Received August 18, 2021, accepted September 19, 2021, date of publication September 23, 2021, date of current version October 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3115087

Quantum-Resistant Cryptography for the Internet of Things Based on Location-Based Lattices

OHOOD SAUD ALTHOBAITI, (Graduate Student Member, IEEE), AND MISCHA DOHLER, (Fellow, IEEE)

Department of Engineering, King's College London, London WC2R 2LS, U.K.

Corresponding author: Ohood Saud Althobaiti (ohood.althobaiti@kcl.ac.uk)

The work of Ohood Saud Althobaiti was supported by the Royal Embassy of Saudi Arabia Cultural Bureau, Taif University.

ABSTRACT An important enabler of the Internet of Things (IoT) is the Narrow-Band Internet of Things (NB-IoT) technology, which is a 3GPP standards compliant connectivity solution. Quantum computing, another emerging technological paradigm, promises novel compute opportunities but is also able to compromise cybersecurity ciphers. Therefore, improved methods to mitigate such security threats are needed. In this research, we propose a location-aware cryptographic system that guarantees post-quantum IoT security. The ultimate value of a location-driven cryptosystem is to use the geographic location as a player's identity and credential. Position-driven cryptography using lattices is efficient and lightweight, and it can be used to protect sensitive and confidential data in many critical situations that rely heavily on exchanging confidential data. At the best of our knowledge, this research starts the study of unconditional-quantum-resistant-location-driven cryptography by using the Lattice problem for the IoT in a pre-and post-quantum world. Unlike existing schemes, the proposed cryptosystem is the first secure and unrestricted position-based protocol that guards against any number of collusion attackers and against quantum attacks. It has a guaranteed authentication process, solves the problems of distributing public keys by removing a public key infrastructure (PKI), offers secure NB-IoT without SIM cards, and resists location spoofing attacks. Furthermore, it can be generalized to any network – not just NB-IoT.

INDEX TERMS Cryptosystem, quantum-resistant cryptography, Internet of Things, lattices, localization, location, Narrow-Band Internet of Things.

I. INTRODUCTION

The internet of things (IoT) is popularly referred to as the large interconnection that exists between visible objects with the ability to communicate and perform computations. It also has the capacity to control, supervise and identify over the internet. In light of this fact, it is estimated that approximately 75.44 billion devices, sensors, and actuators, among others, will be connected to the internet by the end of 2025 [1]. These devices will aim to collect data concerning the real world, which must be transferred to a predominant supply for the purpose of data processing and storage. There are many available IoT technologies, and one of the major technologies is the Narrow-Band Internet of Things (NB-IoT). It was developed to enhance energy and range efficiencies. On the premise that devices such as medical or vehicles play an essential role in our lives, it is therefore important to ensure that strong security requirements associated with the IoT are put in place.

The main IoT security goals are confidentiality, integrity, and authenticity. Confidentiality assures no information leaks out of the transmission channels and hierarchy, integrity maintains the original form of data and information, and authenticity enhances proof of identity. For the information to be certified as clear, the three major traits should not be tampered with to provide secure information. A challenge encountered in the process of ensuring the security of the IoT is that IoT devices are mostly prone to be constrained on the basis of limited resources and memories. Therefore, there are many encrypting systems and methodologies developed and otherwise articulated that propose an alternative set of solutions to IoT security threats. The most common techniques used for such encoding and decoding purposes are the use of cryptography and implementation of cryptosystems.

The IoT uses many protocols and most of these are configured with cryptographic algorithms such as the advanced

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

encryption standard (AES) to cater to confidentiality and integrity and elliptic curve cryptosystems (ECCs), which incorporate other digital signature algorithms to facilitate integrity and authentication [2].

Undeniably, there are numerous problems associated with the usage of symmetric algorithms. The major problem is the key exchange problem and a requirement for a new key for each correspondence. The safety of the current asymmetric (public key) cryptography depends on the degree of difficulty of mathematical problems, which include discrete logarithm and integer factorization problems. It is therefore popularly affirmed that these mathematical problems can effectively be solved using quantum computers. Quantum computers encounter key exchange, encryption and digital signature approaches used in modern society that are likely to be broken [3]. However, the estimated period for the first reliable quantum computer remains uncertain; however, some forecasts show that this scenario will probably occur in the next 5-10 years. In mathematics, there are also some problems that have been stubborn for both traditional computing and advanced quantum computing and simultaneously do not inherit the flaws of quantum computer implementation. These problems have recently prompted research interest. Based on research on asymmetric cryptography, lattice-based cryptography has been considered one of the postquantum cryptography techniques, in lattice-based cryptography: an integration of short keys and fast and high-level effectiveness [2]–[4]. Lattice-based cryptography is promising since it combines small keys and robust security measures that are complex to trace and break. The security of such a system is often linked to the closest shortest vector or learning with error (LWE) problems in lattices to enhance the difficulty of breakage. The major examples of such cryptography include the Nth Degree Truncated Polynomial Ring Units (NTRU) encryption system.

In general, the concept of location-based cryptography was initiated by Chandran *et al.*, although some tasks have appeared previously under several names [5]. The ultimate purpose of location-based cryptosystems is to utilize only the geographic location of a player as its identity and credential. For instance, an individual might be interested in composing and sending a message to a player (receiver) in a different geographic location, guaranteeing that the receiver can decrypt and read this message only if he/she is at pos_p [5]. It is important to note that such a setting can be applied in several scenarios in the real world, especially for the security of wireless networks, which allow access to resources under a condition that the party is at a specific position [6]. To the best of our knowledge, this research initiates the study of unconditional quantum-resistant location-driven cryptography by using lattice theory for the Internet of Moving Things (IoMT) in the pre- and postquantum world.

The major function faced by location-based cryptosystems is the implementation of a verification mechanism (secure positioning). One element called prover P at a certain point Pos_p connects to another set of components called referees (verifiers) V_1, V_2, V_3 and V_4 at different geographical positions Pos_1, Pos_2, Pos_3 and Pos_4, respectively; thus, this claimed prover P is bounded by referees in the quadrangle. The prover P convinces the honest referees using an applicable interactive protocol that verifies the authenticity of the prover P that his geographical location is at Pos_p [5], [6]. For example, this scheme bears similarity to familiar distance bounding schemes [7], [8]. According to the distance bounding scheme, a referee transmits a message to the player and estimates the average time used by the player to return a reply with a certain message in its array of feedback. It is assumed that the signal can be transmitted at light speed. As a result, this scheme gives the distance between the player and the referee.

The task of secure localization has been under study in wireless sensor networks (WSNs) [9]–[12], [13], [14]. From those studies, several proposals have been articulated. Although the protocols have been studied with much effort, researchers [5], [6] stated that protocols for secure position-based verification that can offer security against collaborating attacks without assuming hard hypotheses do not exist. This is because the referees cannot differentiate if the requesters are honest or if they are working with collaborating-location-spoofing adversaries that are not actually at position Pos_p. In other words, there are demerits associated with the implementation of secure positioning. This conclusion excludes other cryptographic mechanisms based on location [6].

Considering the impracticality of implementing position-based cryptography in the standard (vanilla) model, Chandran *et al.* [5] introduce schemes for secure positioning and key exchange based on location that assume constraints on the attacker's memory size based on the ''Bounded Retrieval Model (BRM)''. Although these schemes give us an approach to determine the possibility of position-based cryptography, they are impracticable where inputs must not fit into the attacker's memory size, and the referees may require broadcasting large packets; thus, this requires high bandwidth and frequency. Consequently, an open research issue arises: how can unconditional position-driven cryptography be tractable for the Internet of Moving Things (IoMT) in the pre- and postquantum world?

The main contributions of this paper are as follows:

- A new lightweight cryptographic in terms of 3D position and lattices as a suitable alternative key for fifth-generation and sixth-generation systems and beyond is proposed by taking into account the performance and energy consumption.
- The main benefit of the proposed cryptosystem is solving public key distribution problems and the ridding of public key infrastructure (PKI) because of the very expensive cost and complexity of building PKIs. We solve problems of public key distribution and management by using position-based cryptography, i.e., we do not need to use digital certificates, certificate authorities, a private key generator or a key generation

center in our proposed cryptosystem, unlike existing protocols.

- Although worldwide quantum computers are not built sufficiently and qubit (quantum bit) counters are still limited, they will seriously compromise the security of all current cryptographic algorithms. However, it may take many years to re-encrypt massive amounts of previously stored data for a second time via more robust schemes, so it is important to apply this now. Consequently, it is important to improve postquantum cryptography. Because cryptography is an essential fraction of most systems, the necessity of its development has risen dramatically. Furthermore, the implementation of efficient cryptosystems requires a tremendously long time. According to the rapid development of quantum computers, the world has little time before it encounters this novel cybersecurity threat. As a result, we propose a protocol that is secure against quantum attacks.
- We demonstrate that for attackers that are not restricted to any state or condition, secure localization is practicable.
- To the best of our knowledge, the proposed cryptosystem is the first secure position-driven cryptosystem without any restrictions, and it is secure against any number of collusion attackers in the pre- and postquantum IoMT world, unlike existing schemes. Furthermore, it guarantees a mutual authentication process. This means that the proposed cryptosystem not only enhances the level of confidentiality but also enhances the level of authentication.
- The proposed position-based cryptography resists location spoofing attacks, unlike global positioning systems (GPSs).
- The proposed cryptography offers secure NB-IoT without attached SIM cards to the NB-IoT during its manufacture for purposes of security. This leads to resisting SIM swap fraud, SMS attacks or any attack in which NB-IoT is exposed to because of vulnerabilities in the SIM card. In addition to SIM swap fraud, other attacks on SIM cards, such as SimJacker and side-channel attacks that exploit the leak of information, typically by the use of variation in electromagnetic waves or electric current, as well as other vulnerable SIM technologies, such as the S@T (SIM Alliance Toolbox) browser and WIB (Wireless Internet Browser), could be exploited. These vulnerabilities in the SIM card cause serious harm because the attacker can exploit them to control the victim's device remotely to achieve harmful behaviors, such as stealing all of the victim's information, obtaining the victim's location, tracking the victim, sending messages, and making calls. Another drawback is losses resulting from fraud or cloning opportunities. The average cost of a SIM card is $3, so the cost of replacing it is $30 because of changes relative to databases, customer care, administration systems, etc. Furthermore, investigating suspected cloning is more costly because it demands equipment, technical staff, etc.
- The proposed cryptographic approach is not only for NB-IoT but also a generic cryptosystem for any network.
- The proposed position-based cryptographic protocol could produce more secure communications between devices, in particular in critical (mobile/static) situations established by using only a party's physical location as its credential. For instance, the worldwide coronavirus (COVID-19) pandemic profoundly affected everyday activities. There is an increasing need for automation and electronic services to fight outbreak epidemics, such as e-health applications, e-learning, work from home and geographical tracking of COVID-19. However, internet hackers have exploited these difficult circumstances and have stolen tens of millions of dollars assigned by the German government to counter the spread of COVID-19 [15]. Moreover, an increase in cyberattacks in the next few months and years are expected to come as a result of the COVID-19 outbreak [16]. Consequently, in post-COVID-19 society, IoT applications have a rising influence.
- Our simulation compares NB-IoT without/with proposed cryptography to prove that the proposed cryptography improves IoT security without compromising its performance metrics (i.e., energy consumption, time consumption/delay, stability period and throughput). Consequently, the results indicate an optimized trade-off between security and performance. As a result, the efficiency and reliability of the proposed cryptosystem are proven.
- Combining position verification processes and lattice theory with the internet of (moving) things (IoMT) leads to an efficient protocol to improve security for the IoT in the pre- and postquantum world.

The rest of this research is arranged as follows: Section II describes an overview of problem statement. In Section III, literature reviews related to this work are provided. We propose an unconditional-quantum-resistant-location-driven cryptosystem by using the Lattice problem for the IoMT in pre-and postquantum world in Section IV. Section V discusses analytical-based evaluation and simulator-based results. Finally, Section VI demonstrates concluding remarks and future works.

II. PROBLEM STATEMENT

Security in IoT deployments is very important, as has been shown by various IoT surveys [17]. Whenever criminals take control of IoT devices, they can cause massive losses first by stealing data for malicious gains and tampering with the data stored and other remote assets. This is one of the worries of enterprises regarding the use of IoT devices and their reliability and convenience in business. Although it is possible to ignore such devices as useless and does not make any sense to protect them, hackers have directed their tricks to such devices because of this vulnerability and will greatly interfere with them. Such devices include smart pins and smoke alarms. It is important to keep such devices secure. If hackers decide to empty all the bins in the city by convincing authorities, trigger many smoke alarms or interfere with soil sensors to cause farmers to apply many fertilizers to their farms, chaos will arise [17].

NB-IoT falls under the category of the 3GPP standard and obtains all its security features from the long-term evolution (LTE). The NB-IoT SIM card has a built-in key that is secretly encoded to this device during manufacturing and is used to authenticate the device and network alternately. This will allow encryption of traffic in the device as well as in the core networks because it generates session keys that are frequently updated [17]. It is, however, very clear that LTE has been considered one of the latest technology standards in mobile networks, with a subscriber rate of over 85% worldwide [18]. The information that has been offered by the Global Mobile Suppliers Association (GSA) has indicated that toward the end of 2017, there were approximately 2.36 billion LTE subscriptions, a very inflated number compared with the 1.48 billion subscriptions that were recorded in 2016 [19].

Moreover, LTE is a worldwide standard that is applied in fourth-generation cellular networks after being presented in 3GPP Release 8 as an imperative direction toward future wireless telecommunications. For proper LTE network operation, the use of two standardized algorithms is always required to offer radio frequency. The algorithms are the EIA: EPS integrity algorithm and the EEA: EPS encryptions, all of which have been made and standardized for LTE networks. LTE has three sets of algorithms. These sets are 128-EEA1 and 128-EIA1, whose operations are dependent on the SNOW 3G cipher, 128-EEA2 and 128-EIA2, whose operations are developed on the AES cipher, and 128-EEA3 and 128-EIA3, whose operations are built using the ZUC cipher [18]. The introduction of LTE and NB-IoT seemed to be the solutions by implementing authentication and encryption algorithms; however, the technologies are vulnerable to attacks.

Bikos [20] reported that LTE is exposed to several challenges on the basis of reliability and security. The heterogeneous nature of LTE and operation with IP-based open networks acts as one of the major contributors to vulnerabilities to attacks. Additionally, there are some notable vulnerabilities existing in the current LTE security framework that need adequate and emergent responses [21], [22]. First, flat IP-based 3GPP LTE networks raise risks of eavesdropping, injection, modification and other vulnerabilities greater than those in the previous systems. Second, weaknesses arise from the LTE system base stations, which are regarded as an All-IP network that offers a direct path for malicious attackers to the base stations. This also indicates weak resistance to attackers in the various base station configurations. Third, new challenges associated with handover authentication procedures have emerged [21], [22]. All these security vulnerabilities indicate that there is a need to improve and enhance future LTE and NB-IoT models for better security outcomes.

For cryptography to be implemented correctly, certain elements will be contained in a set of credentials that tend to portray the identities of receivers/senders. Such information will correspond to unique attributes such as biometrics, shared keys, digital certificates from the third party, etc. In most cases, identity is determined by geographical position. For instance, the role of a bank teller is known behind a bulletproof window not because of showing his credential but because of his location behind the bank's bulletproof window [23]. The geographical position of an element is a valuable source of information when the matter of identity is concerned [23]. Therefore, the geographical location of an object can be used as one of the credentials [23]. An open research issue that remains is how can unconditional position-driven cryptography be tractable for the IoMT in the pre- and postquantum world?

III. LITERATURE REVIEW

In location-based cryptography, the main focus is looking at an environment where the only necessary requirement for a player (prover) is its physical position. In other words, with the current advancement in technology, for any entity, it is only required to know its exact location on the Earth's surface to obtain the required credentials. However, position-based cryptography has various problems, although most of these problems have not been unraveled. In the area of wireless network security, secure positioning is one of the challenges that has been widely studied [23], [24]. Some of the protocols that were proposed include [25]–[30], which are prone to location-spoofing attacks by collusion. Perazzo *et al.* [12] proposed secure localization via enlargement miscontrol disclosure (SPEM) in wireless sensor networks. Their localization scheme uses a multilateration and distance bounding protocol used in the IEEE 802.15.4a ultrawideband (UWB) standard. In [31], the researchers suggested three algorithms for drone path planning: first, LocalizerBee produces paths for positioning purposes; second, VerifierBee verifies a set of locations of devices; and third, PreciseVerifierBee verifies with accuracy, i.e., it is the expansion of VerifierBee. However, in [12], [31], they forced a preshared secret key to mitigate the attack. This means that they have restricted the security of their schemes to the secret keys; thus, the potential of compromising these shared secret keys is a highly realistic threat.

Circumventing the issue of multiple cloning adversaries may require the involved parties to assume a given setup phase characterized by unclonable tamper-proof verifications to every possible future prover [23], [24]. However, one of the most stringent quantum principles is that cloning quantum information is impossible (i.e., there is no operation in physical quantum law that accepts a single instance of quantum information as input and yields two copies of this input as outputs). For example, given a single qubit copy that is set to a combination of the two states of zero and one (superposition) $|\psi \geq C_0|0 > +C_1|1 >$, since qubit measurement disturbs its state, it is impossible to "extract" a complete classical definition of C_0 and C_1 [32]. Although it cannot be fully concluded, there are verifiers that are anonymous to hostile parties and players in [33], [34] that present secure localization in a wireless network with radio or ultrasound where the verifiers cannot be easily detected by adversaries or players. When various hostile entities collude, they might be able to subvert the verifiers. Reference [35] focused on a situation where there is a key exchange between Bob and Alice and message authentication in an environment where the two completely understand the presence of the other party within the transmission scope. However, to completely develop secure protocols, an assumption of the adversarial parties not being close to both Bob and Alice should be taken. As such, Bob and Alice should perfectly understand that they are conversing with each other and not to the enemy beforehand. This consequently improves the possibility of a key exchange occurring based on the style of protocol that was developed by Diffie-Hellman [23], [24].

Chiang *et al.* [36] are credited scholars who study the effects of colluding hostile parties in the area of secure localization. In the classical model, one important procedure for secure localization has been postulated to combat the challenge of colluding-location-spoofing attacks. From their investigation, they developed a protocol that can withstand attacks from two colluding hostile provers. When the colluding-location-spoofing adversaries exceed two and advance to three or four, executing attacks becomes possible. It is clearly shown that in addition to any protocol, it is possible to develop a classical model assault through an equivalent number of adversaries, similar to the verifiers found in the protocol [23], [24].

Despite the security of the proposed schemes having been proven against specific attackers, it is very possible to break them using colluding-location-spoofing attacks. The use of multiple attackers that work in unison has the potential of sending a string copy using the closest verifier to all the other attackers. In this case, each attacker is considered to have the potential to emulate the honest actions of a prover to its nearest verifier [37]. Additionally, studies have indicated that there is always a possibility for an attack to occur in the classical world setting after dropping some of the extra assumptions [6], [23]. The researchers in [23] also found that secure localization can be attained by assigning the memory size for attackers [37].

The results of [23], [38] are linked to impossibility due to imposing restrictions on collaborating attackers' devices (i.e., the assumption that an attacker cannot accumulate every bit of information received); however, an attacker actually has the potential to keep all the information received. In addition, the verifiers, in this case, must broadcast large bursts of data, which may be difficult [39]. As a result, quality-of-service (QoS) assurance decreases and a high bandwidth is required, which diminishes utility in the case of IoT or tactile internet applications given the dependence on limited sensors. Furthermore, Brody *et al.* [40] highlighted the negative results for this strong additional restriction in [23]. Based on the localization algorithm, a multiproxy multisignature protocol was introduced in [41]. Dziembowski and Zdanowicz [42] proposed location-based authentication and location-based key exchange in a noisy channel paradigm with essential timing and geometric information. The participating entities gain access to bit sources transmitted to them through autonomous noisy channels. Unfortunately, in [41], [42], the implementing process is challenging in an attempt to satisfy the complicated assumptions, where inputs must not fit into the attacker's memory or the restriction of the adversary's position to be their protocols are secure. In contrast to the literature, we do not enforce any hard conditions for adversarial parties' memory size, location or number.

It is, however, important to note that assuming a bounded retrieval may not be ideal in different settings, thus leading to the development of the question of whether developing extensions may be a possible contributor in achieving top-notch security [37]. A proposal to use quantum information instead of using classical information was then developed to address some of the challenges identified above. This proposal is underpinned by the fact that the classical attack always depends on the adversary's ability to keep and send information simultaneously with the other adversaries, where the researchers believe that copying quantum information is impossible and complex [37]. This complexity and impossibility make it difficult for attackers to penetrate the system [37]. Quantum theory and cryptography have been connected since 1968, and as the first use for a relationship between physical law-based quantum and cryptography, quantum money was suggested [32].

Buhrman *et al.* [6] argue that 'quantum tagging' is a term that was proposed by Kent in 2002, where the first incidences of using quantum schemes to verify the positions were taken into account. With the help of other researchers, a patent that was presented to the Labs of HP in 2004 ended up being reimbursed in 2006 [43]. Scholars' conclusions did not appear in research paper sources until 2010 [44], [45]. In these papers [44], [45], they advanced various concepts on how to disintegrate several schemes by utilizing teleportation-based attacks. Moreover, these teleportation attacks could not break some of the variations they proposed (schemes IV-VI in [45]) but without proving they were unconditionally secure. The attacks that Buhrman *et al.* discussed in [6] have confirmed that schemes IV-VI in [45] are also not secure. In the quantum random oracle model, Unruh [46] presents a localization method and location-based authentication. Additionally, the author claims that the proposed protocols resist colluding attackers and do not need bounded memory/retrieval/entanglement restrictions, unlike previous studies. According to [32], the need for effective methods that do not depend on random oracles remains a significant open issue.

Malaney [47] proposed that it is possible to perform unconditional position verification using quantum channels. This scheme has been stated to be secure despite there being no deep provision of mathematical proof, efficient threat model or effective hardware implementation. However, Malaney's protocol, with the use of teleportation-based attacks, can be broken [6]. By using quantum particle swarm optimization (QPSO), Wu *et al.* [48] presented a range-free localization algorithm for nonhomogeneous wireless sensor networks that is relatively accurate. In [49], analysis of the location-based quantum cryptography used in distributed measurement systems, implementation issues and technical difficulties in quantum communications were discussed. Gao *et al.* [50] proposed quantum position verification with a hard constraint in which the frequency of operations of attackers is bounded. As a negative result, these schemes [48]–[50] may be broken by colluding teleportation-based attacks and side-channel attacks (information leakage attacks). Quantum teleportation attacks can be carried out by proper measurement of the qubit using shared entanglement resources [51].

However, there is a high probability that eavesdroppers exploit the flaws of quantum computing and quantum cryptography, for example, teleportation-based attacks, man-in-the-middle attacks, and denial of service attacks, to threaten security for a system if not resolved. Moreover, these threats involve laser seeding, information leakage attacks (Trojan-horse attacks), source flaws, side-channel attacks, pulse-energy monitoring, laser damage, device calibration and timing attacks [52]. Quantum cryptography, an effective technology to accomplish secure communication, must bridge the gap between theory and actual implementation to avoid vulnerabilities [53]. Therefore, quantum computers are in theory reliable, but in realistic processing of implementations, they still require research and refinement [52], [54]. This means that at present, there are major differences between real and theoretical quantum cryptosystems. In [32], several quantum cryptography shortcomings and problems were discussed. For instance, quantum bit commitment impossibility and secure two-entity computation using the quantum connection are impossible and zero-knowledge against quantum-based attacks. Because of these serious shortcomings and limitations, the search for classical cryptography approaches that resist quantum attacks is a rapidly rising research area. Lattice-based cryptography holds much promise for secure and practical postquantum cryptography [2]–[4], [55].

Furthermore, it is concluded that the work of location-based cryptography occupies several attempts in quantum computing. However, studying a number of different attacks about protocols [43], [45], [47], [51], [56], Buhrman *et al.* [6] cited in [23], [24] concluded that the safe positioning (location-verification) task, as well as cryptography based on position, are unattainable in cases where the involved parties exchange quantum data. Although studies such as [6], [23], [32], [37], [51], [56], [57] have mentioned that it is impossible to propose secure position-based cryptography in a typical model or quantum model without constraints, we can propose a secure and advanced position-driven cryptosystem without any constraint by using the lattice problem for the Internet of Moving Things (IoMT) in the pre- and postquantum world and simultaneously resisting quantum attacks and flaws. The proposed cryptographic protocol in this research not only solves the abovementioned problems but also improves the security of wireless networks.

IV. PROPOSED CRYPTOSYSTEM

Using only the geographical location of a player as a credential rather than an ID or biometrics is the aim of position-based cryptography. It is supposed that Alice (mobile node, e.g., unmanned aerial vehicle collects data from anywhere) needs to send a message to Bob (mobile node) called a prover at a specified three-dimensional location (X_P, Y_P, Z_P) with the guarantee that this message is read only by the player who is located at position (X_P, Y_P, Z_P). This means claimed prover P, who claims that his position at $Pos_p(X_P, Y_P, Z_P)$ connects to another set of components called referees (verifiers) V_1, V_2, V_3 and V_4 at these different known geographical positions $Pos_1(X_1, Y_1, Z_1)$, $Pos_2(X_2, Y_2, Z_2)$, $Pos_3(X_3, Y_3, Z_3)$ and $Pos_4(X_4, Y_4, Z_4)$, respectively, so that this claimed prover is in the quadrangle bounded by referees. Definitely, there is the potential for numerous adversaries. In fact, a verifier V_m can send a message to claimed prover P at a specific time and can additionally record each message that is received from P together with the time it is received. It can be assumed that a message travels at speeds equal to the speed of light, referred to as C, as is the case in a global positioning system (GPS) [23].

Both Alice and Bob are limited resource devices in the IoMT system. By using any localization method, such as range-based localization or nonrange-based localization techniques [10], [58], [59], Alice can recognize his region, so it can also be supposed that the lattice public keys of verifiers, which are in Alice's region, are downloaded on Alice's device, and these keys will be updated when Alice moves from region to another, such as an updating process for any application. Nonetheless, the positioning accuracy of nonrange-based techniques is typically lower than that of range-based techniques, so in this protocol, we focus on range-based methods to achieve very accurate 3-D location information. However, the verifiers can be sinks, base stations (BSs), gateways or even satellites. The prover's position is given to the adversaries and the verifiers [23]. Consequently, Alice sends to the nearest verifier a message containing his lattice public key and a request Bob's public key (intended prover's public key) encrypted by lattice public key of this closest verifier, i.e., Alice → Nereast V_m: $\left\{PK_A, \text{Request Bob's PK}\right\}_{PK_{V_m}}$. The verifiers have secure channels among themselves, allowing them to secretly communicate [23]. Figure (1) shows the proposed model structure.

However, the claimed prover (player) P needs to convince the honest verifiers that he is located at the position (X_P, Y_P, Z_P) by applying the following three verification tests: TDoF (time difference of flight)-based test, RSS

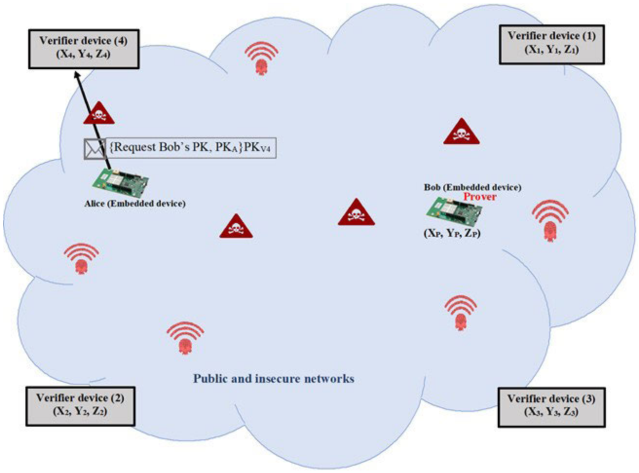


FIGURE 1. The structure of the proposed model.

TABLE 1. Summary of Notations.

Notation	Meaning
T, T_m	Timestamps where $m = 1, 2, 3, 4$
$\bigoplus$	Exclusive-OR (XOR) operation
$\|$	Concatenation
C	Speed of light
R_i	Random challenges, where $i = 1, 2, 3$
V_m	Verifier (referee) where $m = 1, 2, 3, 4$
P	Claimed prover P
(X_m, Y_m, Z_m)	3D location of verifier V_m
(X_P, Y_P, Z_P)	3D location of intended prover (actual coordinates of the aimed position)
$(X_{P_{rss}}, Y_{P_{rss}}, Z_{P_{rss}})$	Claimed prover's position calculated by RSS
$(X_{P_{aoa}}, Y_{P_{aoa}}, Z_{P_{aoa}})$	Claimed prover's location computed by AoA
$(X_{com}, Y_{com}, Z_{com})$	Average of measured coordinates of the claimed prover P
PK_{V_m}	Lattice public key of V_m
PK_A	Alice's lattice public key
PK_p	Lattice public key of P
SK	Lattice secret key of P
D_{TDoF_m}	Distance between Vm and P by using time difference of flight-based verification
D_{RSS_m}	Distance between Vm and P by using received signal strength-based measurement
P_{rm}	Received wireless signal power at V_m
D_{avg_m}	Average of resulting distances from TDoF and RSS computed by V_m
φ	Azimuth (horizontal) angle of received signal at V_m
θ	Elevation (vertical) angle of received signal at V_m

(received signal strength)-based verification and AoA (angle of arrival)-based verification process. Because of these signal features, TDoF, RSS and AoA are widely used for localization. Furthermore, the integration of these three localization schemes leads to high location accuracy while maintaining low energy and time consumption at a low cost of implementation for verifier devices. These measurements only rely on the physical and hardware environment, which means that malicious nodes cannot easily forge, tamper or manipulate these measured values.

Many ways exist for positioning the user of a wireless network. The most frequently used method is by using GPS, the accuracy of which can achieve every requirement of a location-dependent application. The central issue with GPS is that, apart from the user terminal needing to be enabled for GPS, there is the heavy power demand of the unit, latency, and the potential limitations of coverage. Additionally, GPS can be less reliable in towns and cities in proximity to tall structures and in the inside of a tunnel. Another important disadvantage of GPS is vulnerability to location spoofing attacks [60]–[63]. An additional method is to rely on wireless networks themselves through the use of cell ID information, which is extensively utilized in the GSM (Global System for Mobile Communications), despite drawbacks of its accuracy. Additional accuracy can be achieved by using alternative network resources, such as TDoF (hyperbolic localization) [64], RSS or AoA [58], [65], [66]; thus, we combine these three resources to reduce location error, generate high-level security and increase the accuracy of positioning efficiently. Table (1) shows the notation summary of the proposed protocol.

A. FIRST TEST: PROPOSED TIME DIFFERENCE OF FLIGHT-BASED ALGORITHM

In this test, we develop Chandran's protocol [23], which is performed by four verifiers and is detailed in Figure (2) as the following steps.

Step 1: Let T_1, T_2, T_3 and T_4 be the timestamps of radio waves taken to reach points V_1, V_2, V_3 and V_4, respectively, from the claimed prover P. Let C be the speed of light in a vacuum (299,792,458 meters/sec.). To determine the electromagnetic wavelength $C_f = C \div f$, where $f = 200$ kHz, NB-IoT works on the frequency band of licensed 3GPP (200 kHz employed). The derivation is applied to obtain the distance between P and V_m, $D = C_f \times T_m - C_f \times T$.

Step 2: V_1 picks up a random number denoted as key K_1. Additionally, V_2, V_3 and V_4 pick up random challenges R_1, R_2 and R_3, respectively, and then transmit these messages $\left\{ K_1, R_1, R_2 \text{ and } R_3 \right\}$ over the secure channels among themselves.

Step 3: V_1, V_2, V_3, and V_4 precompute $K_{i+1} = R_i \bigoplus K_i$, $1 \leq i \leq 3$.

Step 4: At timestamp T, verifiers V_1, V_2, V_3, and V_4 send K_1, R_1, R_2 and R_3, respectively, to claimed prover P at location (X_P, Y_P, Z_P) in the space.

Step 5: The claimed prover P at location (X_P, Y_P, Z_P) computes $K_2 = R_1 \bigoplus K_1$, $K_3 = R_2 \bigoplus K_2$, $K_4 = R_3 \bigoplus K_3$ in that order. As a result, the claimed prover P returns K_4 and attaches his lattice public key PK_p to all verifiers V_1, V_2, V_3, and V_4.

Step 6: The verifier V_1 receives this reply $\{K_4 \| PK_p\}_{PK_{v_1}}$ from the claimed prover P within timestamp T_1, the verifier V_2 receives this reply $\{K_4 \| PK_p\}_{PK_{v_2}}$ from the claimed prover P within timestamp T_2, the verifier $V3$ receives this reply $\{K_4 \| PK_p\}_{PK_{v_3}}$ from the claimed prover P at timestamp T_3 and the last verifier V_4 receives this reply $\{K_4 \| PK_p\}_{PK_{v_4}}$ from the claimed prover P within timestamp T_4. Therefore, the referee V_m can guarantee that this message was transmitted

```
Algorithm 1: Proposed TDoF-based verification process
$V_1$ : picks up random number $K_1$.
$V_j$: picks up random challenges $R_i$ where j = 2,3,4 & i = 1,2,3
$V_m \rightarrow V_n$ : $K_1$, $R_i$ where m & n = 1,2,3,4; $m \neq n$
$V_m$ : precomputes $K_{i+1} = R_i \oplus K_i$, $1 \leq i \leq 3$
$V_m \rightarrow P$:  $K_1$, $R_i$ respectively at timestamp T
P: computes $K_{i+1} = R_i \oplus K_i$, $1 \leq i \leq 3$
$P \rightarrow V_m$ : $\{K_4 \| PK_p\}_{PKvm}$
$V_m$ : receives $\{K_4 \| PK_p\}_{PKvm}$ at timestamp $T_m$
$V_m$: computes $D_{TDoFm} = C_f \times (T_m - T)/2$
$V_m$ :  decrypts $\{K_4 \| PK_p\}_{PKvm}$ by using $PK_{Vm}$
$V_m$: verifies if his $K_4$ = received $K_4$? and $D_{TDoFm}$ = actual distance between him
& aimed location?
```

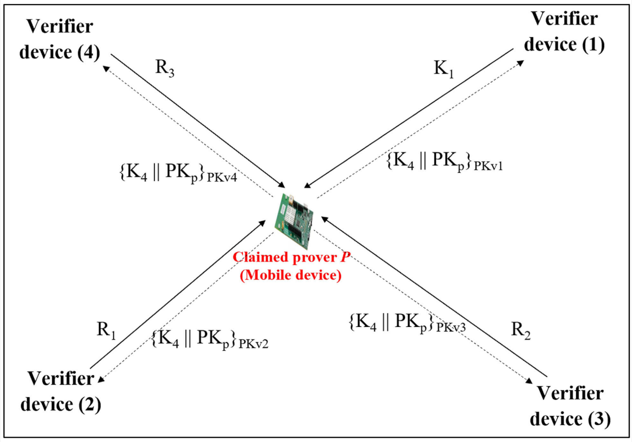


FIGURE 2. Proposed TDoF-based verification.

by the device that is located at distance $D_{TDoF_m} = C_f \times (T_m - T) \div 2$.

Step 7: Each verifier V_1, V_2, V_3 and V_4 decrypts the received message via his lattice public key (PK_{V_m}), then checks that the received K_4 equals the K_4 that he precomputed and checks that the distances $D_{TDoF_1}, D_{TDoF_2}, D_{TDoF_3}$ and D_{TDoF_4} are equal to the actual distance between him and the intended position (X_P, Y_P, Z_P). If this verification process succeeds, it means that the claimed prover P passes the first test (TDoF-based verification) and then moves to the second test (RSS-based verification). Otherwise, the claimed position/prover is rejected.

B. SECOND TEST: ADAPTIVE RSS-BASED MATHEMATICAL MODEL

In wireless communications, RSS represents the average power that a node receives, where the power originates from the source of the emitter. RSS measures the distance between any two nodes from the received signal strength measurement between each node [66], [67]. The majority of wireless devices can measure received signal strength without requiring extra system modification, hardware or overhead from communication. According to Daiya *et al.* [68], the RSS results present the estimated location of the sensor nodes with an estimated error of between 5% and 10%. The widespread exponential path-loss form is a frequent strategy and is the easiest to organize and use. The path-loss exponent form is a log-power scale, which states that the rate of RSS declines linearly with the value of the distance between nodes. This is an approximate estimate; for example, noise levels are high and are dependent on nonline-of-sight (NLOS) and multipath conditions. Because most wireless devices can measure received signal strength, RSS-based localization algorithms have increased in popularity. However, integrating the information from all the verifiers reduces the location error and effectively increases the positioning accuracy.

In contrast to the other localization methods, RSS is representative of the relationship between an obtained power and communication. It is used to determine the distance between a receiver and sender when most propagates of electromagnetic waves in an LOS link. This method is used to handle the mobility of devices in several protocols of mobility-aware media access control (MAC).

When the direct path of transmission exists between two devices and is put into environments where there is no interference of signals, then the received power of signal P_r forms a relationship to the distance, D_{RSS}, between the receiving and transmitting devices in the law of inverse square [69].

$$P_r \propto \frac{1}{(D_{RSS})^2} \tag{1}$$

However, equation (1) states the correlation between the relative distance and RSS. In reality, there are multiple influences on the received signal strength value. For instance, diffraction, refraction, reflection, and scattering of waves are a result of nearby objects and obstacles between receivers and transmitters. It has been discovered through experimentation that walls can lower the signal strength by up to 3 dBm (decibel-milliwatts) on average [69]. In other words, the received power of signal P_r declines more gradually because of shadow fading, nonuniform propagation and multipath propagation. This causes a transfer of the relationship between D_{RSS} and P_r to:

$$P_r = P_t \times (D_{RSS})^{-n} \tag{2}$$

where n refers to exponential path loss and P_t is transmitted signal power.

To express P_r and P_t in dBm, since dBm is a logarithmic unit to measure power, it is taken as 10 times the logarithm function for both sides in (2) as follows:

$$10 \log_{10} P_r = 10 \log_{10} P_t - 10\, n \log_{10} D_{RSS} \tag{3}$$

However, 10 $\log_{10} P$ is the expression of the converted power to dBm. At a distance of one meter, the received power is almost equal to the transmitted power; thus, P_t (dBm) can be measured as the received signal power at a distance of one meter. Consequently, the correlation

TABLE 2. The path-loss exponent value (*n*).

Environment	Exponential path-loss n
Urban area	2.7 – 3.5
Free space	2.0
Obstructed in building	4 – 6
Shadowed urban area	3 – 5

between the value of distance D_{RSS} and received signal strength P_r (dBm) can be written as the following log-formula given in equation (4):

$$P_r\left(D_{RSS}\right)\ \{dBm\} = P_0\left(D_0\right)\ \{dBm\} - 10\,n\ \log_{10}\left(\frac{D_{RSS}}{D_0}\right) + W\ +\ \delta^{best}$$
$$where\ W = \frac{Var}{2\gamma},\quad \delta^{best}\ = 2\left(\varepsilon\ +\ \frac{1}{\mathcal{M}}\right) \tag{4}$$

where $P_r(D_{RSS})$ is the received wireless signal power in decibel-milliwatts (dBm) at the distance D_{RSS}, $P_0(D_0)$ is the reference signal power in dBm from the sender at a reference distance D_0. For most applications, D_0 generally equals one meter, D_{RSS} denotes the real distance between the sender and receiver, n refers to the path-loss or signal decay exponent, which is defined as the rate at which the RSS declines with distance, W is the weight of the power shadow, Var denotes the expected noise variance in the received signal and γ is expressed as the ratio of the received to reference signal powers, i.e., $P_r\ /\ P_0$. δ^{best} will increase the probability that the scheme converges to better localization, ε denotes a random value in the range [0, 1] generated by $Rand()$, and $\mathcal{M}$ is the maximum number of verifiers [70], [71]. In fact, both n and Var depend on the environment. However, n, Var and P_0 can be retrieved for each verifier V_m by using an uncomplicated supervised learning procedure, and we can use intelligent techniques such as deep learning, a nonquantum particle swarm optimization approach and a genetic algorithm to increase the accuracy of RSS-based localization. Both are the most promising techniques for optimization because they combine high accuracy and low computational time. Table (2) illustrates the path-loss exponent value (n) based on the building type and surroundings because it can be determined using the premeasurements [72], [73].

RSS is assessed between the readers and the tag. Wireless signal strength is transformed to distance, giving four distances required for 3D multilateration. In other words, the distance between unknown prover P and the verifiers can be calculated by V_1, V_2, V_3 and V_4 using equations (5), (6), (7), and (8), respectively:

$$D_{RSS1} = 10^{\left(\frac{P_{01}-\ P_{r1}+\ W_1\ +\ \delta_1^{best}}{10n}\right)} \tag{5}$$
$$D_{RSS2} = 10^{\left(\frac{P_{02}-\ P_{r2}+\ W_2\ +\ \delta_2^{best}}{10n}\right)} \tag{6}$$
$$D_{RSS3} = 10^{\left(\frac{P_{03}-\ P_{r3}+\ W_3\ \ +\ \delta_3^{best}}{10n}\right)} \tag{7}$$
$$D_{RSS4} = 10^{\left(\frac{P_{04}-\ P_{r4}+\ W_4\ +\ \delta_4^{best}}{10n}\right)} \tag{8}$$

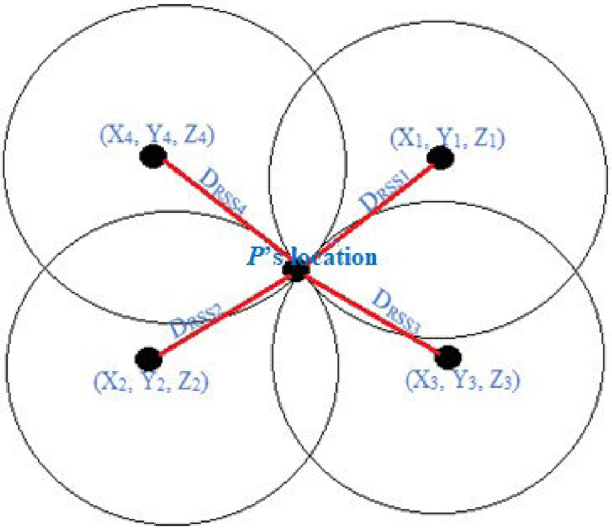


FIGURE 3. RSS-based distance measurements through only four verifiers V_1, V_2, V_3, and $V4$ located in the area and allowing them to validate the claimed prover's location together.

Once each distance has been computed, then they are inserted into a set of quadratic formulas, which is termed trilateration or multilateration. Trilateration enables the finding of the position of claimed prover P on the XY plane, while the multilateration method permits the finding of the position of claimed prover P on the X, Y, and Z axes. Multilateration has the implication of additional reference nodes, which reduces the uncertainty of the position of the mobile node based on the measured distance accuracy. The four verifiers' locations are known along with the distance between each verifier and the unknown prover P for 3-D multilateration to function perfectly. The intersection between all four verifiers is the unknown prover's location, as shown in Figure (3). Before computing 3D multilateration quadratic equations, the average of the resulting distances from the TDoF-based test and RSS-based test is required to reduce the error estimation using the following equations. The verifiers V_1, V_2, V_3 and V_4 compute the average of distances D_{avg1}, D_{avg2}, D_{avg3} and D_{avg4} respectively as the following equations ((9) –(12)) and then transmit these distance averages and 3D position of themselves, i.e., these messages $\{D_{avg1}, D_{avg2}, D_{avg3}, D_{avg4}, (X_1, Y_1, Z_1), (X_2, Y_2, Z_2),$ $(X_3, Y_3, Z_3), (X_4, Y_4, Z_4)\}$ over the secure channels among themselves.

$$D_{avg1} = \frac{D_{TDoF1}\ +\ D_{RSS1}}{2} \tag{9}$$
$$D_{avg2} = \frac{D_{TDoF2}\ +\ D_{RSS2}}{2} \tag{10}$$
$$D_{avg3} = \frac{D_{TDoF3}\ +\ D_{RSS3}}{2} \tag{11}$$
$$D_{avg4} = \frac{D_{TDoF4}\ +\ D_{RSS4}}{2} \tag{12}$$

By using the Euclidean distance between the position of each verifier and the claimed prover's position, each verifier can obtain equations (13), (14), (15) and (16) for 3D multilateration and then compute the 3D position of the claimed

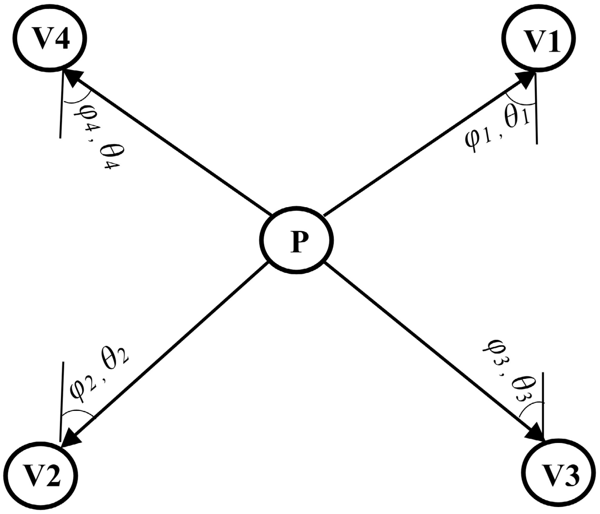


FIGURE 4. The structure of the AoA positioning system.

prover as follows:

$$(X_{Prss} - X_1)^2 + (Y_{Prss} - Y_1)^2 + (Z_{Prss} - Z_1)^2 = D_{avg1}^2 \tag{13}$$

$$(X_{Prss} - X_2)^2 + (Y_{Prss} - Y_2)^2 + (Z_{Prss} - Z_2)^2 = D_{avg2}^2 \tag{14}$$

$$(X_{Prss} - X_3)^2 + (Y_{Prss} - Y_3)^2 + (Z_{Prss} - Z_3)^2 = D_{avg3}^2 \tag{15}$$

$$(X_{Prss} - X_4)^2 + (Y_{Prss} - Y_4)^2 + (Z_{Prss} - Z_4)^2 = D_{avg4}^2 \tag{16}$$

To simplify the above quadratic equation set, equation (13) is subtracted into equations (14), (15) and (16). As a result, the following three linear equations will be produced.

$$\begin{aligned} &2(X_2 - X_1)X_{Prss} + 2(Y_2 - Y_1)Y_{Prss} + 2(Z_2 - Z_1)Z_{Prss} \\ &\quad = \left(D_{avg1}^2 - D_{avg2}^2\right) \\ &\qquad - \left(X_1^2 - X_2^2\right) - \left(Y_1^2 - Y_2^2\right) - \left(Z_1^2 - Z_2^2\right) \end{aligned} \tag{17}$$

$$\begin{aligned} &2(X_3 - X_1)X_{Prss} + 2(Y_3 - Y_1)Y_{Prss} + 2(Z_3 - Z_1)Z_{Prss} \\ &\quad = \left(D_{avg1}^2 - D_{avg3}^2\right) \\ &\qquad - \left(X_1^2 - X_3^2\right) - \left(Y_1^2 - Y_3^2\right) - \left(Z_1^2 - Z_3^2\right) \end{aligned} \tag{18}$$

$$\begin{aligned} &2(X_4 - X_1)X_{Prss} + 2(Y_4 - Y_1)Y_{Prss} + 2(Z_4 - Z_1)Z_{Prss} \\ &\quad = \left(D_{avg1}^2 - D_{avg4}^2\right) \\ &\qquad - \left(X_1^2 - X_4^2\right) - \left(Y_1^2 - Y_4^2\right) - \left(Z_1^2 - Z_4^2\right) \end{aligned} \tag{19}$$

The X_{Prss}, Y_{Prss} and Z_{Prss} coordinates are obtained by resolving the linear equations (17), (18) and (19) using Cramer's rule of 3 × 3 matrices as equations (20) - (22), as shown at the bottom of the next page.

If this verification process succeeds, it means that the measured position $(X_{Prss}, Y_{Prss}, Z_{Prss})$ is equal to the intended position (X_P, Y_P, Z_P), and the third verification can proceed,

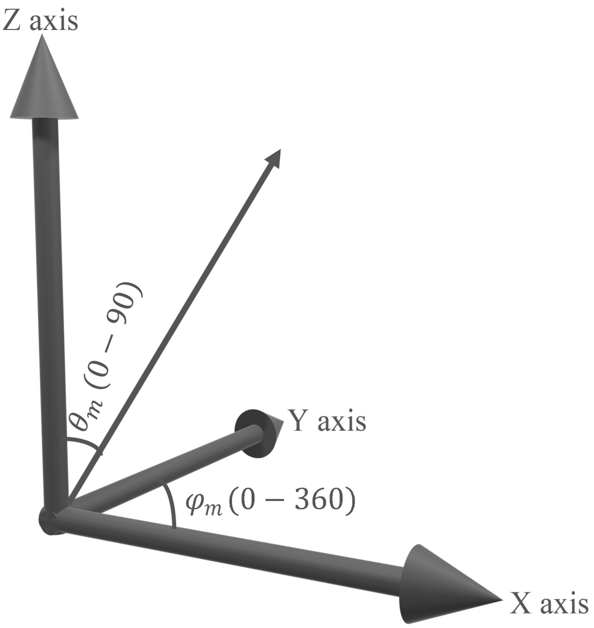


FIGURE 5. Illustration of angles in 3-D space.

which is the AoA-based verification. Otherwise, the claimed position is rejected.

C. THIRD TEST: ADAPTIVE AoA-BASED MATHEMATICAL MODEL

Many future systems of localization will utilize the AoA technique, as the coming fifth-generation networks may be provided with arrays of an antenna that allow assessing the AoA of the received signal [74] from a mobile node. The concept of AoA measurement is utilized in VOR/VORTAC systems for navigation of aircraft. Figures (4), (5) and (6) illustrate the structure of the AoA positioning system in the context of the elevation (vertical) angle θ and the azimuth (horizontal) angle φ of received electromagnetic signals at the verifiers, where the azimuth angle φ is from 0 to 2π and the elevation angle θ is from 0 to 90.

The verifiers V_1, V_2, V_3 and V_4 rely on the relationship between AoA and coordinates [25], [75]–[78] to estimate the horizontal location first via formula (23) and then estimate the vertical location via formula (24) to obtain the three-dimensional location $(X_{Paoa}, Y_{Paoa}, Z_{Paoa})$ of claimed prover P. In terms of noise elimination, we use a Gaussian filter ($G_{X,Y}$ and G_Z) with zero mean to reduce the noise in the received signals at the verifiers. Thus, this leads to enhanced AoA-based positioning as follows:

$$\varphi_m = tan^{-1}\left(\frac{Y_{Paoa} - Y_m}{X_{Paoa} - X_m}\right) + F_{X,Y}^m,$$

$$where$$

$$F_{X,Y}^m = G_{X,Y}^m + \varrho_m,$$

$$G_{X,Y}^m = \frac{2}{\sqrt{\pi\sigma}}\, e^{-\left(\frac{X_m^2 + Y_m^2}{2\ Var}\right)},$$

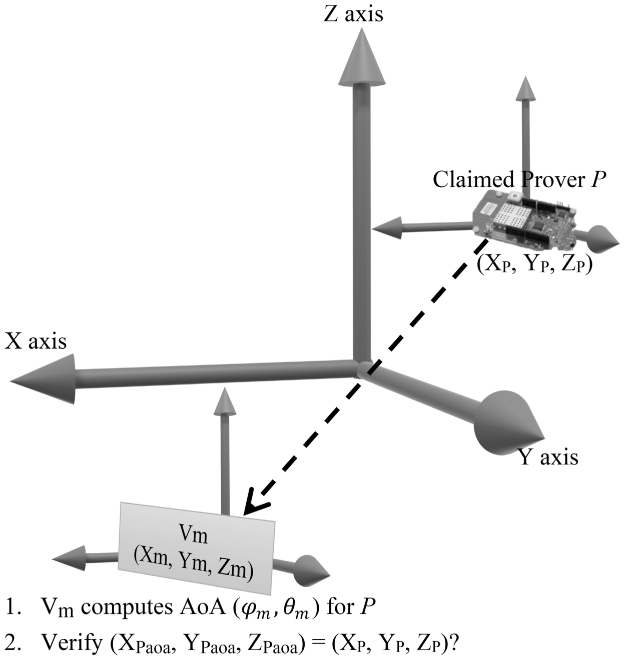

Z axis
Claimed Prover P
(XP, YP, ZP)
X axis
Y axis
Vm
(Xm, Ym, Zm)
1. Vm computes AoA (φ_m, θ_m) for P
2. Verify (XPaoa, YPaoa, ZPaoa) = (XP, YP, ZP)?

FIGURE 6. The geometric AoA localization system.

$$\varrho_m = \frac{\varepsilon}{2\mathcal{M}}, \quad m = 1, 2, 3, 4 \text{ and } \sigma \text{ is standard deviation} \tag{23}$$

$$\theta_m = tan^{-1}\left(\frac{Z_{Paoa} - Z_m}{\sqrt{(X_{Paoa} - X_m)^2 + (Y_{Paoa} - Y_m)^2}}\right)$$

$$+ F_Z^m, \text{ where } F_Z^m = G_Z^m + \varrho_m,$$

$$G_Z^m = \frac{2}{\sqrt{\pi\sigma}}\, e^{-\frac{Z_m^2}{2\,Var}} \text{ and } m = 1, 2, 3, 4 \tag{24}$$

Moreover, to obtain a very high accuracy of AoA-based localization, optimization techniques could be used. Therefore, the verifiers V_1, V_2, V_3 and V_4 transmit these measurements of the elevation angles θ_m and the azimuth angles φ_m over the secure channels among themselves. The equation (23) can be expressed as equation (26).

$$\frac{sin\left(\varphi_m - F_{X,Y}^m\right)}{cos\left(\varphi_m - F_{X,Y}^m\right)} = \frac{Y_{paoa} - Y_m}{X_{paoa} - X_m} \tag{25}$$

$$\frac{sin\varphi_m\, cosF_{X,Y}^m - cos\varphi_m\, sinF_{X,Y}^m}{cos\varphi_m\, cosF_{X,Y}^m + sin\varphi_m\, sinF_{X,Y}^m} = \frac{Y_{paoa} - Y_m}{X_{paoa} - X_m} \tag{26}$$

$$\begin{aligned} X_{Paoa}\, sin\varphi_m\, cosF_{X,Y}^m &- X_{Paoa}\, cos\varphi_m\, sinF_{X,Y}^m \\ &- X_m\, sin\varphi_m\, cosF_{X,Y}^m + X_m cos\varphi_m\, sinF_{X,Y}^m \\ &= Y_{paoa}\, cos\varphi_m\, cosF_{X,Y}^m + Y_{Paoa}\, sin\varphi_m\, sinF_{X,Y}^m \\ &- Y_m\, cos\varphi_m\, cosF_{X,Y}^m - Y_m\, sin\varphi_m\, sinF_{X,Y}^m \end{aligned} \tag{27}$$

Expressing (27) in matrix form we will have (28) and (29), as shown at the bottom of the next page:

As a result, equation (24) can be solved easily to obtain the third coordinate $Z_{P_{aoa}}$ of the claimed prover's location.

$$X_{Prss} = \frac{\begin{vmatrix} \left(D_{avg1}^2 - D_{avg2}^2\right) - \left(X_1^2 - X_2^2\right) - \left(Y_1^2 - Y_2^2\right) - \left(Z_1^2 - Z_2^2\right) & 2\,(Y_2 - Y_1) & 2\,(Z_2 - Z_1) \\ \left(D_{avg1}^2 - D_{avg3}^2\right) - \left(X_1^2 - X_3^2\right) - \left(Y_1^2 - Y_3^2\right) - \left(Z_1^2 - Z_3^2\right) & 2\,(Y_3 - Y_1) & 2\,(Z_3 - Z_1) \\ \left(D_{avg1}^2 - D_{avg4}^2\right) - \left(X_1^2 - X_4^2\right) - \left(Y_1^2 - Y_4^2\right) - \left(Z_1^2 - Z_4^2\right) & 2\,(Y_4 - Y_1) & 2\,(Z_4 - Z_1) \end{vmatrix}}{\begin{vmatrix} 2\,(X_2 - X_1) & 2\,(Y_2 - Y_1) & 2(Z_2 - Z_1) \\ 2\,(X_3 - X_1) & 2\,(Y_3 - Y_1) & 2(Z_3 - Z_1) \\ 2\,(X_4 - X_1) & 2\,(Y_4 - Y_1) & 2(Z_4 - Z_1) \end{vmatrix}} \tag{20}$$

$$Y_{Prss} = \frac{\begin{vmatrix} 2\,(X_2 - X_1) & \left(D_{avg1}^2 - D_{avg2}^2\right) - \left(X_1^2 - X_2^2\right) - \left(Y_1^2 - Y_2^2\right) - \left(Z_1^2 - Z_2^2\right) & 2\,(Z_2 - Z_1) \\ 2\,(X_3 - X_1) & \left(D_{avg1}^2 - D_{avg3}^2\right) - \left(X_1^2 - X_3^2\right) - \left(Y_1^2 - Y_3^2\right) - \left(Z_1^2 - Z_3^2\right) & 2\,(Z_3 - Z_1) \\ 2\,(X_4 - X_1) & \left(D_{avg1}^2 - D_{avg4}^2\right) - \left(X_1^2 - X_4^2\right) - \left(Y_1^2 - Y_4^2\right) - \left(Z_1^2 - Z_4^2\right) & 2\,(Z_4 - Z_1) \end{vmatrix}}{\begin{vmatrix} 2\,(X_2 - X_1) & 2\,(Y_2 - Y_1) & 2(Z_2 - Z_1) \\ 2\,(X_3 - X_1) & 2\,(Y_3 - Y_1) & 2(Z_3 - Z_1) \\ 2\,(X_4 - X_1) & 2\,(Y_4 - Y_1) & 2(Z_4 - Z_1) \end{vmatrix}} \tag{21}$$

$$Z_{Prss} = \frac{\begin{vmatrix} 2\,(X_2 - X_1) & 2\,(Y_2 - Y_1) & \left(D_{avg1}^2 - D_{avg2}^2\right) - \left(X_1^2 - X_2^2\right) - \left(Y_1^2 - Y_2^2\right) - \left(Z_1^2 - Z_2^2\right) \\ 2\,(X_3 - X_1) & 2\,(Y_3 - Y_1) & \left(D_{avg1}^2 - D_{avg3}^2\right) - \left(X_1^2 - X_3^2\right) - \left(Y_1^2 - Y_3^2\right) - \left(Z_1^2 - Z_3^2\right) \\ 2\,(X_4 - X_1) & 2\,(Y_4 - Y_1) & \left(D_{avg1}^2 - D_{avg4}^2\right) - \left(X_1^2 - X_4^2\right) - \left(Y_1^2 - Y_4^2\right) - \left(Z_1^2 - Z_4^2\right) \end{vmatrix}}{\begin{vmatrix} 2\,(X_2 - X_1) & 2\,(Y_2 - Y_1) & 2(Z_2 - Z_1) \\ 2\,(X_3 - X_1) & 2\,(Y_3 - Y_1) & 2(Z_3 - Z_1) \\ 2\,(X_4 - X_1) & 2\,(Y_4 - Y_1) & 2(Z_4 - Z_1) \end{vmatrix}} \tag{22}$$

On average, we can evaluate the suggested localization algorithms as follows (30)–(32), as shown at the bottom of the next page:

If this verification process succeeds, it means that the claimed prover P is verified, and he proves that his position at (X_P, Y_P, Z_P), then the closest verifier to the sender will send the prover's lattice public key encrypted by Alice's lattice public key to sender (Alice) i.e. $Nereast\ V_m \rightarrow Alice : \{PK_p\}_{PK_A}$. After that, the verifiers will delete PK_p and PK_A from their devices because in case any verifier is attacked in the future, the attackers cannot obtain the PK_p and PK_A. Otherwise, the claimed position is rejected.

All entities use lattice theory (lattice-based cryptography) to generate public/private keys and encrypt/decrypt messages [79]–[83]. Hence, we develop the NTRU and Goldreich–Goldwasser–Halevi (GGH) algorithms as follows:

We define an equilateral triangular lattice (hexagonal lattice) $\mathcal{L}$ over $p - adic$ integers to form a subring of $\mathbb{Q}_p$ such that $\mathcal{L} \subset \mathbb{Z}_p^{i \times j}$ good prime integrated polynomial entropies with dimensions i and j. The integral of the polynomial is employed to encrypt the message, whereas the derivative of the polynomial (differential polynomial) is applied to decrypt the message. We select prime modulus p and highest exponent (truncation index) N [84] based on our simulation-based evaluation equal to 2 and 17.5, respectively. N can be increased to obtain more security, but this value is nominated to achieve a relative balance between security and performance, especially for limited resource devices such as in the case of the IoT/IoMT environment. N must not be equal to zero because zero yields infinite order. This evaluation is implemented on a laptop with an Intel Core i7-1165G7 processor (12 MB cache, up to 4.7 GHz) and 16 GB LPDDR4x RAM (up to 4267 MHz) by using MATLAB R2018b. Here, arithmetic operations are performed in the $p - adics$ [84]. However, the number of $p - adic$ integers associated with terminating $p - adic$ integers is a countable set, particularly a countably infinite set [85].

To obtain a high cryptographic quality and information leakage prevention with less complexity time, shifting [86] and Henon shuffling maps [87]–[91] are applied. Therefore, it is effective for the IoT/IoMT system and impossible to break. The Henon shuffling map is a discrete-time dynamical system to shuffle the point position (X_τ, Y_τ) to a new position in the plane in a chaotic manner as follows:

$$\begin{cases} X_{\tau+1} = 1 - aX_\tau^2 + Y_\tau \\ Y_{\tau+1} = bX_\tau \end{cases}$$

The iteration number for the Henon shuffling map here is 100. For chaotic behavior, parameter a is 1.4 and parameter b is 0.3, whereas other values for a and b make the Henon map intermittent, chaotic or converge to a periodical orbit [89].

A message (i.e., plain text) $Msg \in \mathcal{L}$. An example of an equilateral triangular lattice (hexagonal lattice) $\mathcal{L}$ is shown in Figure (7).

Keys generation:

Select prime $\beta, \alpha, \xi \in \mathbb{Z}_p$ good integrated polynomial entropies over the $p - adic$ number field.

Select matrix $S1 \in \mathcal{L}$ good prime integrated polynomial entropies.

Select matrices $\Lambda, \Gamma \in \mathcal{L} \subset \mathbb{Z}_p^{i \times j}$ good prime integrated polynomial entropies over $p - adic$ number system $\mathbb{Q}_p$.

$$\begin{aligned} S_{11} &= Shuffle\left(Shift_\xi\left(S_1\right)\right) \\ S_2 &= \Lambda \oplus \Gamma \\ S_{22} &= Shuffle\left(Shift_\xi\left(S_2\right)\right) \\ &Secret\ key\ (private\ key)\ SK : (S_{11}, S_{22}) \\ PK &= S_{11}^{-1}(mod\ \beta) \cdot S_{22}^T \\ &Public\ key\ PK_p : (PK, \alpha) \end{aligned}$$

Encryption:

$$\begin{aligned} Enc_0 &= Msg(mod\ \alpha) \cdot PK \\ Enc &= Shuffle\left(Shift_\alpha\left(Enc_0\right)\right) \end{aligned}$$

Decryption:

$$\begin{aligned} M_0 &= Shuffle^{-1}\left(Shift_\alpha^{-1}\left(Enc\right)\right) \\ Msg &= [M_0(mod\ \alpha) \cdot S_{11}(mod\ \beta)] \cdot [(S_{22}^T S_{22})^{-1} \cdot S_{22}^T] \end{aligned}$$

$$\begin{aligned} Ax &= b\ where\ A = \begin{bmatrix} sin\varphi_1\ cosF_{X,Y}^1 - cos\varphi_1\ sinF_{X,Y}^1 & -cos\varphi_1\ cosF_{X,Y}^1 - sin\varphi_1\ sinF_{X,Y}^1 \\ sin\varphi_2\ cosF_{X,Y}^2 - cos\varphi_2\ sinF_{X,Y}^2 & -cos\varphi_2\ cosF_{X,Y}^2 - sin\varphi_2\ sinF_{X,Y}^2 \\ sin\varphi_3\ cosF_{X,Y}^3 - cos\varphi_3\ sinF_{X,Y}^3 & -cos\varphi_3\ cosF_{X,Y}^3 - sin\varphi_3\ sinF_{X,Y}^3 \\ sin\varphi_4\ cosF_{X,Y}^4 - cos\varphi_4\ sinF_{X,Y}^4 & -cos\varphi_4\ cosF_{X,Y}^4 - sin\varphi_4\ sinF_{X,Y}^4 \end{bmatrix} \\ x &= [X_{Paoa} \quad Y_{Paoa}]^T\ ,\ here\ T\ refers\ to\ the\ matrix\ transpose\ operation. \\ b &= \begin{bmatrix} X_1\ sin\varphi_1\ cosF_{X,Y}^1 - X_1 cos\varphi_1\ sinF_{X,Y}^1 - Y_1\ cos\varphi_1\ cosF_{X,Y}^1 - Y_1\ sin\varphi_1\ sinF_{X,Y}^1 \\ X_2\ sin\varphi_2\ cosF_{X,Y}^2 - X_2\ cos\varphi_2\ sinF_{X,Y}^2 - Y_2\ cos\varphi_2\ cosF_{X,Y}^2 - Y_2\ sin\varphi_2\ sinF_{X,Y}^2 \\ X_3\ sin\varphi_3\ cosF_{X,Y}^3 - X_3\ cos\varphi_3\ sinF_{X,Y}^3 - Y_3\ cos\varphi_3\ cosF_{X,Y}^3 - Y_3\ sin\varphi_3\ sinF_{X,Y}^3 \\ X_4\ sin\varphi_4\ cosF_{X,Y}^4 - X_4\ cos\varphi_4\ sinF_{X,Y}^4 - Y_4\ cos\varphi_4\ cosF_{X,Y}^4 - Y_4\ sin\varphi_4\ sinF_{X,Y}^4 \end{bmatrix} \end{aligned} \tag{28}$$

$$Thus,\ x = \left(A^T A\right)^{-1} A^T b \tag{29}$$

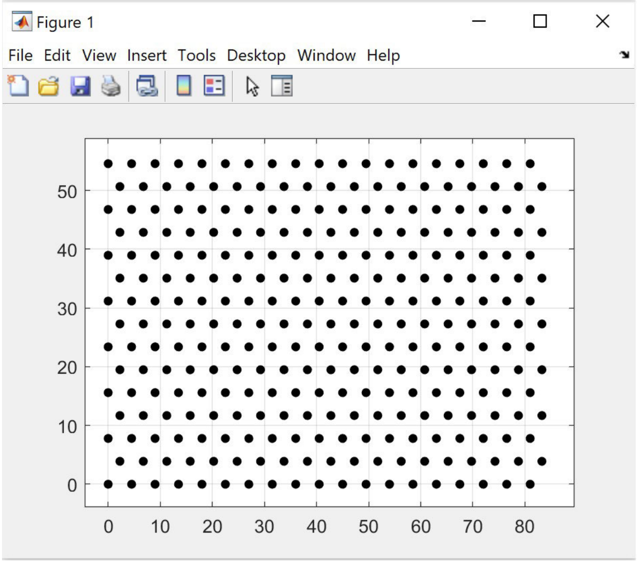


FIGURE 7. Equilateral triangular lattice [92].

V. ANALYTICAL-BASED EVALUATION AND SIMULATION-BASED RESULTS

This section depicts the robustness of the proposed cryptographic scheme in the context of cybersecurity and the effectiveness of performance features, including the energy consumption of normal and advanced sensor devices, stability period of the NB-IoT device-to-device network (NB-IoT D2D), time consumption at the BS, elapsed time for the whole NB-IoT D2D network, and throughput. We demonstrate that the proposed cryptosystem resists key attacks that are highlighted in the state of the art and works efficiently without compromising the performance of the NB-IoT D2D attocell.

Notably, all three verification processes (TDoF, RSS and AoA) are applied by verifiers (V_m) rather than IoT devices (p) in the proposed cryptosystem. As a result, a large part of the energy consumption and time cost is the responsibility of the verifiers V_m, which are gateways, sinks, base stations or even satellites; thus, the proposed 3D-location-driven cryptosystem is effective, especially in the case of IoT or tactile internet applications that contain restricted-resource devices.

The functionality comparison between the proposed cryptosystem and some related schemes is depicted in Table (3). The proposed cryptosystem not only provides communications confidentially but also fulfills all criteria of security without complex conditions or equipment. From these descriptions and simulation outputs, in the next section, it is concluded that our cryptosystem is more practical.

A. SECURITY ANALYSIS VIA THREAT MODEL

To analyze the proposed efficient location-driven cryptosystem, threat modeling is applied. It is assumed in threat modeling that two entities communicate over an untrusted communication channel.

Claim (1): The proposed cryptosystem resists any number of colluding-location-spoofing attacks.

Proof: Colluding positioning spoofing attacks is a case where a number of colluding attackers surrounding the intended position (X_P, Y_P, Z_P) spoof successfully to cheat V_m that their locations at the location of P via a data forgery to obtain illegal advantages. In the proposed cryptographic protocol, the colluding spoofer adversaries must persuade the four verifiers V_m that their locations are at actual 3D coordinates of the aimed location (X_P, Y_P, Z_P) (i.e., receiver's location) to spoof/fraud the aimed position (X_P, Y_P, Z_P). These colluding spoofer attackers cannot persuade the V_m because they do not pass all three tests: TDoF-, RSS- and AoA-based location verification algorithms. These measures are based exclusively on the hardware and physical environment such that these measured values cannot be readily manipulated or forged by location spoofing attacks even by colluding.

$$\begin{aligned} Error_{Avg} &= \frac{\sum_{i=1}^{80}\left[\sqrt{\left(X_{com(i)} - X_{P(i)}\right)^2} + \sqrt{\left(Y_{com(i)} - Y_{P(i)}\right)^2} + \sqrt{\left(Z_{com(i)} - Z_{P(i)}\right)^2}\right]}{80} \\ &= 0.1278, \\ where\ X_{com} &= \frac{X_{Prss} + X_{Paoa}}{2},\ Y_{com} = \frac{Y_{Prss} + Y_{Paoa}}{2}, \\ Z_{com} &= \frac{Z_{Prss} + Z_{Paoa}}{2}\ and\ i\ is\ a\ simulation\ trial\ number. \qquad (30) \\ Error\ percentage &= \frac{Error_{Avg}}{Actual_{Avg}} \times 100\% = 0.9210\%,\quad where \\ Actual_{Avg} &= \frac{\sum_{i=1}^{80}\left[\sqrt{\left(X_{P(i)}\right)^2} + \sqrt{\left(Y_{P(i)}\right)^2} + \sqrt{\left(Z_{P(i)}\right)^2}\right]}{80} \qquad (31) \\ Location\ accuracy\ percentage &= \left[1 - \left(\frac{Error_{Avg}}{Actual_{Avg}}\right)\right] \times 100\% \\ &= 99.0790\% \qquad (32) \end{aligned}$$

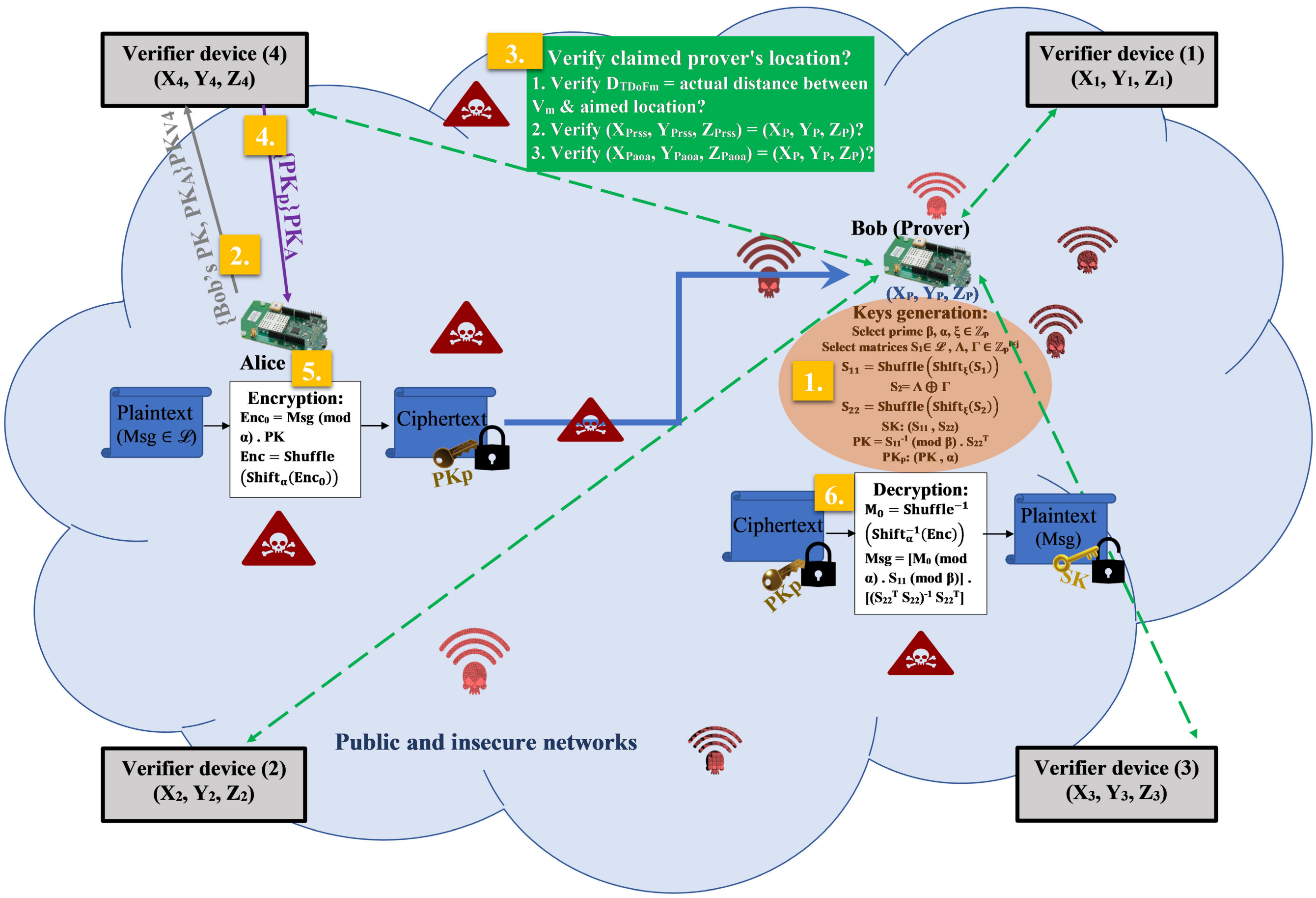

Verifier device (4)
(X_4, Y_4, Z_4)
3.
Verify claimed prover's location?
1. Verify D_{TDoFm} = actual distance between V_m & aimed location?
2. Verify $(X_{Prss}, Y_{Prss}, Z_{Prss}) = (X_P, Y_P, Z_P)$?
3. Verify $(X_{Paoa}, Y_{Paoa}, Z_{Paoa}) = (X_P, Y_P, Z_P)$?
Verifier device (1)
(X_1, Y_1, Z_1)
2.
{Bob's PK, PK_A}PKv4
4.
{PK_p}PKA
Bob (Prover)
(X_P, Y_P, Z_P)
Keys generation:
Select prime $\beta, \alpha, \xi \in \mathbb{Z}_p$
Select matrices $S_1 \in \mathscr{L}$, $\Lambda, \Gamma \in \mathbb{Z}_p^{i \times j}$
1.
$S_{11} = \text{Shuffle}\left(\text{Shift}_\xi(S_1)\right)$
$S_2 = \Lambda \oplus \Gamma$
$S_{22} = \text{Shuffle}\left(\text{Shift}_\xi(S_2)\right)$
SK: (S_{11}, S_{22})
$PK = S_{11}^{-1} \pmod{\beta} . S_{22}^T$
PK_p: (PK , α)
Alice
5.
Plaintext
(Msg ∈ $\mathscr{L}$)
Encryption:
$Enc_0 = Msg \pmod{\alpha} . PK$
$Enc = \text{Shuffle}\left(\text{Shift}_\alpha(Enc_0)\right)$
Ciphertext
PKp
6.
Ciphertext
PKp
Decryption:
$M_0 = \text{Shuffle}^{-1}\left(\text{Shift}_\alpha^{-1}(Enc)\right)$
$Msg = [M_0 \pmod{\alpha} . S_{11} \pmod{\beta}] . [(S_{22}^T S_{22})^{-1} S_{22}^T]$
Plaintext
(Msg)
SK
Verifier device (2)
(X_2, Y_2, Z_2)
Public and insecure networks
Verifier device (3)
(X_3, Y_3, Z_3)

FIGURE 8. General architecture of the proposed cryptosystem.

TABLE 3. Functionality comparison between the proposed cryptosystem and some related schemes.

Criteria	Our Cryptosystem	[5]	[41]	[56]
Colluding-location-spoofing attacks.	Secure.	Not Secure.	Not Secure.	Inefficient.
Mobile/Static Nodes.	Mobile or Static Nodes.	Static Nodes.	Authors claim that their model and [5] can be used in the mobile internet setting.	Not determined.
Quantum computing attacks	Secure.	Secure because string X has large min-entropy in BRM pseudorandom generators (PRG).	Secure because string X has large min-entropy in BRM PRG.	Secure.
Hard/additional constraint assumption.	No.	Yes.	Yes.	Yes.
Inheritance of quantum cryptography shortcomings.	No.	No.	No.	Yes.
Performance.	Efficient (excellent).	Needs huge memory.	Needs huge memory.	Efficient based on high performance for quantum computing.
Experiment/Implementation (software, hardware).	Applied on NB-IoT D2D simulator [93].	Applied in [38].	Analyzed by the universal composition (UC) security framework and ideal functionality.	They prove some technical lemmas.
Colluding Teleportation-based attacks/Side-channel attacks (information leakage attacks).	Secure.	Secure.	Secure.	Not Secure [51].
Suitable for IoT, IoMT and tactile internet applications.	Yes.	No.	No.	No.

Furthermore, the integration of these three adaptive localization schemes leads to reliable locations in the presence of colluding spoofers. However, GPS is exposed to location spoofing attacks because it depends deeply on the time information [60]–[63], [94]–[96]. The colluding spoofing location attacks are solved by using adaptive RSS and AoA-based mathematical models.

Claim (2): The proposed cryptosystem solves the problems for public key distribution and public key infrastructure (PKI).

Proof: Unlike conventional public-key cryptography, there is no real PKI in our cryptosystem, where V_m is responsible for sending public keys between users (IoT devices) after three location verification processes, and these V_m are trusted. PK_A and PK_p are encrypted by PK_{V_m} such that Alice $\rightarrow$ Nereast V_m: $\{PK_A, \text{Request Bob's PK}\}_{PK_{V_m}}$ and $P \rightarrow V_m : \{K_4 \| PK_p\}_{PK_{v_m}}$. In addition, the V_m will delete PK_p and PK_A from their devices because in case any V_m is attacked, the attackers cannot obtain PK_p and PK_A. This means that the process of public key transmission is only performed among the sender, verified receiver and V_m, all of which are trusted. Each device generates its lattice private and public keys. For all these reasons, no requirement is necessary to revoke or change these keys per period. However, V_m may change their keys after a long period depending on the sensitivity of the application. This does not matter because V_m are sinks, base stations, gateways or even satellites, i.e., superstrong equipment. Hence, there is no obligation to distribute the public keys between users' devices via a hierarchy of certificate authorities (path of certification/trust chain), as in traditional PKI, which suffers from multiple issues, such as central authority, validation problems, and certificate revocation, as well as threats to PGP certificates. In other words, in our proposed cryptosystem, there is no need to use digital certificates signed (using a digital signature algorithm) by trusted authorities, certificate authorities, a key generation center or a private key generator.

Claim (3):The proposed cryptography offers resisting SIM swap fraud, SimJacker and side-channel attacks to which NB-IoT is vulnerable, as well as other vulnerable SIM technologies, such as the S@T browser and WIB, that may be exploited.

Proof: Cybersecurity for IoT Technologies in the third-generation partnership project (3GPP), such as NB-IoT and long-term evolution for machine-type communication (LTE-M), and some of the cybersecurity in the context of 5G involve SIM/USIM cards for security purposes, for instance, mutual authentication between a user device (SIM/USIM) and network and encryption features [55]. This leads to SIM swap fraud, SimJacker, SMS attacks and side-channel attacks because of vulnerabilities in the SIM cards. Additionally, there are other vulnerable technologies in SIM that may be exploited, such as the S@T browser and WIB. However, the proposed cryptosystem uses the physical geographical location of the device as an identity rather than a SIM/USIM card; thus, it resists all these attacks, vulnerabilities and impersonation.

Claim (4): The proposed cryptographic scheme resists replay attacks.

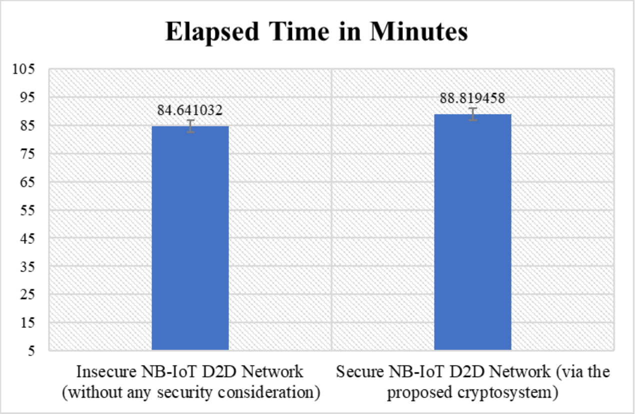


FIGURE 9. Comparison of elapsed times for insecure and secure NB-IoT D2D networks.

Proof: While adversaries eavesdrop on the communication channels between the V_m and sender, between the V_m and receiver or between the sender and receiver, only encrypted (i.e., unreadable form) data are available that cannot be reused. Furthermore, the proposed cryptosystem uses timestamps T and T_m to prevent replay attacks. Therefore, there is no successful replay attack against the proposed cryptosystem.

B. SIMULATION RESULTS

In this section, an averaged simulation-based evaluation concerning the proposed cryptosystem is provided. We use our open-source NB-IoT D2D simulation [93] to compare an insecure NB-IoT D2D network (without any security consideration) and a secure NB-IoT D2D network (via the proposed cryptosystem). This implementation-based evaluation involves not only the cost of cybersecurity operations but also the cost of telecommunications. However, all the performance metrics affected by security operations are studied to achieve a comprehensive evaluation of the proposed cryptosystem. The number of sensor nodes in the NB-IoT D2D attocell network is 300 and distributed randomly in a macrocell of an urban area. The simulator outputs demonstrate the reliability and robustness of the proposed cryptosystem.

The comparison of elapsed time for two cases in the urban macrocell, the first case, insecure NB-IoT D2D attocell (without any security consideration), and the second case, secure NB-IoT D2D attocell (via the proposed cryptosystem), is depicted in Figure (9). This comparison is evaluated until more than half of the sensor devices in the NB-IoT D2D network are dead (800 rounds). In the insecure NB-IoT D2D network, only plain messages were sent regardless of the existence of attackers (eavesdroppers) and without security considerations in such a public network. All communication costs for the insecure NB-IoT D2D network as well as computation and transmission costs of the proposed cryptosystem were taken into consideration in the secure NB-IoT D2D network. With the suggested cryptosystem, the operat-

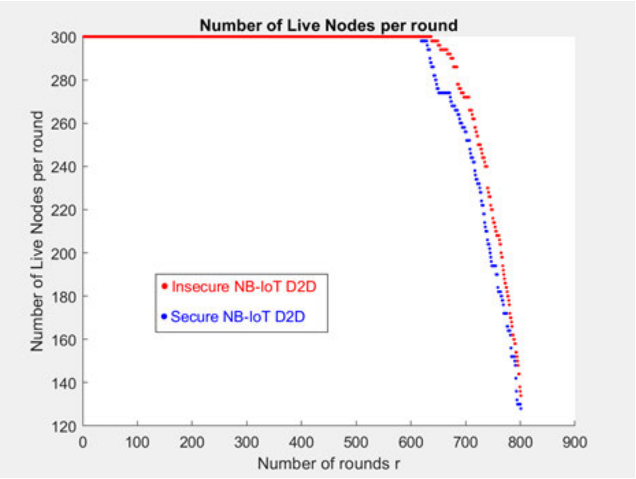


FIGURE 10. The comparison of stability periods.

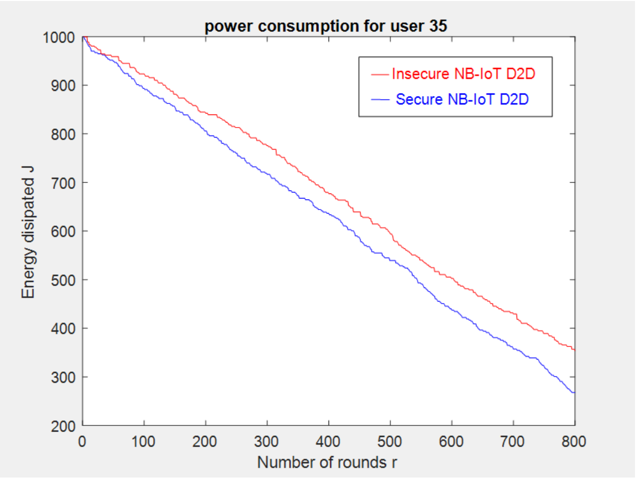


FIGURE 11. Comparison of normal sensor's energy profile (energy consumption for device No. 35) in two scenarios.

ing and transmitting costs are 88.819458 minutes, whereas without any security consideration, they are 84.641032 minutes. This indicates that only 4.178426 minutes is increased in the presence of the proposed cryptosystem. As a result, such a small delay is negligible compared to achieving a secure NB-IoT D2D network.

In view of the wireless communication principles, the stability period is one of the most performance metrics, especially for IoMT. Therefore, it is measured to present an effective evaluation of our proposed cryptosystem. The stability period is defined as the duration of time between the beginning of the network operation and the death of one of the resource-constrained devices in the network [97]. Figure (10) shows the comparison of stability periods for insecure and secure NB-IoT D2D networks. The stability periods for the insecure NB-IoT D2D network and secure NB-IoT D2D network are 638 rounds and 625 rounds, respectively. This means that stability periods are very convergent.

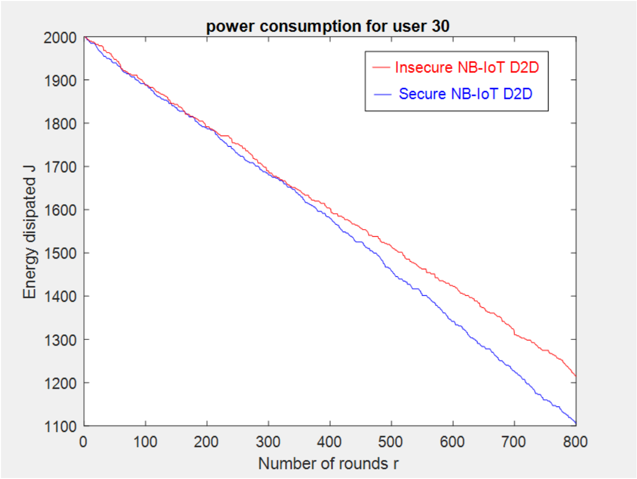


FIGURE 12. Comparison of advanced sensor's energy profile (energy consumption for device No. 30) in two situations.

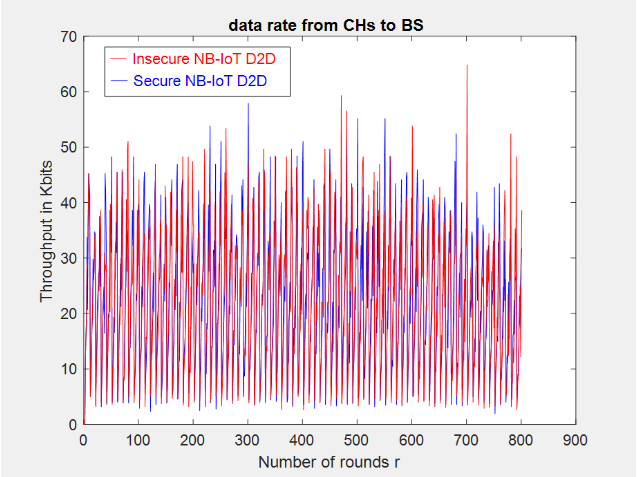


FIGURE 13. Comparison of insecure and secure NB-IoT throughputs.

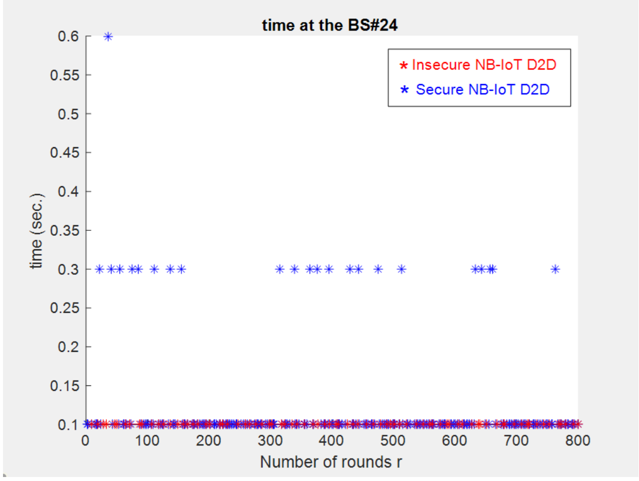


FIGURE 14. Comparisons of delay time at BS No. 24 in two scenarios.

The comparison of the power dissipation profile for normal sensor and advanced sensor is explained in Figure (11) and Figure (12), respectively in insecure and secure NB-IoT D2D attocell networks. This demonstrates that the State of Health (SOH) and State of Charge (SOC) of a sensor's battery are managed proficiently. In other words, there is no significant overhead cost in secure NB-IoT D2D attocell network in exchange for resisting adversarial attacks in such public networks.

Figure (13) depicts the comparison of insecure and secure NB-IoT network throughputs. Accordingly, the successful received packets rate considering the proposed cryptography is still effective. Figure (14) shows the comparisons of delay time at BS No. 24 in insecure NB-IoT D2D network and secure NB-IoT D2D network. However, there is no significant delay time in the second situation.

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed an unconditional quantum-resistant cryptography for the IoT/IoMT based on location-based lattices in the pre- and postquantum world. We compare the proposed cryptosystem and some related schemes. Threat modeling is employed to prove the robustness of the proposed cryptosystem. Additionally, our simulation results compare an insecure NB-IoT network (without any security consideration) and a secure NB-IoT network (via the proposed cryptosystem). These results prove that the proposed cryptography improves IoT security without compromising its performance features, including the energy consumption of advanced and normal nodes, time consumption at the BS, stability period, throughput and elapsed time for the whole network in the presence of cybersecurity computational costs and transmission costs. This expresses an optimized trade-off between security and performance. In the future, we will implement the proposed cryptosystem in the real world using real embedded devices and wireless network hardware (5G infrastructure) to examine its actual productivity and performance.

ACKNOWLEDGMENT

The first author would like to thank Taif University and the Royal Embassy of Saudi Arabia Cultural Bureau for sponsoring her Ph.D. study.ACKNOWLEDGMENT The first author would like to thank Taif University and the Royal Embassy of Saudi Arabia Cultural Bureau for sponsoring her Ph.D. study.

REFERENCES

[1] Statista. (Accessed: Mar. 23, 2020). *IoT: Number of Connected Devices Worldwide 2015-2025*. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[3] Z. Liu, K.-K. R. Choo, and J. Großschädl, "Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 158–162, Feb. 2018.

[4] R. Xu, C. Cheng, Y. Qin, and T. Jiang, "Lighting the way to a smart world: Lattice-based cryptography for Internet of Things," 2018, *arXiv:1805.04880*. [Online]. Available: http://arxiv.org/abs/1805.04880

[5] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position based cryptography," in *Proc. Annu. Int. Cryptol. Conf., Adv. Cryptol. (CRYPTO)*. Berlin, Germany: Springer, 2009, pp. 391–407.

[6] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions," *SIAM J. Comput.*, vol. 43, no. 1, pp. 150–178, 2014.

[7] G. Avoine, M. A. Bingöl, I. Boureanu, S. Čapkun, G. Hancke, S. Kardaş, C. H. Kim, C. Lauradoux, B. Martin, J. Munilla, and A. Peinado, "Security of distance-bounding: A survey," *ACM Comput. Surveys*, vol. 51, no. 5, pp. 1–33, 2018.

[8] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, "Practical and provably secure distance-bounding," *J. Comput. Secur.*, vol. 23, no. 2, pp. 229–257, Jun. 2015.

[9] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," in *Proc. ACM Workshop Wireless Secur. (WiSe)*, 2004, pp. 21–30.

[10] T. Park and K. G. Shin, "Attack-tolerant localization via iterative verification of locations in sensor networks," *ACM Trans. Embedded Comput. Syst.*, vol. 8, no. 1, pp. 1–24, Dec. 2008.

[11] Y. Zengm, J. Cao, J. Hong, S. Zhang, and L. Xie, "Secure localization and location verification in wireless sensor networks: A survey," *J. Supercomput.*, vol. 64, no. 3, pp. 685–701, 2013.

[12] P. Perazzo, L. Taponecco, A. A. D'amico, and G. Dini, "Secure positioning in wireless sensor networks through enlargement miscontrol detection," *ACM Trans. Sensor Netw.*, vol. 12, no. 4, pp. 1–32, Nov. 2016.

[13] M. Fogue, F. J. Martinez, P. Garrido, M. Fiore, C.-F. Chiasserini, C. Casetti, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Securing warning message dissemination in VANETs using cooperative neighbor position verification," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2538–2550, Jun. 2014.

[14] M. Fiore, C. E. Casetti, C. Chiasserini, and P. Papadimitratos, "Discovery and verification of neighbor positions in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 289–303, Feb. 2011.

[15] (Accessed: Jul. 27, 2020). *NRW Stops Corona Emergency Aid After Suspected Fraud*. [Online]. Available: https://www.handelsblatt.com/politik/deutschland/corona-hilfen-nrw-stoppt-corona-soforthilfe-nach-betrugsverdacht-in-tausenden-faellen/25731238.html

[16] *Why Covid-19 is a Gift for Cyber Criminals*, Financial Times, London, U.K., Jul. 15, 2020.

[17] *Narrowband-IoT: Pushing the Boundaries of IoT*, Vodafone, Berkshire, U.K., 2017. [Online]. Available: http://www.Vodafone.com/iot/nb-iot

[18] A. G. Sulaiman and I. F. Al Shaikhli, "Comparative study on 4G/LTE cryptographic algorithms based on different factors," *Int. J. Comput. Sci. Telecommun.*, vol. 5, no. 7, pp. 7–10, 2014.

[19] Global Mobile Suppliers Association. (Accessed: May 7, 2020). *Lte Subscriptions 2q-2017*. GSA Chart Report. Accessed: 2017. [Online]. Available: https://gsacom.com/paper/lte-subscriptions-2q-2017/

[20] A. N. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *IEEE Secur. Privacy*, vol. 11, no. 2, pp. 55–62, Mar. 2012.

[21] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, pp. 1–14, Dec. 2014.

[22] M. Labib, V. Marojevic, and J. H. Reed, "Analyzing and enhancing the resilience of LTE/LTE—A systems to RF spoofing," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2015, pp. 315–320.

[23] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position-based cryptography," *SIAM J. Comput.*, vol. 43, no. 4, pp. 1291–1341, Jan. 2014.

[24] N. Chandran, *Theoretical Foundations of Position-Based Cryptography*. Los Angeles, CA, USA: Univ. of California at Los Angeles, 2011.

[25] A. Shahmansoori, G. E. Garcia, G. Destino, G. Seco-Granados, and H. Wymeersch, "Position and orientation estimation through millimeter-wave MIMO in 5G systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1822–1835, Mar. 2017.

[26] R. D. Taranto, S. Muppirisetty, R. Raulefs, D. Slock, T. Svensson, and H. Wymeersch, "Location-aware communications for 5G networks," *IEEE Signal Process. Mag.*, vol. 31, no. 6, pp. 102–112, Oct. 2014.

[27] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, "5G mmWave positioning for vehicular networks," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 80–86, Dec. 2017.

[28] M. M. R. Akand and R. Safavi-Naini, "POSTER: Privacy enhanced secure location verification," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1793–1795.

[29] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *Secur. Commun. Netw.*, vol. 3, no. 4, pp. 289–302, Jul./Aug. 2010.

[30] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Secure location verification for vehicular ad-hoc networks," in *Proc. IEEE Global Telecommun. Conf. (IEEE GLOBECOM)*, Dec. 2008, pp. 1–5.

[31] P. Perazzo, F. B. Sorbelli, M. Conti, G. Dini, and C. M. Pinotti, "Drone path planning for secure positioning and secure position verification," *IEEE Trans. Mobile Comput.*, vol. 16, no. 9, pp. 2478–2493, Sep. 2016.

[32] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Des. Codes Cryptogr.*, vol. 78, no. 1, pp. 351–382, 2016.

[33] S. Čapkun, K. B. Rasmussen, M. Čagalj, and M. Srivastava, "Secure location verification with hidden and mobile base stations," *IEEE Trans. Mobile Comput.*, vol. 7, no. 4, pp. 470–483, Apr. 2008.

[34] S. Čapkun, M. Čagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," in *Proc. 25TH IEEE Int. Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2006, pp. 1–10.

[35] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *IEEE Trans. Dependable Secure Comput.*, vol. 5, no. 4, pp. 208–223, Oct. 2008.

[36] J. T. Chiang, J. J. Haas, and Y.-C. Hu, "Secure and precise location verification using distance bounding and simultaneous multilateration," in *Proc. 2nd ACM Conf. Wireless Netw. Secur. (WiSec)*, 2009, pp. 181–192.

[37] F. Speelman, "Position-based quantum cryptography and the garden-hose game," 2012, *arXiv:1210.4353*. [Online]. Available: http://arxiv.org/abs/1210.4353

[38] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 799–806, Jan. 2018.

[39] H. Zhang, Z. Zhang, and Z. Cao, "Position-verification in multi-channel models," *IACR Cryptol. ePrint Arch.*, vol. 2011, p. 714, 2011. [Online]. Available: https://eprint.iacr.org/2011/714.pdf

[40] J. Brody, S. Dziembowski, S. Faust, and K. Pietrzak, "Position-based cryptography and multiparty communication complexity," in *Proc. Theory Cryptogr. Conf.* Cham, Switzerland: Springer, 2017, pp. 56–81.

[41] Q. Xue, F. Li, H. Chen, H. Zhang, and Z. Cao, "Multi-proxy multi-signature binding positioning protocol," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3868–3879, Nov. 2016.

[42] S. Dziembowski and M. Zdanowicz, "Position-based cryptography from noisy channels," in *Proc. Int. Conf. Cryptol. Afr.* Cham, Switzerland: Springer, 2014, pp. 300–317.

[43] A. Kent, W. Munro, T. Spiller, and R. Beausoleil, "Tagging systems, 2006," US Patent 2006 00 22 832, 2006.

[44] A. Kent, W. J. Munro, and T. P. Spiller, "Quantum tagging: Authenticating location via quantum information and relativistic signalling constraints," 2010, *arXiv:1008.2147*. [Online]. Available: http://arxiv.org/abs/1008.2147

[45] A. Kent, W. J. Munro, and T. P. Spiller, "Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 1, Jul. 2011, Art. no. 012326.

[46] D. Unruh, "Quantum position verification in the random oracle model," in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2014, pp. 1–18.

[47] R. A. Malaney, "Location-dependent communications using quantum entanglement," *Phys. Rev. A, Gen. Phys.*, vol. 81, no. 4, Apr. 2010, Art. no. 042319.

[48] W. Wu, X. Wen, H. Xu, L. Yuan, and Q. Meng, "Accurate range-free localization based on quantum particle swarm optimization in heterogeneous wireless sensor networks," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 3, pp. 1083–1097, 2018.

[49] P. Bilski and W. Winiecki, "Analysis of the position-based quantum cryptography usage in the distributed measurement system," *Measurement*, vol. 46, no. 10, pp. 4353–4361, Dec. 2013.

[50] F. Gao, B. Liu, and Q. Wen, "Quantum position verification in bounded-attack-frequency model," *Sci. China Phys., Mech. Astron.*, vol. 59, no. 11, pp. 1–11, Nov. 2016.

[51] H.-K. Lau and H.-K. Lo, "Insecurity of position-based quantum-cryptography protocols against entanglement attacks," *Phys. Rev. A, Gen. Phys.*, vol. 83, no. 1, Jan. 2011, Art. no. 012322.

[52] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Eavesdropping and countermeasures for backflash side channel in quantum cryptography," *Opt. Exp.*, vol. 26, no. 16, pp. 21020–21032, 2018.

[53] M. Curty, K. Tamaki, F. Xu, A. Mizutani, C. C. W. Lim, B. Qi, and H.-K. Lo, "Bridging the gap between theory and practice in quantum cryptography," in *Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology*, vol. 9648. Bellingham, WA, USA: SPIE, 2015, Art. no. 96480X.

[54] R. Asif and W. J. Buchanan, "Quantum-to-the-home: Achieving Gbits/s secure key rates via commercial off-the-shelf telecommunication equipment," *Secur. Commun. Netw.*, vol. 2017, pp. 1–10, Jan. 2017.

[55] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the Internet of Things in a post-quantum world," *IEEE Access*, vol. 8, pp. 157356–157381, 2020.

[56] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky, "Position-based quantum cryptography," 2010, *arXiv:1005.1750*. [Online]. Available: http://arxiv.org/abs/1005.1750

[57] X. Zheng, R. Safavi-Naini, and H. Ahmadi, "Distance lower bounding," in *Proc. Int. Conf. Inf. Commun. Secur.* Cham, Switzerland: Springer, 2014, pp. 89–104.

[58] L. Gui, M. Yang, H. Yu, J. Li, F. Shu, and F. Xiao, "A Cramer–Rao lower bound of CSI-based indoor localization," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2814–2818, Mar. 2017.

[59] X. Liu, J. Yin, S. Zhang, B. Ding, S. Guo, and K. Wang, "Range-based localization for sparse 3-D sensor networks," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 753–764, Feb. 2018.

[60] Y. Wang and J. P. Hespanha, "Distributed estimation of power system oscillation modes under attacks on GPS clocks," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 7, pp. 1626–1637, Jul. 2018.

[61] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of synchrophasor-based WAMPAC Applications' to time synchronization spoofing," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4601–4612, Sep. 2017.

[62] L. D. A. Faria, C. A. D. M. Silvestre, M. A. F. Correia, and N. A. Roso, "Susceptibility of GPS-dependent complex systems to spoofing," *J. Aerosp. Technol. Manage.*, vol. 10, pp. 1–11, Jan. 2018.

[63] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, "Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing," *ACM Trans. Privacy Secur.*, vol. 22, no. 2, pp. 1–26, Apr. 2019.

[64] S. Li. (Accessed: Jun. 19, 2021). *Tdoa Acoustic Localization*. Accessed: 2011. [Online]. Available: https://github.com/StevenJL/tdoa_localization

[65] M. Bshara, U. Orguner, F. Gustafsson, and L. Van Biesen, "Fingerprinting localization in wireless networks based on received-signal-strength measurements: A case study on WiMAX networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 283–294, Jan. 2009.

[66] G. Mao and B. Fidan, "Introduction to wireless sensor network localization," in *Localization Algorithms and Strategies for Wireless Sensor Networks: Monitoring and Surveillance Techniques for Target Tracking*. Hershey, PA, USA: IGI Global, 2009, pp. 1–32.

[67] R. Jarvis, A. Mason, K. Thornhill, and B. Zhang, "Indoor positioning system," Dept. Electr. Comput., Tech. Rep. EE 4820, 2011.

[68] V. Daiya, J. Ebenezer, S. S. Murty, and B. Raj, "Experimental analysis of RSSI for distance and position estimation," in *Proc. Int. Conf. Recent Trends Inf. Technol. (ICRTIT)*, Jun. 2011, pp. 1093–1098.

[69] Q. Dong and W. Dargie, "Evaluation of the reliability of RSSI for indoor localization," in *Proc. Int. Conf. Wireless Commun. Underground Confined Areas*, Aug. 2012, pp. 1–6.

[70] P. A. Kowalski and S. Łukasik, "Experimental study of selected parameters of the krill herd algorithm," in *Intelligent Systems*. Cham, Switzerland: Springer, 2015, pp. 473–485.

[71] S. Cheng, H. Lu, X. Lei, and Y. Shi, "A quarter century of particle swarm optimization," *Complex Intell. Syst.*, vol. 4, no. 3, pp. 227–239, Oct. 2018.

[72] A. Singh, A. Kumar, A. Kumar, and V. Dwivedi, "Radio frequency global positioning system for real-time vehicle parking," in *Proc. Int. Conf. Signal Process. Commun. (ICSC)*, Dec. 2016, pp. 479–483.

[73] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. London, U.K.: Pearson, 2010.

[74] H. Nurminen, L. Suomalainen, S. Ali-Loytty, and R. Piche, "3D angle-of-arrival positioning using von mises-Fisher distribution," in *Proc. 21st Int. Conf. Inf. Fusion (FUSION)*, Jul. 2018, pp. 2036–2041.

[75] D. W. Lim, S. Lim, S. Chun, and M. B. Heo, "Considerations for design and implementation of a RF emitter localization system with array antennas," *J. Positioning, Navigat., Timing*, vol. 5, no. 1, pp. 37–45, Mar. 2016.

[76] Y. T. Chan, F. Chan, W. Read, B. R. Jackson, and B. H. Lee, "Hybrid localization of an emitter by combining angle-of-arrival and received signal strength measurements," in *Proc. IEEE 27th Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2014, pp. 1–5.

[77] K. Muthukrishnan and M. Hazas, "Position estimation from UWB pseudorange and angle-of-arrival: A comparison of non-linear regression and Kalman filtering," in *Proc. Int. Symp. Context-Awareness*. Berlin, Germany: Springer, 2009, pp. 222–239.

[78] H.-J. Du and J. P. Lee, "Simulation of multi-platform geolocation using a hybrid TDOA/AOA method," Defence R&D Canada, Ottawa, ON, Canada, Ottawa Tech. Memorandum DRDC Ottawa TM 2004-256, Dec. 2004.

[79] C. Chen, J. Hoffstein, W. Whyte, and Z. Zhang. (2018). *NIST PQ Submission: NTRUEncrypt A lattice based encryption algorithm, NIST Post-Quantum Cryptography Standardization: Round 1 Submissions*. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissions

[80] F. Bergami, "Lattice-based cryptography," Ph.D. dissertation, Universita di Padova, Padua, Italy, Jul. 2016.

[81] Y. Yuan, C.-M. Cheng, S. Kiyomoto, Y. Miyake, and T. Takagi, "Portable implementation of lattice-based cryptography using Javascript," *Int. J. Netw. Comput.*, vol. 6, no. 2, pp. 309–327, 2016.

[82] K. Ahmad, M. Doja, N. I. Udzir, and M. P. Singh, *Emerging security Algorithms and Techniques*. Boca Raton, FL, USA: CRC Press, 2019.

[83] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Proc. Int. Algorithmic Number Theory Symp.* Berlin, Germany: Springer, 1998, pp. 267–288.

[84] Mtholyoke.edu. (Accessed: May 23, 2021). *MATLAB Programs for P-ADICS*. [Online]. Available: https://www.mtholyoke.edu/courses/mpeterso/math251/padic/index.html

[85] T. Cleveland, *Number Theory*. U.K.: Scientific e-Resources, 2018.

[86] M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in *Proc. Annu. Conf. New Trends Inf. Commun. Technol. Appl. (NTICT)*, Mar. 2017, pp. 86–90.

[87] A. Dadheech, "Preventing information leakage from encoded data in lattice based cryptography," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 1952–1955.

[88] H. Kefas. (Accessed: Jun. 2, 2021). *Pixel Shuffling and Inverse Shuffling—MATLAB Answers—MATLAB Central*. Accessed: 2018. [Online]. Available: https://uk.mathworks.com/matlabcentral/answers/323409-pixel-shuffling-and-inverse-shuffling#answer_319011

[89] S. Li and P. Shang, "Analysis of nonlinear time series using discrete generalized past entropy based on amplitude difference distribution of horizontal visibility graph," *Chaos, Solitons Fractals*, vol. 144, Mar. 2021, Art. no. 110687.

[90] S. S. Askar, A. A. Karawia, and F. S. Alammar, "Cryptographic algorithm based on pixel shuffling and dynamical chaotic economic map," *IET Image Process.*, vol. 12, no. 1, pp. 158–167, Jan. 2018.

[91] M. Dichtl, "Cryptographic shuffling of random and pseudorandom sequences," in *Proc. Dagstuhl Seminar*. Wadern, Germany: Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2007.

[92] M. Madelaire. (Accessed: Aug. 7, 2020). *How to Generate Points in Triangular Lattice Pattern*. Accessed: 2019. [Online]. Available: https://uk.mathworks.com/matlabcentral/answers/474193-how-to-generate-points-in-triangular-lattice-pattern#answer_385556

[93] O. S. Althobaiti and M. Dohler, "Narrowband-Internet of Things device-to-device simulation: An open-sourced framework," *Sensors*, vol. 21, no. 5, p. 1824, Mar. 2021.

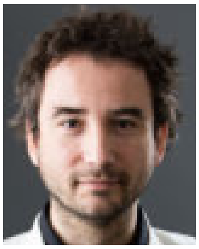
[94] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Secur. J.*, vol. 25, no. 2, pp. 19–27, 2003.

[95] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. 18th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, 2005, pp. 1285–1290.

[96] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Division The Inst. Navigat. (ION GNSS)*, 2008, pp. 2314–2325.

[97] F. A. Aderohunmu, "Energy management techniques in wireless sensor networks: Protocol design and evaluation," Ph.D. dissertation, Dept. Inf. Sci., Univ. Otago, Dunedin, New Zealand, 2010.

OHOOD SAUD ALTHOBAITI (Graduate Student Member, IEEE) received the master's degree (Hons.) in computer science from the College of Computer and Information Sciences, King Saud University, Saudi Arabia, in 2012. She is currently pursuing the Ph.D. degree with the Centre for Telecommunications Research, Department of Engineering, King's College London, London, U.K. She is a Lecturer with the Computer Science Department, College of Computers and Information Technology, Taif University, Saudi Arabia. She has peer-reviewed published articles. Her research interests include cybersecurity, quantum computing, computer networks, pattern recognition, and artificial intelligence (AI), with special focuses on security in the Internet of Things (IoT). She was awarded the Reward Scientific Publishing in ISI journals, the First-Class Honor Award from Taif University, in 2008, and the Scholarship for her Ph.D. degree.



MISCHA DOHLER (Fellow, IEEE) was the Director of the Centre for Telecommunications Research, King's College London, from 2014 to 2018. He worked as a Senior Researcher at Orange/France Telecom, from 2005 to 2008. He is the Co-Founder of the Smart Cities pioneering company Worldsensing, where he was the CTO, from 2008 to 2014. He is currently a Full Professor in wireless communications at King's College London, driving cross-disciplinary research and innovation in technology, sciences, and arts. He is a Serial Entrepreneur, a Composer, and a Pianist with five albums on Spotify/iTunes. He is fluent in six languages. He acts as a Policy Advisor on issues related to digital, skills, and education. He has had ample coverage by national and international press and media. He is a frequent keynote, panel, and tutorial speaker. He has more than 300 highly cited publications and authored several books. He holds a dozen patents, organized, and chaired numerous conferences. He has pioneered several research fields, contributed to numerous wireless broadband, the IoT/M2M, and cyber security standards. He is a fellow the Royal Academy of Engineering, the Royal Society of Arts (RSA), and the Institution of Engineering and Technology (IET); and a Distinguished Member of Harvard Square Leaders Excellence. He has received numerous awards. He was the Editor-in-Chief of two journals.