IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 3, Ser. 2 (May. – June. 2024), PP 47-72
www.iosrjournals.org

Cryptographic Security Engineering For Secure Wireless Sensor Networks

Vaghani Divyeshkumar[1]

[1](*Gannon University, 109 University Square, Erie, Pa 16541, Usa)*

Abstract

Background: *The study present a cryptographic secure engineered intrusion prevention architecture for wireless sensor networks, aiming to extend the network's lifetime through lightweight, secure data routing amongst the network's mobile nodes. The objectives of the study are to; conduct a systematic review of security solutions to address potential attacks on wireless sensor networks; and to propose an algorithm that combines energy-aware routing and secure transmission using clustering along with cryptography.*

Materials and Method: *The model relies on cryptographic techniques like digital envelopes, digital signatures, and Public Key Infrastructure (PKI) to safeguard sensor networks against attacks. Encryption is employed to alter sensitive information so that only the intended recipient can decrypt it. Symmetric cryptography is utilized for secret key generation and message encryption, with the key safeguarded via asymmetric encryption and digital certificates from PKI. Digital envelope technology is employed to encrypt messages and private keys, ensuring that only the designated recipient can access the message content. The proposed framework comprises two main components: a secure data routing model and an initial network deployment with cluster management.*

Result: *This framework offers superior performance across various criteria compared to traditional networks.*

Conclusion: *With a new security codeword generated at each node, the proposed technique enhances secrecy between nodes and simplifies the identification of competing nodes within the network. Furthermore, the method streamlines underlying mathematics, thereby increasing Packet Delivery Ratio (PDR) by minimizing wait times.*

Keywords: *clustering, digital envelopes, digital signature, intrusion prevention, Public Key Infrastructure, secure data routing, secure transmission.*

Date Of Submission: 21-05-2024 Date Of Acceptance: 31-05-2024

I. Introduction

A wireless sensor network (WSN) is utilized for monitoring various parameters such as temperature, humidity, vibrations, seismic activities, and more. This network comprises sensor nodes dispersed across a geographic area, powered by an external energy source. Mobile nodes in wireless sensor networks (WSNs) are compact, cost-effective sensors with significant resource constraints. These nodes are deployed across study areas to collect and analyze various environmental data, including mechanical, thermal, biological, chemical, and optical readings. Applications of WSNs span environmental monitoring (e.g., atmosphere, soil, moisture), condition-based maintenance, ecosystem monitoring (e.g., tracking plant and animal populations), seismic detection, surveillance, inventory management, smart environments, data collection in uninhabitable areas, healthcare, home security, machinery diagnostics, and pollutant detection. Given that most sensors operate on batteries, considerable effort has been directed toward developing energy-efficient protocols, especially at the data link layer. The primary goal of these protocols is to enhance energy efficiency in network communications to extend the network's operational lifespan.

Sensor networks are composed of numerous densely distributed nodes, each with sensing and computing capabilities, connected wirelessly as depicted in Figure 1. These nodes are low-power, autonomous devices capable of environmental sensing, basic processing, and wireless communication. Sensor network data is diverse, with varying formats and standards, applicable in fields ranging from national security to healthcare

and environmental monitoring. Sensor networks enable researchers worldwide to access near real-time data, yet extracting and interpreting this data presents a significant challenge.

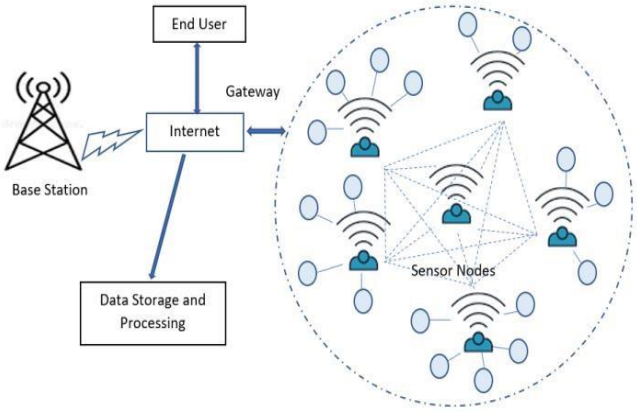


Fig. 1 Typical wireless sensor network structure

WSNs often operate autonomously and without supervision, leaving nodes susceptible to various attacks. Secure routing techniques[1,2,3,4] have been developed to mitigate these vulnerabilities, utilizing encryption and authentication. However, these methods may not effectively prevent malicious activities targeting individual nodes, as they assume all participating nodes are trustworthy. Contrary to this assumption, insider or node misbehavior attacks highlight the need for more robust security measures[5]. The limited memory, computing power, and resources of sensor nodes hinder the implementation of sophisticated security mechanisms.

Key challenges for WSNs include routing, adaptability to different data types, power consumption, fault tolerance, quality of service, accessibility, and security. Our objective is to ensure the secure and efficient delivery of data to the intended destination in WSNs, employing optimal data aggregation and routing to achieve high security levels[6,7]. The primary security concerns are data trustworthiness, integrity, authenticity, and availability. To secure data communication within the network, confidentiality and authenticity at each node are essential[8]. WSNs are vulnerable to attacks such as "Denial of Service (DoS)", "Sybil Assault", "Selective Forwarding", "Sinkhole attack", "Hello Flood assault", "Side-channel attack", "Brute Force attack", and "Node Capture attack"[9].

Most cryptographic methods demand substantial resources in terms of computation, memory, and energy, making them impractical for WSNs[10]. Additionally, many cryptography-based techniques require centralized security management, which is not feasible in WSNs[11]. Traditional security methods are ineffective in unattended environments where adversaries can easily access valid keys and memory contents[12]. Trust and reputation-based techniques, designed to protect WSNs, have shown greater resilience against node misbehavior attacks. Trust-based security[10] eliminates the need for cryptographic methods, representing a recent advancement in WSN security.

WSNs are constrained by limited computational power, energy, and memory resources. Clustering is a strategy to enhance energy efficiency in WSNs; with an appropriate cluster head selection, power consumption can be minimized, thereby extending network lifespan. Various techniques are used for cluster formation in WSNs, which can significantly improve the network's longevity.

Routing protocols identify optimal paths between nodes but do not select monitoring nodes in multi-path setups. To address this, we have developed hybrid networking and monitoring techniques to enhance protection across all channels. This approach combines routing properties with sensor monitoring levels, encrypting channels using a two-fish cryptographic system and unpredictable key shares, ensuring efficient data transmission among ad hoc sensor nodes despite numerous potential threats.

With advancements in internet-based multimedia processing technologies, data masking techniques for protecting 3D models have also evolved[13]. Data hiding techniques[14,15] can protect integrity and copyright by embedding secret data within original content. In scenarios requiring high data security, such as transmitting medical images or certifying legal documents, no alterations to the original data are permissible. Reversible data hiding (RDH) has been explored for such applications[16,17,18]. RDH techniques include difference expansion

(DE), histogram shifting (HS), and lossless compression (LC). DE techniques embed hidden data by increasing differences between adjacent pixels[13,19], while prediction error expansion (PEE) techniques enhance pixel value differences for data hiding[20]. HS-based RDH methods use a histogram of the original image to embed data, and LC-based techniques embed data in compressed regions.

While several methods for securing data transfer have been explored, encryption remains the most widely used and effective approach. Encryption "scrambles" data, rendering it unreadable to unauthorized individuals. It involves converting information into a form decipherable only by authorized parties with a decryption key. Data is called plaintext before encryption and ciphertext after encryption. Encryption protects confidential information during storage or transmission.

Advanced encryption algorithms are being developed to replace or enhance traditional encryption standards, playing a crucial role in data protection. These advanced tools offer features such as data integrity, authentication, and secure transmission, ensuring confidentiality. Authentication verifies the data provider, integrity ensures data is not altered, and non-repudiation prevents senders from denying their data transmission. Early encryption methods involved substituting letters in a sentence, making it unreadable, and time-consuming to decode. Only the recipient with the decryption key could read the message. As code-breaking techniques advanced, encryption methods became more sophisticated to maintain message privacy.

Encryption can be classified into Asymmetric and Symmetric methods. Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses two different keys. Each method has its pros and cons. Symmetric encryption is fast and straightforward but less secure as it relies on a single key. Asymmetric encryption, although slower and more complex, provides higher security. Notable symmetric algorithms include Data Encryption Standard (DES) and Advanced Encryption Standard (AES)[21,22]. Asymmetric cryptography, or public-key cryptography, uses unique keys for encryption and decryption. Examples include RSA and Elliptic Curve Cryptography (ECC), with ECC used in protocols like Diffie-Hellman[23,24,25,26].

Figure 2 illustrates the key exchange process between source and destination using both symmetric and asymmetric encryption methods.

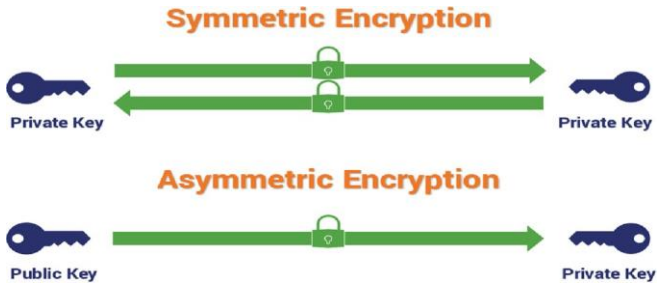


Fig. 2: Symmetric and asymmetric encryption.

We propose a data security model employing encryption, digital envelopes, digital certificates, and public key infrastructure (PKI) to protect information from sensors to wireless communication and applications. This model is applicable in sensor networks and other domains requiring secure data management, independent of underlying communications infrastructure. It meets the requirements for identification, authorization, data security, reliability, non-repudiation, trust, and confidentiality in distributed systems.

This study introduces an intrusion prevention architecture for WSN-based mobile IoT networks, designed to extend network lifespan through lightweight, secure data routing among mobile nodes. Our system uses the uncertainty principle to create clusters of mobile IoT objects and select cluster leaders, determining their latest locations based on network monitoring and analysis. Existing solutions often fail to provide secure, reliable end-to-end data exchanges between mobile IoT devices. Our proposed framework, leveraging blockchain architecture, offers a secure and efficient end-to-end method, enhancing routing performance in terms of data security and energy consumption. The goal is to develop a secure sensor network framework, decoupled from the communications infrastructure, applicable to various domains requiring secure data for administrative purposes.

Objectives

Due to the constrained resources and susceptibility to attacks in WSNs, researchers often face a dilemma between achieving energy-efficient routing and ensuring data security during transmission. Although various attempts have been made to balance these objectives, the dynamic nature of WSNs and the limited resources of sensor nodes make it challenging to develop a secure and optimal network topology that also maintains energy efficiency. Numerous methods for securing data transfer have been explored, but encryption remains the most straightforward and effective technique that all users should be familiar with and capable of using. Meanwhile, clustering enhances routing efficiency in terms of energy consumption.

The aim of this research is to develop an intrusion prevention architecture for WSN-based IoT networks. The objectives of this proposed and implemented work include:

i. Conducting a systematic review of security solutions to address potential attacks in wireless sensor networks.
ii. Proposing an algorithm that combines energy-aware routing and secure transmission using clustering along with cryptography.

Weak security protocols can lead to significant losses of sensitive and confidential data in various WSN applications. In worst-case scenarios, security breaches can result in irrecoverable data loss. Additional consequences of inadequate security measures include high-risk networks, server congestion, loss of user trust, and costly recovery processes. WSNs face multiple challenges in developing secure solutions. We have reviewed the fundamental concepts related to sensor network security, including security risks, energy efficiency, and strategies based on cryptography and clustering. Consequently, we have devised a security solution tailored for wireless sensor networks.

In real-life implementations, random node failures are a common occurrence. The limited resources of sensor nodes render conventional security mechanisms with high computational and connectivity overheads impractical for WSNs. Therefore, creating secure and energy-efficient WSNs is particularly challenging. Our methodology aims to enhance energy efficiency and secure data in WSNs by leveraging cryptography and digital envelope technology.

II. Literature Review

Wireless sensor networks (WSNs) are gaining significant attention due to their vast array of potential applications. Researchers have proposed various protocols to address the challenge of achieving reliability in WSNs, with cryptography being one of the key methods for ensuring data security. Security measures are crucial for protecting personal data during storage and transmission. As adversaries have become more adept at cracking commands, encryption techniques have evolved to maintain message confidentiality. When these methodologies are applied to data transmission, the information is first transformed into unreadable ciphertext and sent in this form, which the receiver then decodes back into its original format using a secret key or password. This ensures that even if an intruder intercepts the file before it reaches its final destination, they will be unable to read it due to the encryption.

The Triple Data Encryption Standard (Triple DES) algorithm enhances security by applying three different block cipher algorithms to each data block, increasing the key size to improve encryption strength. Each data block consists of 64 bits, and the encryption process uses three keys, each 56 bits long. The Blowfish Encryption Algorithm was once a strong contender for being the top encryption standard, but the Advanced Encryption Standard (AES) eventually emerged as the best. Blowfish utilizes key-dependent substitution-boxes (S-boxes), ensuring that despite the presence of the S-box, the ciphertext can only be decrypted using the cipher key. The S-box's purpose is to obscure the link between the encrypted text and the key. The Twofish encryption standard, which uses 128-bit keys, is also widely regarded as a secure option. Due to its unique design, robustness, and speed, Twofish is considered one of the finest AES protocols.

The Advanced Encryption Technology (AES) is currently the most widely used symmetric encryption standard. AES was developed as a successor to DES, which had limitations in key size and processing capabilities. AES is more than six times faster than Triple DES. Elliptic Curve Cryptography (ECC), introduced in 2004-05, uses the mathematical properties of elliptic curves ($y^2 = x^3 + ax + b$) for encryption. In ECC, multiplying a number indicating a curve point by another number results in a new curve point, making it very difficult to deduce the new point even if the original point is known.

Researchers have proposed various algorithms to enhance the efficiency and security of cryptographic approaches. For instance, an algorithm using Diffie-Hellman's key exchange method for ECC has shown improved security and efficiency compared to existing systems. Additionally, a new lightweight encryption strategy has been proposed to enhance network bandwidth and the computational resources of wireless sensor

nodes. This strategy employs genetic operations such as mutation, crossover, and XOR operations, along with a lightweight block cipher.

In another study, Secure Data Aggregation and Verification (SDAV) was proposed using ECC due to its small key size and computational efficiency. In this approach, a single sensor generates a signature while the base station performs verification. The aggregator decrypts the members' encrypted data, averages it, and provides the result back to the members. If the disparity between the unit of measure and the mean exceeds a certain threshold, participants create partial signatures and send them to the aggregator. The Merkle hash tree is used to ensure the authenticity of the measures, making the method resistant to eavesdropping and Sybil attacks. However, this method is vulnerable to selective packet delivery and replay attacks, where packets can be ignored by a compromised aggregator.

Misic and Misic[27] proposed a method to efficiently aggregate encrypted data, ensuring data integrity and confidentiality. Instead of using the XOR operation, their approach utilizes simple modular addition, which is effective against passive attacks. However, this method does not address active threats and employs a probabilistic approach. Their study introduces robust hybrid cryptography, demonstrating that their scheme offers enhanced security while reducing encryption and decryption time. For data encryption and decryption, they used chaotic maps in conjunction with the LEACH protocol for data routing. Nidarsh and Devi[28] indicate that chaotic maps can be compromised using various techniques, while another study employs logistic and Kent chaotic maps[29].

The primary limitations of existing algorithms in the literature include:

Limited Battery Life: Many proposed algorithms assume a finite battery life for nodes, and the depletion of a single node's battery can jeopardize the entire WSN's data transmission.

Inefficiency for Large Data: Algorithms using decryption operations are unsuitable for encrypting large data volumes, leading to significant slowdowns and potential integrity issues[30].

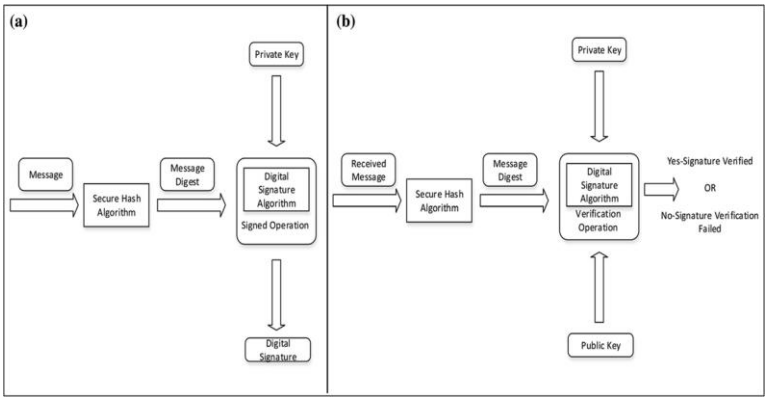


Fig. 3: (a) Elliptic curve digital signature algorithm signing mechanism. (b) Elliptic curve digital signature algorithm verification mechanism DSA, and ECC algorithms, all providing the same level of security.

Table 1 Comparison between RSA, DSA and ECC.

Bits	ECC	DSA	RSA
80	160–223	1024	1024
112	224–225	2048	2048
128	256–383	3072	3072
192	384–511	7680	7680
256	512+	15,360	15,360

The Advanced Encryption Standard (AES) is a symmetric key encryption and decryption technique with three block ciphers: AES-128, AES-192, and AES-256. AES is widely used for encrypting sensitive data globally, both in software and hardware. Developed to replace the vulnerable Data Encryption Standard (DES), AES offers strong security against various attacks. Fig. 4 illustrates the AES design. For a block of messages, AES-128 uses a 128-bit key length, AES-192 uses 192-bit, and AES-256 uses 256-bit. Each cipher encrypts and decrypts data in 128-bit blocks, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The encryption process involves several steps, including substitution, transposition, and mixing, transforming plaintext into ciphertext.

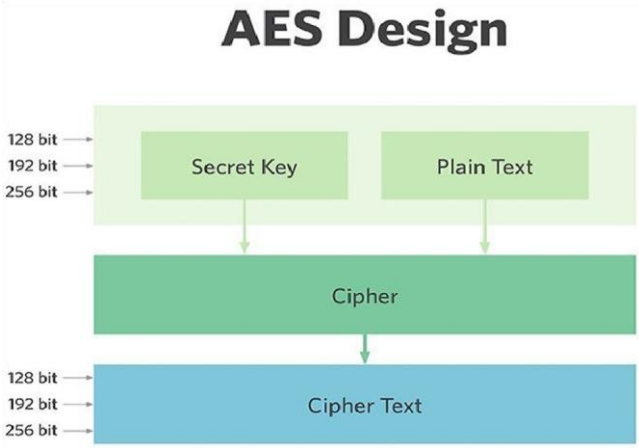


Fig. 4: Relationships between the Secret Key, Plaintext, Cipher, and Cipher Text are depicted in visual diagrams.

Security experts assert that AES is resistant to brute-force attacks, which involve testing all possible key combinations until the correct one is found. However, the key lengths must be sufficient to prevent modern machines from cracking the encryption, even with advances in technology due to Moore's law. AES is favored for its high-speed encryption capabilities and versatility in both software and hardware implementations, utilizing a substitution-permutation network architecture. The finite element model is commonly used for AES calculations.

The number of cycles required to convert plaintext into ciphertext, known as conversion rounds, depends on the key size used in AES encryption. AES encryption and decryption software are widely accessible and are typically utilized for highly sensitive data requiring restricted access. The AES standard, recognized as the foremost encryption standard globally, is frequently encountered in cybersecurity contexts. Comprising three block ciphers, AES employs cryptographic keys to encrypt and decrypt data in 128-bit blocks, ensuring a reasonable level of secrecy for classified information[34].

In Pitchaiah, Daniel & Praveen[34], ECC was employed for plaintext encryption, while Dual RSA was applied to the hash value of the plaintext, exhibiting fourfold speed improvement over conventional RSA and reduced memory usage. However, key encryption proved time-consuming. The AES and ECC sequential encryption method, followed by MD5 hash value computation and plaintext hash calculation, demonstrated reduced memory usage but increased execution time[36]. DES was utilized for data transfer in a subsequent algorithm, with RSA employed to encrypt the DES key, offering enhanced security and efficiency[37]. Kumar[38] utilized symmetric cipher (AES Rijndael) for encryption, and public key cryptography (RSA) for authentication, incorporating SHA-512 hash function for enhanced security during transmission.

The Importance of Security in Wireless Communications

- Safeguarding User Data: User data transmitted over the air interface must be shielded from eavesdropping.
- Protection of Signaling Data: It is imperative to safeguard signaling data from unauthorized interception.
- User Authentication: Effective user authentication is crucial for verifying subscribers to the network, ensuring accurate billing.

Existing Wireless Security Networks

Several wireless security networks are currently in various stages of development and implementation worldwide. These include second-generation digital cellular telephony like GSM, second-generation digital cordless telephony such as DECT and IS-41, third-generation digital cordless telephony like UMTS, wireless LAN for indoor networks, UPT for mobile terminal access, and mobile data networks like CDPD. Details of these networks are outlined below.

UMTS Security

Security Requirements

The primary security requirements of Advanced Security for Personal Communications Technologies (ASPeCT) entail the investigation of the following aspects[39]:

- Transitioning security from existing mobile systems to UMTS.
- Detection and management of fraud in UMTS.
- Trust Third Parties (TTP) for end-to-end security services in UMTS.
- Capabilities of future User Identity Modules (UIMs).
- Security and integrity of billing in UMTS.

Security Mechanisms

The current detailed proposal for authentication mechanisms is as follows:

Challenge-Response using Symmetric Key Techniques (Royal Holloway)

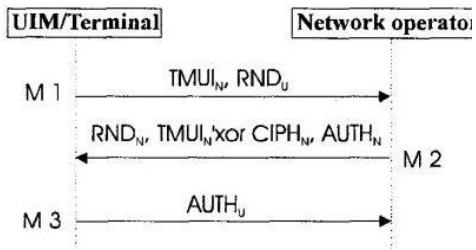


Figure 5 Royal Holloway, current registrations

Protocol Description: The mechanism involves the exchange of three messages between the user and the network during Current Registrations, where the user is already registered with the network operator while roaming. The user and network operator share a TMUIN and KNu operator, with no involvement of the service provider. The three messages are denoted in Figure 5 as M1, M2, and M3. The procedure unfolds as follows:

The UIM/Terminal transmits message M1, containing TMUIN and RNDu, to the Network Operator.

The Network Operator sends M2, comprising RNDN, TMUIN' xor CIPHN, and AUTHN to the UIM/Terminal, calculated as:

AUTH_N = A_U (K_NU, RND_N || RNDu || TMUIN'), where RNDN and TMUIN' are generated by the network operator.

CPH_N = C_U (K_NU, RND_U). Simultaneously, the network operator calculates:

AUTH_U = A_U (K_NU, RNDu || RNDN).

UIM/Terminal computes AUTHy to authenticate the Network Operator and sends it as M3 to the Network Operator.

Upon receiving AUTHu, the Network Operator compares it with the previously calculated one.

UPT Security Overview

Utilizing a universal number, Universal Personal Telecommunication (UPT) enables enhanced access to multiple networks, wired and wireless, from any terminal. Given the nature of the service, a high level of security is imperative[40].

Parties Involved in UPT

Parties within the UPT environment include individuals or company representatives responsible for actions or affected by the UPT service. These parties may encompass:

- UPT user (Uus).
- UPT subscriber (Usb).
- UPT service provider (Usp).
- UPT network operator (Uop).
- Network operator (Nop): Public network operator facilitating UPT communications.
- Line subscriber (Lsb): Individual owning access or terminal to a standard network facilitating UPT communications.
- Other Party (Otp): Individuals calling or being called by UPT users.
- Intruder (Int): Any party posing threats to the UPT service, either by actively masquerading as communication parties or passively intercepting information.

Various relationships exist among UPT parties, governed by appropriate agreements that consider legal variations across countries. Figure 6 illustrates the relationships among UPT parties.

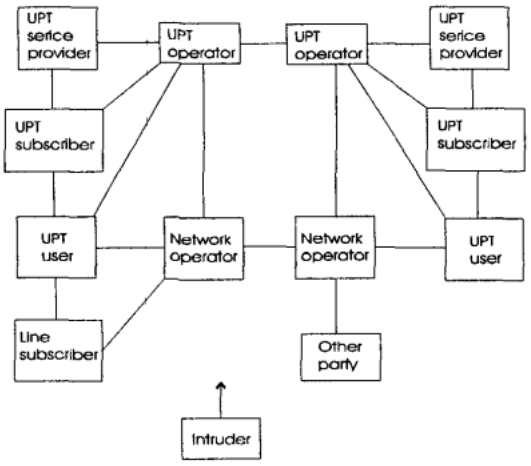


Figure 6 Model of UPT parties and their relations

Threats to the UPT Service

Subscription Process Threats to the subscription process include unauthorized modification of subscription data by the user or subscriber, fake subscriptions by intruders, and unauthorized termination of subscriptions.

Threats to Personal Data Integrity Personal data integrity threats involve the identification of sensitive data, processing functions, and locations within UPT systems. Threats arise when personal data integrity is compromised, affecting parties' behavior profiles.

Threats to UPT Service Providers Systems Internal systems of UPT service providers face threats such as unintended functionalities and insufficient reliability caused by local implementations or operations.

Threats to Inter-Network Communication Inter-network communication threats include network connection to incorrect databases, masquerading of UPT entities by intruders, modification or eavesdropping of signaling data, and manipulation of files or messages for unauthorized purposes.

Data Protection Requirements

The essential requirements for safeguarding individual data include:

Call Forwarding Services: Call forwarding services are permissible only with the consent of the third party, and the calling party must be informed during call setup.

Limitation of Calling Parties Identification: Call forwarding services can restrict identification to calling parties upon the request of the third party.

Limitation on Incoming Calls: Incoming calls reception may be restricted by the called party based on calling line identification.

Blocking Caller ID: The option to block calling line identification on a per-case basis should be available.

Confidentiality of Call Content: Access to call contents by third parties, such as during conference calls, requires the agreement of all involved parties.

Temporary Storage of User Information: User information should only be stored during transmission.

User Data Handling: To ensure users' self-determination over their personal data:

- Data collection, processing, and storage should be solely for service provision.
- Duration of data usage should be minimized.
- Consent for data usage should be obtained for the shortest duration possible.

Confidentiality of Personal Data: Personal data must be kept confidential and not shared with other parties without subscribers' prior consent.

Prohibition of Electronic Profiles Collection: Collection or filtering of subscribers' electronic profiles regarding temporary location, personal, and business circumstances is not allowed.

Security Features

Various security features are devised to counteract identified threats:

Activity Monitoring: Real-time monitoring of user account events, including authentication and call activity, helps detect potential abuses.

User Authentication: Authentication of UPT users and subscribers counters threats like masquerading and profile manipulation.

Service Provider Authentication: Authentication of the UPT service provider safeguards against impersonation.

Access Control to UPT Access Device: Authentication of users and strong access control mitigate unauthorized device use.

Access Control to Service Profile Information: Access control systems prevent unauthorized access to service profile databases, mitigating various masquerading threats.

Secure Subscription Process Management: Stringent administration of subscriptions and access control to subscription databases addresses threats like unauthorized modifications and service denials.

Security Architectures

Authentication Exchange Mechanisms

Various authentication mechanisms exist, with the choice depending on technical capabilities and required security levels. The UPT system proposes two systems to address these authentication mechanisms:

One-Pass Authentication Mechanisms

To prevent replay attacks, the one-pass authentication protocol employs variable Authentication Codes (AC). These ACs must be verifiable by the UPT system and must be both non-predictable and non-replayable. This process necessitates the use of a UPT access device, with a fixed local PIN authenticating the user to their device. Authentication data can include timestamps, sequence numbers, random numbers, or a combination thereof. The user's identity is one-way encrypted for authentication, resulting in a variable Authentication Code

(AC), which is then sent along with parts of the cleartext to the UPT system for verification. The data flow is illustrated in Figure 7.

Note: The authentication may be concatenated with information data (e.g. the UPT number of UPI, respectively, the "LPIN" id checked in the system, and user commands) before enciphering, in order to achieve data integrity.

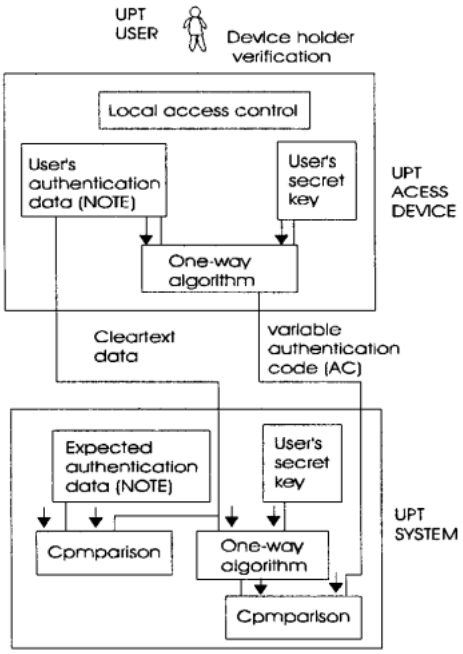


Figure 7: Variable AC

Multiple-Pass Authentication Mechanisms

These protocols operate between the UPT access device (e.g., smart card), the UPT system, and possibly a trusted Third Party (TP). Additionally, a local PIN authenticates the UPT user to their UPT access device.

a) **Mechanisms without Trusted Third Party**

The proposed mechanism involves two-pass authentication with a random number exchanged between the UPT access device and the UPT system. This mechanism can also facilitate authentication of the system to the device, enabling mutual authentication.

b) **Mechanisms with Trusted Third Party**

In this concept, authentication is enabled without sharing a secret key between the involved entities prior to the authentication process. Instead, each entity shares a common secret key with the trusted third party. The proposed mechanism involves four-pass authentication facilitated by the trusted third party, ensuring secure authentication between the UPT system and the UPT access device.

CDPD Security

In a CDPD network, the airlink represents a significant vulnerability to potential hacking attempts. Serving as a virtual wire into customers' networks, the airlink requires robust protection.

Security Architecture

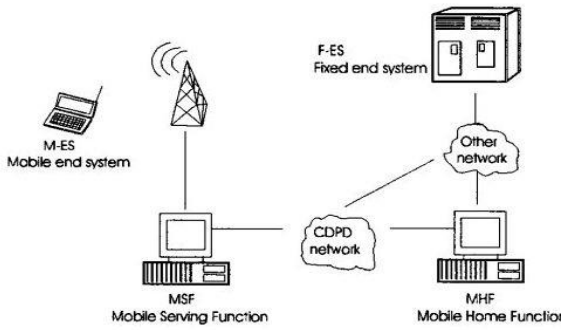


Figure 8 The CDPD network

Each Mobile-End System (M-ES), essentially a computer with a wireless modem accessing the CDPD network through the airlink interface, is assigned one or more unique Network Entry Identifiers (NEIs). Network entities responsible for network routing include the Mobile Host Function (MHF) and the Mobile Serving Function (MSF). Notably, message flows between M-ES and MSF over the airlink are encrypted, while those between MSF and MHF lack encryption or cryptographic authentication. The security architecture is depicted in Figure 8.

Authentication Protocol

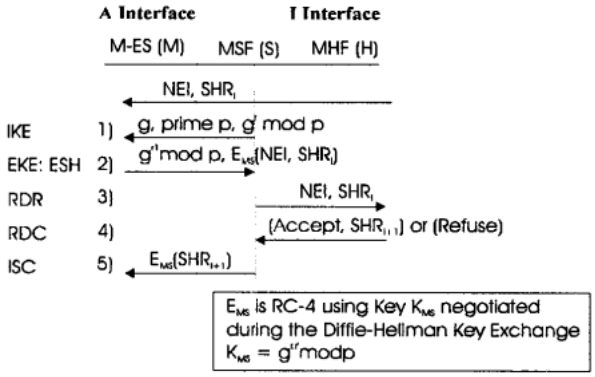


Figure 9: The current M-ES authentication protocol

The current M-ES authentication protocol, executed during call setup and hand-offs, involves several steps as outlined in Figure 9. Initially, an M-ES is initialized by the Mobile Data-Intermediate System (MD-IS) performing MHF services, providing it with a unique NEI and Shared Historical Record (SHR) tuple. Subsequent steps involve transmissions and verifications between the mobile device and its home network, ensuring secure authentication and service confirmation.

GSM Security

A radio access network inherently poses less security than a fixed network due to the ease of intercepting and emitting radio waves from any location without tampering with operator equipment.

Purpose of Security

The primary objectives of security in GSM are to safeguard conversations and signaling data from interception and prevent cellular telephone fraud. These objectives include ensuring correct billing, maintaining radio path security, implementing strong authentication, preventing security compromises between operators, and ensuring security measures do not unduly impact call setup times, increase bandwidth, raise error rates, or add excessive complexity to the system.

Architecture

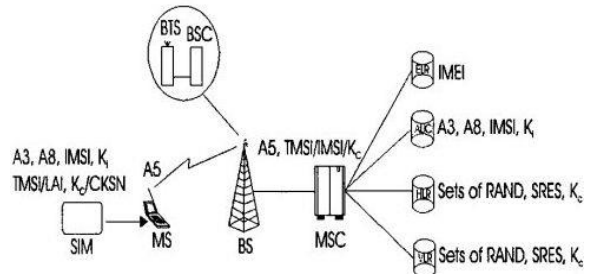


Figure 10: Distribution of Security Features in the GSM Network

Figure 10 illustrates the distribution of security features among Subscriber Identity Modules (SIMs), GSM handsets or Mobile Stations (MSs), and GSM network elements such as Mobile Switching Centers (MSCs), Authentication Centers (AUCs), and Home Location Registers (HLRs) or Visitor Location Registers (VLRs). Each entity contains security-related information contributing to the overall security architecture.

The details of GSM-entities which contain security related information are:

MS	:	A5
SIM	:	A3, A8, IMSI, K_i, TMSI/LAI[2], K_c/CKSN[3]
AUC	:	A3, A8, IMSI, K_i
HLR	:	Sets of IMSI, RAND, SRES, K_c
VLR	:	Sets of IMSI, RAND, SRES, K_c
MSC	:	A5, TMSI/IMSI, Kc
EIR	:	IMEI

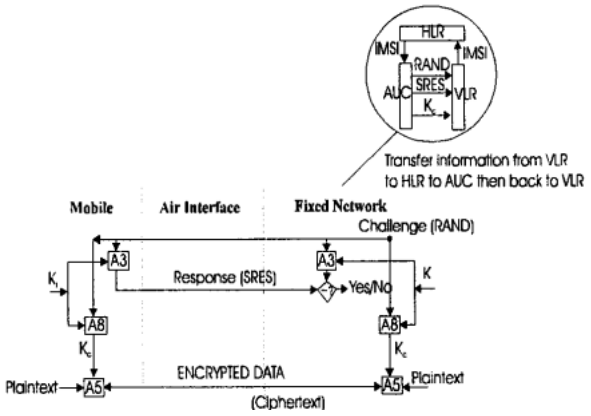


Figure 11: Encryption for GSM

Security Provision

Security mechanisms in GSM systems aim to prevent network misuse and protect subscriber privacy through various mechanisms, including Subscriber Identity Authentication, Subscriber Identity Confidentiality, Signaling Data Confidentiality, and User Data Confidentiality. These mechanisms ensure secure authentication, confidentiality, and anonymity for subscribers while encrypting signaling and user data flows.

Advantages

- Subscribers' anonymity is ensured through the allocation of temporary identification numbers (TMSIs) valid within specific areas, ensuring privacy.
- Communication confidentiality over the radio link is maintained through encryption algorithms.
- Authentication processes remain untraceable, as random challenges change with each authentication request.
- SRES calculation occurs within the SIM, reducing the need for Kc outside the SIM.

Disadvantages

- The centralized security design may incur processing time and cost, potentially hindering future mobile communication service growth.
- Misconceptions about encryption coverage within the GSM network domain, which only applies to the radio channel, may arise.
- Revealing IMSI for certain reasons, such as registration failures, poses risks of eavesdropping.

DECT Security

Security Services

DECT system offers several security services:

Authentication of a Portable Terminal (PT): Initiated by a Fixed Terminal (FT), this service allows authentication of a PT involved in call making or receiving. It ensures secure identification for billing purposes and prevents unauthorized access to private base stations.

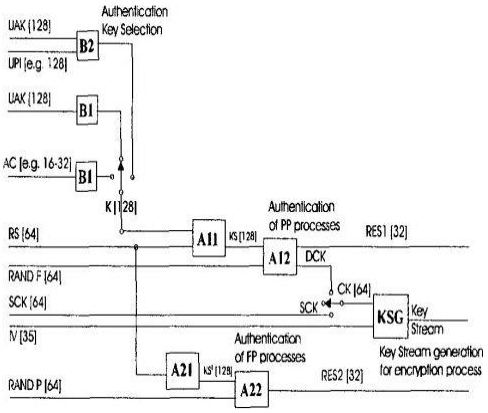
Authentication of an FT: Initiated by a PT, this service enables authentication of an FT involved in call making or receiving. It safeguards against unauthorized loading of information into a Portable Part (PP) and FT impersonation.

Mutual Authentication: Allows both PT and FT involved in a call to authenticate each other.

Data Confidentiality: Ensures confidentiality of user data and certain control data transmitted between PT and FT over the Connection Identifier (CI), excluding cryptographic protection for data through fixed networks.

User Authentication: Enables an FT to authenticate a PT user by checking the User Personal Identity (UPI) value associated with that user, ensuring secure user identification during call initiation.

Security Architecture



AC	:	Authentication Code
IV	:	Initialisation Value obtained from frame counter
CK	:	Cipher Key
SCK	:	Static Cipher Key
Ks	:	Session Authentication Key
Ks'	:	Reverse Authentication Key
RAND F	:	Value generated and transmitted by FP
RAND P	:	Value generated and transmitted by PP
RES 1	:	Value computed and transmitted by PP
RES 2	:	Value computed and transmitted by FP
RS	:	Value transmitted by FP in authentication protocol
UAK	:	User Authentication Key
UPI	:	User Personal Identity
DCK	:	Derived Cipher Key
K	:	Authentication Key
A11, A12	:	Authentication Processes
A21, A22	:	Authentication Processes
B1, B2	:	Authentication Key Stream Processes
KSG	:	Key Stream Generator

Figure 12 Overview of DECT security processes

Figure 12 shows an overview of DECT Security processes.

The security architecture involves various cryptographic elements depicted in Figure 12, including Authentication Code (AC), Cipher Key (CK), Session Authentication Key (Ks), Reverse Authentication Key (Ks'), User Authentication Key (UAK), User Personal Identity (UPI), and Derived Cipher Key (DCK), among others.

Security Mechanisms

Authentication of a PT

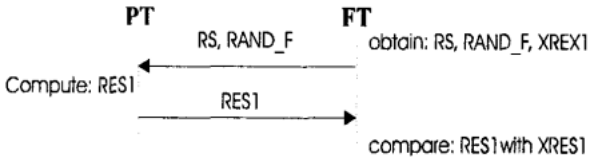


Figure 13 Authentication of PT

This service employs a cryptographic challenge-response mechanism, as illustrated in Figure 13. The FT challenges the PT by sending RS and RAND_F, and the PT responds with a computation result, RES1, using the challenge and its associated authentication key. Successful authentication is confirmed if the calculated value matches the expected value (XRES1), thereby verifying the PT's knowledge of its authentication key.

Authentication of an FT

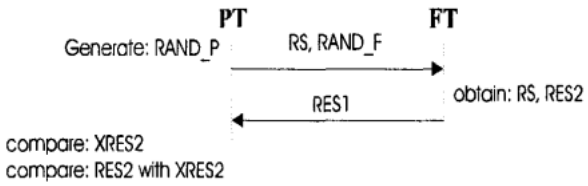


Figure 14: Authentication of FT

Using a similar challenge-response mechanism, shown in Figure 14, the PT sends a challenge (RAND_P) to the FT. The FT responds with a computation result, RES2, using the challenge and authentication key associated with the PT and RS. Authentication is successful if the computed result matches the expected value, demonstrating the FT's knowledge of the authentication key associated with the challenge PT

Wireless LAN Security

Operational Principles

Wireless LAN systems comprise cells, each containing multiple wireless station adapters and an access point that manages the cell and connects to the backbone. Station adapters within a cell can communicate among themselves or access wired LAN resources through the access point. All station adapters in a cell synchronize with the access point by frequency and clock, ensuring data transmission. Intercepting data requires being within the cell's coverage area and synchronized with the access point.

Network Risks

Wireless LANs face significant security risks, including:

Internal Attacks: The primary threat originates from within the network user community. Unauthorized users, including disgruntled employees, may access, distribute, or alter sensitive company data without proper security measures.

Unauthorized Access: External users gaining unauthorized access to the network.

Eavesdropping: Difficulty in detecting outsiders who attempt to intercept data packets.

Security Features

To mitigate these risks, wireless LANs should offer security features such as user authentication and authorization.

Security Theoretical Methods

Secure communication in wireless LANs can be achieved through methods like:

Spread Spectrum: Utilizing Direct Sequence or Frequency Hopping, where the carrier wave frequency changes continuously.

Password Control: Tight control and frequent changes of passwords.

Data Encryption: Adding encryption, either hardware or software-based, to scramble data packets for transmission, with only authorized stations possessing the decryption key.

Practical Security Methods

Wire Equivalency Privacy (WEP): Utilizing WEP, based on RSA RC4, to prevent eavesdropping by initializing a pseudo-random number with a shared secret key.

Extended Service Set ID (ESSID): Configuring a password in the access point, ensuring that only station adapters with the same ESSID can synchronize and join the cell. Changing the ESSID protects against theft, and setting proprietary hopping patterns enhances security by allowing the network to continue functioning even if a unit with a proprietary pattern is stolen.

Security Architecture

University of California at Berkeley: The architecture devised at the University of California, Berkeley, by Vaduvur Bharghavan, constitutes a mobile computing environment featuring indoor wireless nanocells supported by a wired backbone network. Computers within this environment are either static workstations or mobile notebooks. Each static computer possesses a wired network interface, while each mobile computer is equipped with a wireless network interface. Special static computers, termed base stations, feature both wired and wireless network interfaces and provide network connectivity to mobile computers. Mobile computers can only access network connectivity by communicating with a base station; direct communication between mobile computers is prohibited. The geographical region served by a base station is referred to as its cell. The wireless medium operates on a single-channel near-field radio with a bandwidth of 256 kbps and a range of approximately 30 feet. Each mobile computer has a home computer on the wired backbone network, which is fully trusted with any information regarding the mobile computer. Home computers and base stations are considered trusted special machines. The architecture is depicted in Figure 15.

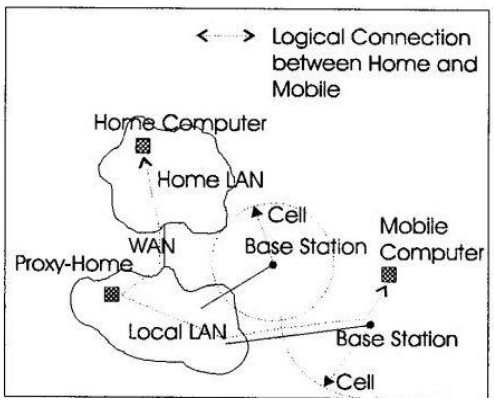


Figure 15: Mobile Computing Environment

Ashar Aziz: This mechanism, proposed by Ashar Aziz, aims to ensure both privacy and authenticity among communicating parties. The details, including three messages, are outlined in Figure 16:

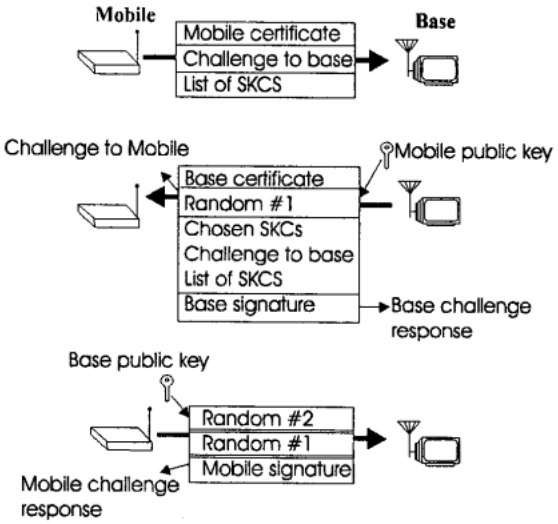


Figure 16: Secure protocol for wireless LAN networks

Message #1: Mobile to Base.

Message #2: Base to Mobile.

Message #3: Mobile to Base.

IS-41 Security

Security Architecture

Figure 17: Privacy and Authentication of IS-41

In the United States, within IS-41-based digital wireless telephone systems, users input a security parameter known as the "A-key" into their handsets via a keypad. This process begins when the service provider confidentially sends the 64-bit A-key to the user, typically through mail. This direct link between the user and the service provider aims to bypass potential fraud originating from service shops due to intentional or careless mishandling of security information. It is imperative for the service provider to store the user's A-key within the "home network." This entire process is illustrated in Figure 17. The A-key remains within the "home network," similar to how Ki never leaves its GSM "home" network.

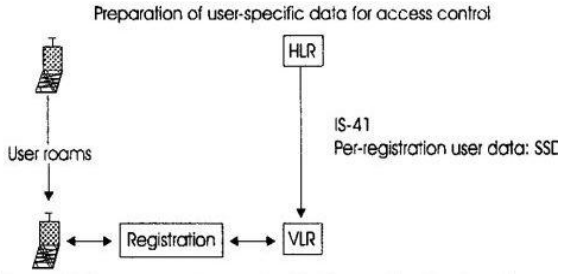


Figure 18 Roaming support: secret key systems

Figure 18 illustrates the process of access control in a roaming scenario, where a handset has moved from its home network, served by its HLR, to another network, where it is served by VLR. Authentication is performed upon handset registration with the VLR. IS-41 systems support roaming subscribers by transporting SSD from HLR to VLR, enabling autonomous authentication of the user.

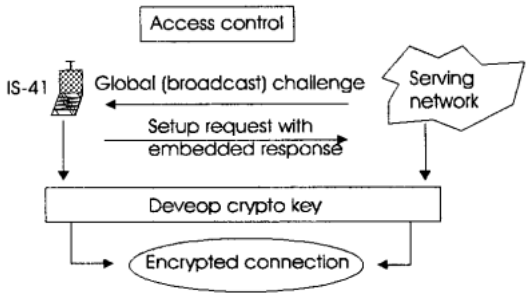


Figure 19 Authentication and Key Agreement protocols for IS-41: secret key systems

Figure 19 depicts simplified call flow models for Authentication and Key Agreement in IS-41-based systems. The objectives are to confirm to the serving network that the handset is entitled to service and to generate cipher bits for protecting user traffic over the RF link. In an IS-41-style network, a single 32-bit "global" challenge is generated at regular intervals and broadcast throughout the service area on a system information channel. Handsets attempting system access compute an 18-bit authentication response using an authentication algorithm operating on their individual SSDs and the current global challenge.

Empirical Studies

A multitude of security issues have been identified within Wireless Sensor Networks (WSNs), leading to the proposal of various models and methods in existing literature to address them. Karlof and Wagner[41] delve into sensor network attacks, defenses against them, and future directions. Roberto et al.[42] offer a valuable solution aimed at safeguarding WSNs from common assaults, particularly focusing on Unattended WSNs (UWSNs) where central authority may be absent for prolonged periods. Eschenauer and Gligor[43] propose random key distribution as a security measure. Song et al.[44] introduce two techniques, the Generalized Extreme Studentized Deviate (GESD) method and a present value-based filter, to protect WSNs from delay attacks. Shu, Krunz, and Liu[45] present a solution prioritizing compromised node and Denial of Service (DoS) attack mitigation using a multi-path random routing technique. Xiaojiang et al.[46] propose a method for ensuring network safety through time synchronization of cooperative sensor networks.

In addition, Zhang, Zhu, and Cao[47] explore secret key-sharing approaches to establish communication sessions in WSNs and mitigate complications arising from compromised nodes.

However, a significant portion of WSN security research focuses on identifying and enhancing alternatives to traditional public-key algorithms and Public Key Infrastructures (PKIs). Gura et al.[48] demonstrate the feasibility of RSA and elliptic curve cryptography (ECC) on 8-bit Processors, with ECC showing greater efficiency. Watro et al.[49] illustrate partial deployment of the RSA cryptosystem on real-world wireless sensors,

utilizing the sensors for public operations and offloading private operations to other machines better suited for heavier computations.

Mihaela et al.[50] propose a generic architecture where the sink node is positioned at the center, and sensor nodes are divided into coronas. Yang and Cardei[51] design a protective measure for WSNs to enhance reliability and reduce power consumption. Dvir et al.[52] present a lightweight security solution using one-way hash function and bitwise exclusive operation to enhance data security across various parameters.

Furthermore, Zhenghong and Zhigang[53] suggest a safe cluster formation method for creating trustworthy clusters using pre-distributed keys. Tao Shu et al.[54] propose secured routing with intrusion detection using a WSN clustering architecture to enhance node safety during cluster formation and thwart routing infrastructure attacks.

Routing methods[55] play a crucial role in wireless sensor networks, where adversaries obtaining the routing protocol algorithm can pose significant risks. Modirkhazeni, Ithnin, and Ibrahim[56] propose multi-path routing as a solution to counter such assaults, making it challenging for adversaries to deduce data packet routes.

Tripathy et al.[57] introduce the Hybrid Encryption Technique (HET) evaluating the efficacy of two-key and single-key encryption in securing data in sensor networks. Sachin, Bhushan, and Surender[58] suggest a hybrid encoding approach combining asymmetric and symmetric algorithms for enhanced security with low key management overhead. Anwar and Maha[59] propose a lightweight hybrid cryptographic method (AES and Modified Playfair Cipher) for WSNs, prioritizing security while considering energy consumption.

An analysis of various research publications reveals that asymmetric cryptography incurs performance degradation due to limited memory, energy, and computing resources. Conversely, symmetric cryptography poses risks to data transit security if the algorithm's key is compromised, endangering the entire system's security. Hence, it is imperative to develop a secure yet simple algorithm ensuring data integrity and confidentiality.

The development of a comprehensive reliability strategy involved exploring various methods and identifying the most effective combination of available security options in WSNs. Protection and communication in wireless sensor networks (WSNs) are fundamental properties, where security assesses the efficacy of network monitoring, while connectivity facilitates the transmission of sensed data to the sink.

III. Material And Methods

The model integrates criteria for ensuring sensor network security, aiming to furnish dependable information for decision-making while facilitating secure identification of communication participants and data transmission. It relies on cryptographic techniques like digital envelopes, digital signatures, and Public Key Infrastructure (PKI) to safeguard sensor networks against attacks. Encryption is employed to alter sensitive information so that only the intended recipient can decrypt it. Symmetric cryptography is utilized for secret key generation and message encryption, with the key safeguarded via asymmetric encryption and digital certificates from PKI.

Digital envelope technology is employed to encrypt messages and private keys, ensuring that only the designated recipient can access the message content. Initially, the message content is encrypted with a symmetric algorithm (e.g., DES, 3-DES, RC2, AES), creating a digital envelope. Subsequently, the recipient's public key, extracted from their digital certificate, encrypts the envelope using an asymmetric cryptographic technique (e.g., RSA algorithm) to generate a secret key. The recipient's private key decrypts the secret key, which then decrypts the message.

Message signing involves reducing the message to a digest and encrypting it with the signatory's private key using an asymmetric cryptographic technique like RSA. The resulting digital signature becomes an integral part of communication, with the recipient responsible for verifying it. Certificates play a crucial role in associating public and private keys with an identifiable entity. The Certification Authority signs the certificate with its private key, making it verifiable by anyone possessing the Certification Authority's public key.

Attacks in WSN

Attacks on WSNs can manifest in various forms, such as injecting unauthorized data bits into the network or relaying previously sent packets. Adversaries might deploy malicious nodes that mimic legitimate ones or intercept and wipe the memory of deployed nodes. The chosen layer of attack dictates the type of

assault, with each network layer vulnerable to specific attacks aimed at hindering its function or degrading performance. These assaults can originate from within the network or externally. External attacks often involve malware like worms and Trojan horses, phishing, and other tactics to gain access to sensitive information from government and business systems. Internal threats arise when disgruntled insiders misuse access to servers and sensitive data for theft or sabotage.

Proposed Structure

The proposed framework comprises two main components: a secure data routing model and an initial network deployment with cluster management. Initially, the routing architecture is established to enable each node to track its neighbors in an internal database. A mobile cluster head system is introduced to optimize energy consumption, ensuring efficient data forwarding channels to the current locations of mobile cluster heads. The second phase implements a blockchain-based data security architecture to fortify networks against infiltration threats and enhance reliability. Blockchain technology secures data in blocks linked by cryptographic hashes, ensuring data packet tracking and network integrity. This framework offers superior performance across various criteria compared to traditional networks.

Network Deployment

Network deployment in the initial stages involved locating base stations (BS) by emitting "beacon" signals into the network's background noise. Neighboring nodes updated their routing tables based on this information, with source nodes increasing packet transmission. If a node received BS detection messages from multiple neighbors, the routing path with the shortest hop count to the BS was prioritized, and the information was stored in the routing table. Each node constructed its forwarding table based on the shortest path determined in this manner, allowing only nodes with a hop count of 1 towards the BS to engage in direct transmission.

The network field was then partitioned into smaller "cells" using the Voronoi architecture. Each sensor node was associated with the cell whose mean value was closest to its own, treating each Voronoi cell as a separate cluster. A limit was established to determine movable nodes, gradually increasing until any movable node was located within the perimeter of the Voronoi cell, upon which it was promoted to the position of cluster leader. The proposed framework utilized the variational principle to find the least-variable relative positions of mobile nodes, as described in Equation (1).

$$\Delta a \, \Delta q \approx \frac{k}{2} \quad (1)$$

One Δa represents the node's current location, one Δq represents its momentum or speed per unit of time, and one $k$represents the Planck constant. Using the relative location provided by Equation.1, the proposed framework chooses the mobile node as the cluster leader. After mobile nodes are designated as cluster leaders, they will flood the network with data, while regular nodes will modify their routing tables to include the mobile node's unique identifier. The suggested system only updates the routing tables whenever a new mobile cluster head is chosen rather than doing so regularly. The motivation for the proposed platform's employment of base stations as cluster members is the need to speed up communication links and timely data delivery. A decrease in the ratio of power consumption across sensor nodes also improves network security. Algorithm 1 controls Voronoi cells and the identification of roving cluster heads.

The proposed framework employed blockchain technology for secure data routing between sensor nodes, mobile cluster heads, and the base station. Hash databases on mobile cluster nodes allowed remote access, enabling auditing of communications and redirection of hashes. Continuous two-way communication occurred between sensor nodes and mobile cluster heads, which then connected to the base station (BS). Private keys were distributed to all mobile cluster heads for establishing encrypted connections to sensors and the BS. Each message had a unique hash computed using Equation (2).

$$h(z) = k \quad (2)$$

Algorithm 1 selection of moving cluster heads

1. Set of sensor nodes $N_i = \{S_1, S_2. \ldots\ldots\ldots S_n\}$, Cluster head

C_h , distance d, threshold t, status

2. message M_i, voronoi cell V_i, routing table R_i

3. For each node n in N_i
4. do
5. ifC_h. $d < t$then
6. calculate $\Delta a \, \Delta q \approx \frac{-}{2^k}$
7. end if
8. End for
9. setC_h
10. End for
11. for each $S_1 \in C$
12. updateM_i
13. For each $N_i \in V_i$
14. do
15. k.response
16. updateR_i
17. End for
18. End for
19. End for

The bitwise XOR operation is chosen as a hash function in the suggested architecture based on its minimal processing needs and computational efficiency. Another reason hash values are used in the proposed framework is because of their irreversible methodology. This method guarantees that identifying the output does not reveal the message's source.

The suggested architecture centres on the BS, whose primary duties are publishing payment systems, analysing sensor data, and issuing activities.

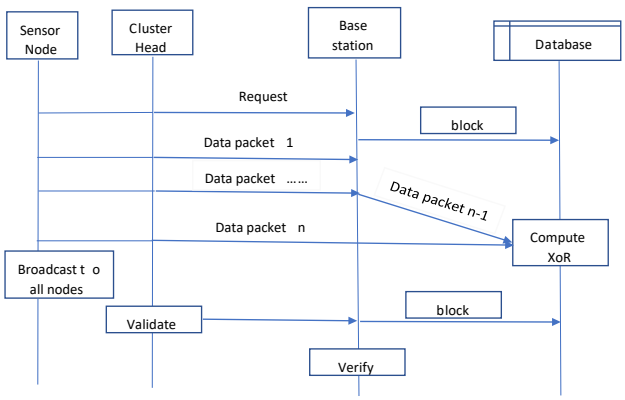


Fig. 20: Proposed data security

Each data packet's history, including sensor locations and mobile cluster head identifiers, is recorded in the Base Station's immutable databases. A limited number of approved sensor nodes and the BS are the only entities with access to the unchangeable database. On top of that, the mobile cluster heads use the private keys they've already acquired to ensure the integrity of the data packets they're sending out. In Fig. 20, we can see how the proposed security method uses blockchain technology to encrypt the routing data sent between wireless clusters and BS, rendering it traceable and irreversible for harmful threats. In addition, the BS acts as a supervisory body, keeping tabs on the operational state of mobile cluster heads and sensor nodes. As the BS is the ultimate authority in the proposed architecture and controls the routing for the whole network, it may kick any dead sensor node or questionable portable cluster head off the network.

IV. Result

Table 2: Simulation setup

Parameter	Value
Number of nodes	250
Simulation Area	300 m×300 m
MAC	802.11
Simulation duration	800s
Packet size	64bits
Payload	1024bytes
Deployment	Random

In this subsection, we show the mobile IoT-based WSN simulation scenario using the default settings listed in Table 2. As a means of gauging the effectiveness of the proposed framework, a range of experiments are carried out, with network node sizes and data transfer speeds manipulated. Sending speeds are also predetermined, ranging from 2 seconds to 4 seconds per node and 50 to 250 nodes in total.

Network Simulator 2 (NS2) simulations are used to validate the proposed method by comparing the simulated results to those obtained using the established method. The variables taken into account during the simulation are listed in Table 2.

The following criterion is applied to determine the efficacy of the suggested method. These include safety, key expansion time, energy use, and Packet Delivery Ratio (PDR). In this study, we present the mean of 10 simulation findings. The following factors are emphasised in the simulations' performance metrics: One of the most important aspects of protecting online conversations. As soon as security is compromised, the network as a whole is open to attack. Security is a fundamental concern for the many applications of WSNs in the Internet of Things. Network energy consumption refers to the total amount of power the network uses during data transmission, data processing, and reception between sensors and sink nodes. An efficient algorithm will have a low "key generation time," which is the amount of time needed to complete the key expansion procedure. The packet delivery ratio (PDR) is the ratio of transmissions at the sink node or default gateway to the entirety of the packets sent by all nodes. Data collisions, failed intermediary nodes, path-switching orders, heavy data traffic, and intrusion threats are all examples of PDR.

In Figure 21, we can see how the PDR changed during the course of the experiment. When compared to MECA's method (a somewhat recent research effort) and Tang's method (very recent research work), the proposed methodology proves superior. Initially, the provided method achieves a PDR that is comparable to Tang's method, but when the simulation duration is extended, the current method's PDR improves.

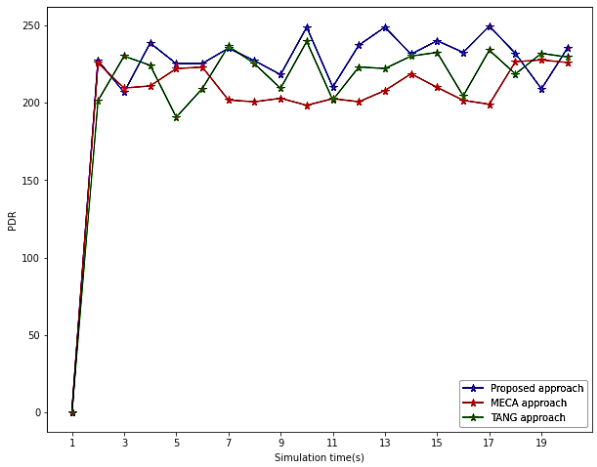


Fig. 21 PDR vs Simulation time

In this part, we compare the efficiency of the proposed framework to that of the existing solutions for various network nodes. Compared to existing methods, the proposed framework extends network lifespan by 25%, 28%, and 32%, as shown in Fig. 22.

In particular, present solutions' performance decreases the network's lifetime by building unstable network areas. As an added downside, the prior systems' routing choices are robust and suboptimal. As a result, the suggested architecture maintains relatively steady performance regarding network lifespan.

This is because we may create energy-efficient pieces using Voronoi cells dispersed throughout the structure. Also, building Voronoi cells may distribute the burden on the individual sensor nodes more evenly. Moreover, the suggested framework records the close relative position of movable cluster heads, which results in minimal communication overheads. The experimental findings show that the suggested framework outperforms competing alternatives in terms of extending the network's lifetime across a wide range of nodes.

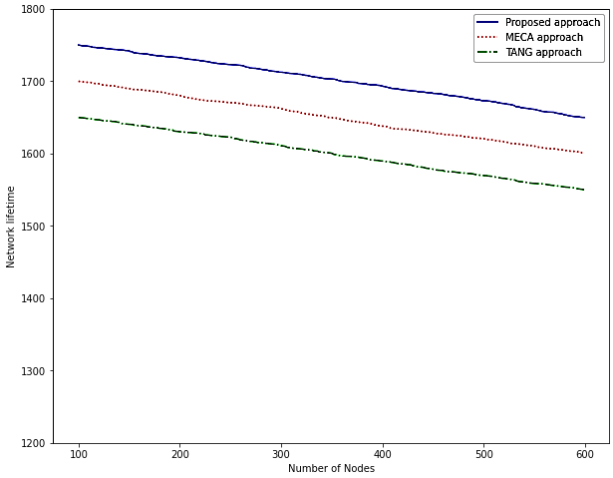


Fig. 22 Number of nodes vs Network lifetime

As shown in Figure 23, the shortest amount of time required by TANG to produce a key is 80 milliseconds when the key length is 10 bits, while the most amount of time required is 150 milliseconds when the key length is 256 bits. Because TANG has a difficult and lengthier key expansion procedure that employs mathematical operations, the time it takes to execute is quite long. The security of the key is in danger if it is compromised in any way. If the execution time is prolonged, the adversary has more time and opportunity to manipulate or change the key and then resend it simply; as a result, the data's security will be compromised. The proposed solution outperforms both TANG and MECA while requiring less effort for essential connection since it was able to break their encryption.

The suggested framework for routing overheads is shown in Figure 24, which compares it to existing solutions under a range of different data transmission rates. According to the findings of the experiments, the newly suggested framework cuts routing overheads by 25%, 27%, and 30% compared to the solutions already in place. In contrast to other solutions, which suffer from high overheads when it comes to re-discovering routes more quickly in the presence of harmful actions, ours doesn't.

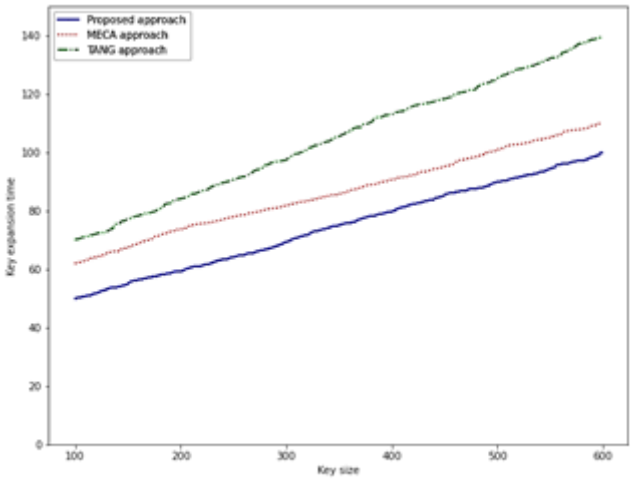


Fig.23 Key size vs Key expansion time

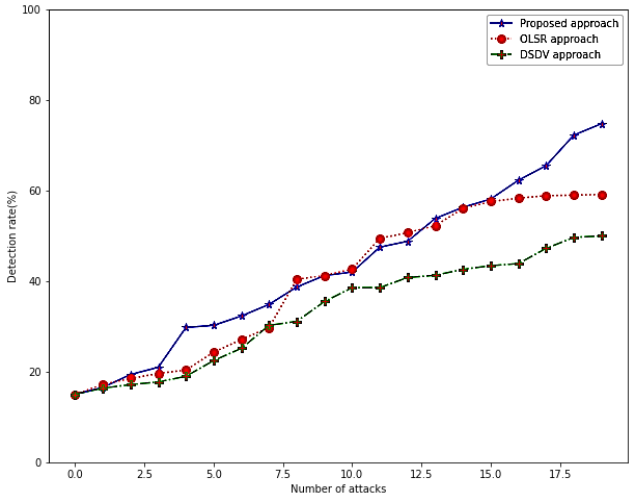


Fig. 24: Routing overheads vs Data sending rate

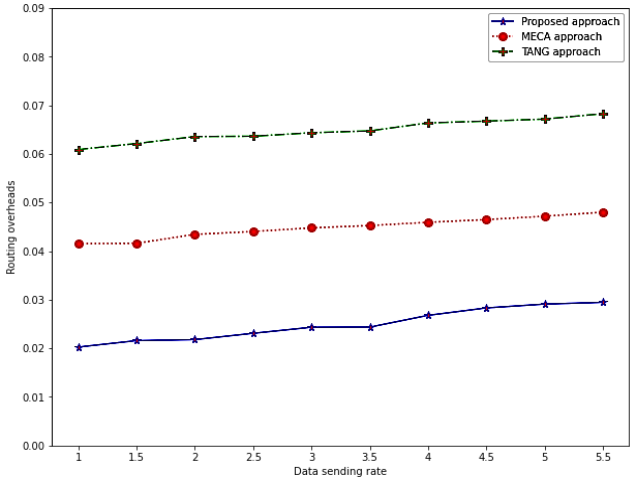


Fig. 25: Number of attacks vs Detection rate

A blockchain-based encryption system that is both lightweight and extremely safe is presented as part of the proposed architecture.

The proportion of wormhole and IP spoofing attacks that are detected is depicted in Fig 25. To listen in on MAC and routing layer data transfer, attackers attempt to breach channels or nodes. The story makes us feel safe in a world where attacks using mobile sensors are on the rise. The attack detection ratio across the sensor monitor nodes of choice is displayed, along with the results for various assaults on network lines and nodes. As an added bonus, it shows the outcomes of routing overhead in network route construction regarding mobility considerations. The suggested secure routing strategy was compared to the currently used protocols by comparing the outcomes of the tests. This shows that even when the network is busy, or nodes are moving randomly, the suggested method can discreetly handle the initial routing burden.

In addition, the currently available solutions have extra routing overheads, which increase when the number of mobile nodes is considerable. Current developments in cryptography and cybersecurity may be broken down into two distinct categories: symmetric and asymmetric. Because of their lesser complexity, symmetric cyphers have shorter key durations than asymmetric algorithms, making them less safe. On the other hand, unilateral cyphers require a higher level of complexity to protect the IoT communication network successfully. But, because of the longer key length, these cyphers are inefficient. After taking into account all of these significant aspects, it is necessary to devise an algorithm that would consume the smallest amount of power, call for the shortest amount of time, start providing the first and most basic level of security to low-end Internet of Things devices, and also reduce the amount of sophistication.

V. Conclusion

In conclusion, this study presents an intrusion prevention architecture tailored for wireless sensor networks (WSNs), aiming to ensure secure routing in mobile Internet of Things (IoT) networks. The main objective is to extend the network's lifespan while enhancing data reliability and network security against malicious attacks. Most energy-efficient systems focus on stationary sensor nodes and utilize the greedy algorithm for data routing, rendering them unsuitable for dynamic environments. The proposed structure comprises movable cluster heads and network nodes distributed across various voronoi cells, emphasizing optimal decision-making and the shortest, most energy-efficient routing paths.

Utilizing the uncertainty principle, mobile cluster heads with minimal momentum fluctuations are selected, reducing communication and routing costs in large networks. Additionally, blockchain technology is leveraged to implement a lightweight XOR hash function, enabling secure and reliable data routing. Future studies will evaluate the performance of the proposed framework in a hardware environment more representative of real-world conditions.

The strategy presented is straightforward and highly effective when numerous competing nodes are distributed across different network hops. With a new security codeword generated at each node, the proposed technique enhances secrecy between nodes and simplifies the identification of competing nodes within the network. Furthermore, the method streamlines underlying mathematics, thereby increasing Packet Delivery Ratio (PDR) by minimizing wait times.

References

[1] Haque, M. M., Et Al. "An Asymmetric Key-Based Security Architecture For Wireless Sensor Networks." Ksii Transactions On Internet And Information Systems 2, No. 5 (2008): 265–279.
[2] Hu, Y.-C., D. B. Johnson, And A. Perrig. "Sead: Secure Efficient Distance Vector Routing For Mobile Wireless Ad Hoc Networks." Ad Hoc Networks 1, No. 1 (2003): 175–192.
[3] Zhang, K., C. Wang, And C. Wang. "A Secure Routing Protocol For Cluster-Based Wireless Sensor Networks Using Group Key Management." In 2008 4th International Conference On Wireless Communications, Networking And Mobile Computing. Ieee, 2008.
[4] Mohaisen, A., Et Al. "On The Insecurity Of Asymmetric Key-Based Architecture In Wireless Sensor Networks." Ksii Transactions On Internet And Information Systems 3, No. 4 (2009): 376–384.
[5] Hamza, R., Et Al. "A Privacy-Preserving Cryptosystem For Iot Ehealthcare." Information Sciences 527 (2020): 493-510.
[6] Qureshi, K. N., And A. H. Abdullah. "Adaptation Of Wireless Sensor Network In Industries And Their Architecture, Standards And Applications." World Applied Sciences Journal 30, No. 10 (2014): 1218–1223.
[7] Kumar, V., A. Jain, And P. Barwal. "Wireless Sensor Networks: Security Issues, Challenges And Solutions." International Journal Of Information And Computer Technology 4, No. 8 (2014): 859–868.
[8] Kumar, D., S. Chand, And B. Kumar. "Cryptanalysis And Improvement Of An Authentication Protocol For Wireless Sensor Networks Applications Like Safety Monitoring In Coal Mines." Journal Of Ambient Intelligence And Humanized Computing 10, No. 2 (2019): 641–660.
[9] Hari, P. B., And S. N. Singh. "Security Issues In Wireless Sensor Networks: Current Research And Challenges." In Proceedings Of The 2016 International Conference On Advances In Computing, Communication, & Automation (Icacca), 2016.
[10] Cordasco, J., And S. Wetzel. "Cryptographic Versus Trust-Based Methods For Manet Routing Security." Electronic Notes In Theoretical Computer Science 197, No. 2 (2007): 131–140.

[11] Das, M. L. "Two-Factor User Authentication In Wireless Sensor Networks." Ieee Transactions On Wireless Communications 8, No. 3 (2009): 1086–1090.
[12] Becher, A., Z. Benenson, And M. Dornseif. "Tampering With Motes: Real-World Physical Attacks On Wireless Sensor Networks." Technical Report, Springer Berlin, Heidelberg, 2006.
[13] Chen, J., Et Al. "A Lossless Watermarking For 3d Stl Model Based On Entity Rearrangement And Bit Mapping." International Journal Of Digital Crime And Forensics 9, No. 2 (2017): 25–37.
[14] Zhang, X., And S. Wang. "Fragile Watermarking With Error-Free Restoration Capability." Ieee Transactions On Multimedia 10, No. 8 (2008): 1490–1499.
[15] De Vleeschouwer, C., J.-F. Delaigle, And B. Macq. "Circular Interpretation Of Bijective Transformations In Lossless Watermarking For Media Asset Management." Ieee Transactions On Multimedia 5, No. 1 (2003): 97–105.
[16] Tian, J. "Reversible Data Embedding Using A Difference Expansion." Ieee Transaction On Circuits And Systems 13, No. 8 (2003): 890–896.
[17] Hu, Y., Et Al. "Difference Expansion Based Reversible Data Hiding Using Two Embedding Directions." Ieee Transaction On Multimedia 10, No. 8 (2008): 1500–1512.
[18] Poljicak, A., L. Mandic, And D. Agic. "Discrete Fourier Transform–Based Watermarking Method With An Optimal Implementation Radius." Journal Of Electronic Imaging 20, No. 3 (2011).
[19] Ou, B., Et Al. "Pairwise Prediction-Error Expansion For Efficient Reversible Data Hiding." Ieee Transactions On Image Processing 22, No. 12 (2013): 5010–5021.
[20] Li, X. W., And S. T. Kim. "Optical 3d Watermark Based Digital Image Watermarking For Telemedicine." Optics And Lasers In Engineering 51, No. 12 (2013): 1310–1320.
[21] Singh, G., And Supriya. "A Study Of Encryption Algorithms (Rsa, Des, 3des And Aes) For Information Security." International Journal Of Computer Applications 67, No. 19 (2013): 33–38.
[22] Burr, W. "Selecting The Advanced Encryption Standard." Ieee Security & Privacy 1, No. 2 (2003): 43–52.
[23] Frunza, M., And Gh. Asachi. "Improved Rsa Encryption Algorithm For Increased Security Of Wireless Networks." In Isscs International Symposium (Vol. 2), 2007.
[24] Kodali, R., And N. Sarma. "Energy Efficient Ecc Encryption Using Ecdh." In Lecture Notes In Electrical Engineering (Vol. 248), 471–478, Springer, 2013.
[25] Johnson, D., A. Menezes, And S. Vanstone. "The Elliptic Curve Digital Signature Algorithm (Ecdsa)." International Journal Of Information Security 1, No. 1 (2001): 36–63.
[26] Balitanas, M. "Wifi Protected Access-Pre-Shared Key Hybrid Algorithm." International Journal Of Advanced Science And Technology 12 (2009).
[27] Misic, E., And V. Misic. Wireless Personal Area Networks: Performance, Interconnections, And Security (Ieee 802.15.4). John Wiley & Sons Ltd, 2008.
[28] Nidarsh, M. P., And M. G. P. Devi. "Chaos-Based Secured Communication In Energy-Efficient Wireless Sensor Networks." Chaos 5, No. 6 (2018): 742–747.
[29] Sobhy, M. I., And A.-E. Shehata. "Methods Of Attacking Chaotic Encryption And Countermeasures." In Proceedings Of The 2001 Ieee International Conference On Acoustics, Speech, And Signal Processing, 1001–1004. Ieee, 2001.
[30] Zhang, X., And X. Wang. "Digital Image Encryption Algorithm Based On Elliptic Curve Public Cryptosystem." Ieee Access 6 (2018): 70025–70034.
[31] Panda, M. "Security In Wireless Sensor Networks Using Cryptography Techniques." American Journal Of Engineering Research (Ajer) 3 (2014): 50–56.
[32] Rajput, M., And U. Ghawte. "Security Challenges In Wireless Sensor Networks." International Journal Of Computer Applications 168 (2017): 24–29.
[33] Yetgin, H., K. T. K. Cheung, M. El-Hajjar, And L. H. Hanzo. "A Survey Of Network Lifetime Maximization Techniques In Wireless Sensor Networks." Ieee Communications Surveys & Tutorials 19, No. 2 (2017): 828–854.
[34] Gyrard, A., And M. Serrano. "Connected Smart Cities: Interoperability With Seg 3.0 For The Internet Of Things." In 2016 30th International Conference On Advanced Information Networking And Applications Workshops (Waina), 796-802, 2016.
[35] Pitchaiah, M., P. Daniel, And Praveen. "Implementation Of Advanced Encryption Standard Algorithm." International Journal Of Scientific And Engineering Research 3, No. 3 (2012).
[36] De, S., P. Barnaghi, M. Bauer, And S. Meissner. "Service Modelling For The Internet Of Things." In Federated Conference On Computer Science And Information Systems (Fedcsis), 949–955, 2011.
[37] Subasree, S., And N. K. Sakthivel. "Design Of A New Security Protocol Using Hybrid Cryptography Algorithms." International Journal Of Recent Research And Applied Studies (Ijrras) 2, No. 2 (2010): 95–103.
[38] Kumar, N. A Secure Communication Wireless Sensor Networks Through Hybrid (Aes+Ecc) Algorithm. Vol. 386. Lap Lambert Academic Publishing, Koln, Germany, 2012.
[39] Aspect. Ac095: Initial Report On Security Requirements. February 1996.
[40] Gundlach, M. "A Security Architecture For Upt." In International Conference On Universal Personal Communications, September 1994.
[41] Karlof, C., And D. Wagner. "Secure Routing In Sensor Networks: Attacks And Countermeasures." In Proceedings Of The First Ieee International Workshop On Sensor Network Protocols And Applications, 2003.
[42] Di Pietro, R., Et Al. "Data Security In Unattended Wireless Sensor Networks." Ieee Transactions On Computers 58, No. 11 (2009): 1500–1511.
[43] Eschenauer, L., And V. D. Gligor. "A Key Management Scheme For Distributed Sensor Networks." In Proceedings Of The 9th Acm Conference On Computer And Communications Security, 41–47, 2002.
[44] Song, H., S. Zhu, And G. Cao. "Attack-Resilient Time Synchronization For Wireless Sensor Networks." In Ieee International Conference On Mobile Adhoc And Sensor Systems Conference, 2005.
[45] Dutta, A., K. N. Kumar, N. Sai, And R. R. Chintala. "An Efficient Lightweight Cryptography Algorithm Scheme For Wsn Devices Using Chaotic Map And Ge." International Journal Of Pure And Applied Mathematics 118, No. 20 (2018): 861–875.
[46] Du, X., Et Al. "Secure And Efficient Time Synchronization In Heterogeneous Sensor Networks." Ieee Transactions On Vehicular Technology 57, No. 4 (2008): 2387–2394.
[47] Zhang, W., S. Zhu, And G. Cao. "Pre-Distribution And Local Collaboration-Based Group Rekeying For Wireless Sensor Networks." Ad Hoc Networks 7, No. 6 (2009): 1229–1242.
[48] Gura, N., Et Al. "Comparing Elliptic Curve Cryptography And Rsa On 8-Bit Cpus." In 2004 Workshop On Cryptographic Hardware And Embedded Systems, 2004.

[49] Watro, R., Et Al. "Tinypk: Securing Sensor Networks With Public Key Technology." In Proceedings Of The 2nd Acm Workshop On Security Of Ad Hoc And Sensor Networks (Sasn '04), 59–64. Acm Press, 2004.
[50] Ni, Z., Et Al. "Reversible Data Hiding." Ieee Transaction On Circuits Systems For Video Technology 16, No. 3 (2006): 354–362.
[51] Yang, Y., And M. Cardei. "Movement-Assisted Sensor Redeployment Scheme For Network Lifetime Increase." In Proceedings Of The 10th Acm Symposium On Modeling, Analysis, And Simulation Of Wireless And Mobile Systems, 2007.
[52] Dvir, A., Et Al. "Stwsn: A Novel Secure Distributed Transport Protocol For Wireless Sensor Networks." International Journal Of Communication System 31, No. 18 (2018): E3827.
[53] Zhenghong, X., And Zhigang, C. "A Secure Routing Protocol With Intrusion Detection For Clustering Wireless Sensor Networks." In International Forum On Information Technology And Applications, 2010.
[54] Shu, T., M. Krunz, And S. Liu. "Secure Data Collection In Wireless Sensor Networks Using Randomized Dispersive Routes." Ieee Transactions On Mobile Computing 9, No. 7 (2010): 941–954.
[55] Chen, S., G. Yang, And S. Chen. "A Security Routing Mechanism Against Sybil Attack For Wireless Sensor Networks." In International Conference On Communications And Mobile Computing, 2010.
[56] Modirkhazeni, A., N. Ithnin, And O. Ibrahim. "Secure Multipath Routing Protocols In Wireless Sensor Networks: A Security Survey Analysis." In Second International Conference On Network Applications, Protocols And Services, 2010.
[57] Tripathy, A., Et Al. "Hybrid Cryptography For Data Security In Wireless Sensor Network." In Data Engineering And Intelligent Computing. Advances In Intelligent Systems And Computing, Edited By V. Bhateja, S. C. Satapathy, C. M. Travieso-González, And V. N. M. Aradhya, 1407. Springer, Singapore, 2021.
[58] Sachin, L., S. Bhushan, And Surender. "Hybrid Encryption Algorithm To Detect Clone Node Attack In Wireless Sensor Network." In Proceedings Of The International Conference On Innovative Computing & Communications, 1-6, 2020.
[59] Anwar, M. N. B., And M. M. M. Maha. "Ampc: A Lightweight Hybrid Cryptographic Algorithm For Wireless Sensor Networks." International Journal Of Innovative Science And Research Technology 5, No. 6 (2020): 1142-1146.