time t, a set of unknown parameters $\{b_k^{GU}\}$, and of thermal noise $w^{GU}(t)$. The total frequency occupation of the signal being B^{GU}. Where $''G''$ and $''U''$ represent GNSS and UWB measurements respectively. The ToF CRLB equations for GNSS and UWB can be expressed as:

$$\sigma^G = \sqrt{\mathrm{CRB}^G} = \sqrt{\frac{1}{8\pi^2 \cdot \frac{1}{2\beta^G} \cdot C/N_0(\theta) \cdot \int_{-F_s/2}^{F_{s/2} f^2 \cdot G_s(f) df} n}} \tag{1.1}$$

Where T^G is the GNSS total integration time, F_s is the sampling frequency, $C/N_0(\theta)$ is the SNR of the GNSS signal in function of satellite elevation θ, $G_s(f)$ is the GNSS power spectral density and $T^G = 1/\left(2B^G\right)$ is the relationship between bandwidth and integration time.

$$\sigma^U = \sqrt{\frac{1}{8\pi^2 \cdot \beta_f^2 \cdot SNR \cdot n \cdot c}} \tag{1.2}$$

Where c is the speed of light, σ^U is the variance, $\beta_f^U[\,\mathrm{Hz}]$ is the received signal spectral bandwidth, $SNR = E_b/N_0$, E_b is the energy per bit, N_0 is the noise power and n is the total number of averaged ToF measurements.

Therefore, the CRLB for GNSS/UWB can be written as:

$$\sigma = \sigma^U + \sigma^G \tag{1.3}$$

Figure 1.7 shows a significant improvement in positioning accuracy when GNSS combines with UWB, compared to GNSS/cellular and UWB solutions.

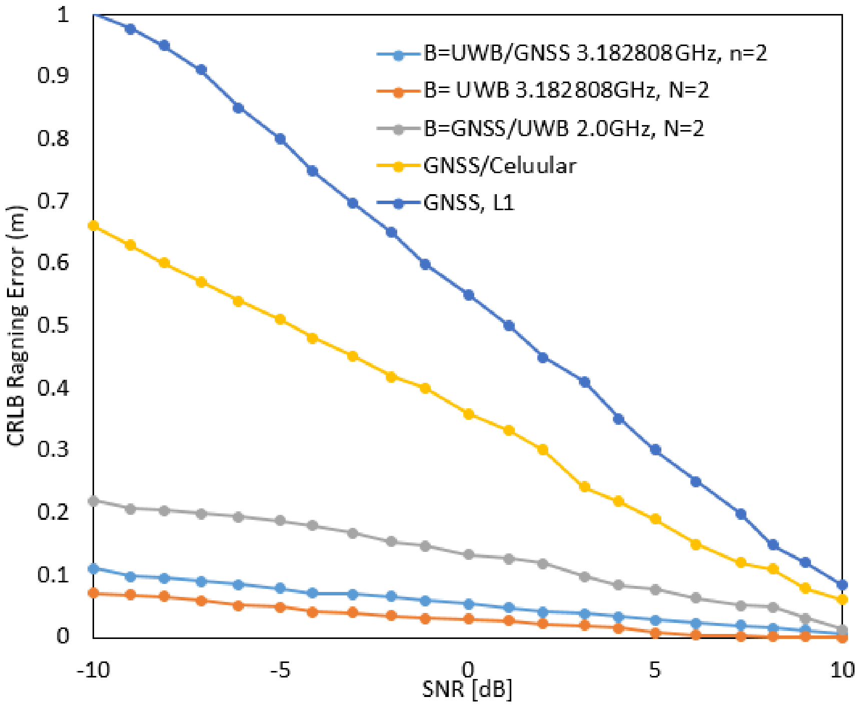


FIGURE 1.7: Cooperation Ranging Errors between GNSS, UWB/GNSS, UWB, GNSS/Cellular Network Lower Bound of Time-of-Arrival for Different Frequency Bands.

Automatic Data Collection and Transfer to the Cloud

Data collection is performed by a group of skilled personals (land surveyors) and local authorities depending on the needs after digital points are collected by the land surveyor(s) and transfer to the cloud. The CSP automatically generates and distributes secrets to all participants in a hierarchical manner in a situation where there is a user authentication mechanism, as shown in Figure 1.8. In a condition without a pre-existing authentication mechanism, I proposed a method for the anchor nodes to securely generate an authentication mechanism based on user location and OHTSSS.

Authentication

In this section, I proposed a two-layer protocol for already exiting land management information systems such as ArcGIS for global positioning systems and non-existing protocols such IEEE 802.15.4 as shown in Fingure 1.8.

Prevention Against Physical Layer Attacks

Recently, the 802.15.4z standard for UWB ranging can achieve security only for short symbol lengths (SSL), thereby limiting the maximum measured distance. On the other hand, it can risk security by using longer symbol lengths. To increase the DBP multiple pulses are generated as shown in Figure 2.6. The UWB preamble scrambled timestamp sequence (STS) was proposed in [25] as a method used to prevent relay attacks in longer DBP. Therefore, 802.15.4z is limited because; different HRP implementations still suffer from attacks. In the literature, they are no clarifications if a fully secure and efficient HRP can be built, and HRP security is proprietary. To prevent relay/replay attacks at

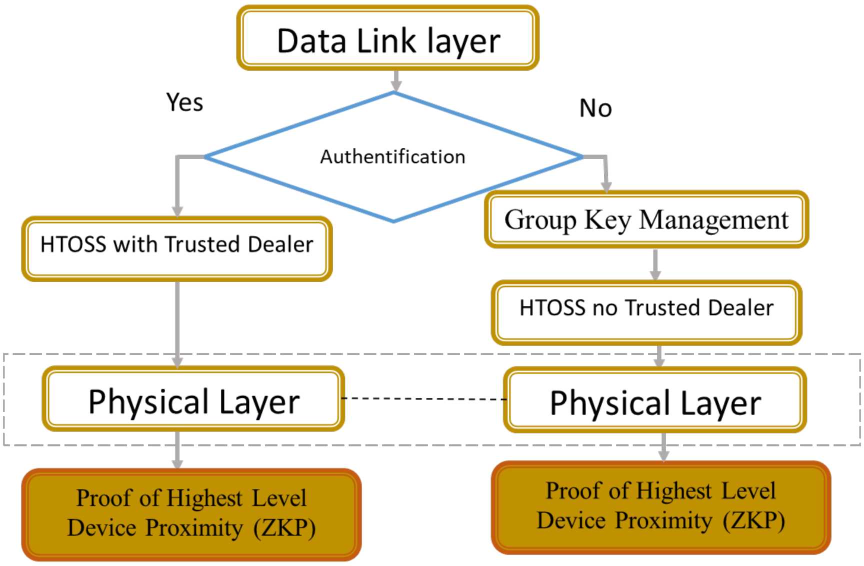
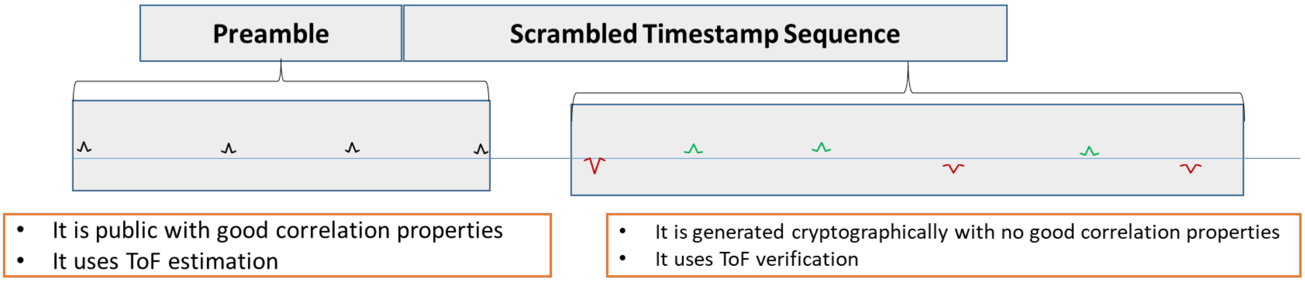
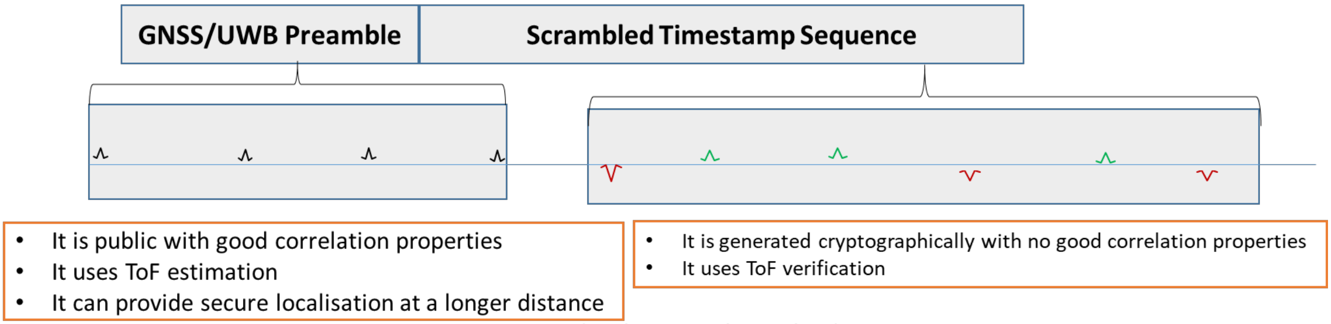

Data Link layer
Yes
No
Authentification
HTOSS with Trusted Dealer
Group Key Management
HTOSS no Trusted Dealer
Physical Layer
Physical Layer
Proof of Highest Level Device Proximity (ZKP)
Proof of Highest Level Device Proximity (ZKP)

FIGURE 1.8: Two layer Authentication Protocol for Land Management and Collection

the physical layer, I proposed a hierarchical network model based on GNSS/UWB and secret sharing, as shown in figure 1.9


Preamble
Scrambled Timestamp Sequence
It is public with good correlation properties
It uses ToF estimation
It is generated cryptographically with no good correlation properties
It uses ToF verification

A. Conventionally Relay Attack Method


GNSS/UWB Preamble
Scrambled Timestamp Sequence
It is public with good correlation properties
It uses ToF estimation
It can provide secure localisation at a longer distance
It is generated cryptographically with no good correlation properties
It uses ToF verification

B. Proposed Relay Attack Method

FIGURE 1.9: Preambel and UWB Random Bit Reordering

Chapter 2

Related works

In this section, related works in hierarchical secret sharing, verifiable secret sharing, homomorphism secret sharing, cadastral map, and zero-knowledge proof are presented.

2.1 Homomorphism Secret Sharing

Homomorphism secret sharing propose in [26] described the property of homomorphism secret sharing. There is a great need to securely store land data information in other to prevent theft of information and leakage. Secret sharing is an important tool with many applications [27], [28] proposed general ideas of secret sharing. Hierarchical secret sharing is the problem in which a secret (b_0) is shared among a group of participants that are partition into levels depending on their authority.[29], [30] present important notions on (t,n) threshold secret sharing. Unfortunately, these schemes cannot prevent malicious behaviours in addition, only a single secret can be shared at a time. In [31] the author introduced the notion of multistage secret sharing base on Lattice and could quantum attacks resistance. The malicious behaviour of participants can be prevented using the concept proposed in [32]–[34]. However, new participants can not be added to the scheme. [35], [36] proposed the possibility of adding new participants into the scheme without changing the secret. Take for example [26], consider two secrets B_1 and B_1, which are shared by polynomials $p(x)$ and $p'(x)$. If I add the shares $f(i) = p(i) + p'(i), 1 \leq i \leq n$, each of $f(i)$ can be viewed as a sub-share of secret $B_1 + B_2$. Suppose that B is defined as the secret domain, and ϕ is defined as the share domain. A set of functions $F_I : \Sigma^t \longrightarrow B$ can be calculated, where $I \subseteq \{1, 2, \ldots, n\}$ and $|I| = t$. Given a random set of t values $B_{i_1}, \ldots, B_{i_i}$, I can define the following equation for the secret k :

$$B = F_I\left(B_{i_1}, \ldots, B_{i_t}\right), \quad \text{for } I = \{i_1, \ldots, i_t\} \tag{2.1}$$

Definition 1. Suppose that they are two operations $\oplus$ and $\otimes$ on the secret domain B and share domain Σ, respectively. There are

$$B = F_I(B_{i_1}, \ldots, B_{i_i})B' = F_I(B'_{i_1}, \ldots, B'_{i_t}) \tag{2.2}$$

then

$$B \oplus B' = F_I\left(B_{i_1} \otimes B'_{i_i}, \ldots, B_{i_t} \otimes B'_{i_t}\right) \tag{2.3}$$

From definition 1, Shamir's polynomial is (+,+)-homomorphic, which indicates that the sum of the secret shares is equivalent to shares of the sum.

2.2 Hierarchical Threshold Scheme (t,n)

Definition 2: Let $\mathcal{A}$ be a set of n participants and assume that $\mathcal{A}$ is composed of levels, i.e., $\mathcal{A} = \bigcup_{i=0}^{m} \mathcal{A}_i$ where $\mathcal{A}_i \cap \mathcal{A}_j = \emptyset$ and $\mathcal{A}_0$ is the highest level for all $0 \leq i < j \leq m$. Let n_l be the number of shareholders associated with level $\mathcal{A}_l$, I can obtain $n = |\mathcal{A}| = \sum_{l=0}^{m} n_l$. Then, I define a threshold U_l for $l = 0 \cdots m$, which satisfies $0 < k_0 < \cdots < k_m$. In addition, I set $\mathbf{k} = \{k_l\}_{i=0}^{m}$, $k = k_m$, and $k_1 = 0$ Then the $(\mathbf{k}, n)$ -hierarchical threshold access structure is

$$\Gamma = \left\{ \nu \subset \mathcal{A} : \left| \mathcal{V} \cap \left(\bigcup_{j=0}^{i} \mathcal{A}_j \right) \right| \geq k_i, \quad \forall i \in \{0, 1, \ldots, m\} \right\} \tag{2.4}$$

A corresponding (k, n)-hierarchical threshold secret sharing scheme is a scheme that realizes this access structure; namely, a method of assigning each participant $u \in \mathcal{A}$ a share $\sigma(u)$ of a given secret S such that authorized subsets $\mathcal{V} \in \Gamma$ may recover the secret from the shares possessed by their participants, $\sigma(\mathcal{V}) = \{\sigma(A) : u \in \mathcal{V}\}$, while the shares of unauthorized subsets $\mathcal{V} \notin \Gamma$ do not reveal any information about the value of the secret.

Next I describe the procedure for Birkhoff interpolation to reconstructs the secret. The elements of $e_{i,j}$ are 0 or 1 and $\sum e_{i,j} = N + 1$. Not that there should be no empty row or namely an i for which $e_{i,j} = 0, j = 0, \cdots, n$. Supposed that, $X = |x_1, \cdots, x_l|$ be a given set of l distinct points where $x_1 < \cdots < x_l$. The Birkhoff interpolation problem of Tassa that corresponds to the triplet (E, X, U_c) and given data $c_{i,j}$ one must find a polynomial f of degree $t - 1$, that satisfies the conditions

$$f^{(j)}(x_i) = c_{i,j}, \quad e_{i,j} = 1 \tag{2.5}$$

For each given set of the triplet (E, X, U_c) there is a unique solution for each given set of $c_{i,j}$ if and only if the determinant of D(E, X, U_c) is different from 0. Let $U_c = \{u_0, u_1, u_2, \ldots, u_{t-1}\} = \{1, x, x^2, \ldots, x^t\}$ where u_k^j the j -the derivative of u_k, for $k = 0, \ldots, t-1$. Then the matrix $A(E, X, U_c)$ is defined as follows:

$$A(E, X, U_c) = \begin{pmatrix} u_0^{j_1} u_1^{j_1} u_2^{j_1} \cdots u_{t-1}^{j_1} \\ u_0^{j_2} u_1^{j_2} u_2^{j_2} \cdots u_{t-1}^{j_2} \\ \vdots \\ u_0^{j_c} u_1^{j_c} u_2^{j_c} \cdots u_{t-1}^{j_c} \end{pmatrix}$$

Then polynomial f(x) $\in R_{t-1}[x]$ is constructed as

$$f(x) = \sum_{k=0}^{t-1} \frac{det(A(E, X, U_{ck}))}{det(A(E, X, U_c))} x^k \tag{2.6}$$

Where $A\ (E, X, U_{ck})$ is obtained from $A(E, X, U)$ by replacing its $(k+1)$ -th column with the shares $c_{i,j}$.

2.3 Multi-Prover Zero-Knowledge Argument (MPZKA)

MPZKA is an interactive proof that permits a group of shareholders or provers (P) to synchronously prove to a verifier (v) many times that they share a secret in such a way that V will not obtain any information about the secret. This group proves is either accepted or rejected by the verifier. MPZKA was first studied in [37]. The zero-knowledge protocol has recently gained significant acceptance in [38]–[40]. In the group base zero-knowledge proof proposed in [41] secret were chosen from finite filed FG(q) and distributed to roadside units (RSU) and onboard units (OBU). In this protocol, a duplicate of each of the secret chosen from FG(q) was made and later on distributed to a group of RSUs (prover). The problem with this protocol is that a malicious RSU can decide to share the secret with another RSU which is not in the group. This problem can be overcome using secure Multiparty Computation that was introduced in [42]. Unconditionally secure multiparty computation (MPC) was equally introduced in [43] and was subsequently studied in the literature of [44]–[46].

My scheme assumes the presence of a trusted center (CSP) that is involved in distributing secret shares to shareholders as presented in the procedure of land parcel registration. After distributing secret shares, the center becomes inactive or closed. The MPZKA scheme relay that a group of provers P_i synchronously prove to a verifier V that they share a secret or that they do not share any secret without revealing any information about the secret.

2.4 Geo-localization Technologies

Generally, geo-localization technologies can be classified into three categories, namely: Global (GNSS such as GPS), regional (cellular) positioning, and local (Local positioning technologies such as Zigbee [47], Wi-Fi [48] Ultra-Wideband (UWB) [49], Radio Frequency Identification (RFID), Bluetooth [50], Pseudolite [51], and so on) positioning techniques, in this research worm, my main point of interest is GNSS and UWB . I can use these positioning technologies in different life scenarios, as presented in the following section. GNSS indicates a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. The receivers then use this data to determine location, which means that GNSS provides coverage of the planet earth. GNSS is managed by different organizations such as US NASA, European GSA, and Japanese JAXA. 2G/3G/4G, 5G mobile communication systems can render canopies environment and indoor location. However, the positioning accuracy is too poor to satisfy most of the requirements because of multipath, interference (Non-Line of Sight (NLOS) [52]), and the poor time synchronization between Base stations (BSs).

2.4.1 GNSS Global Positioning

In General, GNSS systems are easy to use, do not drift, and achieve high accuracy levels. However, they're not perfect. From source to destination, GNSS signals need a clear and uninterrupted view of the sky. However, precise positioning can be achieved when working in the middle of a field and good weather.

FIGURE 2.1: GNSS Positioning Technique

Limitation of GNSS Positioning Techniques

When working under bridges and in tunnels or trying to survey city streets. The accuracy reduces because of obstructions from tall buildings, trees, or in some situations, and you get no measurements at all as shown in the figure

Previous research proposed precise point positioning technology [53], static surveying [54], [55], differential code measurement [56], method of absolute measurement [57] and RTK [58] to reduced positioning error in such environment; however, the positioning accuracy was poor. Mieczysław Bakuła, et. al, analyses the accuracy conditions with limited visibility of satellites using three GPS/GLONASS receivers set up on a particular measurement beam [59]. However, many visible satellites are observable for multi-GNSS positioning, which becomes very cumbersome to mitigate. A method of satellite selection was proposed in [60] to minimize this effect. The primary source of high-accuracy field surveys is (challenging to eliminate) the multipath error[61]. Multipath is the recording of reflected signals by the GNSS receiver. This signal reflection can be of two types. It can reflect the ground that arrived at the receiver's antenna [62] or obstacle standing near the receiver (trees, mountain, tall buildings). The satellite movement and the orbit cost continually satellites geometry change; the multipath impact level depends on the altitude of a given satellite and time. Signals high in the zenith are of less risk to multipath effect compare to low satellites. [63] proposed that at reference stations, measurements can be done in 15-30min cycles in other to minimized multipath error. The required observation time is a disadvantage. In kinematic and rapid static GNSS surveys, the multipart effect was considered the main source of error [64] and increased observation time to several minutes. proposed that the multipath effect can be minimized using several receivers.

GNSS Positioning Equation

The GNSS pseudo-range observation equation is given by

$$\rho_i = R_i + c(\delta t_u - \delta t_i^{sate}) + \varepsilon_i + I_i + T_i \tag{2.7}$$

where δt_u is the receiver clock offset, δt_i^{sat} is the satellite clock offset, I_i is the ionospheric error, T_i is the tropospheric error, $\mathcal{E}_i$ is the measurement noise and c is the speed of light.

The observation equation from m^{th} satellite to receiver can be written as;

$$\begin{aligned} R_{i,j} = & \sqrt{\left(x_{i,j}^{sat} - x_u\right)^2 + \left(y_{i,j}^{sat} - y_u\right)^2 + \left(z_{i,j}^{sat} - z_u\right)^2} \\ & + \omega_e \left(x^{sat} y_u - y^{sat} x_u\right) / c \\ & = \left\| \mathbf{x}_{i,j}^{sat} - \mathbf{x_u} \right\| + \psi_e V \end{aligned} \tag{2.8}$$

where $\mathbf{x}_{i,j}^{sat} = \left[x_{i,j}^{sat}, y_{i,j}^{sat}, z_{i,j}^{sat}\right]^T$, $\mathbf{x_u} = [x_u, y_u, z_u]^T$ and ψ_e is the angular velocity of earth rotation (m/s) Equation (2.7) can be represented in vector form as:

$$\rho_{i,j} = \left\| \mathbf{x}_{i,j}^{sat} - \mathbf{x_u} \right\| + \varepsilon_{ß,j} + I_{i,j} + T_{i,j} \tag{2.9}$$

In [60] a method to subtract tropospheric delay T and satellite clock offset $\delta t_{i,j}^{clk}$ from pseud-orange such that (2.9) become With the availability of multi-GNSS in the sky, a grant number of the satellite can be observed simultaneously, with some having very bad GDOP. Therefore, it becomes vital to select satellites having good GDOP. The absolute value of residual ranging error can be used as an evaluation method to determine satellites with good GDOP, as proposed [60].

$$P_{i,j} = |\rho_{i,j} - \hat{\rho}_{i,j}| \tag{2.10}$$

where

$\hat{\rho}_{i,j} = \hat{R}_{i,j} + c\left(\hat{\delta} t_u - \hat{\delta} t_{i,j}^{sat} + \hat{\delta} t_{syn}\right) + \hat{I}_{i,j} + \hat{T}_{i,j} \cdot \hat{R}_{i,j}$, $\hat{\delta} t_{syn}$, $\hat{\delta} t_u$, $\hat{\delta} t_u$ are the estimated values from all visible satellites and $\hat{\delta} t_{i,j}^{sat}$, $\hat{T}_{i,j}$ are the broadcast ephemeris correct values. The residual ranging error includes ephemeris error, satellite vehicle clock error, positioning error, multipath effect, modeling of the ionosphere and troposphere error, and measurement noise. The positioning accuracy becomes worse if the measurement value of residual ranging error is high. Therefore, if the residual range error meets equation (2.11), then it should be eliminated.

$$P_{i,j} > \alpha + 2\wp \tag{2.11}$$

where $\wp, \alpha$ are the standard deviation (STD) and average residual ranging errors.

The position state $\mathbf{x}$ is in rectangular coordinates so, these coordinates have to be converted from Cartesian to Geodetic coordinates as follows:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} (F_r + h) \cos\varphi \cos\lambda \\ (F_r + h) \cos\varphi \sin\lambda \\ \left\{F_r\left(1 - e^2\right) + h\right\} \sin\varphi \end{bmatrix} \tag{2.12}$$

Where (F_r) is the Earth's ellipsoid meridian radius of curvature, and Meridian ellipse eccentricity is e.

2.4.2 Multipath in wireless Communications

Multipath nullification happens when a multipath signal arrives at the anchor node partially or totally out of phase with the direct signal as shown in figure 2.2. It causes a reduced amplitude response. With a short period of signal pulses, direct signals will arrive before indirect signals. As a result, they are less multipath cancellation effects with UWB signals. UWB, like GNSS technology, is still subject to physics laws for radio frequency signals such as trade-off versus bandwidth. Another issue with UWB is its ranging accuracy that is; UWB provides reliable and precise results regarding relative positioning concerning a local frame, at the cost of covering the working area with expensive antennas, thereby limiting UWB technology only to a relatively small extent outdoor and applicable indoor. On the other hand, GNSS is a cheap technology that offers an adequately accurate localization outdoor worldwide, in terms of a global frame (longitude, altitude, latitude). Using UWB to increase GNSS enlarges navigating and positioning in areas where GNSS typical falters; this is mostly indoors or in hostile signal environments. Because both systems are harmonious, integrating these sensors for precise positioning draws benefits from both types of sensors while reducing their drawbacks. Previous sensor fusion proposed that a particle filter can combine GPS/UWB for and out/indoor scenarios, but there were no descriptions on anchor node placement. Besides, GPS provides low accuracy when compared to GNSS technology [18]. [19] equally shown that they were improvement in combining UWB and GPS. However, precision is also a function of the UWB beacon's location; besides, the estimation was slightly sensitive to the location's initial guess. Finally, [20] uses a single UWB range to increase GPS in hostile environments. The analysis shows a rapid convergence of the Kalman filter positioning and a reduction in Dilution of Precision (DOP) values with the UWB range's augmentation. The goal of this research work can be summarized as follow:

- Show that an integrated GNSS-UWB solution is more accurate and reliable than a GNSS-only solution under conditions with limited access to satellite signals.
- Show that the accuracy depends on anchor node positioning.
- Show a reduction in observation time.

Previours This paper focuses on the probabilistic combination of sensor data acquired from different sources; GNSS global and a local positioning technique like UWB. More precisely, I propose a Monte Carlo (Particle Filter) localization algorithm, representing the target node's position poses using a set of weighted samples (particles). As an advantage, this approaches ability to combine measurements from different sensors while considering their probabilistic behaviors appropriately.

2.4.3 UWB Local Positioning Technologies

Ultra-wideband (UWB) is a radio technology that uses a very low energy level for short-range, high-bandwidth communications across a considerable radio spectrum. UWB has inherited applications in non-cooperative radar imaging. Most current applications target precision locating, sensor data collection, and tracking applications. Since September 2019, mobile phone companies have started integrating UWB chips into high-end smartphones. UWB information is transmitted through a series of baseband pulses instead of the modulated sinusoidal carrier in an impulse signal. On the other

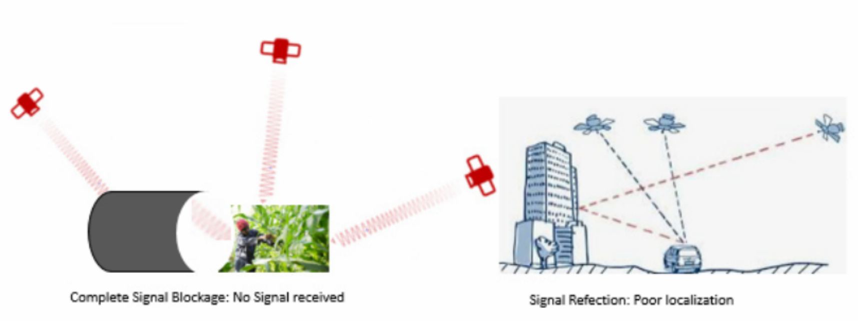

Complete Signal Blockage: No Signal received
Signal Refection: Poor localization

FIGURE 2.2: Effect of Environment of GNSS Signal

hand, multi-carrier UWB signals use a set of sub-carriers. Each of these sub-carriers must not interfere with one another and should overleap. The ability of multi-carrier UWB signals to minimize interference with bands used by different systems sharing the spectrum is advantageous [16]. UWB gives significant advantages in numerous applications, including industrial RF monitoring systems, high-speed LAN, Unmanned Aerial Vehicle (UAV), Intrusion Detection Radars, and Unmanned Ground Vehicle (UGV) precise positioning, Tactical Handheld Radios, and more. Other additional advantages of UWB include;

- With power spread over huge bandwidth, frequency selective fading from multipath/materials is mitigated [17]
- Ranging – very fine precision distance and range resolution.
- Low energy density gives less interference to closer systems and minimal RF health hazards
- Minimal multipath cancellation effects

.

UWB Positioning Equation

In order to compute the user position a minimum of three UWB reference nodes are required for UWB TDOA-based positioning. According to [65] the actual range equation of UWB is given by

$$\rho^{W}_{i,j} = \theta_{i,j} + \vartheta_{i,j} + \xi^{W}_{i,j} \tag{2.13}$$

Where θ_i is the range estimation error, ϑ_i, is the TOA estimation at reference node i, and r^{W}_{i} is the pseud-orange measurements.

$$\begin{aligned} \xi^{w}_{i,j} &= \sqrt{\left(x^{w}_{i,j} - x_{sat}\right)^2 + \left(y^{w}_{i,j} - y_{sat}\right)^2 + \left(z^{w}_{i,j} - z_{sat}\right)^2} \\ &= \left\|\mathbf{x}^{w}_{i,j} - \mathbf{x}_{\mathbf{sat}}\right\| + \psi^{w}_{e} \end{aligned} \tag{2.14}$$

where, ψ^{w}_{e} is UWB positioning error, $\left(x^{w}_{i,j}, y^{w}_{i,j}, z^{w}_{i,j}\right)$ are the coordinates of the ith UWB reference node, and $(x_{sat}, y_{sat}, z_{sat})$ are the satellite coordinate. Repeating steps in section 2.2, I can deduces UWB estimated position as in (11)

2.4.4 Ranging Techniques

Time-of-Arrival (TOA) TOA/TWR DTOA TOA/OWR TDOA Received signal strength (RSS) Angle-of-Arrival (AOA) Direct line of sight Static channel condition Anchor (reference) nodes and the nodes are static when distances are measured. Anchor nodes positions are known to each other.

Assumption with Ranging Techniques

Direct line of sight Static channel condition Anchor (reference) nodes and the nodes are static when distances are measured. Anchor nodes positions are known to each other. Time Of Arrival (TOA) – 1: TOA/TWR – Two way ranging (Single packet exchange)

Time of Arrival (TOA) - 2

TWR with Double packet exchange; known as DTOA (Differential Time of Arrival) DTOA is a modification of TOA/TWR technique, to remove effects of protocol/response delay (turn around time)

2.4.5 Fusion Techniques

Various filtering algorithms have been introduced to date to achieve highly accurate and computationally possible position-ranging techniques that could further enhance localization systems' accuracy. Bayesian filters have been trendy among these proposed filters and are widely used in position-ranging approaches [66]. The Kalman filter gives the optimum solution in a linear system with the Gaussian probabilistic model [67]. Nonetheless, when the system is non-linear, the performance of the Kalman filter degrades and then filters like Unscented Kalman Filter, Extended Kalman Filter (EKF), or Sigma Point Kalman filter come into play. These filters work well when the noise distribution is Gaussian, and the system is non-linear, but still, precise tuning of covariance of the supported probabilistic model is required.

In non-Gaussian noise distribution, sequential Monte Carlo-based filters such as particle filters are gaining attention. They are more robust than the Kalman filters but are computationally more expensive [68]. In addition, they need accurate specifications of the probability distribution model, which can be unknown in most practical applications such as UWB. In such situations, these filters have to make assumptions for the models, and if these assumptions change significantly from the actual model, their performance will be highly degraded. Thus, it is essential to have a more robust filter and broader acceptance in application scenarios. Cost- Reference Particle Filter (CRPF) has surfaced as one of the most reliable filtering algorithms to trade with the ambiguities of the models. CRPF filter does not make any assumptions about the distribution and propagates the particles based on a user-defined cost function [69].

In a discrete state space setting, the problem of filtering is presented as shown in Figure 2.3 It consists of attempting to make the estimated state $\hat{\mathbf{x}}_k$ the closest possible to the real value $\mathbf{x}_k$. Where it state can be calculated using two optimality criterion namely; least square and maximum likelihood.

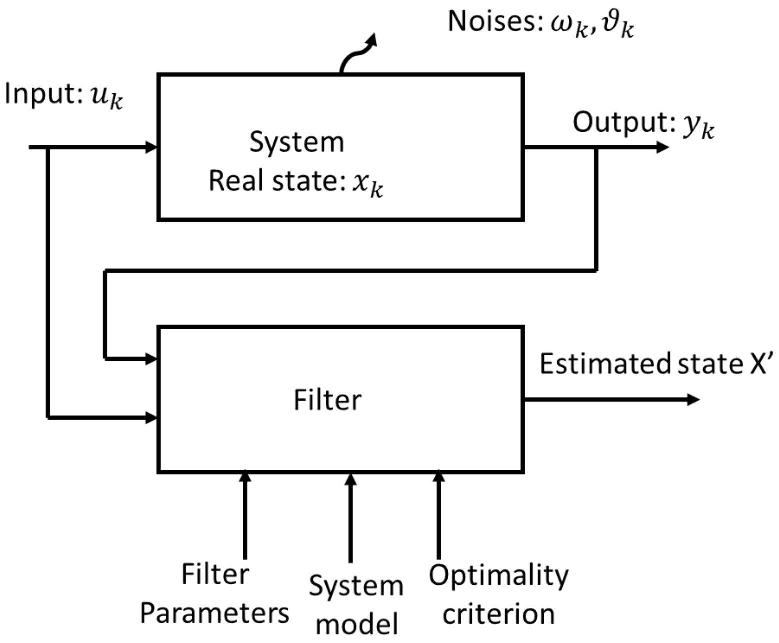


FIGURE 2.3: Properties of Filtering

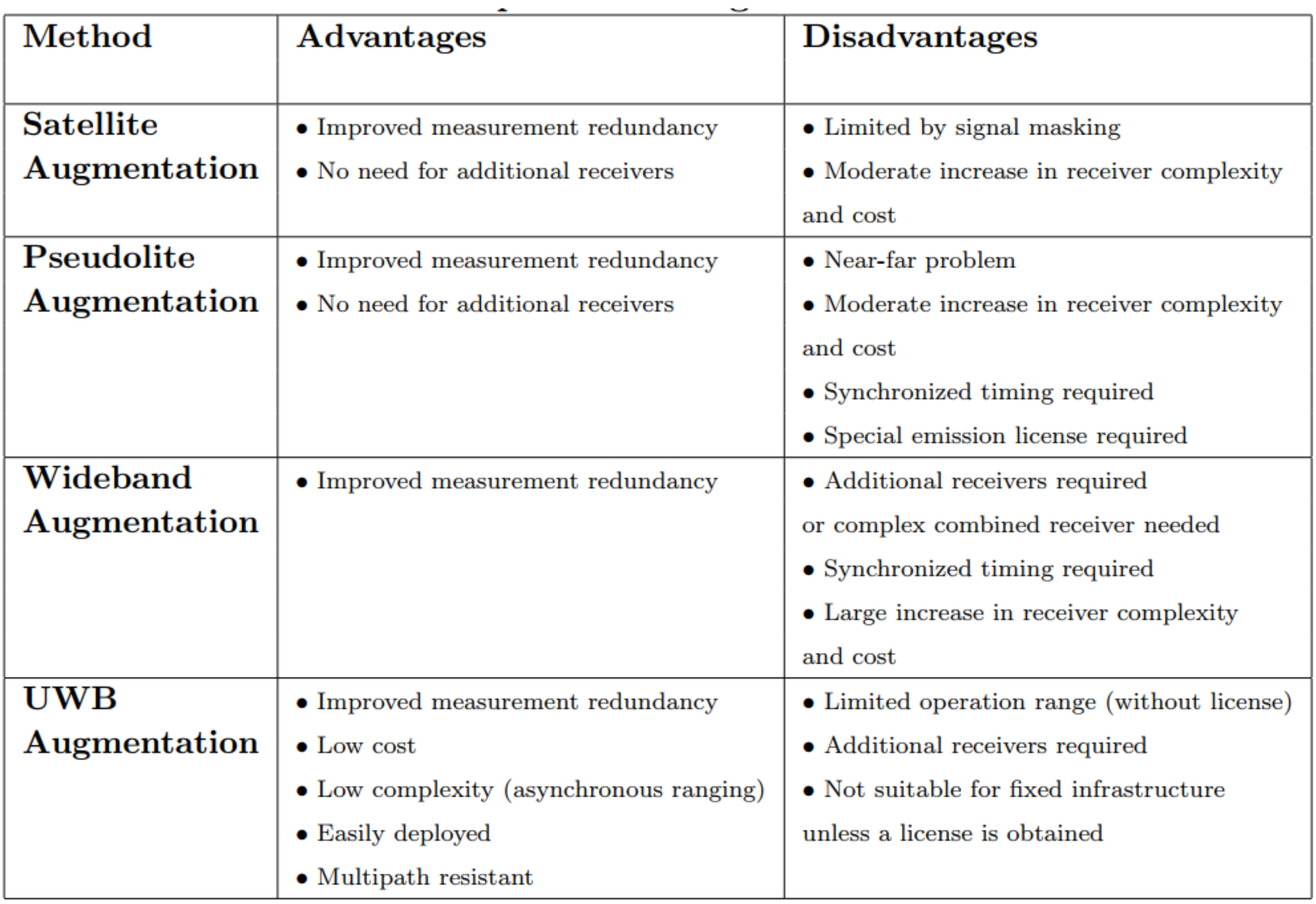
2.4.6 Particle Filter

This is a recursive filtering algorithm use in handling non-linear and non-Gaussian parameter and system state estimation. I employ Particle Filter because the probabilistic observation model of UWB sensors is non-linear. Also, it leads to distributions that can be difficult to approximate by Gaussian, and PF is good for arbitrary distributions, which enable global localization of anchor nodes at start-up. [70]–[72] presented the principle of particle filter algorithm as a non-parametric form of Bayes filter. The state-space generates random samples in groups that depend on the posterior conditional for distributing system state vector. The particle's position and weight are adjusted continuously [73] based on its measured value until the convergence of state quantity.

PFs are suitable to work with almost random sensor characteristics, noise distributions, even non-linearities, and motion dynamics if and only if some likelihood model of their uncertainty can be given. They can simultaneously sustain different hypotheses about the pose of a target node. This ability permits the localization system to track a target node within complex and self-similar scenarios. As particle filters sample the space of possible positions up to a given sampling density, their computational cost can be limited, and they are easy to implement

The following parameters characterize a particle filters; the resampling indicator, the number of particles, and the resampling scheme.

The different resampling schemes are: the multinomial resampling, systematic resampling [74], the residual resampling [75], and the branching algorithm [76]). Experiments have shown that [77] all produce similar results. Therefore, the best choice is to choose the most straightforward algorithm, such as systematic resampling, because it has a minimal variance. The contribution of resampling is real, but it is not good to use it at each step. To decide if redistribution is necessary, one has to calculate the effective numb er of particles and the entropy of the particles system. The results are presented in Figures 2.2 and 2.1 on a filter with N = 1000 particles. I arbitrarily choose the entropy-based estimator. The threshold value compromises the resampling ; $\ln(N/50)$ and, the



Method	**Advantages**	**Disadvantages**
Satellite Augmentation	• Improved measurement redundancy • No need for additional receivers	• Limited by signal masking • Moderate increase in receiver complexity and cost
Pseudolite Augmentation	• Improved measurement redundancy • No need for additional receivers	• Near-far problem • Moderate increase in receiver complexity and cost • Synchronized timing required • Special emission license required
Wideband Augmentation	• Improved measurement redundancy	• Additional receivers required or complex combined receiver needed • Synchronized timing required • Large increase in receiver complexity and cost
UWB Augmentation	• Improved measurement redundancy • Low cost • Low complexity (asynchronous ranging) • Easily deployed • Multipath resistant	• Limited operation range (without license) • Additional receivers required • Not suitable for fixed infrastructure unless a license is obtained

FIGURE 2.4: Comperation Between Different Localization Technologies

TABLE 2.1: Indicator of number of effective particles

Threshold	N/10	N/30	N/50	N/75	N/100
Filter's variance	1.51	1.69	1.75	1.60	1.66
NR*	0.7	0.6	0.56	0.5	0.49

TABLE 2.2: Entropy based indicator

Threshold	$\ln(N/10)$	$\ln(N/30)$	$ln(N/50)$	$\ln(N/100)$	$\ln(N/150)$
Filter's variance	1.46	1.63	1.69	2.01	2.33
NR*	0.69	0.56	0.50	0.50	0.46

filter's variance, has been retained.

The choice of the state estimator: Generally, maximum likelihood and least square methods are used. The last thing to determine is the number of particles. The strategy adopted is to do the simulation with different particles and choose the best compromise between computation time and particles. As shown in TAble 2.3, the number of particles used is 1000. Where NR* (number of resampling) is the number of resampling divided by the running length. $N = 1000$ is the total number of particles.

2.5 Keyless entry systems

An intelligent entry system is an electronic lock that controls access to a vehicle or building without using a conventional mechanical key. The term "keyless entry system" basically meant a lock controlled by a keypad placed at or near the driver's door, which necessitated entering a self-programmed numeric code. The term remote keyless system (RKS), also termed a keyless entry or remote central locking, attributes a lock that utilizes an electronic remote control as a key activated automatically or by proximity a handheld device. They are popularly used in automobiles to executes the functions of a standard car key without physical contact. Within a few meters from the car, pushing a button on the remote can lock or unlock the doors and perform other functions.

The key management system in automobiles has emerged significantly from the original usage of a mechanical key. Today, vehicle manufacturers have migrated to passive keyless entry vision [25], [78] a car automatically opens itself when the person carries a key fob or smartphone is in its proximity. The vehicle can be started only when the smart device is inside the vehicle. The modern, state-of-the-art solution uses a mixture of low-frequency and ultra-high frequency (LF-UHF) channels to realize this dua functioning. Nevertheless, these systems can be subject to early detect/late-commit (ED/LC) attacks [25], these UWB modules are robust to relay attacks. IEEE 802.15.4z − 2020 UWB standard explicitly includes timing information and can resist must multipart effects. But it is still limited because UWB only provides local coordinates of a point, which is a potential security threat to car monitoring service. That is,

TABLE 2.3: The variance of PF (VPF) in function of the number of particles (N)

N	50	100	500	1000	2000	5000	10000
VPF	9.77	4.21	2.15	**1.82**	1.63	1.11	1.04

a company can not have remote control over the vehicle. The IEEE 802.15.4z Enhanced Impulse Radio Task Group (IRTG) is currently tasked by the Car Connectivity Consortium(CCC) to develop more accurate ranging methods for UWB keyless access, which is one of its principal pilot applications. Therefore, to attain a precise position, UWB has to be combined with GNSS technology.

Malicious and false anchor nodes (AN) in positioning are accessed anchor nodes, deliberately sending misleading information to other ANs in the network such as; AN position and AN identity. Types of malicious ANs attacks related to IoT positioning can be paraphrased as follows: Relay/Replay Attack, On-off attack: a malicious AN can transmit incorrect positioning-related data only at random intervals, Conflicting behavior attack: the deceitful node can send partly trustful information (correct IP address) and partially inaccurate information (faking its position), Sybil attack [79], [80]: it refers to malicious AN using more than one IP address to prevent their identification by the unexpected change in identity and Newcomer attack [81]: an anchor node earlier identified as malicious can modify its IP and join the network again as a new anchor node.

2.5.1 Distance Bounding Protocol

Distance Bounding Protocols protocol (DBP) faces different scenarios/attacks such as Mafia fraud, distance fraud, distance hijacking, terrorist fraud, etc. In general, a verifier (V) and a prover (P) want to measure how far they are located from each other while trusting themselves, an attacker (A) tries to manipulate the process as shown in figure 2.5. V and P share a preshared key, and they equally agree on some cryptographic materials that permit them to perform a challenge-response protocol and measure the round-trip ToF. For an A sitting in the middle and tries to reduce this measured distance, it is difficult because of secure cryptography for short DB. This attack model is simple to analyze compared to some DB protocols presented in the literature based on some unprovable assumptions because of the physical layer.

2.5.2 Pedersen's (n, t, n) secret sharing

In this section, I briefly introduce Pedersen's (n,t,n) secret sharing scheme [82]. In this scheme, shareholder can cooperates to distribute and reconstruct the secret without the present of a trusted dealer as defined below:

Definition 1 : $A(n,t,n)$ secret sharing. Let AN_i be a set of n anchor nodes (participants) $i = 1,..,n$ Each AN wants to cooperate in other to generate and share a master secret MS. And AN_i can randomly select a sub-secret $S*_i$ that satisfies $MS = S*_1 + S*_2 + \ldots + S*_n$. Each AN_i can share the sub-secret $S*_i$ with other anchor nodes by generating sub-shares $s*_{i,j}$, for $j = 1,2,\ldots,n$ and,$i = 1,2,\ldots,n$, using Shamir's secret sharing scheme. Next, each anchor node calculate it master secret share s_i by combining all sub-shares for $i = 1,2,\ldots,n$, and $j = 1,2,\ldots,n$ received from other anchor nodes. Each anchor node performs the following steps to generate it master secret share:

- Step 1. Each anchor node makes a random selection of a sub-secret $S*_i$ that satisfies the master secret $MS = S*_1 + S*_2 + \ldots + S*_n$
- Step 2. The dealer AN_i constructs a random polynomial $f_i(x)$ of degree $t-1$ that satisfies $S*_i = f_i(0)$ there after, AN_i utilizes Shamir's (t,n) secret sharing scheme to generate sub-shares, $s*_{i,j} = f_i\left(x_j\right)$, for $j = 1,2,\ldots,n$ and $i = 1,2,\ldots,n$. Then,

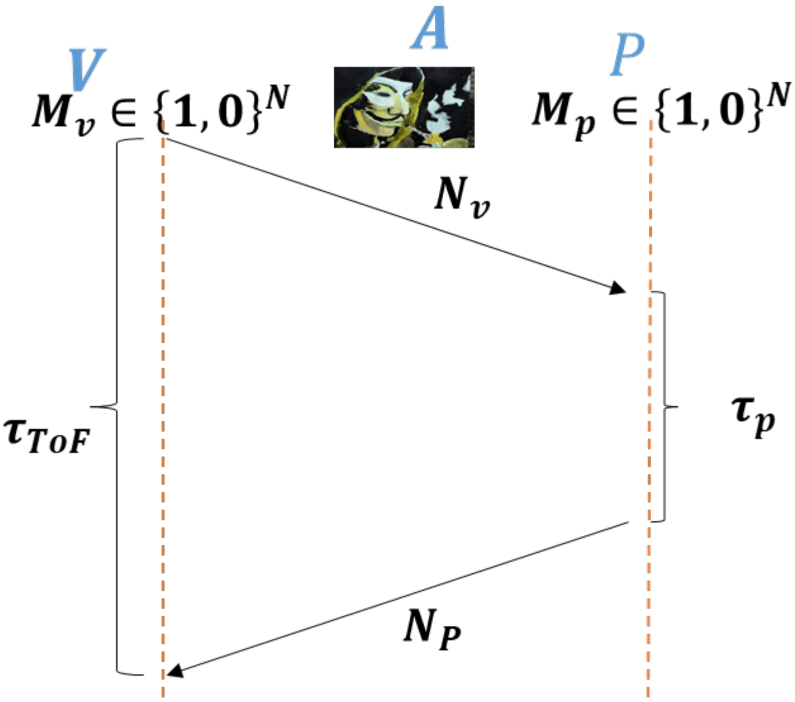


FIGURE 2.5: Logical Layer: Distance Bounding Protocol

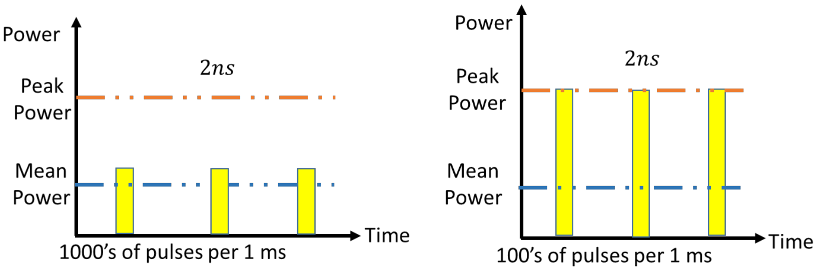


Fig. (a) High Rate Pulse (Multi-Pulse)/bit for Long DB

Fig. (b). Low Rate Pulse (LRP) (Single-Pulse)/bit for Short DB

FIGURE 2.6: Distance Bounding LRP and HRP Representation

AN_i distributes each $s*_{i,j}$ to other dealer AN_j, for $i = 1, 2, \ldots, n$, and $j = 1, 2, \ldots, n$, and $j \neq i$

- Step 3. Each AN can generate the master share $s*_i$ by computing $s*_i = \sum_{j=1}^{n} s*_{j,i} = \sum_{j=1}^{n} f_j\left(x_i\right)$.
- Step 4. Given any group of $t \geq t-1$ master shares, the master secret MS can be reconstructed using the Lagrange interpolation polynomial.

Chapter 3

Integrated GNSS/UWB Positioning using Particle Filter

3.1 Introduction

Global navigation satellite system (GNSS) is the must use relative positioning technology today for geo-positioning. However, this positioning method is not suitable for indoor or dense urban environments because the positioning accuracy is greatly affected by obstructions from tall buildings and trees that can cost the deviation of signals. On the other hand, Ultra- wideband (UWB) is a local positioning technology used for local measurements in a high multipath environment. The focus of this section is the integration methodology between GNSS and UWB (GNSS/UWB) for outdoor positioning ToF/TDoA, and I equally proposed a method for anchor notes positioning used to determine the target node coordinates. Simulation results with Matlab showed that the combination of GNSS/UWB was a quite efficient technology for the environment with very poor satellite visibilities and allowed for reliable millimeters accuracy. The coordinates of each point were obtained in less than 2 minutes of the observational sessions.

I consider a set of anchor nodes (UWB radios mount on a GNSS receiver) position, as presented in fig. 3.1 arrangement 2. These anchor nodes use TDoA to measure the mobile handset position. The land surveyor moves from one point to another, collecting digital land points and an embedded processor to signal particle filter processing. The mobile handset held by the land surveyor equally contains a GNSS receiver, a UWB TOA transceiver.

Next, I derive the equations of my particle filter. Let z_t, v_t, s_t denote the observation for any given time step t, mobile user action and system state respectively. However, I are interested in the target pose. Unknown biases are used to augment the system state b_{kk-1}^{N} of each UWB beacon, where N is the set of beacons which determine 3D position B_{kk}^{N}. Knowing that s_t evolves as a Markov chain, I can write my estimation problem as:

$$\begin{aligned} & p\left(s_t \mid v_{1:t}, z_{1:t}\right) \propto p\left(z_t \mid s_t, v_{1:t}, z_{1:t-1}\right) p\left(s_t \mid v_{1:t}, z_{1t-1}\right) \\ = \quad & \underbrace{p\left(z_t \mid s_t\right)}_{\text{Obeervation model}} \quad \int \underbrace{p\left(s_t \mid s_{t-1}, v_t\right)}_{\text{Evolution model}} p\left(s_{t-1} \mid v_{1:t-1}, z_{1:t-1}\right) d s_{t-1} \end{aligned} \tag{3.1}$$

Considering that samples are drawn from the system transition model,

$$q\left(s_t \mid s_{t-1}, v_t, z_t\right) = p\left(s_t \mid s_{t-1}, v_t\right) \tag{3.2}$$

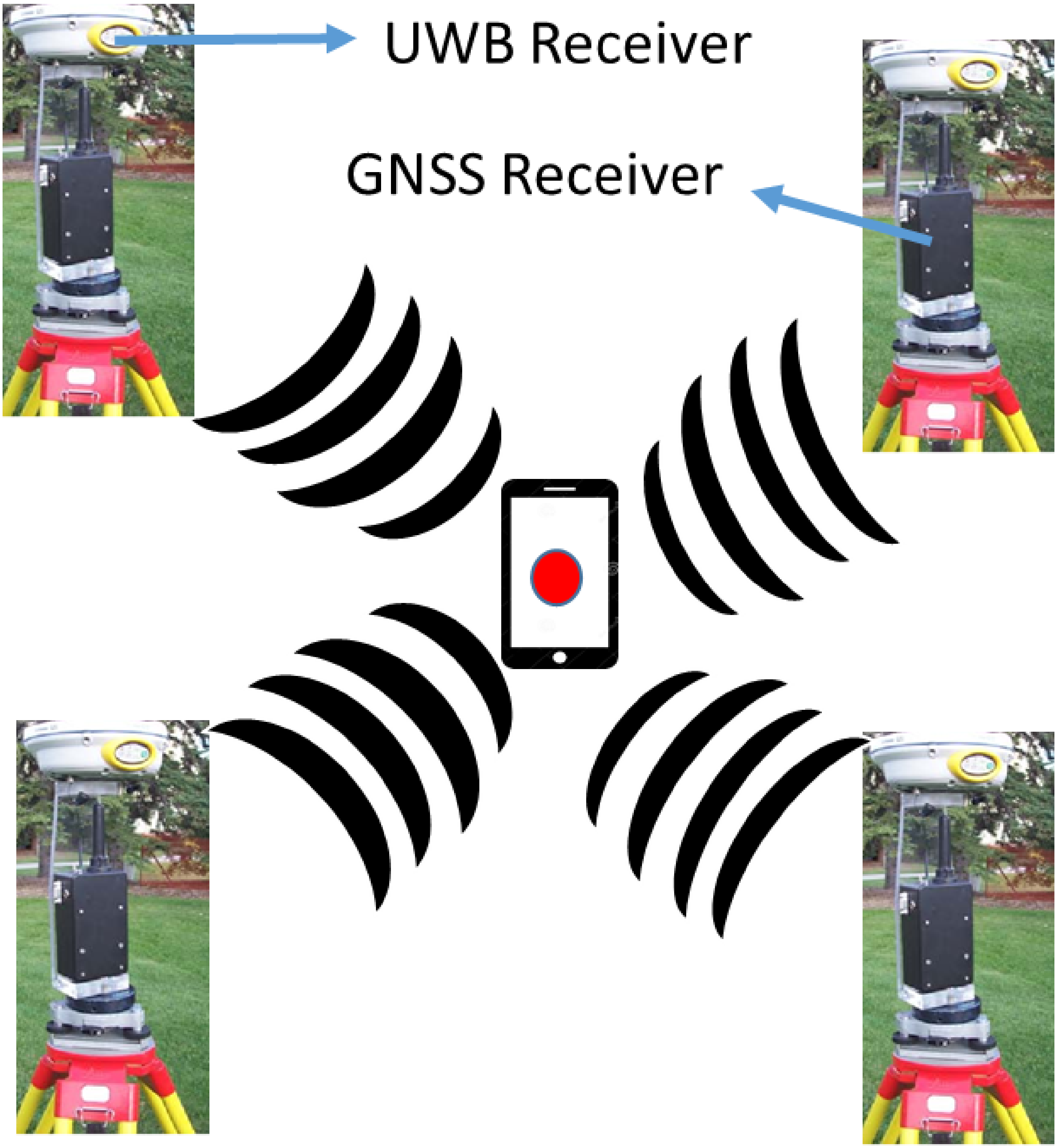


FIGURE 3.1: live view of GNSS/UWB surveying based on my proposed method.

The important weight can be updated as

$$\omega_t^{i]} \propto \omega_{t-1}^{\{i]} p\left(z_t \mid s_t^{[i]}\right) \tag{3.3}$$

I consider that the observation z_t contains GNSS reading and UWB range reading at a time step t. The observation variables can be defined as:

$$z_t = (z_t^{GNSS,1}, \ldots, z_t^{GNSS,N}, z_t^{UWB,1}, \ldots, z_t^{UWB,M}) \tag{3.4}$$

Considering that the random error of each of the measurements are independent, the observation likelihood can be summarised as:

$$P\left(z_t \mid s_t\right) = \prod_{k=1}^{N} P\left(z_t^{GNSS} \mid s_t\right) \prod_{k=1}^{N} P\left(z_{k,t}^{UWB} \mid s_t\right) \tag{3.5}$$

The position of each UWB can be appropriately modelled by a Gaussian distribution obtained from GNSS satellites as

$$p\left(z_t^{GNSS} \mid s_t^{[i]}\right) = \mathrm{N}\left(\zeta_t^{[i]W}; z_t^{GNSS}, \Sigma_t^{GNSS}\right) \tag{3.6}$$

where Σ_t^{GNSS} is the number of satellites observed at each instant (t), and $\zeta_t^{[i]W}$ is the position of each UWB. The sensor model is accountable for the Gaussian noise only because the bias $b_{k,t}^{[i]}$ is jointly estimated to the system state:

$$p\left(z_{k,t}^{UWB} \mid s_t^{[i]}\right) = \mathrm{N}\left(\mathbf{x} + b_{k,t}^{[i]}; z_{k,t}^{UWB}, \epsilon_{UWB}^2\right) \tag{3.7}$$

where $\mathbf{x}$ is the target position and ϵ_{UWB}^2 is the positioning error.

Denote $\mathcal{N}^{(i)}$ as the set of AN of the target, $M^{(i)}$ as the number of visible satellites, and k is the GNSS output time. I now formulate the integrated positioning as follows: find the posterior target distribution having state $\mathbf{x}_k$ with the information collected by GNSS/UWB as shown in (5.2)

$$\Psi(\mathbf{X}_k) = p(\mathbf{X}_k | \zeta_{1:k}), \quad \forall i \in \mathcal{M} \tag{3.8}$$

where Ψ is the collected information at corresponding time. $\zeta_k^{(ii)}$ includes the GNSS and UWB measurement of AN, $i\left(\zeta_{G,k}^{(i)}\right)$, and $\left(\zeta_{W,k}^{(i)}\right)$, respectively. Then, the $\mathbf{X}_k$ which makes a maximum with $\Psi\ (X_k)$ is the integrated position. $\Psi\ (\mathbf{X}_k)$ can be expressed in (5.11) as shown at the top of the next page.

3.2 Anchor node positioning

Dilution of Precision (DoP) **dpop**, **gdop**, **dop** This is the measure of the quality of GPS position base on the geometric of the satellite use to compute target's position. Positioning accuracy depends on the DoP value, the greater the value the higher is the positioning error. In general, at list four satellites are required for position with one satellite directly overhead and the other three equally space close to the horizon.

```
Algorithm III:

Time slot 0 is the initial distribution
$\hat{\mathbf{X}}_k^{(l)}$ is the estimate
1. For each particle $i = 1, 2, 3 \ldots, N_P$, sample the initial state $PX_{X0}^{(N^{(i)})}$ from the initial distribution $p(\mathbf{X}_0^{(N^{(i)})})$ and the different error variances.
2. Calculation and normalization of the weights.
3. for time slot $k = 1, 2, \ldots$ do
    4. Use the important distribution to sample the particles of time slot $k$ $P\mathbf{X}_k^{(N(i))}(m) \sim q(\mathbf{X}^{(N(i))} \mid \mathbf{X}_{k-1}^{(N(i))})$
    5. In my simulations, I model the ionospheric, PDoP , GDoP as in (??), (3.11) and (x) respectively, I also assumed that other errors (tropospheric, multipart, interference and clock) are lumped together in zero-mean additive Gaussian noise constant $\epsilon_{\text{noise},i,k}^2$ variance (here I took $\epsilon_{\text{noise},i,k} = 2$m because the sum of clock, tropospheric, and orbital errors are below this range). Average the $\sum \epsilon$ over the number of Monte Carlo iterations. If this number is sufficiently high, then a lower bound on the performance with any GNSS/UWB geometry is achieved;
    6. Calculate the weights: $\omega_{p,k}^{(N(i))}(m) \propto p(\xi_{G,k}^{(i)}, \hat{X}_{k-1}^{(N(i))}, \xi_{W,k}^{(N(i))} \mid X_k^{(N(i))})$
    7. Normalize the weights: $\omega_{p,k}^{(N(i))}(m) = \omega_{p,k}^{(N(i))}(m) / \sum_{m=1}^{N_p} \omega_{p,k}^{(N(i))}(m)$
    8. Resampling and update the set of the particle $PX_k^{(N(i))}(m)$ then the weights become: $\omega_{p,k}^{(N(i))}(m) = \frac{1}{N_p}$
    9. Project the particles to the $\hat{X}_k^{(i)}$ dimension, such that the new marginal particles are $PX_k^{(i)}(m)$. Then, the integrated state become $\hat{X}_k^{(i)} = \frac{1}{N_p} \sum_{m=1}^{N_P} PX_k^{(l)}(m)$
9. end for
```

TABLE 3.1: GNSS/*UWB* Integrated Positioning by Particle Filter

DoP is of the following types: Geometric dilution of precision (GDoP) it is the uncertainty of all parameters (clock offset, latitude, longitude, height), position dilution of precision (PDoP) it is the uncertainty of 3D parameters (longitude, latitude and height) it is a combination of both HDoP and VDoP, horizontal dilution of precision (HDoP), vertical dilution of precision (VDoP) and time dilution of precision (TDoP). Satellite from four compass quadrant will provide a good HDoP and satellite from less than four quadrant will provide a poor HDoP. Using satellites which are well spread out will provide good VDoP while satellites that are located low on the horizon will provide poor VDoP. In this section, I adopt the GDop positioning for satellite to UWB and the principle of PDoP for UWB to target positioning as I are much interested in the [x, y, z] coordinates of the target.

a Fig.4.4. The horizontal axis represents the standard deviation of the ranging error, and the vertical axis is the positioning error. It was found that positioning accuracy of Arrange 1 which is the optimum arrangement by PDOP is high. To guarantee that the target well get continuous accuracy positioning, I must make sure that the target should not move out of range and that a maximum number of AN are placed such that the distance between the target and ANs is not greater than parameter $\lambda_{\max}$, I start by defining some useful notations;

TG	is the target
$\lambda_{\max}$	the maximal spacing constraint
$TG = (x_u, y_u, z_u)$	the location of target TG
$b = (x_c, y_c, z_c)$	the location of AN
b^*	the number of AN
A	is the coverage area

Anchor nodes placement can be represented as a coverage area, such that $g = (L_1 \cup L_2, A)$, where $L_1 = TG, L_2 = b$. $(TG, L) \in A, \iff \exists TG = (x_u, y_u, z_u)$, such that $c = (x_c, y_c, z_u) \in b$, and $\sqrt{(x_u - x_c,)^2 + (y_u - y_c)^2 + (z_u - z_c,)^2} \leq \lambda_{\max}$. As shown in figure 3.3. In [65] it was proven by computer simulation that an increase in the distance from one AN to another reduces positioning error why closer ANs further increases the positioning error. Considering this critical fact, I proposed the following UWB/target error model base on the Dilution of Precision (DoP) technique: Here, I defined the following matrix: considering the unit vector from the target node to AN direction.

$$A = \begin{bmatrix} \frac{(x_2^G - x_u)}{r_2^G} & \frac{(y_2^G - y_u)}{r_2^G} & \frac{(z_2^G - z_u)}{r_2^G} & 1 \\ \frac{(x_3^G - x_u)}{r_3^G} & \frac{(y_3^G - y_u)}{r_3^G} & \frac{(z_3^G - z_u)}{r_3^G} & 1 \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} \tag{3.9}$$

let the matrix h be

$$h = \left(A^T A\right)^{-1} \tag{3.10}$$

then, PDOP can be expressed as

$$PDOP = \sqrt{h_{11} + h_{22} + h_{33}} \tag{3.11}$$

The smaller the value of PDOP, the better is AN arrangement with higher positioning accuracy. Therefore, to achieve high positioning accuracy, the target node will be at the origin, and the receiver AN centered on the hemisphere. Since it is difficult to find a combination of four (x_i, y_i, z_i) that minimizes (3.11), spread the virtual particles on the hemisphere and randomly add particles. Take out and compare the respective PDOPs to find the optimum placement. As shown in figure 3.2, I represent in the polar coordinate system for simplicity. The optimum particles were selected from the particles sampled at $\phi = 30°$ and $\alpha = 30°$. In addition to the optimal arrangement, a graph that randomly places two patterns, and a ranging error is caused to evaluate the positioning accuracy is a 3.4. The horizontal axis represents the standard deviation of the ranging error, and

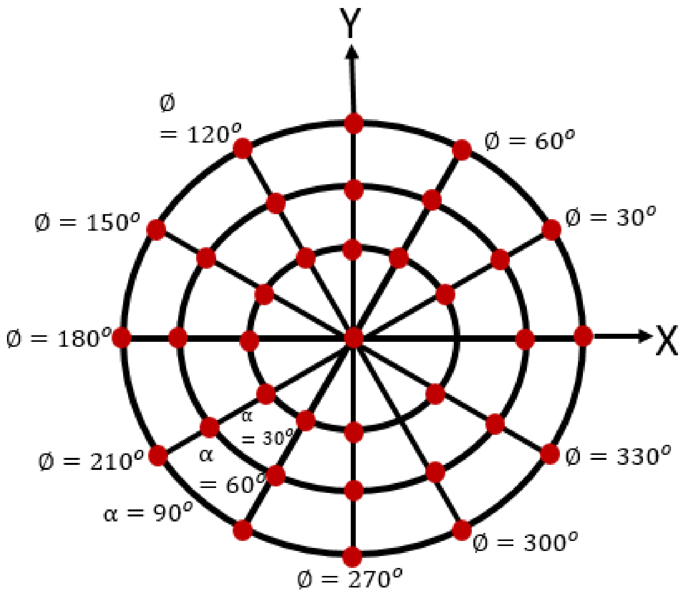
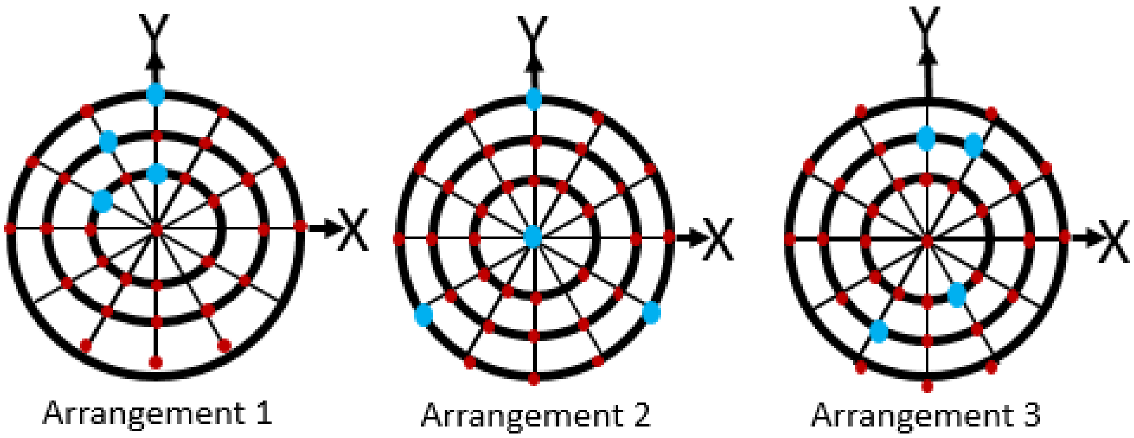


FIGURE 3.2: Virtual Scattering of Particles on the Hemisphere

the vertical axis is the positioning error. It was found that positioning accuracy of Arrange 2 which is the optimum arrangement by PDOP is high. In addition to the optimal arrangement, a graph that randomly places two patterns, and a ranging error is caused to evaluate the positioning accuracy is

3.2.1 Positioning Error Model

The main performance condition in a ranging system is its accuracy, commonly characterized by the root mean square error (RMSE). RMSE indicates the difference between the real and estimated position of a target node. It can be calculated by expressing the estimated point in the latitude-longitude-height (LLH) coordinates using the origin's



Arrangement 1 Arrangement 2 Arrangement 3

FIGURE 3.3: AN optimal placement and random placement

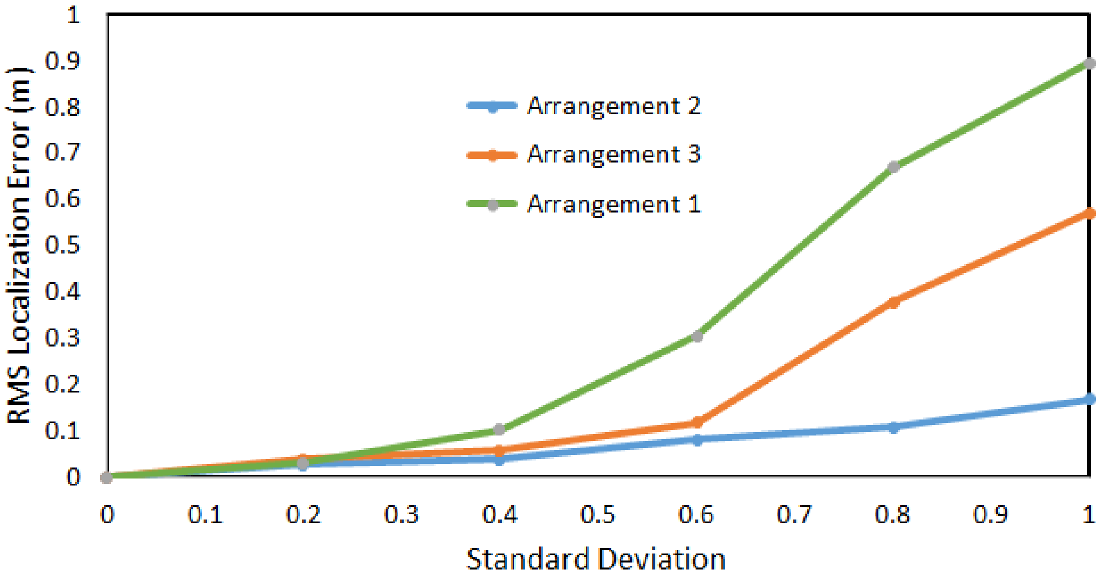


FIGURE 3.4: Difference in positioning error due to AN arrangement

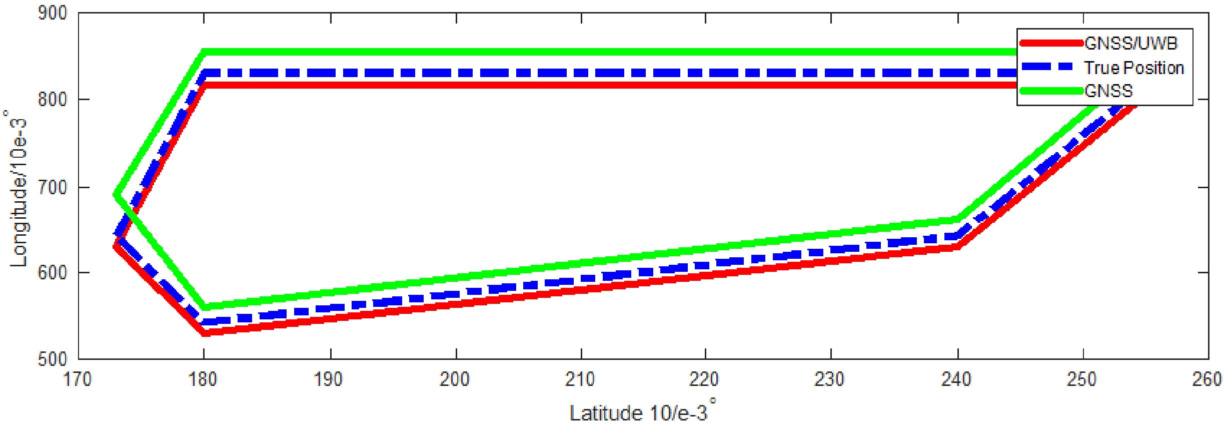


FIGURE 3.5: Trajectory for various positioning schemes with AN arrangement 3

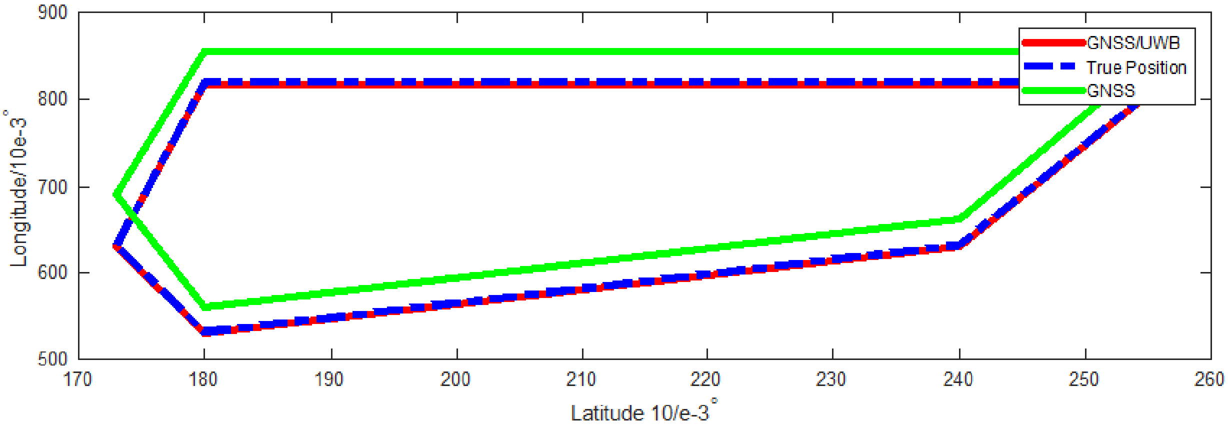


FIGURE 3.6: Optimized GNSS/UWB Positioning with AN arrangement 2

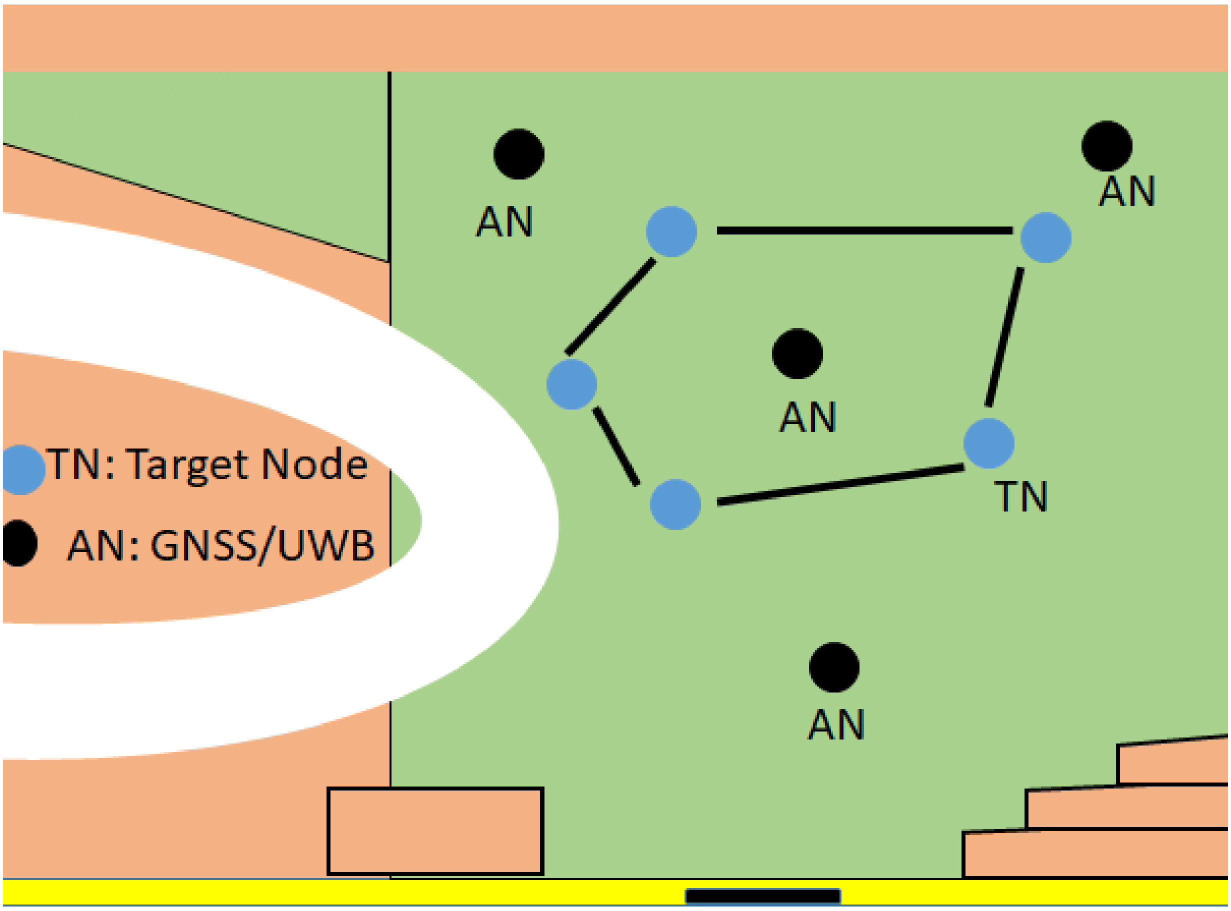


FIGURE 3.7: The target node will stop on the blue dots and travel along the trajectory. The blue dots designate positions that have been surveyed.

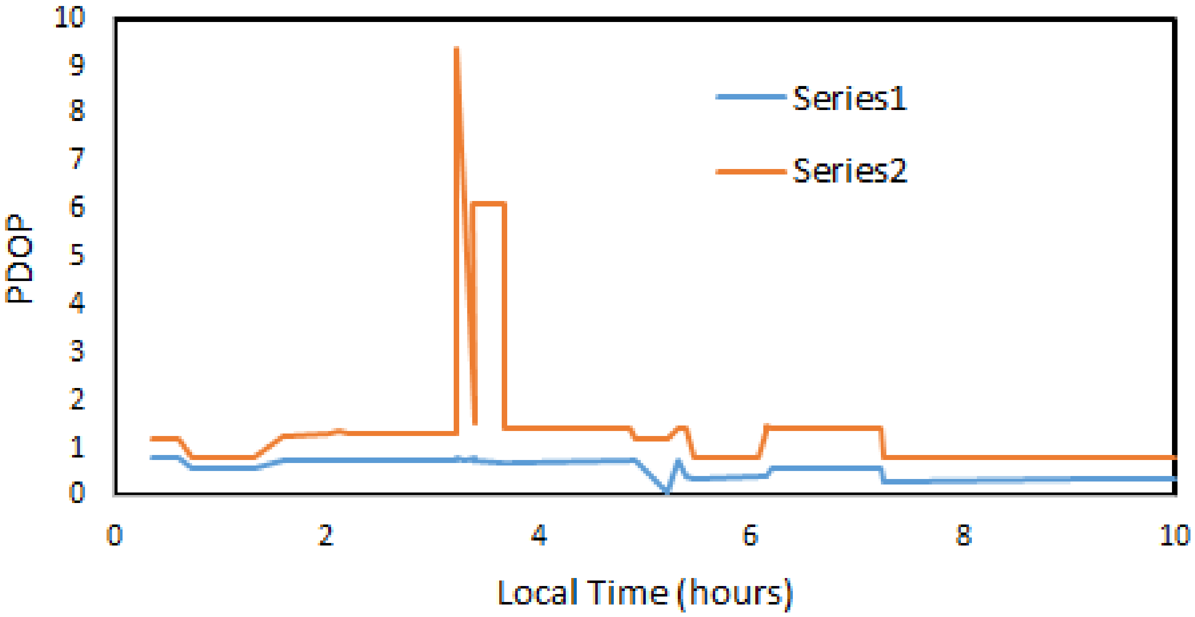


FIGURE 3.8: PDOP for various positioning schemes

true target node position. The height error is given by

$$Horizontalerror = \sqrt{La^2 + Lo^2} \tag{3.12}$$

Where La and Lo and the latitude and Longitude errors, respectively. The height RMSE is given by

$$\text{HRMSE} = \sqrt{LoRMSE^2 + LaRMSE^2} \tag{3.13}$$

where $LoRMS$ and $LaRMSE$ is the latitude and longitude error respectively.

The optimal positioning error variance is the average some of various errors presented above is

$$\epsilon_{av}^2 = \frac{\epsilon_x^2 + \epsilon_y^2 + \epsilon_z^2}{3} \tag{3.14}$$

where

In the same manna, I adopt GDoP for satellite to UWB position as follows:

$$GDOP = \sqrt{\frac{0.5l_1^3 - 1.5l_1l_2 + l_3}{3l_4}} \tag{3.15}$$

where where l_1, l_2, l_3 is the first, second, and third degree power sum The author whet further to prove that the lowest GDoP can be achieved if one satellite have the highest elevation and the other satellites are distributed homogeneously with a low elevation.

3.2.2 Optimization Model

In equation (3.6), only the Gaussian noise was considered as the main source of error. In this section, I further model other sources of errors to optimize positioning accuracy. Such that (3.6) become

$$p\left(z_{k,t}^{UWB} \mid s_t^{[i]}\right) = \mathrm{N}\left(\mathbf{x} + b_{k,t}^{[i]}; z_{k,t}^{UWB} \sum \alpha^2\right) \tag{3.16}$$

where $\mathbf{x}$ is the target position and ν^2 is the positioning error, and $\sum \alpha^2$ is the sum of different error sources analyzed above.

Denote $\mathcal{N}^{(i)}$ as the set of AN of the target, $M^{(i)}$ as the number of visible satellites, and k is the GNSS output time. I now formulate the integrated positioning as follows: find the posterior target distribution having state $\mathbf{x}_k$ with the information collected by GNSS/UWB

3.3 Simulation and Experiment of My Proposed Methodology

In order to test my proposed method for land survey, I have carried out computer simulation within a mixed mountain, dens urban and forest scenario, combining UWB and GNSS readings. I assume that all the GNSS systems have, on average, a similar geometry configuration of all the available N_{sv} satellites per system, number of particles is 1000, number of UWB is 4, the field is $100x100x100m$ and standard deviation of moving error 0.5m.

In my simulation, four GNSS/UWB receivers where placed as show in fig. 3.3 to cover the environment under analysis. During the simulation data was simultaneously collected from the GNSS/UWB receivers to determine the position of the anchor node as it moves from one point to the other collecting digital land points. In this analysis I compare three different situations;

1. A mixed environment with anchor nodes position according to arrange 1, arrangement 2 and arrangement 3
2. Analysis the positioning accuracy of GNSS/uwb and GNSS only environment
3. Time taking by the target node using GNSS only and GNSS/UWB to determine it position

The optimal positioning arrangement in fig. 3.4 exiting at the origin is Arrangement 2 with three AN placed at the vertices of an equilateral triangle on the ground and the other placed at the zenith. Fig. 3.5 shows target node trajectory in hostile conditions comparing with two different solutions and with anchor node position as in arrangement 3. In the figure, the green and red solutions show the difference between augmenting GNSS with and without UWB measurements, and the blue lines show the true position of the target node. It can be seen that GNSS/UWB is more accurate compare to GNSS only solution. Fig. 3.6 shows the optimum placement of the anchor node as in arrangement 2. It can be clearly seen anchor node placement significantly affects positioning accuracy. In Fig. 3.7 blue dots designate locations where the target node is stopped on along the trajectory. The Position Dilution of Precision (PDOP) solution in fig. 3.8 GNSS/UWB ranges has the lowest PDOP values. At about 3, GNSS spikes up to over 9, while the solution with GNSS/UWB does not observe such a dramatic increase. This can be attributed to the fact that the target node was in the densest environment. However, GNSS/UWB was able to weather this obstruction shows that my proposed GNSS/UWB gives a stronger geometric strength on positioning accuracy.

3.4 Conclusion

This paper has implemented and evaluated a probabilistic framework for a land survey that merges different sensory sources. Based on the particle filter, my approach considers UWB, GNSS, and the combination of both technologies to reliably estimate a target node that moves from one point to the other, collecting digital land points in outdoor scenarios. Because UWB signals have characteristics that enable them to range accurately high multipath and indoor conditions, its combination with GNSS is both beneficial and complimentary. The RMS error for the coordinate determination was 0.012 m, 0.017 m 0.023 m for the northern, eastern, and height, respectively. my proposed method performed much better, with 91% of the reliablity also it considerably reduced systematic errors and allowed all gross errors to be eliminated; however, this combination resulted in obtaining reliable coordinates with millimeters accuracy. my proposed method permits a target node to rapidly and accurately collect the coordinates of a point. Results from computer simulation have been presented, proving the suitability of the proposed approach for land survey.

Chapter 4

Hierarchical threshold outsource secret sharing and interactive proof scheme: The care study of land conflict

4.1 Introduction

In this chapter, I present a model for ownership proof of digital land certificates as follows:

i) I start by proposing an innovative secret sharing scheme, as shown in figure 4.1. During ownership transfer (selling or inheritance for example) the land certificate is verified to convince the buyer that the land certificate presented is from a bonafide certificate. In my proposer, secret shares are distributed to dissimilar levels of shareholders (state authorities, land owner, and neighbours). The shareholders can get the secret justly with a small amount of operations. Costly computation is outsourced to a cloud service provider (CSP) and the CSP can gain no information about the secret. In addition, the reputation system can successfully prevent shareholders from colluding with the server.

ii) Zero-knowledge interactive proof scheme is use during the resolution of a land dispute.

When compared with earlier schemes, my proposed scheme has the following advantages:

(i) The scheme can accurately check the malevolent behavior of shareholders or the server.

(ii) Costly computing is outsourced to a CSP. With the CSP computational power, it can execute complex verification and homomorphic encryption operations, and the CSP will obtain no information about the secret.

(iii) Through a combination with the zero-knowledge protocol (zkp), a proposed interactive proof scheme using HTSS (hierarchical secret sharing scheme) which can Counter-attack collusion between the shareholders and the server. In addition, ZKP proof of ownership competes with the state of the act in terms of security guarantees and performance. That is, my approach demonstrates proof of ownership without revealing any information about the secret that was distributed to shareholders.

iV) Share holders can be added and remove from the scheme.

I describe preliminaries in section II. In section III, I construct zero-knowledge interactive proof scheme base on outsourcing HTSS. In section IV, I indicate the security of my proposed scheme and in section V, I compare my scheme with conversional schemes. Finally, in section V, I present the conclusion of my proposed scheme.

Cadastral maps are certificate-having law forces held by the land creditor. It described the geographical location of cadastral, boundary points, boundary lines, and the adjacent relationship between cadastral. Da Bing Yang, et. al. proposed that land mapping was a necessary complement of land certificates' records and addressed the importance of handling land ownership certificates [83]. A method to improve the digital map's reliability and accuracy using GPS/INS based low-order EKF has been proposed. The accuracy of cadastral mapping is a critical technology in the establishment of a cadastral management system. Cadastral mapping is a combination of spatial data and attributes data. In practice, Static and Real-time Kinematic (RTK) positioning is used in GPS surveys. Artur Oruba, et. al. proposed a network of a reference system that enables the automatic processing of static data observed from any user, which reduces the minimum observation period to about 15min for line-of-sight [84]. Satellite observation methods require measurements to be carried out in an open area, which is a major limitation. When there is no direct path from the satellite to the receiver, the survey becomes difficult, sometimes impossible, using traditional GNSS techniques [85]. The avoidance of GNSS measurements in the forest, a very dense urban and mountain environment, is increasing due to poor localization. Previous research proposed precise point positioning technology [53], static surveying [54], [55], differential code measurement [56], method of absolute measurement [57] and RTK [58] to reduced positioning error in such environment; however, the positioning accuracy was poor. Mieczysław Bakuła, et. al, analyses the accuracy conditions with limited visibility of satellites using three GPS/GLONASS receivers set up on a particular measurement beam [59]. However, many visible satellites are observable for multi-GNSS positioning, which becomes very cumbersome to mitigate. A method of satellite selection was proposed in [60] to minimize this effect. The primary source of high-accuracy field surveys is (challenging to eliminate) the multipath error[61]. Multipath is the recording of reflected signals by the GNSS receiver. This signal reflection can be of two types. It can reflect the ground that arrived at the receiver's antenna [62] or obstacle standing near the receiver (trees, mountain, tall buildings). The satellite movement and the orbit cost continually satellites geometry change; the multipath impact level depends on the altitude of a given satellite and time. Signals high in the zenith are of less risk to multipath effect compare to low satellites. [63] proposed that at reference stations, measurements can be done in 15-30min cycles in other to minimized multipath error. The required observation time is a disadvantage. In kinematic and rapid static GNSS surveys, the multipart effect was considered the main source of error [64] and increased observation time to several minutes. [86] proposed that the multipath effect can be minimized using several receivers.

In dense urban, mountain, forest, and indoor environments, precise positioning has always been a more challenging problem for many reasons. The GNSS signal is not strong enough to penetrate most materials. As soon as an object hides the GNSS satellite from the target's view, the signal is corrupted, limiting GNSS's usefulness to open environments and limiting its performance in the mountains, dense urban, and forest environments, as retaining a lock on the GNSS signals becomes very difficult. GNSS typically becomes almost useless in such challenging environments. However, there is an increasing need for precise localization in cluttered environments, in addition to open spaces. For example, in a land survey, accurate localization of digital land points is an emerging need, "blue force tracking" that knows where friendly force is, is of great significance, must especially in urban scenarios. A promising solution to minimize the multipath effect and increase position accuracy is radio signals like UWB technology because UWB ranging has several characteristics, which give them superiority over GNSS signals in low to limited signal environments. UWB's sufficient time resolution ability, high-speed data transmission, accurate position estimation, low power transceiver designs, and its robust performance in dense multipath environments enable the GNSS navigation system, such as for land survey, to boost its operational environment. Furthermore, UWB ranging provides the capability to augment GNSS through high accuracy ranges. UWB information is transmitted through a series of baseband pulses instead of the modulated sinusoidal carrier in an impulse signal. On the other hand, multi-carrier UWB signals use a set of sub-carriers. Each of these sub-carriers must not interfere with one another and should overleap. The ability of multi-carrier UWB signals to minimize interference with bands used by different systems sharing the spectrum is advantageous [16]. UWB gives significant advantages in numerous applications, including industrial RF monitoring systems, high-speed LAN, Unmanned Aerial Vehicle (UAV), Intrusion Detection Radars, and Unmanned Ground Vehicle (UGV) precise positioning, Tactical Handheld Radios, and more. Other additional advantages of UWB include;

- With power spread over huge bandwidth, frequency selective fading from multipath/materials is mitigated [17]
- Ranging – very fine precision distance and range resolution.
- Low energy density gives less interference to closer systems and minimal RF health hazards
- Minimal multipath cancellation effects

Multipath nullification happens when a multipath signal arrives at the anchor node partially or totally out of phase with the direct signal. It causes a reduced amplitude response. With a short period of signal pulses, direct signals will arrive before indirect signals. As a result, they are less multipath cancellation effects with UWB signals. UWB, like GNSS technology, is still subject to physics laws for radio frequency signals such as trade-off versus bandwidth. Another issue with UWB is its ranging accuracy. In addition, UWB provides reliable and precise results regarding relative positioning concerning a local frame, at the cost of covering the working area with expensive antennas, thereby limiting UWB technology only to a relatively small extent outdoor and applicable indoor. On the other hand, GNSS is a cheap technology that offers an adequately accurate localization outdoor worldwide, in terms of a global frame (longitude, altitude, latitude). Using UWB to increase GNSS enlarges navigating and positioning in areas where GNSS typical falters; this is mostly indoors or in hostile signal environments. Because both systems are harmonious, integrating these sensors for precise positioning draws benefits from both types of sensors while reducing their drawbacks. Previous sensor fusion proposed that a particle filter can combine GPS/UWB for and out/indoor scenarios, but there were no descriptions on anchor node placement. Besides, GPS provides low accuracy when compared to GNSS technology [18]. [19] equally shown that they were improvement in combining UWB and GPS. However, precision is also a function of the UWB beacon's location; besides, the estimation was slightly sensitive to the location's initial guess. Finally, [20] uses a single UWB range to increase GPS in hostile environments. The analysis shows a rapid convergence of the Kalman filter positioning and a reduction in Dilution of Precision (DOP) values with the UWB range's augmentation. The goal of this research work can be summarized as follow:

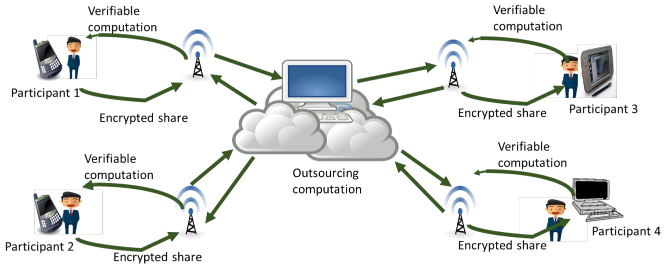


FIGURE 4.1: Outsource Secret Sharing

- Show that an integrated GNSS-UWB solution is more accurate and reliable than a GNSS-only solution under conditions with limited access to satellite signals.
- Show that the accuracy depends on anchor node positioning.
- Show a reduction in observation time.

Previours This paper focuses on the probabilistic combination of sensor data acquired from different sources; GNSS global and a local positioning technique like UWB. More precisely, I propose a Monte Carlo (Particle Filter) localization algorithm, representing the target node's position poses using a set of weighted samples (particles). As an advantage, this approaches ability to combine measurements from different sensors while considering their probabilistic behaviors appropriately.

I consider that the data collected is directly stored in the cloud. During the transfer of data to the cloud a secret is generated and distributed to each participant using my proposed scheme. Figure 4.2 presents the general procedure of digital land data collection. This data collected needs to be protected from unauthorized persons. In this section, I propose a novel hierarchical outsource secret sharing scheme (HOSSS) and a multi zero-knowledge proof method to protect the misappropriation of data and the proof of ownership right respectively. In the protocol, t or more participants from an authorized sub set can recover the secret. my scheme consists of initialization, distribution of secret to each participants, manipulation of digital land data, decryption and verification of each participant's share, adding new participant, remover of participant, and multi proof zero-knowledge phases.

In the hierarchical model of figure 1.3, a dealer divides the secret into three hierarchical levels with the highest level belonging to the landowner(s) and the lowest level to neighbours. In such a way that manipulation of data can only be done if a certain group of participant combines their shares together then, access can be granted to the state authority to manipulate data and transfer ownership right or perform any lager operation. A dealer randomly chooses two large primes p and q, such that q/(p-1) and g as generator of the q-th order subgroup in finite filed (FG(q)) and H(X) is a one way hash function.

A secret S is shared among n participants p_i in a hierarchical manner $A_0, A_1, \dots A_m$, where t_h is the threshold associated with group A_h and n_h is the number of participants associated with group A_h for $h = 0, 1, \dots, m$. The identity of participant $p_i, j \epsilon A_h$ is the pair (i,j) for $i = 1, \dots, n_h,, j = t_h - 1$ and $t_1 = 0$.

A trustable dealer takes the following steps to distribute shares among all participants:

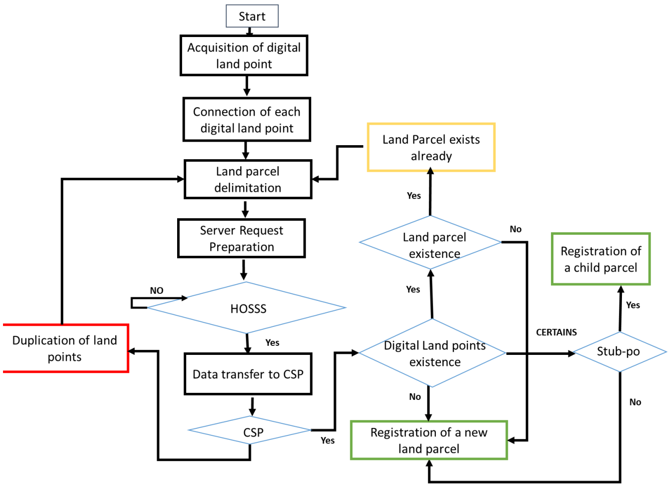

Start
Acquisition of digital land point
Connection of each digital land point
Land parcel delimitation
Land Parcel exists already
Yes
Land parcel existence
No
Registration of a child parcel
Server Request Preparation
NO
HOSSS
Yes
Duplication of land points
Data transfer to CSP
Yes
Digital Land points existence
CERTAINS
Yes
Stub-po
No
No
CSP
Yes
Registration of a new land parcel

FIGURE 4.2: Flow Chart of Land Parcel Registration

a) The dealer selects random elements from the finite filed GF(q) to constitute a polynomial with t-1 degree

$$f(x) = \sum_{v=0}^{t-1} b_i x^v \bmod q \tag{4.1}$$

where b_0 = S is the secret. The corresponding shares $\omega_{i,j} = f^j(i)$, where $f^j(i)$ is the j-th derivative of the polynomial f(x).
b) The dealer randomly chooses t-l coefficients $b'{}_1, \ldots, b'_t$ from FG(q) and generate a polynomial with t-1 degree.

$$f'(x) = \sum_{v=0}^{t-1} b'_i x^v \bmod q \tag{4.2}$$

Where b'_0 distributed to all participants is a random value from FG(q) and the corresponding shares are $\omega\prime_{i,j} = f\prime(i)$.
c) According to the property of homomorphism secret sharing [87] the share of each participants is

$$\gamma_{i,j} = \omega_{i,j} \oplus \omega'_{i,j} \tag{4.3}$$

d) The dealer distribute $(\gamma_{i,j}, H(b_0))$ to the participants for $i = 1, \ldots, n_h$, $j = t_{h-1}$, and $h = 0, \ldots, m$. Where $h(b_0)$ is a one way hash function.
e) The dealer broadcast verification information

$$\psi_v = g^{b_j \oplus b_j'} \bmod p, v = 0, 1, 2, \ldots, t-1 \tag{4.4}$$

HTSSS, all the n shareholders are divided into m disjoint levels $H_1, H_2, \cdots H_m$. Which constitute an hierarchical assess structure. The i^{th} level is made up of n_i shareholders and any t_i or more shareholders can recover the secret on i^{th} level. When the number of shareholders in the i^{th} level is less than t_i, say v_i, then the $t_i - v_i$ remaining shareholder can be taken from higher levels. Mathematically an authorized set of n shareholders in hierarchical threshold SS can be defined as;

$$\Gamma = \left\{ B \subseteq \mathcal{P} : \left| B \cap \left(\bigcup_{j=1}^{i} L_j \right) \right| \geq t_i, 1 \leq i \leq m \right\} \tag{4.5}$$

1. Any authorized subset of t_i or more shareholders at level L_i can reconstruct the secret using Lagrange polynomial interpolation.

2. Whenever the number of shareholders in the i^{th} level is less than t_i, shareholders from the higher levels can provide their shares.

3. To reconstruct the secret,

4.2 Manipulation of Digital Land Data

In order to manipulate digital land date an authorized group of participants must agree by providing their shares to the CSP as follows;
a) An authorized subset of t participants send $(\gamma_{i,j}, \psi_v)$ to the CSP.
b) CSP runs verification algorithm to check whether equation (11) is correct.

$$g^{\gamma_{i,j}} \equiv \prod_{v=j}^{t-1} \psi_v^{\frac{v!}{(v-j)!} i^{v-j}} = g^{f^j(i)} \tag{4.6}$$

where $v = 0, 1, \ldots, t-1$
c) If equation (11) holds then, CSP use Birkhoff interpolation to reconstruct the secret s_0' with any **k** points $(\mathrm{X}, \mathrm{E}, \mathrm{U}_c)$ otherwise, protocol is aborted and the decryption behaviour of p_i is broadcast. From (3) s_0' can be deduced as

$$f(x) = s_0' = \sum_{k=0}^{t-1} \frac{det(A(E, X, U_{ck}))}{det(A(E, X, U_c))} x^k \tag{4.7}$$

From equation (12), $s_0' = F(0) = b_0 \oplus b_0'$. CSP returns s_0' to t active participants.

4.2.1 Decryption and Verification of Each Participant's Share

To achieve decryption and verification, each participant can obtain the secret by ruing a small amount of computation using the following steps:
a) The result returned by CSP $a_0 = s_0' - b_0'$ where b_0' is known by all participants.
b) Each participant then verifies the correctness of it share by checking if $h(a_0) = h(s)$. If it is correct then the computation of CSP is correct, otherwise the result is wrong.

Example 1: I start by defining a neighbour, in a cadastral survey, a neighbour is a person that shares an edge or vertices of a land parcel with another person. Figure 4.3 shows the demarcated land parcel (a,b,c,d,e), it can be seen that this land parcel have seven neighbours $(\mathbb{K}, \mathbb{L}, \mathbb{M}, \mathbb{O}, \mathbb{S}, \mathbb{Q}, \mathbb{R})$. In this example it is assumed that there are two landowners and three state authority defined as $[k_0, k_1, k_2]$ = [2,3,7], where $k_m = k_2 = 7$.
a) The dealer select random values (a_0, $a_1, \ldots, a_6$) from finite filed to construct a polynomial of degree 6 such that

$$F(x) = a_0 + \sum_{i=1}^{6} a_i x^i \bmod q \tag{4.8}$$

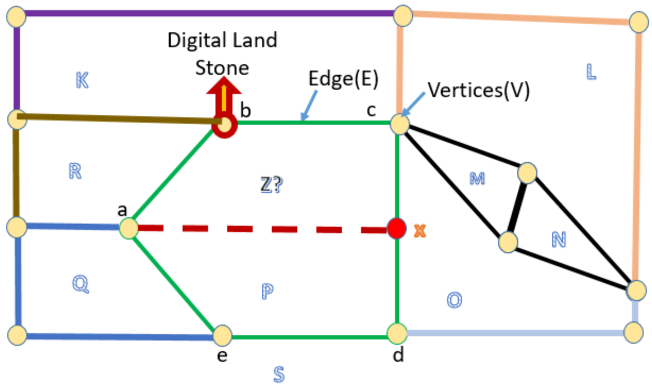


FIGURE 4.3: An Example of a Digital Land Map

where a_0 is the secret. The dealer then distributes shares $\gamma_{i,j}$ to all participants as presented in table 4.1 with g_0 belonging to landowners of the land parcel (a,b,c,d,e), g_1 belonging to state authorities and g_2 to neighbours. These neighbours are determine from figure 4.3. The secret a_0 is computed using H(E,X,U_c) and H(E,X,U_0)

TABLE 4.1: Secret Share distribution

Participants	Shares u_a	Share u_b	shares (U_c)
$p_1 \in g_0$	$\mathrm{F}(p_1)$	$\mathrm{G}(p_1)$	$\mathrm{F}(p_1) \oplus \mathrm{G}(p_1)$
$p_2 \in g_0$	$\mathrm{F}(p_2)$	$\mathrm{G}(p_2)$	$\mathrm{F}(p_2) \oplus \mathrm{G}(p_2)$
$p_3 \in g_1$	$F^2(p_3)$	$G^2(p_3)$	$\mathrm{F}(p_3) \oplus \mathrm{G}(p_3)$
$p_4 \in g_1$	$F^2(4)$	$G^2(4)$	$\mathrm{F}(p_4) \oplus \mathrm{G}(p_4)$
$p_5 \in g_2$	$F^3(p_5)$	$G^3(p_5)$	$\mathrm{F}(p_5) \oplus \mathrm{G}(p_5)$
$p_6 \in g_2$	$F^3(p_6)$	$G^3(p_6)$	$\mathrm{F}(p_6) \oplus \mathrm{G}(p_6)$
$p_7 \in g_2$	$F^3(p_7)$	$G^3(p_7)$	$\mathrm{F}(p_7) \oplus \mathrm{G}(p_7)$

$$H(E, X, U_c) = \begin{bmatrix} 1 & P_1 & P_1^2 & P_1^3 & P_1^4 & P_1^5 & P_1^6 \\ 1 & P_2 & P_2^2 & P_2^3 & P_2^4 & P_2^5 & P_2^6 \\ 0 & 0 & 1 & P_3 & P_3^2 & P_3^3 & P_3^4 \\ 0 & 0 & 1 & P_4 & P_4^2 & P_4^3 & P_4^4 \\ 0 & 0 & 0 & 0 & 1 & P_5 & P_5^2 \\ 0 & 0 & 0 & 0 & 1 & P_6 & P_6^2 \\ 0 & 0 & 0 & 0 & 1 & P_7 & P_7^2 \end{bmatrix} \tag{4.9}$$

$$\mathrm{H}\,(E, X, U_0) = \begin{bmatrix} u_1 & P_1 & P_1^2 & P_1^3 & P_1^4 & P_1^5 & P_1^6 \\ u_2 & P_2 & P_2^2 & P_2^3 & P_2^4 & P_2^5 & P_2^6 \\ u_3 & 0 & 1 & P_2 & P_3^2 & P_3^3 & P_3^4 \\ u_4 & 0 & 1 & P_4 & P_4^2 & P_4^3 & P_4^4 \\ u_5 & 0 & 0 & 0 & 1 & P_5 & P_5^2 \\ u_6 & 0 & 0 & 0 & 1 & P_6 & P_6^2 \\ u_7 & 0 & 0 & 0 & 1 & P_7 & P_7^2 \end{bmatrix} \tag{4.10}$$

4.2.2 Adding a New Participant

Here I consider a situation where landowner wants to split their lots and sell or give it to another person, thereby introducing a new neighbour. New neighbour (s) can be added using the add algorithm as presented below.

Definition 2: Let Γ be an access structure arranged in different groups $G_0, \ldots, G_\ell$, with t_h being the threshold of group G_h for $h = 0, \ldots, \ell$. Consider a secret S, a group of shares Ω, and a set of participants P where the pair $(i, j) \in \mathcal{I} \times \mathcal{I}$ is the unique ID of participant $p_{i,j} \in P$, such that $j = t_{h-1}$ $(j = t_\ell - t_h)$ and $t_{-1} = 0$. Therefore, I can define the algorithms Add, Reset, and Reconstruct as follows.

Add algorithm: It takes as input a set of shares $\gamma_1, \ldots, \gamma_w$ held by a subset $W \subset P$ of participants and the ID (i', j') of the new participant. If W is unauthorized, that is $W \notin \Gamma$ it outputs ϕ otherwise, $W \in \Gamma$ and participants compute $\gamma_{i',j'} := f^{j'}(i')$ in distributed fashion. That is, each participant $p_l \in W$ performs the following steps: for $l = 1, \ldots, w$
a) The derivative of each participant's partial Birkhoff interpolation polynomial at $x = i'$ is computes as j' -th

$$y_l = \gamma_l \sum_{V=j'}^{t-1} \frac{V!}{(V-j')!}(-1)^{l-1+V} \frac{d(A_{l-1,V}(E, X, U_c))}{d(A(E, X, U_c))} i'^{V-j'} \tag{4.11}$$

where j'=j'-th derivative of its partial Birkhoff interpolation polynomial.
b) p_i randomly splits the result into w values such that; $y_l = \beta_{1,l} + \cdots + \beta_w, l$ and sends $\beta_{m,l}$ to CSP $p_{m,j} \in W$, for $m = 1, \ldots, w$ and $m \neq l$ using a secure network.
c) CSP collects all values $\beta_{l,m}$ received and computes

$$\beta_l := \sum_{m=1}^{w} \beta_{l,m} \tag{4.12}$$

d) CSP sends β_l to the new participants $p_{i',j'}$ through a secure network and broadcasts $c_0, \ldots, c_{t-1}$ that was receive from the sharing algorithm.
e) The new participants $p_{i',j'}$ computes it share $\gamma'_{i',j'}$ by adding all values β_l such that;

$$\Gamma'_{i',j'} = \sum_{l=1}^{f} \beta_l \tag{4.13}$$

f) The correctness of share is verify using the following equation:

$$g^{\gamma'_i{}',j'} \equiv \prod_{V=j'}^{t-1} d_V^{\frac{V!}{(V-j')!} i'^{V-j'}} = g^{f^{j'}(i')} \tag{4.14}$$

Example 2: In land registration their are three groups of participants namely; landowner, state authorities and neighbours. Share of each participant can be generated by the dealer as follows; G_1, G_2 and G_3 based on $f(x) = 11 + 5x + 8x^2 mod 17$, that is, $\varphi_1 = 3, \varphi_2 = 7$ and $\varphi_3 = 8$. The add algorithm can create a share for a newcomer (P_4) as follows;
a) Each participant P_i privately computes $\varphi_i \times \gamma_i$ as $\varphi_1 \times \gamma_1 = 7 \times (4-2)(4-3)/(1-2)(1-3) = 4$ $\varphi_2 \times \gamma_2 = 4 \times (4-1)(4-3)/(2-1)(2-3) = 6$ and $\varphi_3 \times \gamma_3 = 13 \times (4-1)(4-2)/(3-1)(3-2) = 7$.
b) Each p_i randomly split the results and exchange them, as shown in the share-exchange matrix $\mathcal{E}_{t \times t^*}$. Participants then compute and send $\sigma_1 = 5, \sigma_2 = 3$ and $\sigma_3 = 8$ to P_4.
c) P_4 adds up these values to compute $p\prime_4$ share $\varphi_4 = 16$

$$\mathcal{E}_{t \times t} = \begin{pmatrix} \partial_{11} = 2 & \partial_{21} = 1 & \partial_{31} = 1 \\ \partial_{12} = 1 & \partial_{22} = 1 & \partial_{32} = 4 \\ \partial_{13} = 2 & \partial_{23} = 2 & \partial_{33} = 3 \end{pmatrix}$$

4.2.3 Remover of a Participant

Here I consider a situation where a landowner wants to transfer ownership of the lot to another person. At this point, the landowner needs to be removed from the scheme and replace with the new owner or during fusion of a lot a neighbour can equally be removed. In other to remover a participant I use the reset algorithm. This algorithm takes as input a set of shares $\gamma_1, \ldots, \gamma_v$ belonging to $V \subset P$ of participant $P' = \{p'_1, \ldots, p'_{n'}\}$, with their respective unique ID (i', j'). That is, each old participant $p_l \in V$ performs the following steps, for $l = 1, \ldots, v$
a) Each participant p_i computes its partial Birkhoff interpolation coefficient

$$b_{l,0} = \omega_l (-1)^{l-1} \frac{d(A_{l-1,0}(E, X, U_c))}{d(A(E, X, U_c))} \tag{4.15}$$

$(b_{l,t-1} = \gamma_l (-1)^{l+t-2} \frac{d(A_{l-1,t-1}(E,X,U_c))}{d(A(E,X,U_c))})$
b) Each participant construct a polynomial $f'_l(x) = a'_{l,0} + a'_{l,1}x + a'_{l,2}x^2 + \cdots + a'_{l,t'-1}x^{t'-1}$ of degree $t' - 1$, where $b'_{l,0} = b_{l,0}(b'_{l,t-1} = b_{l,t-1}$ is the partial Birkhoff interpolation coefficient and coefficients $b'_{l,1}, \ldots, b'_{l,t'-1} \in FG(q)(b'_{l,0}, \ldots, b'_{l,t'-2} \in$. FG(q)) randomly selected.
c) Each p_i computes fα= $b_{l,0} + b_{l,t-1}$
d) It compute sub-share $\gamma_{l,i',j'}$ for each participant $p'_{i',j'} \in P'$ as

$$\gamma_{l,i',j'} = f\alpha^{j'}(i') \tag{4.16}$$

and sends sub-share $\gamma_{l,i',j'}$ to participant $p'_{i',j'} \in P$ using a secure network and broadcasts the audit data, composed of commitments to each coefficient of polynomial $f'_l(x)$,. $\gamma'_{l,k} := g^{b_{l,k}}$, for $k = 0, \ldots, t' - 1$, and commitment $\gamma_0 = g^m$ $(\omega_{t-1} = g^m)$ of the old polynomial $f(x)$
e) Each p_i erases it share from previous time period and compute it final new share form the secret b_0 as $p_{i',j'} \in P'$ computes its share $\gamma'_{i',j'}$ adding all sub-shares $\omega_{l,i',j'}$ received

as;

$$\gamma'_{i',j'} := \sum_{l=1}^{v} \beta_{l,i',j'} \tag{4.17}$$

Share verification $\gamma_{l,i',j'}$, each new participant $p_{i',j'} \in P'$ performs the following steps.
a) p_i checks the function value of each polynomial,

$$g^{\gamma_{i'j'}} \equiv \prod_{k=j'}^{t-1} \gamma_k^{\frac{k'}{(k-j')!} i^{i^{k-j}}} = g^{f^{(j')}(i')} \tag{4.18}$$

, for $l = 1, \dots, r$
b) Each p_i checks whether the free coefficient (last coefficient) of all polynomials $f'_l(i')$ leads to the original secret $s \in \mathcal{S}$,

$$\gamma_0 \equiv \sum_{l=1}^{v} \gamma'_{l,0} \tag{4.19}$$

$\left(\gamma_{t-1} \equiv \sum_{l=1}^{v} \gamma'_{l,t'-1}\right)$
c) If equations (23) and (34) are satisfied, it accept $\gamma'_{i',j'}$ as its valid share otherwise it reject the response.
Reconstruct It takes as input shares held by a subset $V \subset P$ of participant. If $V \in \Gamma$, it outputs $m \in \mathcal{M}$ reconstructed using Birkhoff interpolation. It outputs ϕ otherwise. Having access to the original audit data $\omega_0 = g^{b_0}$ $\left(\gamma_{t-1} = g^{b_{t-1}}\right)$ it is possible to verify whether the reconstructed of the secret $s \in \mathcal{S}$ is a correct opening value for commitment $\gamma_0 \left(\gamma_{t-1}\right)$, i.e. $g^s \equiv \gamma_0$ $\left(g^s \equiv \gamma_{t-1}\right)$

4.3 Multi-Prover Zero-Knowledge Argument.

In this section I consider the falsification of a land title of a particular piece of land. Each of the claimer have to prove in a law court which one of them is the rightful owner of that land parcel. Using multi-prover zero knowledge argument in such a way that the Lawyers (Verifier) do not learn anything about the secret as follows:
a) The dealer use secret b_0 to calculate $h = g^{b_0} mod p$, such that the verifier who gets p, q, g, h can verify that p, q are prime and that g, h are of other q
b) Supposed that a group of participant have come to present themselves as witnesses by pooling their shares γ_i, j. Every p_i has a secret input $Y_{si} = \gamma_i, j$. The secure multi-party computation (SMC) is run by t shareholders for a function $f(Y_{s1}, \dots, Y_{st}) = Y$, where $Y = f(0)$ and

$c_i = b_{l,0} = \omega_l(-1)^{l-1} \frac{d(A_{l-1,0}(E,X,U_c))}{d(A(E,X,U_c))}$ as in (20).

After running the SMC protocol ever p_i has a secret H_i such that $Y = \sum_{i=1}^{t} b_i H_i mod p$, where $b_i (\leq i \leq n)$ which can publicly be computed [45]
c) Every p_i chooses randomly a number $s_i \in Z_p$ and compute $t_{i,j} = g^{s_i} mod p$ and send $t_{i,j}$ to V, for $i = 1, 2, \dots, n$
d) V chooses a random number using non linear feedback shift register (NLFSR) [40] in $m \in [1, 0]^*$ and sends it to every p_i
e) p_i computes $d_i = s_i - m(\gamma_i - b_0\prime)$ mod q and sends d_i to V, for $i = 1, 2, 3, \dots, n$
f) V accepts the fact that p_i share a secret Y such that $g^Y = h$ else, V rejects the response.

Note that the verifier can only be convinces that p_i share $s\prime$ after a certain number of rounds.

4.4 Security Analysis

Here my security analysis is based on the throughput,

In this section, I analyse the security performance of my proposed HOSS scheme as follows:

Theorem 1. In HOSS scheme any $t-1$ or fewer participants get nothing about the secret

Proof. In my scheme, any $t-1$ or fewer participants from different levels can cooperate by providing their share $\gamma_{i,j}$ for $i = 1, \ldots, n_h, j = t_{h-1}$, and $h = 0, \ldots, m$ but, they cannot obtain the secret b_0 because the Birkhoff interpolation requires t values to determine the unique solution. In addition, The CSP does not know any valuable information about b_0. The participant's privacy is protected by the scheme since the CSP knows nothing about the input and output of p_i. The share sent by an authorized set of p_i to the CSP is encrypted thus, the CSP cannot obtain any valuable information about b_0. In [29] is proved that perfect security of hierarchical secret sharing holds for the (K,n) where K=$k_{i_i}^{m} = 0$ and that k=k_m. To add new participant ($p_{i',j'}$), each existing participant $p_l \in W$ of an authorized subset $W \in P$ computes $f_l^{j'}(i')$. During this operation, this sub-share of participants leaks information about their own share as they randomly split and distributes secret share to the other participants. But confidentiality is preserved as a participant only forwards the sum of all values received while hiding the individual sub-shares. The additive property of homomorphic used during distribution of sub-shares and the polynomials use in secret sharing guarantees accessibility.

Theorem 2: Participants and CSP use public verification information to verify the correctness of shares and the malicious behavior of participants can be noticed in time.

Proof: the correctness of shares γi can be verified by using public verification information of each participant $p_{i,j}$ and the commitment c_r to its share $\gamma_{i,j}$ using the commitments received as follows: $p_r = \prod_{k=j}^{t-1} d_k^{(k-j)!} = g^{f^{(j)}(i)}$, where d_k is the commitment to coefficient b_k for $k = 0, \ldots, t-1$. Thus, by verifying $p_r \equiv g^{c_{i,j}}$ the correctness of its share can be checked.

TABLE 4.2: Time Complexity Analysis

Threshold(t)	3	4	5	6	7
Secret reconstruction time	2.17	2.2	2.39	2.94	3.38
Secret verification time	791.52	868.21	1103.42	7370.42	9576.21

In my proposed approach for zero-knowledge proof, the secret value of shareholders cannot be revealed to any other shareholder or verifier even if shareholders exchange their secret shares. As shareholders use SMC protocol in the interactive poof to jointly compute the secret over their inputs (secret shares) while keeping their secret shares private to them. Therefore, the privacy of all shareholders is maintained.

4.4.1 Security Complexity Analysis

In this section I analyzed the encryption security performance matrices base on its throughput, knowing that the higher the throughput of an algorithm the better it is secured.

a) Encryption: for the encryption matrix, throughput is the average of total plain text divided by the average encryption time. In general, secret sharing schemes use random variable measure in bits. To distribute a secret of one-bit, one polynomial (κ) with a threshold t participants, it requires κ(t-1) random bits. To distribute a secret of length n bits, the entropy of $(t-1)n\kappa$ bits is required. Therefore, the throughput can be deduced as

$$Throughput = \frac{Entropy}{Computational - time} \tag{4.20}$$

4.5 Performance Evaluation

The performance evaluated was on an Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz 1.80 GHz, 10 GB RAM, 64-bit, the server, and all hosts were running on the same computer in other to ignored network latency. Table 4.2 shows the time verification and time reconstruction of the secret. Table 4.3 show the comparison results of my proposed scheme and the schemes E. Zhang [87] proposed an outsourcing secret sharing scheme but this scheme can to not be used in the hierarchical model. , Tassa [29] Propose a hierarchical secret sharing schemer but the scheme requires that shareholders must have a device with high computational power, Traverso [35] proposed a hierarchical verifiable and dynamic schemer that and add, remove and renew secret shares which can detect invalid secret shares but it does not guarantee fairness in addition, the communication cost is high. [88] proposed a secret sharing scheme that guarantees fairness.

In my proposed scheme, the protocol is executed only once, shareholder only has to run a small amount of decryption and verification with a communication cost of O(1). Figure 4.4 shows the runtime of secret verification, it is clearly visible that as the number of participants increase, the runtime grows exponentially, this time varies from 291.52 to 9576.24 according to the test results. Figure 4.5 reconstruction time complexity between my proposed and conventional scheme with different file size. Figure 4.6 shows the time to reconstruct the secret and return the result to the participants and the time taken to distribute the secret to each participant. Shows that the run time grows linearly as the number of participants increases with variable file size. It can be seen that the time increases as the size of the file increases. The fair secret sharing scheme proposed in [88] requires multiple rounds and cannot operate effectively on devices that have poor computational complexity however, [87] proposed an outsources secret sharing scheme which permit participants to perform the decryption operation only with a computational cost of O(1) while the complex computation operation is sent to the CSP and it equally requires a dealer (trusted third party). But the outsourcing scheme was limited to only one level. In [29] the author presented a hierarchical secret sharing scheme with a flexible way of dividing participants into levels depending on their authority with a high computational cost. In figure 4.7 I presented the different between my proposed HOSSS and the conventional OSSS interns of security complexity. I can clearly see that my propose scheme is better secure compare to the conversational scheme.

On the contrary in my proposed scheme, the protocol needs to be executed only once. The complex operations are sent to CSP and the participant only has to run a small amount of verification and decryption. In addition, I can use the add and delete algorithm proposed in [35] to add new participant in my scheme without changing the original secret also, participant can be remove from the scheme in a case of transfer of landownership right. My scheme equally, provide an interactive proof system for any verifier to verify that an authorized set of participant shares the secret without getting any information about the secret b_0.

TABLE 4.3: Feature comparison of schemes

	E. Zhang [87]	Tassa [29]	Traverso[35]	Proposed Scheme
Number of Iterations	1 Round	1 Round	1 Round	1 Round
Fairness	Yes	Yes	No	Yes
Computation	CSP	Participant	Participant	CSP
communication Cost	O(1)	O(1)	O(t)	O(1)
Interaction	No	No	Yes	No
Number of Levels	One	Multiple	Multiple	multiple
Dealer	Yes	Yes	Yes	No

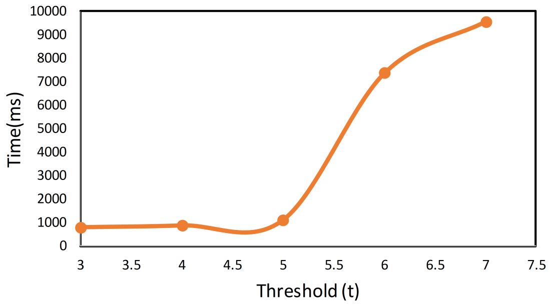


FIGURE 4.4: Time taking by participant to Verify the Secret

4.6 Conclusion

Combining hierarchical threshold and outsourcing computation property, I propose a HOSSS protocol base on homomorphism. Computational weak participants can obtain the secret with only a small amount of operations while expensive reconstruction and verification computation is outsourced to a CSP and the CSP cannot learn anything about the secret. Participants can be added or remove from the scheme using the add and delete algorithm without changing the original secret. Moreover, the malicious behavior of CSP and participant can be accurately checked on time and no multiple interactions are required between CSP and participants. In the second phase of this paper, a secure multi-Prover zero-knowledge argument was used to prove that all active participants actually shared the secret. Although my scheme has been proven to

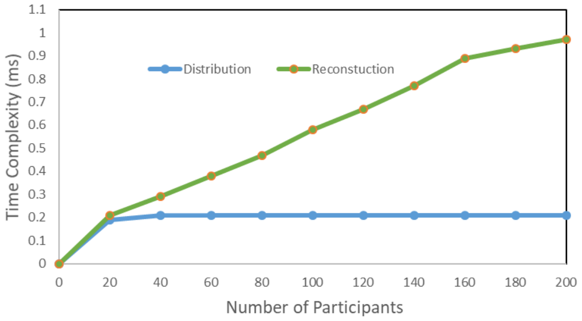


FIGURE 4.5: Reconstruction Time Complexity Between my Proposed and Conventional Scheme with different file size.

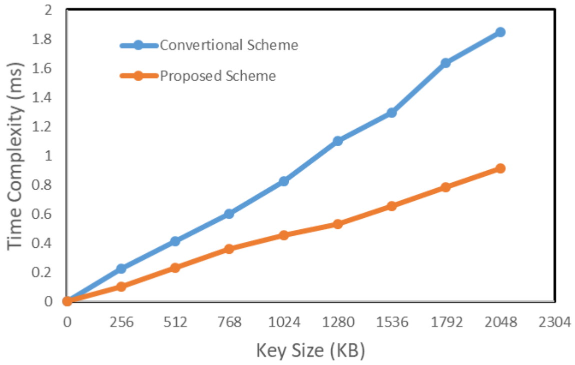


FIGURE 4.6: Reconstruction and Distribution Time Complexity With Variable File Size

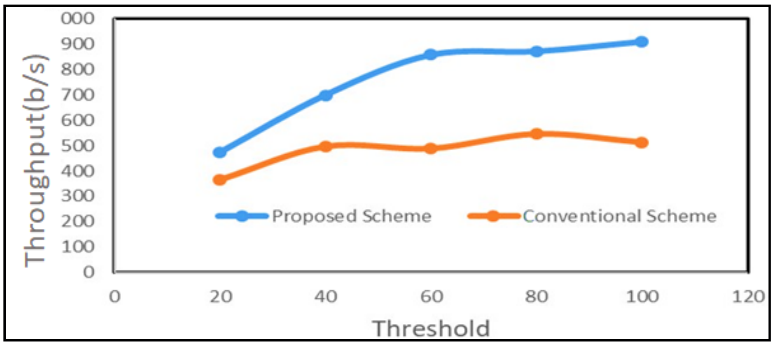


FIGURE 4.7: Comparing Security level of OSSS and OHSSS

be better performant than the conventional method, the calculation investigated an increase of complexity according to the number of participants the time complexity as compared to the conventional method. The theoretical analysis of my proposed scheme demonstrated that Security requirements are satisfied in addition, my computer simulation results demonstrated that my scheme is more secure compare to the conventional scheme.

Chapter 5

Advanced GNSS/UWB Security Enhancement Scheme Against Relay Attack to Keyless Entry System

5.1 Introduction

The Open Systems Interconnection (OSI) reference model has different network layers. These layers define how data is transmitted through the network. In the same manner, consider the hierarchical network security model of figure 5.1, which combines two models: hierarchical geo-localization information and hierarchical secret sharing. Each of these models has a specific rule to play in the security of my system. Localization technologies such as Global Navigation Satellite System (GNSS) like GPS and regional cellular positioning systems are the most trusted localization methods because they have been well standardized and available worldwide. GNSS is managed by different organizations such as US NASA, European GSA, and Japanese JAXA, managed by each country's authorities. Therefore, localization information can not easily be compromised. However, GNSS is still exposed to relay attacks. Also, a mobile cellular network such as 3G, 4G and 5G has been globally standardized. On the other hand, an Ultra-Wide Band (UWB) radio can perform accurate local positioning and secure ranging as proposed in [25]. For low rate pulse (LRP) car keyless entry system with an open security specification for short-distance ranging and the high rate pulse (HRP) for longer distances is proprietary. Furthermore, IEEE802.15.4z is still undergoing standardization for individual applications. However, the security of IEEE802.15.4z is questionable. Therefore, there is a chance for combining GNSS and UWB localization for global and local localization for a new standard. UWB provides more accurate information compared to GNSS. Without losing generality, to meet today's high demand for precise localization information, a combination of GNSS/UWB will be a better solution. GNSS provides the uniqueness of geolocalization points on the planet earth, meaning that they are no two points on the earth's surface with the exact longitude and latitude. Therefore, GNSS is considered to have the highest level of unique information. Standalone GNSS depends solely on information from satellites. An assisted GNSS (A-GNSS) augments using cell tower data to enhance quality and accuracy in poor satellite signal conditions. In deplorable signal conditions, for example, in urban areas, satellite signals may manifest a multi-path environment where signals skip off structures or are weakened by tree canopy or meteorological conditions. Similarly, UWB augmentation GNSS (U-GNSS) can eliminate most of the multi-path manifestations and provide more accurate positioning information but indoor and outdoor. In an information system,

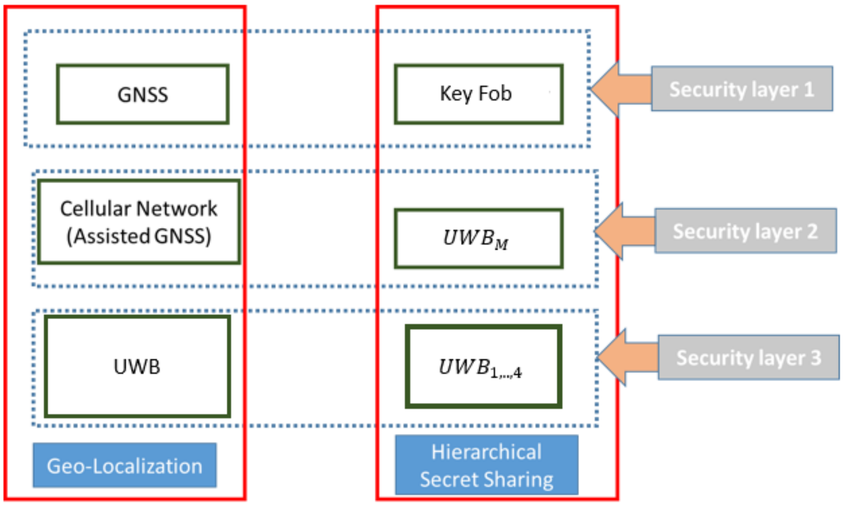


FIGURE 5.1: Anchor Node Positioning in between High level and lower level Participants

confidential, secret information can be distributed hierarchically to all shareholders depending on their operation level. Any meaningful information can be made available only when a group of participants agrees. Consider the hierarchical network security model of Figure 5.1 where three layers of the hierarchy have been considered, with each having a specific rule to play. For a replay attack to be successful, at least two higher levels of the system must be compromised.

In geo-localization, they are two crucial factors that should be considered. First is the accuracy of localization information (time, date, longitude, latitude, and height). Therefore, GNSS/UWB combinations provide more accurate positioning information chapter 4. The second factor is security. The existing positioning techniques are vulnerable to physical layer attacks. For example, relay attacks on passive entry systems in vehicles [78], eavesdropping, relay, interference, jamming [89], credit card payments [90], and the spoofing attacks on GPS [91], [92]. Those vulnerabilities are threats to the real world, as attested by a recent vehicle theft that found public media attention [93].

Ranging attacks on the physical layer permit the attacker to diminish distances that devices measure, violating the defense systems that rely on this information [78]. The Mafia Fraud Attacks manipulated at the logical layer can be easily prevented with the help of distance-bounding protocols (DBP) [94]. The physical layer attack requires manipulating signal characteristics to trick the receiver into decoding bits or incorrectly measured signal phase, time of arrival (ToA), amplitude. Compare to the logical-layer attacks that use manipulations of message bits only. Several ranging systems are vulnerable to physical-layer attacks. For example, UWB 802.15.4a to Cicada attack [95] early detect / late commit (ED/LC) [21], Phase ranging [96], Chirp Spread Spectrum to ED/LC [97] and phase manipulation [98]. These attacks are successful notwithstanding authentication and DBPs [94] because their target is the physical layer and not the message content. Recently, the 802.15.4z standard for UWB ranging can achieve security only for short symbol lengths (SSL), thereby limiting the maximum measured distance. On the other hand, it can risk security by using longer symbol lengths. To increase the DBP multiple pulses are as shown in Figure 2.6. To prevent relay attack in longer DBP the UWB preamble scrambled timestamp sequence (STS) was proposed in [25]. Therefore, 802.15.4z is limited because; different HRP implementations still suffer from attacks. In the literature, they are no clarifications if a fully secure and efficient HRP can be built, and HRP security is proprietary.

Many cryptographic and authentication methods have been proposed to encrypt the conversation between the vehicle and key fob to authenticate the key fob [99] -[100]. Nevertheless, They are limited to the fact that many participants can not participate in the protocol. The PKES system is still exposed to relay attacks because the enemies do not need to decrypt or alter communication. They boost the communication signal between the key fob and vehicle to ultra-high frequency. In addition, computationally secure encryption or decryption can be time-consuming [101] which is vital in a real-time transportation system [102]. The earlier research also proposes other solutions such as location-based authentication (LBAM) mechanism [103]. LBAM does not provide security against relay attacks because the attackers can still relay the key fob data.

In chapter 3, a hierarchical threshold outsources secret sharing, and an interactive proof scheme for land conflicts was proposed. In this scheme, participants were partitioned into different hierarchies depending on their responsibility to manage digital land data (land administration). Secret reconstruction was outsourced to the cloud service provider (CSP) by the dealer. All participants also use a zero-knowledge interactive proof scheme to prove ownership right in case of land conflict. However, the dealer was considered a trusted third party, a single point of failure. In chapter 4, the author proposes a GNNS/UWB geo-localization technique for precise point positioning using the Particle filter in dense urban and mountain areas. The mobile terminal (MT) measures how long it takes for the radio signal to travel from the MT to the anchor nodes (ANs) and back to the MT using the time difference of arrival (TDoA). These measurements can be used to calculate the distance from the MT to each AN. TDoA positioning technique chapter 4 uses the arrival time difference, and the Hyperbolic algorithm is usually adopted to calculate location. The positioning precision is high within the area surrounded by ANs but low outside the scope. Additionally, complex environmental situations such as power plants make it challenging to meet project specifications with TDoA positioning because of the problematic system construction. Considering the points mentioned above, I will use the ToF positioning technique in this research work.

In this paper, a nouvelle proximity, distance, and secure localization scheme based on user location and outsource hierarchical threshold secret sharing scheme (OHTSSS) chapter 3 for proximity, distance, and secure localization has been proposed. After authentication, the anchor nodes can securely generate the master secret (secret shares). OHTSSS is limited because a trusted dealer can create and distribute the master key pair to all participants. In this research work, no authorized dealer is required to generate and distribute secret shares to each participant. Instead, all participants jointly generate the master secret.

The important contributions of this paper can be summed as follows.

1. I suggest a secure authentication technique based on OHTSS to improve the symmetric key used in ED/LC UWB bit reordering.

2. GNSS/UWB - ToF is introduced as a security measure against distance reduction and enlargement attacks.

3. In the distance-bounder access control system with many users required, I combine zero-knowledge and OHTSS in the challenge-response design.

4. I show that my proposal is an enhancement to [25].

5.2 Preliminaries

The key management system in automobiles has emerged significantly from the original usage of a mechanical key. Today, vehicle manufacturers have migrated to passive keyless entry vision [25], [78], [104] a car automatically opens itself when the person carries a key fob or smartphone is in its proximity. The vehicle can be started only when the smart device is inside the vehicle. The modern, state-of-the-art solution uses a mixture of low-frequency and ultra-high frequency (LF-UHF) channels to realize this dual functioning. Nevertheless, these systems can be subject to early detect/late-commit (ED/LC) attacks [25]. These UWB modules are robust to relay attacks. IEEE 802.15.4$z - 2020$ UWB standard explicitly includes timing information and can resist most multipart effects. But it is still limited because UWB only provides local coordinates of a point, which is a potential security threat to car monitoring service. That is, a company can not have remote control over the vehicle. The IEEE 802.15.4z Enhanced Impulse Radio Task Group (IRTG) is currently tasked by the Car Connectivity Consortium(CCC) to develop more accurate ranging methods for UWB keyless access, which is one of its principal pilot applications. Therefore, to attain a precise position, UWB has to be combined with GNSS technology.

Malicious and false anchor nodes (AN) in positioning are accessed anchor nodes, deliberately sending misleading information to other ANs in the network such as; AN position and AN identity. Types of malicious ANs attacks related to IoT positioning can be paraphrased as follows: Relay/Replay Attack, On-off attack: a malicious AN can transmit incorrect positioning-related data only at random intervals, Conflicting behavior attack: the deceitful node can send partly trustful information (correct IP address) and partially inaccurate information (faking its position). Sybil attack [79], [105]: it refers to malicious AN using more than one IP address to prevent their identification by the unexpected change in identity. Newcomer attack [81]: an anchor node earlier identified as malicious can modify its IP and join the network again as a new anchor node.

5.3 Secure Authentication Technique base on GNSS/UWB Positioning using Particle Filter

5.3.1 System Model

I focus on a situation where mutually trusted fixed nodes are interested in estimating the position of a mobile node securely, as shown in Figure 5.3. The system includes five fixed transceivers ($GNSS/UWB_1..4 and GNSS/UWB_M$) to localize the key fob (smartphone) and a controller. $GNSS/UWB_M$ is electrically coupled to the controller effectively such that it can be operated by the controller and sends signals to the controller. The $GNSS/UWB_M$ is installed on a car and is configured to send a request pulse at a request time, and the key fob transmits a reply pulse in reply to the request pulse. The controller (verifier) includes a processor configured to manage the localization system. The nodes measure the ToF between them, relying on GNSS/UWB signals for accurate time resolution. The nodes use OHTOSS and zero-knowledge for logical-layer data and any other information needed for secure ranging. I suppose that the attacker has sophisticated hardware and processing capabilities to eavesdrop on communications between honest nodes and get information at the granularity of the GNSS/UWB-pulse level. The malicious node can synchronize eavesdrop on the communication between anchor nodes and equally adapt the signal's transmission power. An attacker can control the communication channel and relay secure communications between honest mobile nodes or eavesdrop on the data they transmit. The inability of the attacker to predict this secret information is a security measure against the logical layer attack. Nevertheless, sophisticated hardware and processing power permit an attacker to launch an ED/LC attack at the physical layer.

ED/LC attack occurs because of predictable symbols, which are amplified by long symbols. To prevent ED/LC attacks on the physical layer, I propose a GNSS/UWB-Zero-knowledge as a secure modulation scheme to prevent ED/LC attacks as descried in the flow chart of Figure 5.2.

5.3.2 Group Management System Base on OHTSS for Key Management and Authentication

In the Original Pedersen (n, t n), all participants have the same authority level. In this section, I propose an enhancement of Pedersen's secret sharing in which a secret S can be distributed to a group of participants depending on their authority chapter 3. I start by discussing my assumptions about the network. After that, I propose enhancing Pedersen's (n, t, n) secret sharing scheme to the OHTSS authentication approach.

Compare to other proposed schemes chapter 3, [106] my proposer does not rely on any underlying secret management subsystem assumption. There is no trusted third party to generate and distribute the private/public keys because there is no pre-built trust relationship between nodes in the network. The network generated and maintained all the user keys (secrets) in a self-organized way.

I assume that each anchor node carries an identity or an IP address, which is unique and cannot be changed during its lifetime in the network. Each participant anchor node can obtain its identity through dynamic address allocation or static configuration. I equally assume that each anchor node has a mechanism to discover and build an identity routing table for other anchor nodes in the network. Also, each anchor node has a build-in GNSS/UWB chip. Consider a situation where the network is divided into three hierarchical levels. The highest level belongs to the Key fob, level two is the controller, and lower levels belong to other anchor nodes in the vehicle system.

Anchor Node Positioning: I consider a set of anchor nodes (UWB) radios mount on a GNSS receiver position, as presented in Figure 5.3. The model use ToF to measure it position and particle filter is use for the fusion of GNSS/UWB. In general, time of flight is calculated as

$$\text{dist} = \frac{t_s^V - t_r^V - \delta}{2} \cdot c \tag{5.1}$$

where t_s, t_r are challenge and response time respectively, δ is the time delay taking by the receive to respond to the challenge, and c is the speed of light.

Next, I derive the equations of my particle filter using the method in chapter 4. Let z_t, v_t, s_t denote the observation for any given time step t, mobile user action and system state respectively. However, I are interested in the distance between mobile terminal and fixed terminals. Unknown biases are used to augment the system state $b_{k k-1}^{N}$ of each UWB beacon, where N is the set of beacons which determine 3D position $B_{k k}^{N}$.

Denote $\mathcal{N}^{(i)}$ as the set of AN of the target, $M^{(i)}$ as the number of visible satellites, and k is the GNSS output time. I now formulate the integrated positioning as follows:

$$\begin{aligned} \Psi(\mathbf{X}_k) &= \int p(\mathbf{X}_k \mid \zeta_{1:k}) \partial \mathbf{X}_k \\ &\propto \underbrace{p\left(\zeta_{G,k}^{(i)}, \hat{X}_{k-1}, \zeta_{W,k}^{(i)} \mid \mathbf{X}_k\right)}_{} \; \underbrace{p\left(\mathbf{X}_k \mid \mathbf{X}_{k-1}\right)}_{\text{Likelihood of information}} \; \underbrace{\Psi(\mathbf{X}_{k-1})}_{\text{Prediction}} \end{aligned} \tag{5.11}$$

find the posterior target distribution having state $\mathbf{x}_k$ with the information collected by GNSS/UWB as shown in (5.2)

$$\Psi(\mathbf{X}_k) = p(\mathbf{X}_k|\zeta_{1:k}), \quad \forall i \in \mathcal{M} \tag{5.2}$$

where Ψ is the collected information at corresponding time. $\zeta_k^{(ii)}$ includes the GNSS and UWB measurement of AN, $i \left(\zeta_{G,k}^{(i)}\right)$, and $\left(\zeta_{W,k}^{(i)}\right)$, respectively. Then, the $\mathbf{X}_k$ which makes a maximum with $\Psi\ (X_k)$ is the integrated position. $\Psi\ (\mathbf{X}_k)$ can be expressed in (5.11) as shown at the top of the next page.

Group Management System: my proposed approach comprises of identity-based authentication and distributes key (secret) generation. Each anchor node is provided with a private/public key pair by the key generation component in a distributed way. The private keys generated are used for authentication. The identity base mechanism for authentication provides end to end confidentiality and authentication between the communication anchor nodes. A successful authentication process is followed by exchanging a session key by the communication nodes, which is then used for future communication.

Master Key (Secret) Generation: Consider a network with n anchor nodes in the initial phase with a private/public key pair, call master key (MSk, MPK) used to provide key generation service to all anchor nodes in the network. The key generation component generates the master public key pair so that the master (MPK) is known to all the anchor nodes in the network. All the anchor node shares the master private key MSK in a (k, n) OHTSSS fashion. Each anchor node holds a unique secret share of the MSK, and no anchor node can reconstruct the MSK using only its secret share. Any K or more anchor nodes can reconstruct the MSK, whereas it is infeasible for any $K - 1$ anchor nodes to reconstruct the MSK.

my proposed distributed key generation technique is different from the basic OHTSS scheme. There is no dealer to safely compute the master key, separate, and share the master key (secret) to all anchor nodes. Instead, the master key pair is generated collaboratively by the initial network anchor nodes.

All participating anchor nodes agree on a value a_0. Each anchor node $UWB_{M,1,..,4}$ randomly chooses a secret $b0_i$ and two polynomials $f_i(x)$, $f_i^{'}(x)$ over finite filed of degree $k - 1$, such that

$$f(x) = \sum_{v}^{t=1} b_i x^v mod q \tag{5.12}$$

$$f^{'}(x) = \sum_{v}^{t=1} a_0 x^v mod q \tag{5.13}$$

and computes it sub-share for node $UWB_{M,1,..,4(j)}$ using the method proposed in chapter 3 as

$$\lambda_{i,j} = f_i^j \bigotimes f'^j_i \tag{5.14}$$

for $j = 1, 2 \dots n$, f_i^j and f'^j_i are the j-th derivatives of the polynomial f(x)/ f′(x) and sends λ_{ij} securely to the P_j. After sending the $n - 1$ sub-shares, P_j can computes the $UWB_{M,1,..,4(j)}$ master private key (MPK) share as

$$\sigma_j = \lambda_{1,j} + \lambda_{2,j} + \dots, +\lambda_{n,j} \tag{5.15}$$

Let the polynomial generated in OHTSS be

$$f(x) = S + b_1 x + b_2 x^2 + \dots b_{k-1} x^{k-1} \tag{5.16}$$

then the polynomial generated by AN_i in my scheme is

$$f_i(x) = c_i + b_{i,1} x + b_{i,2} x^2 + \dots b_{i,k-1} x^{k-1} \tag{5.17}$$

It can be seen that

$$f(x) = f_1(x) + f_2(x) + \dots f_n(x)$$

Therefore, jointly generated master private key is

$$S = \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} f_i(0) \tag{5.18}$$

Each participant can verifier the malicious behaviour of other participant to prevent secret generation as:

$$\psi_v = g^{\sum_i^n \sigma_j} modp, v = 0, 1, 2, \dots, t-1 \tag{5.19}$$

After generating the master private key, $UWB_{M,1,..,4(i)}$ publishes $S_i D$, where D is a common parameter use in the Identity-based scheme. Therefore, the master public key can be computed as

$$Q_M = \sum_{i=1}^{n} S_i D \tag{5.20}$$

I consider identity-based cryptography use to generate a node's public key. An anchor node's public key can be any arbitrary string. In my proposer, the public key is computed as:

$$Q_{ID} = H(ID, \Psi(X_k), EPT) \tag{5.21}$$

where $H()$ is a one-way hash function, ID is the anchor node's identity, and $\Psi(X_k)$ is the position of each anchor node as shown in (5.11) and EPT is a time stamp shielding to generate new key pairs for the entire system.

Since each anchor node's public key is known to all nodes in the network, I can define this public key as a network identifier (NID) for the requesting node. In my case, I consider that only the nodes in the highest level of the hierarchy can initialize a secret reconstruction request.

Take the case of a smart car keyless entry system; I consider the node at the hierarchy to be an intelligent key, as shown in Figure 5.1.

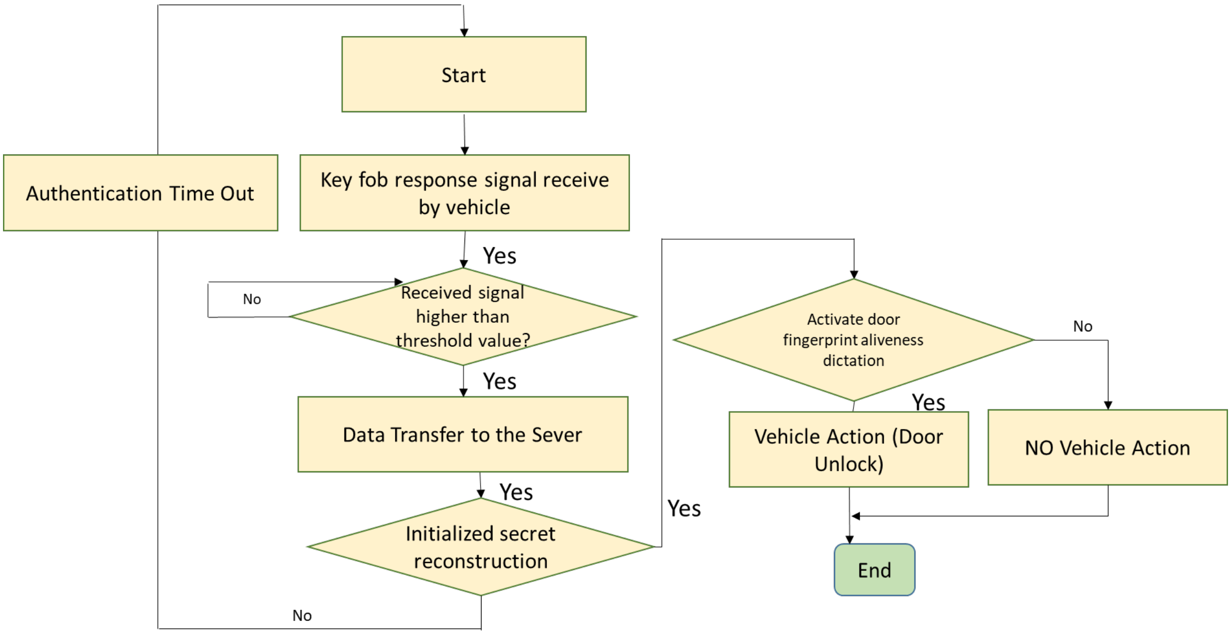

Start
Authentication Time Out
Key fob response signal receive by vehicle
Yes
No
Received signal higher than threshold value?
Yes
Data Transfer to the Sever
Yes
Initialized secret reconstruction
No
Yes
Activate door fingerprint aliveness dictation
No
Yes
Vehicle Action (Door Unlock)
NO Vehicle Action
End

FIGURE 5.2: Flow Chart of Relay Attack Prevention Algorithm

Adding New Anchor Node: When a new node joins the network, it presents a self-generated temporary public key, identity, and other significant physical evidence (depending on key issuing method) to k neighbor ANs. Next, the new node requests its share of the master private key and master public key from the PKG service. Each node in the system verifies the legality of the identity of the new node (ND). If the verification is successful, using the method proposed in chapter 3 section *E* the process of adding a new participant, the private key share can be generated as follows:

Each node (AN_i) generate the partial private key share for ND as shown in point "a" of chapter 3 section *E*, AN_i randomly splits the result into h values such that; $c_l = \beta_{1,l} + \cdots + \beta_h, l$, encrypts the partial secret share using the temporary public key of demanding node and sends $\beta_{m,l}$ to $NDp_{m,j} \in h$, for $m =$ to ND. ND receive all values $\beta_{l,m}$ and computes it private key share as

$$\beta_l = \sum_{m=1}^{w} \beta_{l,m} \tag{5.22}$$

The correctness of private key share is verify using (19) of chapter 3 section *E* the process of adding a new participant. Thant is

$$g^{\lambda'_i, j'} \equiv \prod_{V=j'}^{t-1} d_V^{\frac{V!}{(V-j')!} i'^{V-j'}} = g^{f^{j'}(i')} \tag{5.23}$$

After receiving the share of the master secret key, the new joining node is ready to provide PKG service to other new nodes.

5.3.3 Identity-based Authentication

All keys generated in the previous sections are used for authentication. The authentication process permits the mobile anchor node to ensure that the peer node's identity the node is communicating with is from a reliable source. They by preventing an attacker

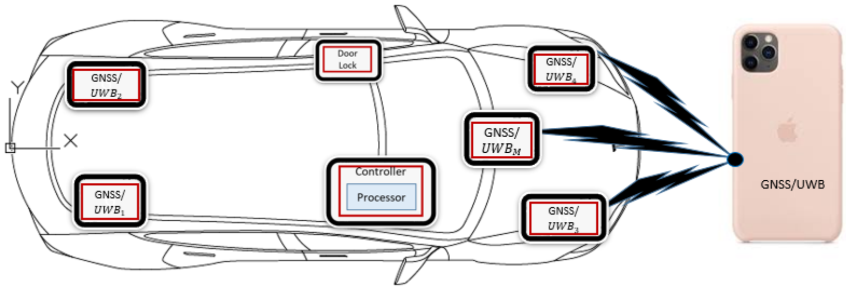


FIGURE 5.3: diagram of a passive entry passive start (PEPS)

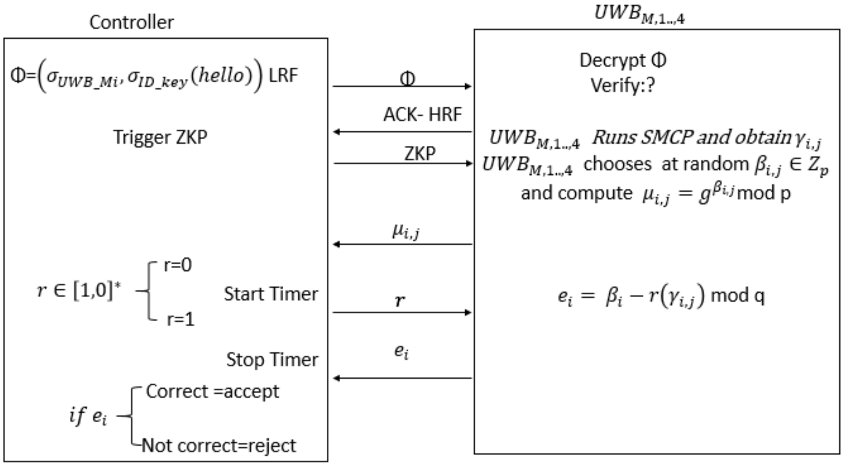

Controller
$UWB_{M,1..,4}$
$\Phi = (\sigma_{UWB\_Mi}, \sigma_{ID\_key}(hello))$ LRF
Decrypt Φ
Verify:?
Φ
ACK- HRF
Trigger ZKP
ZKP
$UWB_{M,1..,4}$ Runs SMCP and obtain $\gamma_{i,j}$
$UWB_{M,1..,4}$ chooses at random $\beta_{i,j} \in Z_p$
and compute $\mu_{i,j} = g^{\beta_{i,j}}$ mod p
$\mu_{i,j}$
$r \in [1,0]^*$
r=0
r=1
Start Timer
r
$e_i = \beta_i - r(\gamma_{i,j})$ mod q
Stop Timer
e_i
$if\ e_i$
Correct =accept
Not correct=reject

FIGURE 5.4: Proposed Authentication Protocol

from launching any replay attack on the network. The identity-based encryption (IBE) used in this research work provides end-to-end authentication. The IBE mechanism uses the public key infrastructure (PKI)-support approaches [107]–[109]; also, no handshake and exchange of certificate is required. A successful authentication procedure is illustrated in Figure 5.4.

5.3.4 Distance bounding proof based on multi-prover ZKP

Consider the case of a vehicle and key fob of Figure 5.1 it is assumed that they is a Smartphone (key-fob), immobilizer anchor node (UWB_M) and other anchor nodes ($UWB_{1,..,4}$) defined as $[K_0, K_1, K_2]$=[1,1,4], where $k_m = k_2 = 4$. Supposed that the key fob wants to unlock the vehicle all participant pooling their shares $\lambda i, j$. Every p_i has a secret input $\text{Y}_{si} = \gamma_i, j$. The secure multi-party computation (SMC) is run by t shareholders for a function f $(\text{Y}_{s1}, \ldots, \text{Y}_{st}) = \text{Y}$, where $\text{Y} = f(0)$ and

In ZKP, the verifier (immobilize) sends challenge to the key fob (prover) to proof that it is not located above a predefined distance τ as follows;

Every $UWB_{M,i,..4}$ chooses at random a number $\beta_i \in Z_p$ and compute $\mu_{i,j} = g^{\alpha_i}$ mod p and send $\mu_{i,j}$ to CON_M, for $i = 1, 2, \ldots, n$. I consider CON_M to be the verifier, $UWB_{M,i,..4}$ and $keyfob$ to be the provers. CON_M chooses a number at random using non linear feedback shift register (NLFSR) [20] in $r \in [1, 0]^*$ and sends it to every $UWB_{M,i,..4}$. $UWB_{M,i,..4}$ computes $e_i = \beta_i - r(\lambda_i)$ mod q and sends e_i to CON_M, for $i = 1, 2, 3, \ldots, n$. CON_M accepts the fact that $UWB_{M,i,..4}$ share a secret Y such that equations (5.22) and (5.23) are correct and measures the time $t_s^V - t_r^V$ between the challenge and the response, else, V rejects the response. This process is repeated a predetermined number of times before the verifier is convinced that $UWB_{M,i,..4}$ and CON_M share MPS. Following the execution of the ZKP protocol, the verifier knows that the prover (Key fob) is within a certain distance. Note that only the distance between the key fob and CON_M is determined in this research work.

5.4 Performance Analysis

In this section, I start by analyzing my proposed method at a high level to meeting security service requirements, followed by the analysis of computational complexity and communication overhead. Finally, I show the simulation results.

5.4.1 Analysis of Different types of Attacker

The distance between the prover and verifier can leak. The attacker can infer its position (x, y) relative to the prover and verifier if D knows the distance between P and V. These two attack models are illustrated in this section.

Distance leakage: The following assumptions are made: firstly, three types of anchor nodes, the prover $UWB_{M,i,..4}$, the verifier V or CON_M, and the attacker D. Secondly, $UWB_{M,i,..4}$, and verifier execute ZKP described in Section 4.5. Thirdly, V is trusted and can not be compromised. Also, both $UWB_{M,i,..4}$ and V are honest and compile with ZKP. Fourthly, D can listen to the communication of ONAs and V. Also, D does not hold any secret information that forms part of the protocol between $UWB_{M,i,..4}$ and CON_M.

To mount an attack, the attacker needs to record when the messages from ZKP arrive at its radio interface. The attacker must register three consecutive arrival times of the messages between $UWB_{M,i,..4}$ and CON_M to obtain enough information to calculate the distance between them. The arrival times τ_i of three consecutive messages can be described by the following three equations:

$$\tau_0 = t_0 + t_{vd} \tag{5.24}$$

$$\tau_1 = t_0 + t_d + \delta_p + t_{pd} \tag{5.25}$$

$$\tau_2 = t_0 + 2t_d + \delta_p + \delta_v + t_{vd} \tag{5.26}$$

Where t_0 is the time at which the signal was sent to P, t_{vd} is the travel time of the signal from V to D, τ_1 is the time at which the attacker receives the massage, t_d is the time it took the signal to propagate from V to P, δ_p is the time taken by P to process the massage, δ_p is the time it took the signal to propagate from P to D, τ_2 is a response to τ_1 which includes two circulation times between $P^1 2t_d$ and δ_v is the processing times at V. Therefore, the attacker can calculate the signal time of flight as

$$t_d = \frac{(\tau_2 - \tau_0) - \delta_p - \delta_v}{2} \tag{5.27}$$

Thus the distance from V to P is deduced by multiplying (5.27) by the speed of light c

$$D_d = c \cdot t_d \tag{5.28}$$

Location leakage: The attacker can obtain information about its position relative to $UWB_{M,i,..4}$ and CON_M by calculating the difference between the arrival times of two subsequent signals Δ_1. The difference between the arrival times of two is deduced from (5.24) and (5.25) as

$$\tau_1 - \tau_0 = \Delta_1 \tag{5.29}$$

Multiplying Δ_1 with c gives the distance as:

$$c\left(\Delta_1 - \delta_p\right) - D_d = \sqrt{x^2 + \left(D_d - y\right)^2} - \sqrt{x^2 + y^2} \tag{5.30}$$

In (5.30), I assume that CON_M is located at (0,0) and the OAN (key fob) position is in the positive direction of the y-axis, that is, the key fob is located at $\left(0, d_{vp}\right)$. Let the left side of (5.30) be a pseudo distance Δ_{sp} :

$$\Delta_{sp} \equiv c\left(\Delta_1 - \delta_p\right) - D_d \quad \text{for } -D_d \leq \Delta_p \leq D_d \tag{5.31}$$

which become

$$\begin{aligned} \Delta_{sp} &= \sqrt{x^2 + \left(D_d - y\right)^2} - \sqrt{x^2 + y^2} \\ y &= \frac{\pm\Delta_{sp}\sqrt{4x^2 + D_d^2 - \Delta_{sp}^2} + D_d\sqrt{D_d^2 - \Delta_{sp}^2}}{2\sqrt{D_d^2 - \Delta_{sp}^2}} \end{aligned} \tag{5.32}$$

Attacker initiates the ZKP: Suppose that the attacker takes the position of either the prover (or verifier) and initiates a ZPK session with other nodes. They by deviation from the passive attacker model because the attacker is now actively transmitting bits to force the distance to leak. This is a common problem in must relay attack models [78], [110] and distance bounding protocols [100] which do not have any form of authentication. Therefore, even if the attacker does not have a valid key, the attacker can still initiate the protocol and trick the $UWB_{M,i,..4}$ or the attacker into believing its validity. In the country, in my proposed ZKP, no secret information is transmitted between $UWB_{M,i,..4}$ and CON_M in addition to my proposed authentication algorithm.

5.4.2 Security Analysis

Availability assures the survivability of network services, notwithstanding the denial of service attacks. In my proposal, In other to ensure availability, I use the (k, n) OHTSSS algorithm, as any k or more participants work together for key management. Therefore, my security solution is tolerant of any $k - 1$ compromised nodes. The adversaries have to jeopardize at least $k - 1$ participants to break the key management services.

UWB is designed to provide performant ranging while ensuring security against physical layer attacks. In particular, such an attack should fail to reduce or increase the distance of mutually trusted network nodes through a relay or by conducting any other physical-layer attack. A well-designed ToF DBP is naturally resistant to a relay attack. An ED/LC attack is the only option for an attacker to reduce the distance measured. In addition, UWB alone can not provide the uniqueness of a point because UWB only provides local coordinates. Therefore, for unique localization, UWB needs to be combined with GNSS.

Since my proposal relies on a challenge-response for distance measurement, the attacker must compromise both preamble and payload data. The preamble is not a secret, and the attacker can see it in advance but, the payload is generated cryptographically. The receiver can sample the payload signal depending on the information available in the preamble. An attack is successful if the signal sent by the attacker at a given instant produces the same similarity output at the receiver as that from the legitimate user. For an ED/LC attack to be successful, the attacker must predict and advance the challenge-response bits.

Seemly multi-pulse UWB systems assist an attacker with that due to their anticipated symbol structure. On the other hand, in my proposed GNSS/UWB-OHTSS, the communication is protected by homomorphism property. Also, the pulses depend not only on UWB but on a combination of both GNSS and UWB pulses. Therefore, an attacker can only try to guess this information.

5.4.3 Simulations

To further evaluate the performance, I run simulations on a Linux machine $P4-2.0GHz$ with 512MRAM. I implement identity-based encryption into $ns-2$[19] environment, in which the IEEE 802.15.4z is used in the MAC layer. The radio model has a bit-rate of 2Mb/sec with a transmission range of 250 meters. The transport protocol that I used for my simulations is User Datagram Protocol (UDP). The mobile nodes move from a random starting point to a random destination with a maximum speed of each node is 5 m/s. Once the destination is reached, another random destination is targeted after a pause time of 10 seconds.

5.4.4 Communication Overhead

my proposed approach has a lower communication overhead when compared to the conventional PKI-supported security solutions. In my proposal, the PKG service anchor nodes generate the public/private key pair using the identity of each node. Therefore, certificate generation, propagation, and storage are not required. While the traditional PKI-based key management methods use a trusted authority to generates MSK/MPK key pairs for each anchor node, and the public key is propagated in the network. A trusted certificate authority (CA) must sign the public key to identify each node in the network. Each node's certificate is spread in the network for other nodes to get their certifications. Diffusing these public keys and certificates overwhelms network bandwidth and generates a considerable network/connection setup delay.

my method's public key is based on each node's identity, which can be much shorter than the 1024 bits public key in the RSA cryptosystem. The characteristics of using shorter public/private key pairs and without dispersing the long-size certificates decrease the computational complexity and communicational overhead. Nonetheless, in a conventional PKI-based approach, accumulating those public keys and certificates adds significant overhead on local storage for large ad hoc networks. In my proposal, the communication overhead is introduced by the key generation component. In the initial phase of the network, n anchor nodes have to generate the key pair in an organized manner jointly, which causes an increase in the network setup time.

I use hierarchical threshold secret sharing to enhance the network's fault tolerance while adding more communication overhead. One attractive point is that much more significant communication overhead is expected if I realize a similar system with the same characteristics using conventional PKI-based methods. Also, the hierarchical network mode equally prevents shareholders from faking their position.

5.4.5 Setting the Energy Thresholds

Determining the upper-bound threshold (Γ) : The receiver relies on the distance between sender and itself to set Γ. A more significant committed space causes the receiver to anticipate less power, thus establishing a lower Γ. Therefore, by raising the committed distance, the adversary helps disclose its evil plans.

The path loss [111] function for outdoor GNSS is given by

$$f(d)^G = PL\left(d_0^G\right) + 10\gamma \log\left(d/d_0\right) + z_\sigma \tag{5.33}$$

Where γ is the propagation factor which depends on the environment, free space loss form distance d_0 to d, d_0 is the reference distance and z_σ is a random zero-mean Gaussian variable having a standard deviation of σ that reflects the variation of path loss. The free space propagation factor is $2, 2.8/3$ for outdoor environment, $4/6$ for indoor environment and 4 for wet soil.

The path loss function for UWB can be deduced from [112] as

$$f(d)^U = PL_0 + 10 \cdot n \cdot \log\left(\frac{d}{d_0}\right) \tag{5.34}$$

Therefore, path loss for GNSS/UWB can be expressed as

$$f(d)^{GU} = (PL_0)^{GU} + 10 \cdot n \cdot \gamma \cdot \log\left(\frac{d}{d_0}\right) + z_\sigma \tag{5.35}$$

The power loss is given by

$$f(d) = 10 \log\left(\frac{(\lambda_b)^2}{(\lambda_{\text{st}})^2}\right) \tag{5.36}$$

where the pulse instantaneous power expected by the receiver is $(\lambda_b)^2$, and $(\lambda_{\text{st}})^2$ is that the sender has truly sent, both in Watt such that $(\lambda_b)^2 = (\lambda_{\text{sent}})^2 10^{f(x)/10}$.

$$\Gamma = \beta\left(\lambda_b + N\right)^2 + \alpha(N)^2 \tag{5.37}$$

Figure 5.5 shows the path loss function in 5.35, which the receiver used to detect the threshold Γ as well as the worst signal received after expected additional deterioration. The receiver fixes the threshold based on the best-expected signal. The most convenient situation to the enemy is when the received signal power is the lowest (E), which enables the enemy to amplify the signal near the transmitter until the key fob signal strength is in uniform with the predicted path loss over the claimed distance. Where N is the receiver instantiation zero-mean Gaussian noise, β and α is the number of nonces and zeros in the zero knowledge interactive proof respectively.

5.4.6 Computational Complexity

my approach's main computations come from key generation and key management such as encryption, decryption, and verification. The master key generation uses a outsource hierarchical threshold secret sharing scheme, and the computational quality depends on the number of participants. Compared to the conventional method, the identity-based signature has the same computational complexity with an insignificant

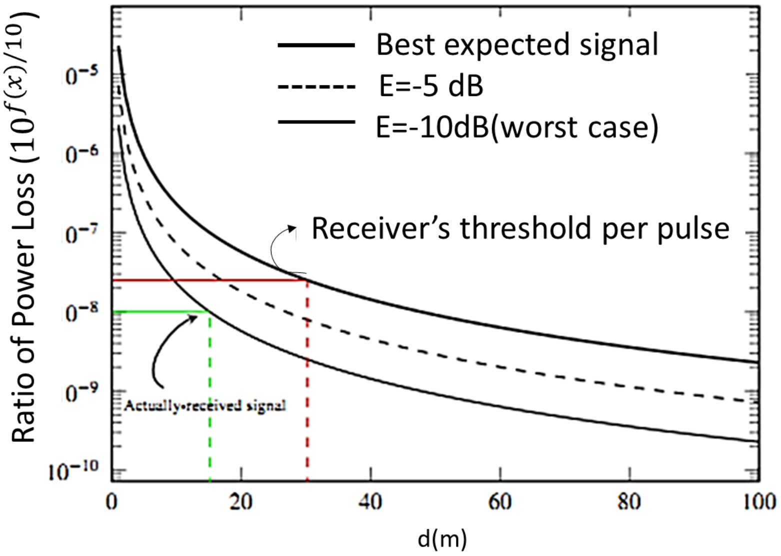


FIGURE 5.5: The best-expected signal power as determined by the key fob using path loss function.

difference. Finally, during the interactive proof phase, an attacker that eavesdrops on the communication will not get any useful information because of the homomorphism property. As I mentioned initially, using a shorter key size in my proposal results in less resource consumption.

Figure 5.8 shows the ratio of successful PKG issuing by altering the threshold value. A considerable threshold value needs the node to collect many shares for combining its private key in PKG service. However, in some situations, the requesting anchor node only has a few neighbors. From Figure 5.8, the ratio of successful PKG service diminishes as I increase the threshold value. When I alter the threshold value from low to high, most mobile anchor nodes could not get sufficient PKG service neighbors.

Figure 5.9 show that the attack success probability decrease exponentially as the number of rounds increased in the challenge-response increases. Figure 11 shows that an attacker's average delay time to attack the GNSS/UWB system is 13.42ms, while the average delay time for an attacker to launch an attack on the system is 7.74ms. Thus my proposed GNSS/UWB localization improves system security compared to UWB only ToF relay attack prevention method.

5.5 Conclusion

Radio networks are an emerging research area with essential applications. However, the security problem in the radio network is not trivial to solve. This paper proposes a new efficient key authentication and management approach for securing the radio network. The principal contribution of the work depends on the following aspects: First, I use the concept of identity-based cryptography to implement authentication and confidentiality. Secondly, I avoid a trusted third party or centralized certification authority to share the public keys and certificates. Thirdly , I use GNSS/UWB ToF to determine user position, which adds another security level to my proposal, therefore improving the network's tolerance to compromised nodes and saving network bandwidth. Lastly,

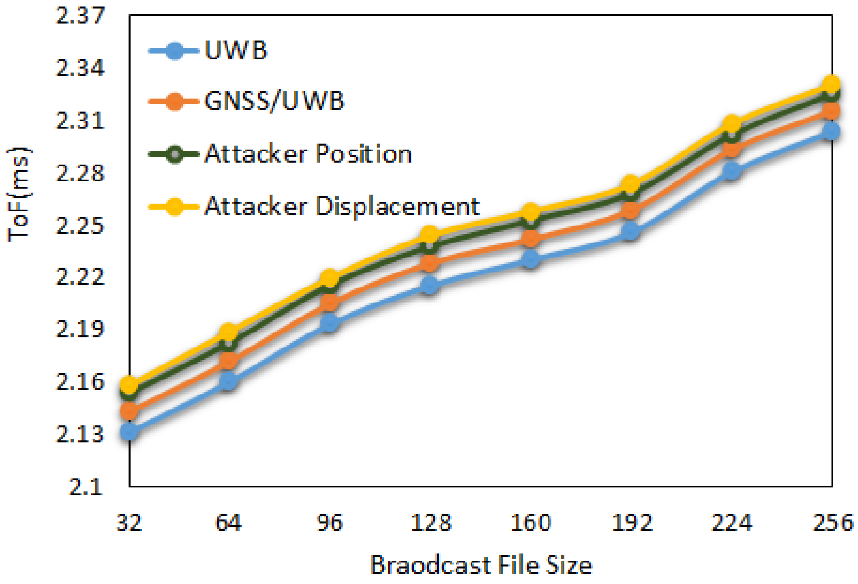


FIGURE 5.6: Time taking by CON_M to localize key fob and time taking buy attacker to determine its position.

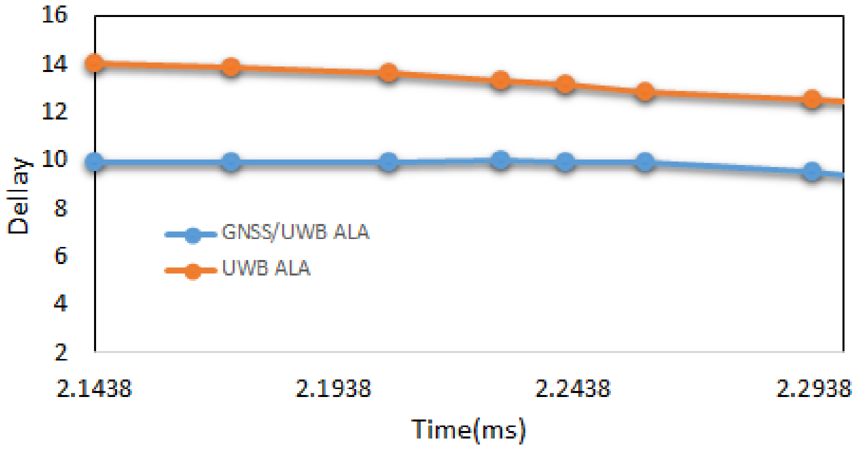


FIGURE 5.7: The delay between the time requires to initiate the ZKP after authentication and the time needed to launch an attack.

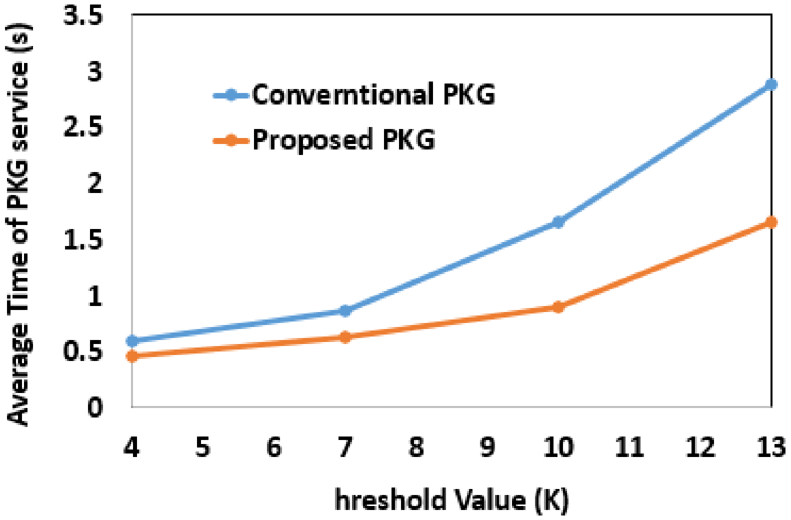


FIGURE 5.8: Cooperation Between Conventional and Proposed Average PKG Service Time.

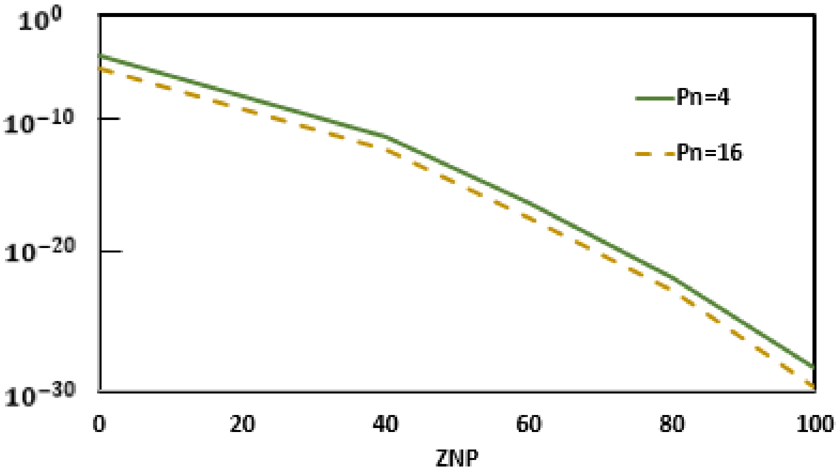


FIGURE 5.9: Simulation results for Zero-Knowledge Interactive Proof Scheme.

a session key is generated without an additional handshake, which reduces the communication cost. My scheme's most significant benefit lies in enhancing security while decreasing the communication overhead and resource consumption.

I have seen that many security solutions have been proposed to secure radio networks, but no one can challenge that it solves all the security problems. Securing the radio network is still new and would be a long-term continuous research topic.

Chapter 6

Conclusion

New proximity, distance, and secure localization scheme based on user location and OHTSSS [23] for proximity, distance, and secure localization were proposed. I used an existing authentication protocol in combination with the ZKP over a secure network. After authentication, the anchor nodes were able to generate the master secret (secret shares) securely. Two use cases (car keyless entry system and land survey) were presented as examples of integrated technology between UWB and Hierarchical secret sharing. This thesis is divided into two sections. One section is for data collection and navigation (preamble), and the other section is for secure ranging (payload), as shown in Figure 6.1.

1. At the preamble, positioning was considered in two scenarios. The first situation is when the target node is surrounded by anchor nodes, which applies to TDoA (for example, in the land survey). The second situation is when the target is not covered by anchor nodes which applies to ToF (car keyless system).
2. The second case is at the payload, where two conditions were considered for the ZKP.
    (a) Case location information is not required, such as ownership proof. For example, in the case of land disputes proposed in chapter 3, the landowner, state authority, neighbors must jointly prove that they share a secret belonging to a particular land parcel following a $(1, 2, 3_T)$ access structure. Here, participants from each level are required (6.2).
    (b) ANs location information is required; for example, consider the case of car keyless entry system 5 where the door can not be open without the key-fob in a pre-defined domain.

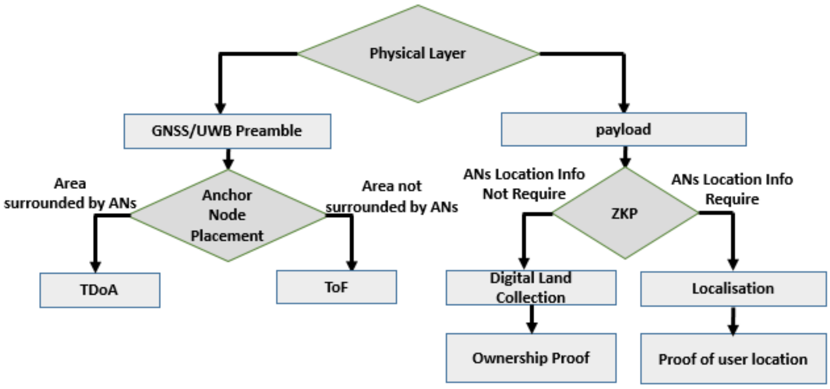


FIGURE 6.1: Summary of different subsection proposed in this thesis

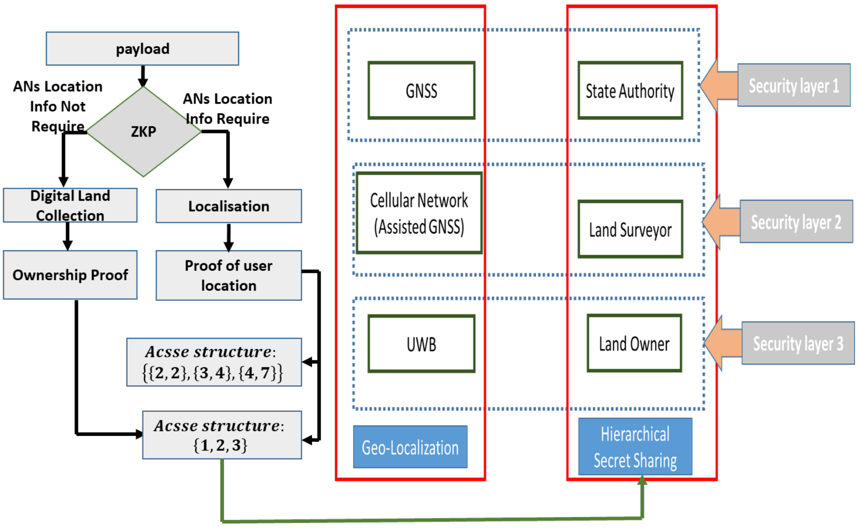


FIGURE 6.2: Prove of Land Ownership Right

FIGURE 6.3: Search and rescue in disaster scenarios

6.1 Applications of my research works

6.1.1 Privacy-Preservation Contact Tracing Attack

This is one of the most recent physical layer attacks proposed by Google and Apple where mobile phones are in the system transmitting information to locate another mobile phone jointly. So, attackers can easily relay/replay such identity information being transmitted.

6.1.2 Search and Rescue in Disaster Scenarios

Another situation is search and rescue in disaster scenarios, where the GNSS signal is completely blocked as the drone moves from outdoor to indoor. In such a situation, location information will be based on the last signal received from GNSS and UWB, as shown in Figure 6.3. Figure 6.4 shows the results of an experiment of a drone moving from outdoor to indoor. I considered two cases (green rectangles present an outdoor situation where GNSS and UWB signals are available and the distance between the two rectangles is the remaining situation where only UWB measurements are available).

Figure 6.4 shows the localization error as the smartphone holder movies from outdoor to indoor. The dotted green rectangle represents the parts where GPS and UWB data are combined outdoor, and the distance between the rectangles is the indoor potion.

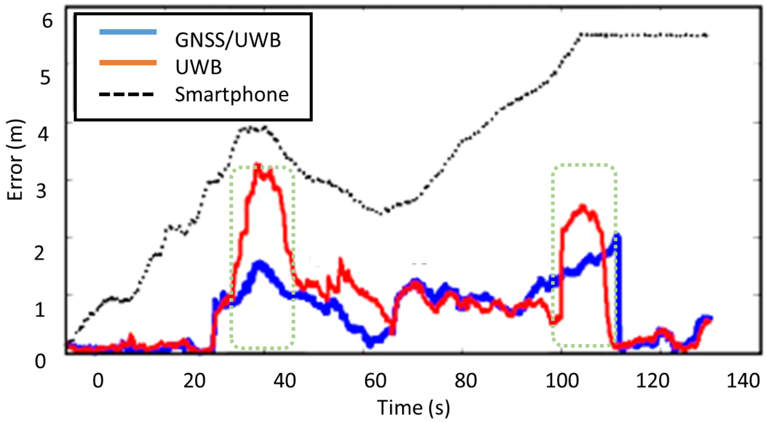


FIGURE 6.4: Estimated paths and localization errors from Outdoor to Indoor

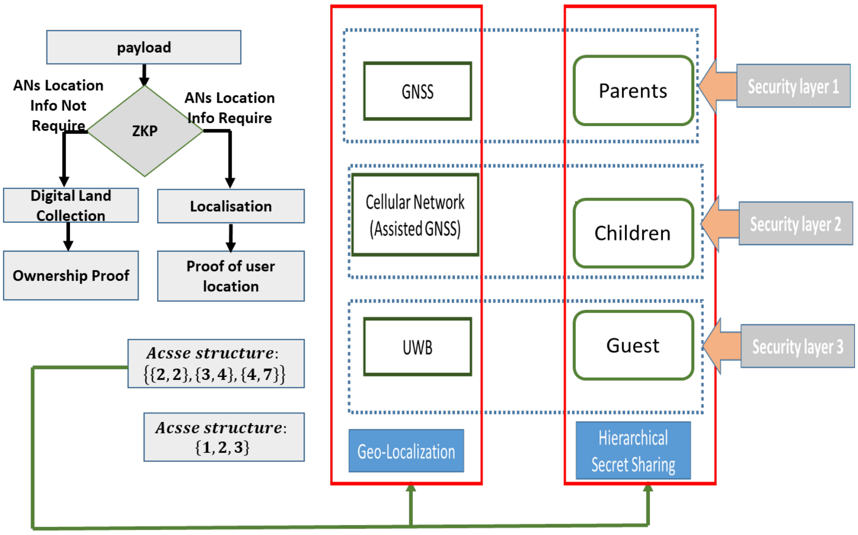


FIGURE 6.5: Smart House security of the opening and closing of the main door/gate of the house

6.1.3 Home Door Unlock

In a house unlock system where at least one member (mother, father, child) of the household holding a smartphone is needed to open the house's main door, the secret reconstruction (action to open the door) can be performed using Lagrange interpolation. As can be seen from the figure, they are three hierarchy, at the lowest level (L_1), at least 4 participants are required to reconstruct the secret, at L_2 at least 3 participants are needed, and at the highest level, at least 2 participants are required. In the same way, If we consider that every member of the household went out, then signals from GNSS and UWB are also needed as shown in Figure 6.5.

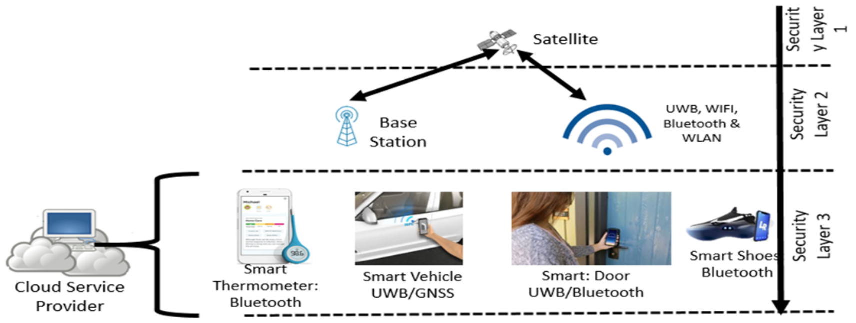


FIGURE 6.6: Hierarchical IoT Network Architecture for the interconnection and management of IoT devisees

6.2 Future Works

6.2.1 Advance Wireless Hierarchical Network Secure Model for IoT based on machine learning

Internet of Things (IoT) is transforming lives by providing innovations such as monitoring and controlling the connected, intelligent objects. IoT utilization range from smart cities, manufacturing, homes, vehicles, e-healthcare to the intelligent control system, wearables, farming, transportation, to name a few. The acclimatization of these devices increases exponentially, which generates a large amount of data for processing and analyzing. Thus, besides bringing ease to human lives, IoT devices are susceptible to threats and security difficulties that bother the users for using them in sensitive environments such as transportation, e-health, smart home, etc. In addition, a significant problem is identifying each device because IoT devices do not have any manufacturer standards. In this research work, an advanced wireless security technique based on machine learning is considered as a potential solution for exiting IoT device uniqueness identification, followed by investigating and proposing advanced security methods for next-generation IoT devices with more infancy on device uniqueness identification.

Motivation

1. To propose a method for exiting IoT device identification by combining the global navigation system, local position system, device characteristic (date, manufacturer, component IDs, etc.), and some other factors are still to be determined.

    1. Prove that machine learning can be considered as an effective way of identifying each IoT device.
    2. Propose a method of identifying next-generation IoT device.
    3. Propose an intelligent soft handover technique for IoT devices for the interconnection to the wireless network, as shown in Figure 6.6

Review on machine learning (ML) in the security of IoT was done based on search engine like Elsevier, IEEE, Springer, Wiley, Hindawi, MDPI, Arxiv, and Taylor and Francis by sorting out to cross-check the title, abstract, and keywords from journal and conference papers. Authors tried their best to incorporate all possible related articles and in this regard, authors manually.

TABLE 6.1: Existing Surveys Relating to IoT Device Identification

Convertional	[113]	[114]	[115]	[116]	[117]	[118]	My Proposal
Deep Learning (DL)	*Yes*	−−	*Yes*	−−	−−	*Yes*	*Yes*
Rogue device detection (RU)	−−	−−	−−	−−	*Yes*	*Yes*	*Yes*
Device type Identification (DTI)	−−	*Yes*	*Yes*	−−	−−	*Yes*	*Yes*
Feature-base specific device Identification	*Yes*	*Yes*	*Yes*	*Yes*	1.63	*Yes*	*Yes*
Unsupervised device detection	−−	−−	−−	−−	*Yes*	*Yes*	*Yes*
Still do be determine characteristics	−−	−−	−−	−−	−−	−−	*Yes*

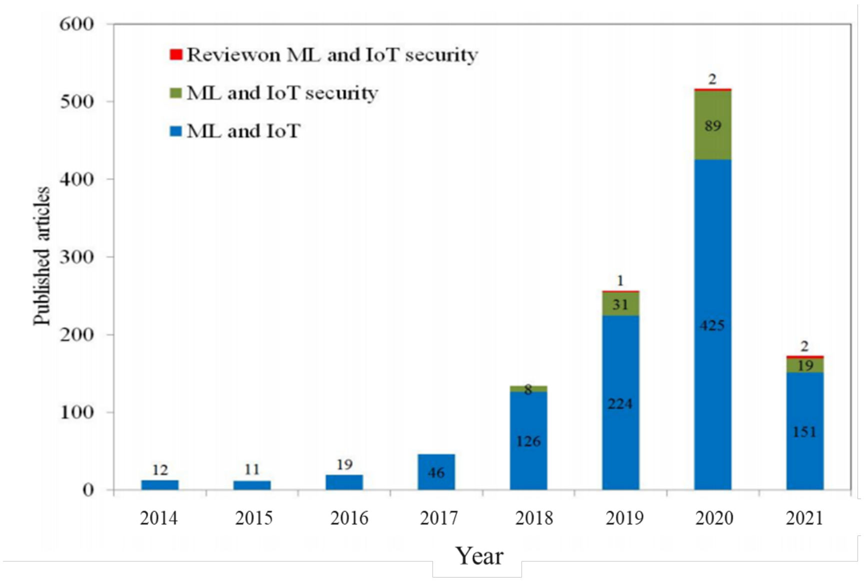


FIGURE 6.7: A Statistic on paper published on ML and IoT, ML and security of IoT, and survey on ML and security of IoT till March 2021

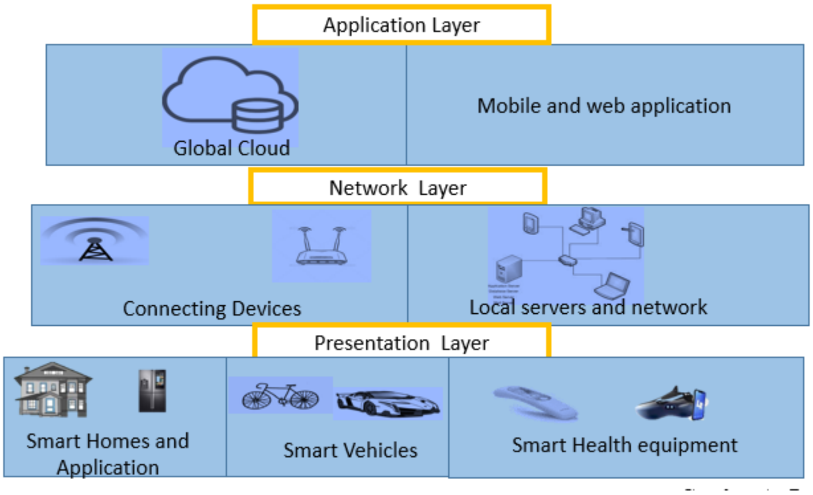


FIGURE 6.8: IoT layer Structure

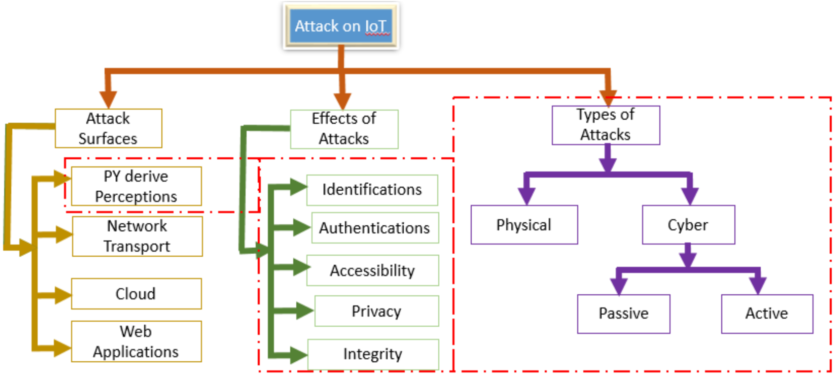


FIGURE 6.9: Attacks on IoT Devices

In this research work, my main point of focus is the presentation layer which is made up of physical (PHY) and medium access control (MAC) layers. The PHY layer mainly deals with sensors and devices that are used to transmit and receive information using different communication protocols such as RFID, Zigbee, Bluetooth and UWB.

The number of interconnected IoT devices and the global market of IoT systems so far and future predictions are illustrated in Figure 6.7, which means that IoT research, development, and security have received massive attention in the last decades. A conventional architecture of IoT consists of three layers, namely physical (perception) network and application (web) layers [20], as shown in Figure 6.8. Each of these layers requires different security techniques.

6.2.2 Importance of Security in IoT

IoT devices are used for multiple purposes within an open network, making them more accessible to users. On the one hand, IoT makes human life easygoing, comfortable, and technologically advance; on the other hand, IoT puts users' privacy in danger because of different attacks/threats [37], [38]. Since anyone can access specific IoT devices from anywhere and anytime without user authorization, in addition, they are no unique ways to identify these devices, which makes the security of IoT devices a burning question. Therefore, they are needs to implement a wide range of security systems to protect IoT devices. It is very challenging to implement a highly secure method for IoT devices because of the low computational and storage capacity.

The optimal approach depends on the data to be analyzed. Figure 6.10 shows that the decision tree has about 32% of the most used technique for the security of IoT devices compared to other approaches like Random Forest. Random Forest is based on ensemble learning of decision trees, and state-of-the-art deep learning could improve performance compared with DTs. A comparative analysis between Random Forest and decision tree is considered as the next step.

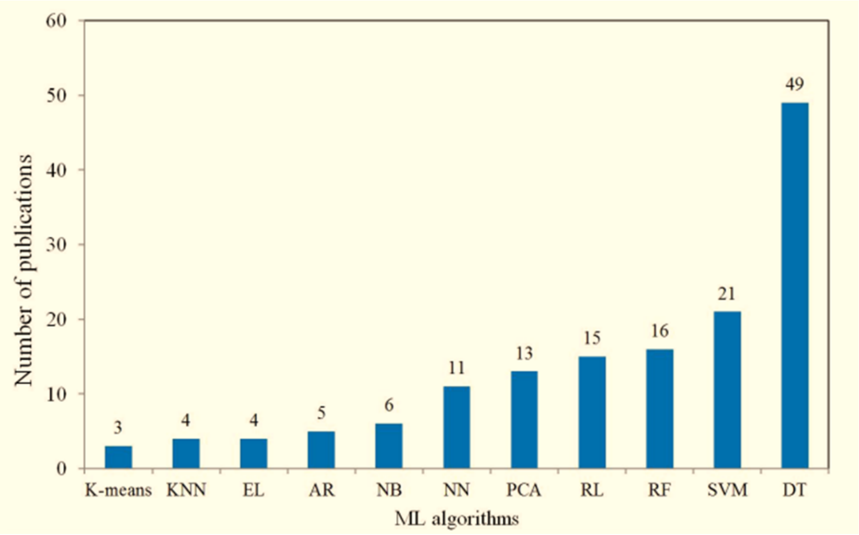


FIGURE 6.10: A Statistic on papers published on various ML algorithms used in security of IoT until May 2021

Publications

Reviewed Journal Papers

1. **Ngye Antoinette Agwa**, Takumi Kobayashi, Chika Sugimoto, Ryuji Kohno, "Hierarchical Threshold Outsource Secret Sharing and Interactive Proof Scheme for Land Conflicts" International Journal of Computer Science and Telecommunications (ISSN: 2047-3338), Volume 11, Issue 04, September/October 2020. (Published)

2. **Ngye Antoinette Agwa**, Takumi Kobayashi, Chika Sugimoto, Ryuji Kohno, "A GNSS/UWB Integrated Positioning Methodology for Geo-Positioning," International Journal of Computer Science and Telecommunications (ISSN: 2047-3338), (Published)

3. **Ngye Antoinette Agwa**, Takumi Kobayashi, Chika Sugimoto, Ryuji Kohno, "Advanced GNSS/UWB Security Enhancement Against Relay Attack to Keyless Entry System" IEEE Open Journal of the Computer Society (ISSN: 2047-3338), . (Submitted

Reviewed International Conference Papers

1. **Ngye Antoinette Agwa**, Takumi Kobayashi, Chika Sugimoto, Ryuji Kohno, "Security of Patient's Privacy in E-Health Using Secret Sharing and Homomorphism Encryption," The 31st International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2020), paper ID 1055, Nagoya, Japan, July 3-6, 2020 (Published)

2. **Ngye Antoinette Agwa**, Takumi Kobayashi, Chika Sugimoto, Ryuji Kohno, "GNSS/UWB-based secure automated land survey Positioning Method. (Submitted)

Bibliography

[1] D. B. Jourdan, D. Dardari, and M. Z. Win, “Position error bound for uwb localization in dense cluttered environments,” *IEEE transactions on aerospace and electronic systems*, vol. 44, no. 2, pp. 613–628, 2008.

[2] S.-G. Kwon, S.-H. Lee, K.-R. Kwon, E.-J. Lee, S.-Y. Ok, and S.-H. Bae, “Mobile 3d game contents watermarking based on buyer-seller watermarking protocol,” *IEICE transactions on information and systems*, vol. 91, no. 7, pp. 2018–2026, 2008.

[3] L. Qiao and K. Nahrstedt, “Watermarking schemes and protocols for protecting rightful ownership and customer’s rights,” *Journal of Visual Communication and Image Representation*, vol. 9, no. 3, pp. 194–210, 1998.

[4] M. Ramkumar and A. N. Akansu, “A robust protocol for proving ownership of multimedia content,” *IEEE Transactions on Multimedia*, vol. 6, no. 3, pp. 469–478, 2004.

[5] A. Rial, J. Balasch, and B. Preneel, “A privacy-preserving buyer–seller watermarking protocol based on priced oblivious transfer,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 202–212, 2010.

[6] A. Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, “A provably secure anonymous buyer–seller watermarking protocol,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 920–931, 2010.

[7] J. Zhang and L. Liu, “Publicly verifiable watermarking for intellectual property protection in fpga design,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 4, pp. 1520–1527, 2017.

[8] J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. M. Hassan, and A. Alelaiwi, “Secure distributed deduplication systems with improved reliability,” *IEEE Transactions on Computers*, vol. 64, no. 12, pp. 3569–3579, 2015.

[9] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, “Deypos: Deduplicatable dynamic proof of storage for multi-user environments,” *IEEE Transactions on Computers*, vol. 65, no. 12, pp. 3631–3645, 2016.

[10] C.-M. Yu, C.-Y. Chen, and H.-C. Chao, “Proof of ownership in deduplicated cloud storage with mobile device efficiency,” *IEEE network*, vol. 29, no. 2, pp. 51–55, 2015.

[11] S. Mishra, S. Singh, and S. T. Ali, “Mpows: Merged proof of ownership and storage for block level deduplication in cloud storage,” in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE, 2018, pp. 1–7.

[12] X. Jin, L. Wei, M. Yu, N. Yu, and J. Sun, “Anonymous deduplication of encrypted data with proof of ownership in cloud storage,” in *2013 IEEE/CIC International Conference on Communications in China (ICCC)*, IEEE, 2013, pp. 224–229.

[13] A. Brimicombe and C. Li, "Location-based services and geo-information engineering," vol. 21, 2009.

[14] S.-l. Zhang, S.-s. Ma, and Y.-m. Zhang, "Research on collaborative environment of data collection and application in mobile gis," pp. 421–428, 2009.

[15] S. Ilarri, E. Mena, and A. Illarramendi, "A system based on mobile agents to test mobile computing applications," *Journal of Network and Computer Applications*, vol. 32, no. 4, pp. 846–865, 2009.

[16] J. M. Dow, R. E. Neilan, and C. Rizos, "The international gnss service in a changing landscape of global navigation satellite systems," *Journal of geodesy*, vol. 83, no. 3-4, pp. 191–198, 2009.

[17] J. R. Hoffman, "Measurements to determine potential interference to gps receivers from ultrawideband transmission systems," ITS, 2001.

[18] J Gonzalez, J. Blanco, C Galindo, A Ortiz-de Galisteo, J. Fernández-Madrigal, F. Moreno, and J. Martinez, "Combination of uwb and gps for indoor-outdoor vehicle localization," in *2007 IEEE International Symposium on Intelligent Signal Processing*, IEEE, 2007, pp. 1–6.

[19] K. M. Tan and C. L. Law, "Gps and uwb integration for indoor positioning," in *2007 6th International Conference on Information, Communications & Signal Processing*, IEEE, 2007, pp. 1–5.

[20] J. Johnson and B. Dewberry, "Ultra-wideband aiding of gps for quick deployment of anchors in a gps-denied ad-hoc sensor tracking and communication system," *Ion GNSS (Portland, OR Sep. 10-23, 2011)*, pp. 1–8, 2011.

[21] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: Distance-bounding attacks in wireless networks," pp. 83–97, 2006.

[22] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Effectiveness of distance-decreasing attacks against impulse radio ranging," pp. 117–128, 2010.

[23] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "Uwb rapid-bit-exchange system for distance bounding," pp. 1–12, 2015.

[24] S. M. Kay, "Fundamentals of statistical signal processing," 1993.

[25] M. Stocker, B. Großwindhager, C. A. Boano, and K. Römer, "Towards secure and scalable uwb-based positioning systems," pp. 247–255, 2020.

[26] J. C. Benaloh, "Secret sharing homomorphisms: Keeping shares of a secret secret," in *Conference on the Theory and Application of Cryptographic Techniques*, Springer, 1986, pp. 251–260.

[27] D. R. Stinson and R. Wei, "Unconditionally secure proactive secret sharing scheme with combinatorial structures," in *International Workshop on Selected Areas in Cryptography*, Springer, 1999, pp. 200–214.

[28] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: How to cope with perpetual leakage," in *Annual International Cryptology Conference*, Springer, 1995, pp. 339–352.

[29] T. Tassa, "Hierarchical threshold secret sharing," *Journal of cryptology*, vol. 20, no. 2, pp. 237–264, 2007.

[30] N. Pakniat, M. Noroozi, and Z. Eslami, "Distributed key generation protocol with hierarchical threshold access structure," *IET Information Security*, vol. 9, no. 4, pp. 248–255, 2015.

[31] H. Pilaram and T. Eghlidos, "An efficient lattice based multi-stage secret sharing scheme," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 1, pp. 2–8, 2015.

[32] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," pp. 427–438, 1987.

[33] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," pp. 129–140, 1991.

[34] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," pp. 27–35, 1988.

[35] G. Traverso, D. Demirel, and J. Buchmann, "Dynamic and verifiable hierarchical secret sharing," pp. 24–43, 2016.

[36] M. Nojoumian and D. R. Stinson, "On dealer-free dynamic threshold schemes.," *Adv. Math. Commun.*, vol. 7, no. 1, pp. 39–56, 2013.

[37] C. Tang and Z.-a. Yao, "Definition and construction of multi-prover zero-knowledge argument," vol. 3, pp. 375–379, 2009.

[38] L. Lu, J. Han, Y. Liu, L. Hu, J.-P. Huai, L. Ni, and J. Ma, "Pseudo trust: Zero-knowledge authentication in anonymous p2ps," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 10, pp. 1325–1337, 2008.

[39] M. Shoaran and A. Thomo, "Zero-knowledge-private counting of group triangles in social networks," *The Computer Journal*, vol. 60, no. 1, pp. 126–134, 2017.

[40] D. Saha and S. Sur-Kolay, "Secure public verification of ip marks in fpga design through a zero-knowledge protocol," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 20, no. 10, pp. 1749–1757, 2011.

[41] A. A. Rasheed, R. N. Mahapatra, and F. G. Hamza-Lup, "Adaptive group-based zero knowledge proof-authentication protocol in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 2, pp. 867–881, 2019.

[42] O. Goldreich, "Foundations of cryptography: Volume 2, basic applications," 2009.

[43] R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin, "Efficient multi-party computations secure against an adaptive adversary," pp. 311–326, 1999.

[44] T. Rabin and M. Ben-Or, "Verifiable secret sharing and multiparty protocols with honest majority," pp. 73–85, 1989.

[45] Z. Beerliova-Trubiniova and M. Hirt, "Efficient multi-party computation with dispute control," pp. 305–328, 2006.

[46] A. Choudhury and A. Patra, "An efficient framework for unconditionally secure multiparty computation," *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 428–468, 2016.

[47] C. Jihong, "Patient positioning system in hospital based on zigbee," pp. 159–162, 2011.

[48] Q. Yang, S. J. Pan, and V. W. Zheng, "Estimating location using wi-fi.," *IEEE Intell. Syst.*, vol. 23, no. 1, pp. 8–13, 2008.

[49] M. M. Saad, C. J. Bleakley, T. Ballal, and S. Dobson, "High-accuracy reference-free ultrasonic location estimation," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 6, pp. 1561–1570, 2012.

[50] S. Zhou and J. K. Pollard, "Position measurement using bluetooth," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 2, pp. 555–558, 2006.

[51] X. Wang, "Research on pseudolite positioning technique," *Shanghai Jiao Tong University: Shanghai, China*, 2011.

[52] S. Mazuelas, F. A. Lago, J. Blas, A. Bahillo, P. Fernandez, R. M. Lorenzo, and E. J. Abril, "Prior nlos measurement correction for positioning in cellular wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 5, pp. 2585–2591, 2008.

[53] E. Næsset and J. G. Gjevestad, "Performance of gps precise point positioning under conifer forest canopies," *Photogrammetric Engineering & Remote Sensing*, vol. 74, no. 5, pp. 661–668, 2008.

[54] E. Naesset, "Effects of differential single-and dual-frequency gps and glonass observations on point accuracy under forest canopies," *Photogrammetric engineering and remote sensing*, vol. 67, no. 9, pp. 1021–1026, 2001.

[55] H. Hasegawa and T. Yoshimura, "Application of dual-frequency gps receivers for static surveying under tree canopies," *Journal of Forest Research*, vol. 8, no. 2, pp. 0103–0110, 2003.

[56] R. Valbuena, F. Mauro, R. R.-S. Suárez, and J. Manzanera, "Accuracy and precision of gps receivers under forest canopies in a mountainous environment," *Spanish Journal of Agricultural Research*, no. 4, pp. 1047–1057, 2010.

[57] C. Edson and M. G. Wing, "Tree location measurement accuracy with a mapping-grade gps receiver under forest canopy," *Forest Science*, vol. 58, no. 6, pp. 567–576, 2012.

[58] A. Pirti, K. Gümüş, H. Erkaya, and R. G. Hoşbaş, "Evaluating repeatability of rtk gps/glonass near/under forest environment," *Croatian Journal of Forest Engineering: Journal for Theory and Application of Forestry Engineering*, vol. 31, no. 1, pp. 23–33, 2010.

[59] M. Bakuła, P. Przestrzelski, and R. Kaźmierczak, "Reliable technology of centimeter gps/glonass surveying in forest environments," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 53, no. 2, pp. 1029–1038, 2014.

[60] N. Kinugasa, F. Takahashi, and R. Kohno, "Mitigation of ionospheric effect on multi-gnss positioning with ionosphere delay estimation using single-frequency measurements of selected satellites," *Journal of Aeronautics, Astronautics and Aviation*, vol. 49, no. 2, pp. 93–100, 2017.

[61] K. Yedukondalu, A. D. Sarma, and S. S. Vemuri, "Estimation and mitigation of gps multipath interference using adaptive filtering," *Progress in Electromagnetics Research*, vol. 21, pp. 133–148, 2011.

[62] P. Misra and P. Enge, "Global positioning system: Signals, measurements and performance second edition," *Global Positioning System: Signals, Measurements And Performance Second Editions*, vol. 206, 2006.

[63] G. Seeber, *Satellite geodesy 2nd completely revised and extended edition*, 2003.

[64] L. Wanninger and M. May, "Carrier phase multipath calibration of gps reference stations," in *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, 2000, pp. 132–144.

[65] F. Lazzari, A. Buffi, P. Nepa, and S. Lazzari, "Numerical investigation of an uwb localization technique for unmanned aerial vehicles in outdoor scenarios," *IEEE Sensors Journal*, vol. 17, no. 9, pp. 2896–2903, 2017.

[66] B Shalon, X Li, and T Kirubarajan, "Basic concepts in estimation," *Estimation with Applications to Tracking and Navigation*, pp. 89–121, 2001.

[67] R. E. Kalman and R. S. Bucy, "New results in linear filtering and prediction theory," 1961.

[68] A. Dhital, "Bayesian filtering for dynamic systems with applications to tracking," 2010.

[69] J. Míguez, M. F. Bugallo, and P. M. Djurić, "A new class of particle filters for random dynamic systems with unknown statistics," *EURASIP Journal on Advances in Signal Processing*, vol. 2004, no. 15, pp. 1–17, 2004.

[70] A. Doucet, N. De Freitas, and N. Gordon, "An introduction to sequential monte carlo methods," pp. 3–14, 2001.

[71] B. Siciliano and O. Khatib, "Springer handbook of robotics," 2016.

[72] N. Gordon, B Ristic, and S Arulampalam, "Beyond the kalman filter: Particle filters for tracking applications," *Artech House, London*, vol. 830, no. 5, pp. 1–4, 2004.

[73] M. S. Arulampalam, S. Maskell, N. Gordon, and T. Clapp, "A tutorial on particle filters for online nonlinear/non-gaussian bayesian tracking," *IEEE Transactions on signal processing*, vol. 50, no. 2, pp. 174–188, 2002.

[74] G. Kitagawa, "Monte carlo filter and smoother for non-gaussian nonlinear state space models," *Journal of computational and graphical statistics*, vol. 5, no. 1, pp. 1–25, 1996.

[75] J. S. Liu and R. Chen, "Blind deconvolution via sequential imputations," *Journal of the american statistical association*, vol. 90, no. 430, pp. 567–576, 1995.

[76] D. Crisan and M. Grunwald, "Large deviation comparison of branching algorithms versus resampling algorithms: Application to discrete time stochastic filtering," *Statist. Lab., Cambridge Univ., Cambridge, UK, Tech. Rep., TR1999-9*, 1999.

[77] R. Douc and O. Cappé, "Comparison of resampling schemes for particle filtering," pp. 64–69, 2005.

[78] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," 2011.

[79] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[80] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Multi-channel based sybil attack detection in vehicular ad hoc networks using rssi," *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 362–375, 2018.

[81] H. Hu, R. Lu, Z. Zhang, and J. Shao, "Replace: A reliable trust-based platoon service recommendation scheme in vanet," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1786–1797, 2016.

[82] T. P. Pedersen, "A threshold cryptosystem without a trusted party," pp. 522–526, 1991.

[83] Y. D. Z. W. Y. Qing, "Research of mining subsided land reclamation system based on gis [j]," *Metal Mine*, vol. 10, 2011.

[84] J. Bosy, A. Oruba, W. Graszka, M Leończyk, and M. Ryczywolski, "Asg-eupos densification of euref permanent network on the territory of poland," *Reports on Geodesy*, pp. 105–111, 2008.

[85] M. Bakuła, S. Oszczak, and R. Pelc-Mieczkowska, "Performance of rtk positioning in forest conditions: Case study," *Journal of Surveying Engineering*, vol. 135, no. 3, pp. 125–130, 2009.

[86] J. M. Dow, R. E. Neilan, and C. Rizos, "The international gnss service in a changing landscape of global navigation satellite systems," *Journal of geodesy*, vol. 83, no. 3, pp. 191–198, 2009.

[87] E. Zhang, J. Peng, and M. Li, "Outsourcing secret sharing scheme based on homomorphism encryption," *IET Information Security*, vol. 12, no. 1, pp. 94–99, 2017.

[88] L. Harn, C. Lin, and Y. Li, "Fair secret reconstruction in (t, n) secret sharing," *Journal of Information Security and Applications*, vol. 23, pp. 1–7, 2015.

[89] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[90] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," pp. 21–32, 2012.

[91] P. Papadimitratos and A. Jovanovic, "Gnss-based positioning: Attacks and countermeasures," pp. 1–7, 2008.

[92] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, P. M. Kintner, *et al.*, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," pp. 2314–2325, 2008.

[93] .

[94] S. Brands and D. Chaum, "Distance-bounding protocols," pp. 344–359, 1993.

[95] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "The cicada attack: Degradation and denial of service in ir ranging," vol. 2, pp. 1–4, 2010.

[96] "Atmel phase difference measurement,"

[97] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun, "Physical-layer attacks on chirp-based ranging systems," pp. 15–26, 2012.

[98] H. Ólafsdóttir, A. Ranganathan, and S. Capkun, "On the security of carrier phase-based ranging," pp. 490–509, 2017.

[99] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[100] S. Brands and D. Chaum, "Distance-bounding protocols," pp. 344–359, 1993.

[101] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "A secure lightweight texture encryption scheme," pp. 344–356, 2015.

[102] A. Jolfaei and K. Kant, “Data security in multiparty edge computing environments,” 2019.

[103] R. Y. Asmar, D. T. Proefke, C. J. Bongiorno, and A. P. Creguer, “Method and system for authenticating vehicle equipped with passive keyless system,” 2017, US Patent 9,710,983.

[104] A. Francillon, B. Danev, and S. Capkun, “Relay attacks on passive keyless entry and start systems in modern cars,” 2011.

[105] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, “Multi-channel based sybil attack detection in vehicular ad hoc networks using rssi,” *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 362–375, 2018.

[106] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, “Self-securing ad hoc wireless networks.,” vol. 2, pp. 548–555, 2002.

[107] M. Blaze, J. Feigenbaum, and A. D. Keromytis, “Keynote: Trust management for public-key infrastructures,” pp. 59–63, 1998.

[108] J. Linn, “Trust models and management in public-key infrastructures,” *RSA laboratories*, vol. 12, 2000.

[109] J. A. Buchmann, E. Karatsiolis, and A. Wiesmaier, “Introduction to public key infrastructures,” 2013.

[110] A. Francillon, B. Danev, and S. Capkun, “Relay attacks on passive keyless entry and start systems in modern cars,” 2011.

[111] T. K. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, “A survey of various propagation models for mobile communication,” *IEEE Antennas and propagation Magazine*, vol. 45, no. 3, pp. 51–82, 2003.

[112] A. F. Molisch, K. Balakrishnan, C.-C. Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak, “Ieee 802.15. 4a channel model-final report,” *IEEE P802*, vol. 15, no. 04, p. 0662, 2004.

[113] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “A survey of machine and deep learning methods for internet of things (iot) security,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[114] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, “Physical-layer security of 5g wireless networks for iot: Challenges and opportunities,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[115] G. Baldini and G. Steri, “A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1761–1789, 2017.

[116] B. Danev and S. Capkun, “Physical-layer identification of wireless sensor nodes,” *Technical Report/ETH Zurich, Department of Computer Science*, vol. 604, 2012.

[117] K. Zeng, K. Govindan, and P. Mohapatra, “Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks],” *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, 2010.

[118] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, “Machine learning for the detection and identification of internet of things (iot) devices: A survey,” *arXiv preprint arXiv:2101.10181*, 2021.