BLOCK QUANTUM COMPUTING FOR SECURE SATELLITE COMMUNICATION

[1]Mrs.N.Suriyapriya, [2]B. Amritha, [3]S. Lavanya, [4]N. Nivetha
[1]A.P, [1,2,3,4]Dept.of :Information Technology
Vivekanandha College Of Technology for Women
Namakkal, India
[1]me.suriyapriya@gmail.com, [2]amrithasusila@gmail.com, [3]slavanya170302@gmail.com, [4]niveeit2019@gmail.com

Abstract— Satellite communication networks have gained a lot of attention recently as a solution to mitigate the limitations of terrestrial networks such as stability and coverage. Due to satellite physical constraints in terms of available power and area, data processing capacity is low, storage and security are limited such that the data may be vulnerable to tampering or contamination by attackers. Since satellite communication has been more and more important in developing global communication networks, there have been concerns about the security in satellite communication. It is a challenge to protect satellite network from illegal information access and use storage space effectively. The integration of satellite systems with smart computing and networking technologies, such as Block chain and Quantum Computing, has intensely augmented sophisticated cyber attacks against satellite environments. In this project, a Block chain technology and Quantum Key Distribution QKD protocol based on authentication and privacy protection scheme is proposed for a satellite communication network. To this aim, an architecture consisting of both conventional and restricted devices connected to the Block chain via a wireless heterogeneous network is deployed, Secure communications by introducing the variant of pre-quantum RSA called lattice-based RSA generates quantum key pool (QKP) to relay keys for ground stations device and satellites. The communication is carried out through registration, authentication and revocation. In this scheme, the satellite will forward the collected information to the ground base station, which will record all key parameters on the distributed Block chain and all malicious node certificates will be cleared from the Block chain by the ground base station. The proposed satellite-based Block chain and Quantum Key Distribution system provides high security level for the coming 6G and beyond networks, the Internet of things, self-driving cars, and other fast developing applications.

I. INTRODUCTION

A satellite is a body that orbits around another body in space. There are two different types of satellites –natural and man-made.

fig 1 satellite

A. *SatelliteCommunication*

Satellite communication is the method of transporting in formation from one place to another using a communication satellite in orbit around the Earth. A communication satellite is an artificial satellite that transmits the signal via a transponder by creating a channel between the transmitter and the receiver located at different

DOI: 10.21276/ijcesr.2023.10.4.3

locations on the Earth. Telephone, radio, television, internet, and military applications use satellite communications.

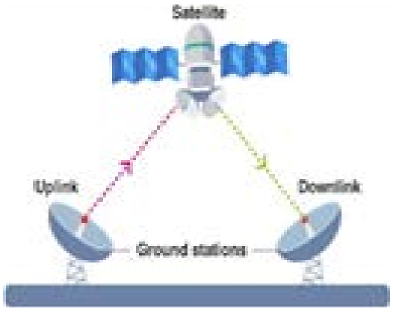


fig 2 satellite communication

Satellite orbits

In general, orbit is described as a pathway, which one space body makes around the other space body, because they are both influenced by gravity and centripetal force. often categorized into the following classes:

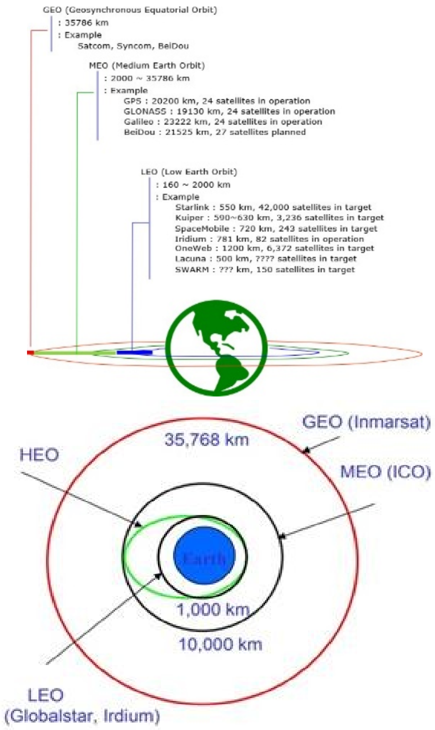

GEO (Geosynchronous Equatorial Orbit)
: 35786 km
: Example
Satcom, Syncom, BeiDou
MEO (Medium Earth Orbit)
: 2000 ~ 35786 km
: Example
GPS : 20200 km, 24 satellites in operation
GLONASS : 19130 km, 24 satellites in operation
Galileo : 23222 km, 24 satellites in operation
BeiDou : 21525 km, 27 satellites planned
LEO (Low Earth Orbit)
: 160 ~ 2000 km
: Example
Starlink : 550 km, 42,000 satellites in target
Kuiper : 590~630 km, 3,236 satellites in target
SpaceMobile : 720 km, 243 satellites in target
Iridium : 781 km, 82 satellites in operation
OneWeb : 1200 km, 6,372 satellites in target
Lacuna : 500 km, ???? satellites in target
SWARM : ??? km, 150 satellites in target
GEO (Inmarsat)
35,768 km
HEO
MEO (ICO)
Earth
1,000 km
10,000 km
LEO
(Globalstar, Irdium)

Fig 3 Satellite orbits

Low Earth Orbit (LEO)

LEO finds its place from 200 km to 1200 km height above the earth. The advantage of this orbit is the shorter signal traveling time and lower possibility to lose its path. On the other hand, the coverage zone is quite small (in comparison with GEO) and the connection to satellite from ground station time is shorter, because the satellite moves quicker as the earthnis turning.

Medium Earth Orbit (MEO)

MEO is located between 1200 km and 35286 km altitude above earth surface. Some literature sources indicate that the Medium Earth Orbit is located between 5000 km and 13000 km height or between two Van Allen belts [Walke00]. Van Allen belts are two high intensity radiation zones of the earth,

II. where highly charged particles and high energy neutrons take place.

GEOSTATIONARY ORBIT (GEO)

GEO is placed 35786 km above Earth&#39;s surface. The orbit is called geostationary orbit, because satellites’, placed in this orbit, speed is matched with earth turning speed so that the satellite moves always together with the earth. In other words, to say, if the one would be able to see the satellite from the earth, the satellite would always stay in the same point of the space from the earth perspective. Most of the communication satellites are place in GEO.

C. Satellite Applications

The applications of satellite communication systems include the following.

1 Military
2 Navigations
3 Amateur Radio
4 TV broadcasting like DTH (Direct to Home)
5 Radio Broadcasting
6 Remote sensing applications

D. Cryptography

Cryptography provides for secure communication in the presence of malicious third-parties—known as adversaries.

Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., cipher text). A given algorithm will always transform the same plaintext into the same cipher text if the same key is used. Algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the cipher text. An attacker should not be able to determine anything about a key given a large number of plaintext/ciphertext combinations which used the key.

TYPES OF CRYPTOGRAPHY

Cryptography can be broken down into three different types:

1. Secret Key Cryptography
2. Public Key Cryptography
3. Hash Functions

QUANTUM CRYPTOGRAPHY

Quantum cryptography is a science that applies quantum mechanics principles to data encryption and data transmission so that data cannot be accessed by hackers – even by those malicious actors that have quantum computing of their own.

The broader application of quantum cryptography also includes the creation and execution of various cryptographic tasks using the unique capabilities and power of quantum computers. Theoretically, this type of computer can aid the development of new, stronger, more efficient encryption systems that are impossible using existing, traditional computing and communication architectures.

BLOCKCHAIN TECHNOLOGY

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger. 'Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.

KEY ELEMENTS OF A BLOCKCHAIN

DISTRIBUTED LEDGER TECHNOLOGY

All network participants have access to the distributed ledger and its immutable record of transactions.

With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

Smart contracts

To speed transactions, a set of rules called a smart contract is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

II RELATED WORKS

A. Eavesdropping Detection in
BB84 Quantum Key
Distribution Protocols

Author: Chankyun Lee; Ilkwon
Sohn
Year:2022
Doi:10.1109/TNSM.2022.3165
02

PROBLEM IDENTIFIED

The nature of quantum mechanics provides us with an opportunity to statistically detect eavesdropping in quantum key distribution (QKD) protocols, which is unimaginable in classical digital communications..

PAPER OBJECTIVE

By utilizing Hoeffding's inequality, this study analyses the upper bounds of the falsepositive ratio (FPR) and false-negative ratio (FNR) of eavesdropping detection in the Bennett-Brassard-84 (BB84) QKD protocol, where eavesdropping is detected if the measured quantum bit error rate (QBER) is equal to or higher than a threshold.

METHODOLOGY

Proposed a simple eavesdropping detection algorithm that is highly compatible with the classical BB84 protocol. The algorithm judges the intercept-and- resend-attack from Eve by comparing the QBER and θ QBER . By exploring Hoeffding's inequality, we indicate the presence of a trade-off between the accuracy of eaves dropping detection and the economy of quantum resources. The upper bounds of the FPR and FNR of eavesdropping detection in the proposed algorithm exponentially decrease with respect to the increase in K

FINDINGS

In this study, the author developed simplified models and assumptions to provide straightforward analysis and intuition.

Moreover, this study does not consider intercept and-resend- attack to a part of qubits between Alice and Bob. The Intercept-and-resend- attack to a part of qubits can degrade the eavesdropping detection performance of the proposed protocol and algorithm, by lowering QBER with the presence of Eve.

B. ANALYSIS OF THE NTRU POST-QUANTUM CRYPTOGRAPHIC

SCHEME IN CONSTRAINED IOT EDGE DEVICES

Author: Jaime Señor; Jorge Portilla
Year:2022
Doi:10.1109/JIOT.2022.3162254

PROBLEM IDENTIFIED

Research on post-quantum cryptography aims to solve the problematic of modern public-key cryptography being broken by attacks coming from quantum computers in the future and, moreover, by using classical electronics. This task is so critical that the National Institute of Standards and Technology is in the final process of standardizing post-quantum schemes for the future protection of embedded applications. Though there are some research works done on embedded systems, it is important to study the impact of these proposals in realistic environments for the Internet of

PAPER OBJECTIVE

In this work, the performance of one of the finalists of the standardization process called NTRU is studied and implemented in a custom wireless sensor node designed for applications in the extreme edge of the Internet of Things.

METHODOLOGY

The cryptosystem is implemented and evaluated within the processes of the Contiki-NG operating system. Furthermore, additional experiments are performed to check if commonly integrated hardware peripherals for cryptography inside modern microcontrollers can be used to achieve better performance with

NTRU, not only at single node level but also at network level, where the NTRU key encapsulation mechanism is tested in a real communication process.

FINDINGS

The results derived from these experiments show that NTRU is suitable for modern microcontrollers targeting wireless sensor networks design, while old devices present in popular platforms might not afford the cost of its implementation.

C. RELIABILITY AND SECURITY ANALYSIS OF AN ENTANGLEMENT BASED QKD PROTOCOL IN A DYNAMIC GROUND-TO-UAV FSO COMMUNICATIONS SYSTEM AUTHOR:TAWFIK ISMAIL

Year:2021

Doi:10.1109/ACCESS.2021.3137357

PROBLEM IDENTIFIED

Quantum cryptography is a promising technology that achieves unconditional security, which is essential to a wide range of sensitive applications. In contrast to optical fibres, the free-space optical (FSO) link is efficiently used as a quantum channel without affecting the polarization of transmitted photons. However, the FSO link has several impairments, such as atmospheric turbulence and pointing errors, which affect the performance of the quantum channel.

PAPER OBJECTIVE

This paper proposes a quantum key distribution (QKD) scheme that uses a time-bin entanglement protocol over the FSO channel that suffers from various channel impairments.

Due to the interest in unmanned aerial vehicles (UAVs) and their usefulness for many social, internet-of-things (IoT), civil, and military applications, the proposed QKD- FSO system is integrated with the ground-to-UAV platform.

METHODOLOGY

This work proposes an FSO system from Earth to UAV to satisfy on-demand services while achieving security requirements using the E91-QKD protocol.(1) develop an automatic correction-tracking system that minimizes the error- variance of tracking system between mobile UAV and fixed ground station; (2) introduce a QKD system over an optical free space channel applying time-bin with EBP considering a variety of channel impairments; (3)propose closed-form expressions of average- symbol error rate (ASER) and outage probability for UAV-based FSO communication link considering misalignment due to tracking errors and non-zero boresight pointing errors; (4) obtain expressions of raw-key and secret-key rates to perform the security analysis and capacity of the QKD system;

FINDINGS

The derived expressions and analytical results in this paper will help design and optimize such integrated systems. This study might further be extended to include the implementation of different QKD protocols, the Malaga distribution, which can be used as a general statistical model, and fine-tracking techniques.

D. MACHINE LEARNING TECHNIQUES FOR DETECTING ATTACKERS

DURING QUANTUM KEY DISTRIBUTION IN IOT NETWORKS WITH APPLICATION TO RAILWAY SCENARIOS

Author: Hasan Abbas Al-Mohammed

Year:2021

Doi:10.1109/ACCESS.2021.3117 405

PROBLEM IDENTIFIED

Internet of Things (IoT) deployments face significant security challenges due to the limited energy and computational power of IoT devices. These challenges are more serious in the quantum communications era, where certain attackers might have quantum computing capabilities, which renders IoT devices more vulnerable.

PAPER OBJECTIVE

This paper addresses the problem of IoT security by investigating quantum key distribution (QKD) in beyond 5G networks. An algorithm for detecting an attacker between a transmitter and receiver is proposed, with the side effect of interrupting the QKD process while detecting the attacker.

METHODOLOGY

Proposing an architecture for performing QKD in IoT networks, without affecting the computation and power consumption limitations of the IoT sensors. Describing the implementation of the proposed architecture in a railroad IoT scenario as a practical example. Designing a simple algorithm for detecting an attacker between a transmitter and receiver, without resorting to machine learning techniques, with the side effect of interrupting the QKD process while detecting the attacker.

FINDINGS

In addition, an implementation scenario for securing IoT communications for sensors deployed in railroad networks is described. The results show that the proposed ML techniques can reach 99% accuracy in detecting attackers..

E. A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications

Author: Iqra Mustafa

Year:2020

Doi:10.1109/ACCESS.2020.2995801

PROBLEM IDENTIFIED

Conventional RSA algorithm, being a basis for several proposed cryptosystems, has remarkable security laps with respect to confidentiality and integrity over the internet which can be compromised by state-of-the-art attacks, especially, fordifferent types of data generation, transmission, and analysis by IoT applications.

PAPER OBJECTIVE

In this research, the author proposes a post-quantum lattice-based RSA (LB-RSA) for IoT-based cloud applications to secure the shared data and information..

METHODOLOGY

The proposed LB-RSA algorithm has four subsystems: key generation, encryption, decryption, digital signing and verification. In lattice-based cryptography, key selection is not just strong but also hard to break. The private-key for these schemes is a lattice point while the public-key is an arbitrary location in space, which can be the nearest point.

FINDINGS

Moreover, the proposed LB-RSA technique is compared with the existing state-of-the-art techniques. The empirical results advocate that the proposed lattice-based variant is not only safe but beats counterparts in terms of secured data sharing.

III PROPOSED SYSTEM

There are essentially three types of orbits classified by the satellite altitude: geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO). Among them,

GEO satellites are stationary relative to the earth’s surface so that the doppler shift is negligible and has a lower transmission outage probability than non-GEO satellites. The

GEO satellites work at very high altitudes ($\approx$35,786 km) and can offer the most extensive coverage. Thanks to the low outage probability and wide coverage, GEO satellites are preferred in our proposed protocol.

Satellite communications systems enable the sending andreceiving of information worldwide, offering internet access, television, telephone, radio, and other civilian and military operations. The advent of HTS (high-throughput satellite) systems has greatly enhanced technical capabilities and offered wideband services at lower costs. Significant improvements are expected on the forthcoming mega-constellations in low Earth orbits that will deploy thousands of satellites, providing full earth coverage to minimize delays in addition to wide bandwidth. The use, given these characteristics, can increase efficiency in providing large sets of services and applications that are security-sensitive, such as telemedicine, banking, search and rescue, sensor networks, and content delivery network feed. However, in many cases, the security of satellite communication has been seriously compromised, resulting in covert dangers. In satellite communications (and even in terrestrial systems), hackers can interfere, intercept, or modify wireless network systems remotely, attack the equipment of flight crews, and control the positioning and transmission of satellite communication antennas. According to satellite communication protocols, the use of space in satellite communications can be developed independently to enhance communication security. Recommendations have been proposed to further increase the unity and compatibility of communication protocols for space. A single security mechanism is insufficient to meet the security requirements for satellite communication services. In this project, Quantum Key Cryptography and blockchain technology is introduced to analyse the security of satellite communication networks in terms of access control, confidentiality, and security authentication.

IV PROBLEMS IDENTIFIED

SAT COMs are particularly prone to eavesdropping due to the broadcast nature of the wireless medium and the very large coverage area..

A.TRAFFIC REDIRECTION ATTACK

The attacker may send a fake binding update message to the CN claiming that a node (victim) has changed its care-of address due to its movement to a new location. Consequently, the CN will start sending packets to the new CoA and the victim node will not get any traffic.

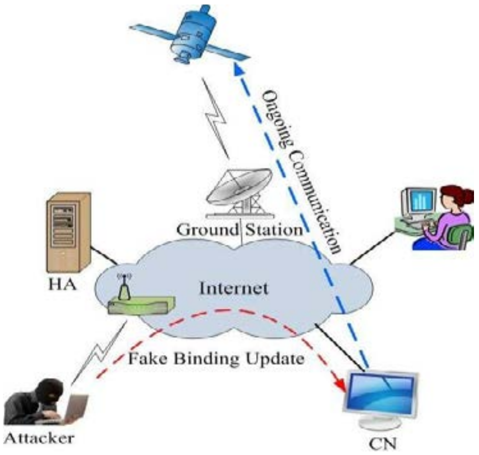


Fig. 4 Traffic redirection attack

The attacker sends fabricated BU to the CN to modify the binding cache for the MH (Satellite)to some fictitious IP address.

B. Man-in-the-middle attack

The attacker might send spoofed binding update message to the CN telling it to update the cache entry to its own(attacker's)IP address. Consequently, the CN will starts ending the packets to the attacker instead of the Satellite. The attacker may learn the confidential information of the message, may modify the packet before forwarding it to the Satellite. Thus, the attacker might act as a man-in-the-middle getting the all-important private data destined to the victim satellite (device)without the knowledge of the concerned parties

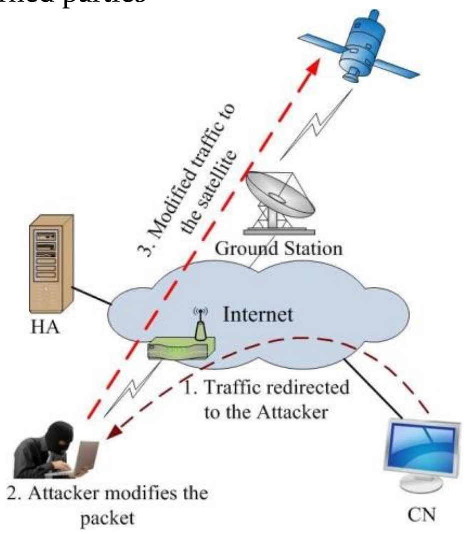
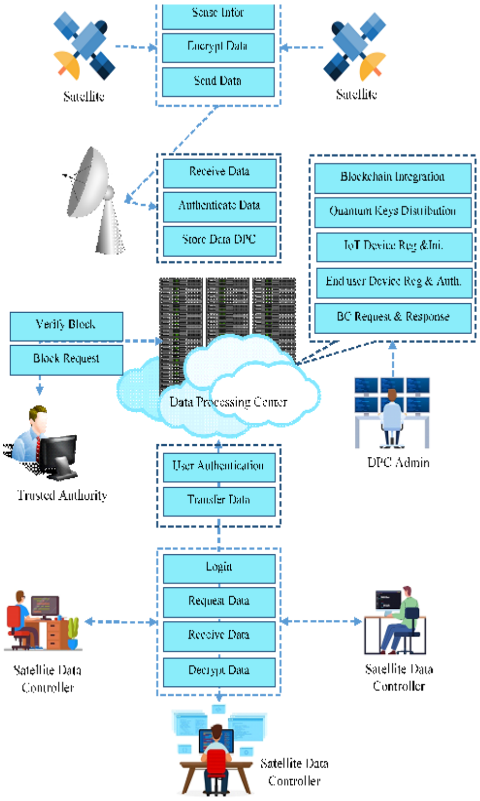

3. Modified traffic to the satellite
Ground Station
HA
Internet
1. Traffic redirected to the Attacker
2. Attacker modifies the packet
CN

Fig.5 Man-in-the-middleattack

V. SYSTEM ARCHITECTURE



VI ADVANTAGES

1. The ability to make secured communications with a satellite through an untrusted ground station.

2. The ability to have separate channels of communication while keeping as many points of contact to satellites as possible.
3. Immutable, non-repudiable, distributed record of commands and communications
4. Automation of satellite observations
5. Automatic routing of commands to any ground stations with line of sight to satellites
6. Downlink satellites data at any ground station and automatically distributed to all desired parties
7. Pass secured, encrypted data through unsecured ground stations

VII MODULES DESCRIPTION

A DATA PROCESSING CENTRE

The Satellite network system structure model in this project is composed of a Satellite, Ground Station, Data Processing Center, Satellite Controller or Operator through a lightweight wireless network connection.

Registration and Initialization Phase

Registration and initialization phases are critical for establishing a reliable and secure communication link between the user&#39;s terminal and the satellite network. These phases ensure that the user terminal is authorized and authenticated to access the satellite network, and that the satellite is properly configured for communication with the user terminal.

DEFAULT USERS

In satellite communication, the default user is typically a remote terminal or earth station that communicates with the satellite to exchange data or information with another remote terminal or earth station. The remote terminal can be a fixed installation or a mobile device that is designed to communicate with the satellite using specific frequencies, modulation schemes, and protocols.

CUSTOMIZED USERS

Customized users in satellite communication refer to the ability to provide tailored services and features to individual users based on their specific requirements. This can include customizing the bandwidth, data rate, coverage area, and other parameters to meet the specific needs of a particular user or group of users.

B. Quantum Key Generation and Distribution

The process of using quantum communication to establish a shared key between two trusted parties so that an untrusted eavesdropper cannot learn anything about that key. Quantum key distribution utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology.

Quantum Key Generation: Internet key exchange version 2 (IKEv2) Internet Key Exchange (IKEv2) is a protocol used to establish keys and security associations (SAs) for the purpose of setting up a secure Satellite Network (SN) connection that protects data packets from being read or intercepted over a public Internet connection. This allows a remote computer on a public network to access resources and benefit from the security of a private closed network without compromising security. The IKE protocol standard is rigid and does not permit SN designers to choose beyond a small set of cryptographic algorithms.

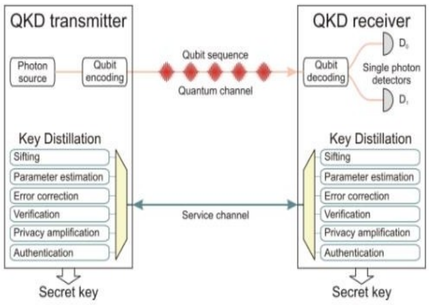


Fig. 6 Quantum Key Distribution

IKE also provides authenticated connections, using RSA, DSS or MAC with a pre-shared secret. While the MAC option with proper key and MAC tag length justification is quantum safe, RSA and DSS algorithms are not. Simply specifying the use of a MAC with pre-shared secret is not an adequate substitute for a public key-based algorithms because a large network with individual pre shared secrets for every connection does not scale well and quickly becomes a key management problem as the network grows. Pre-shared keys are also problematic in a large network because, if a global key is being used it is very hard to keep such a global key a secret, representing a vulnerability with a single point of failure.

Internet Protocol Security (IPSec) encryption has been the standard used to secure data any time it moves between two or more classical computers and/or networks over the internet.

Internet Key Exchange (IKE) is the protocol used to set up a security association in the IPSec protocol suite, and it comes in two flavours, IKEv1 and IKEv2.IKEv2 is based on the Diffie-Hellman (DH) exchange, created to allow two parties to jointly establish a shared secret cryptographic key over an insecure public channel. Today, all of the authentication methods that make IKEv2 possible can be broken by a large- scale quantum computer. Common methods for establishing authentication over IKEv2 include RSA and Elliptic Curve Digital Signature Algorithms (ECDSA).

C. SAT CHAIN

A consortium blockchain is introduced for sharing information among cooperative satellite constellations. In this section, a new concept, called Sat Chain, is proposed. Sat Chain's are a way to tokenize space transactions as digital tokens that can be processed using a blockchain protocol to authenticate space transactions. SDTs can be broadcast within a swarm of satellite networks called a satellite constellation.

Hence, blockchain can work in this scenario as an authenticator for all communication patterns that can occur within a specific satellite's constellation. Sat Chain's are used to process sensing data between satellites and DPC; hence, block chain can work in this scenario as a tracking system to detect expected space collisions between satellites and DPC

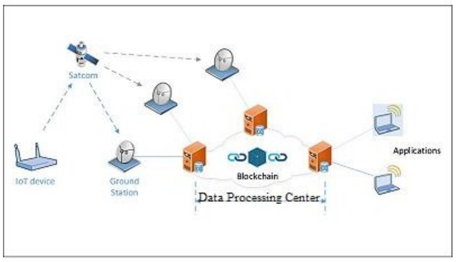


Fig. 7 Sat Chain

D. End User and Device Registration

End user registration involves collecting information about the user, such as their name, address, contact information, and credentials, to verify their identity and ensure that they are authorized to access the network. This information is usually stored in a database and used to authenticate the user each time they attempt to connect to the network.

Device registration involves registering the physical device that the user will be using to access the satellite network. This process involves collecting information about the device, such as its unique identifier, technical specifications, and software configurations, to ensure that it is compatible with the network and meets the necessary security requirements. This information is also stored in a database and used to verify the device identity and authenticate it each time it attempts to connect to the network.

VIII PERFORMANCE ANALYSIS

The performance analysis of block quantum computing for secure satellite communication involves evaluating the speed, efficiency, security, and scalability of the technology. As block quantum computing is still a relatively new concept, further research is required to fully understand its potential and limitations in the context of secure satellite communication.

IX FUTURE ENHANCEMENT

In the future, the blockchain-satellite system will depend on cloud constellations for managing data centers in orbit, where companies can upload their data and bypass ground networks this approach will help governments and companies obtain information from different sources and orbits in space20

X CONCLUSION

The satellite communication channel is different not only from the common mobile channel but also from the ground station channel. The satellite communication channel is the fusion of the satellite channel and the mobile communication channel. Satellite communication channels are extremely vulnerable to hackers and external interference signals.

Protecting satellite networks from illegal information access and use can be extremely challenging. In this project, Quantum Key Cryptography and blockchain technology is introduced to analyze the security of satellite communication networks in terms of access control, confidentiality, and security authentication. The proposed scheme is developed to solve the security problem of using a centralized database in satellite communication. The simulation results show that the proposed method was able to significantly improve security and protection for satellite communications.

XI REFERENCES

[1] S. Fu, J. Gao, and L. Zhao,``Integrated resource
management for terrestrial-satellite systems,&#39;&#39; IEEE
Trans Veh. Technol., vol. 69, no. 3, pp. 3256-3266,Mar. 2020.

[2] H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang,``Blockchain- based secure distributed control forsoftware defined optical networking,‘’ China Commun., vol. 16, no. 6, pp. 42- 54, Jun. 2019.

[3] C. Li, L. Zhu, Z. Luo, and Z. Zhang, ``Solutions to data reception with improve blind source separation in satellite.

[4] communications,‘’ in Proc. IEEE Int. Symp. Netw., Comput. Commun. (ISNCC), Montreal, QC, Canada, Oct. 2020, pp. 1-5.