POLITECNICO DI TORINO

MASTER OF SCIENCE IN COMMUNICATIONS AND COMPUTER NETWORKS ENGINEERING

MASTER'S THESIS TITLE

SECURITY ANALYSIS OF WIRELESS SENSOR NETWORKS

(IN HEALTHCARE APPLICATIONS)

Academic Candidate:
Supervisor: Prof. LADISLAU MATEKOVITS

Advisor:
Nasser Karimi (S274302)

APRIL 2023

Introduction :

Background:

Wireless sensor networks (WSNs) have been gaining significant attention in recent years due to their wide range of applications, including environmental monitoring, device monitoring, traffic control, and intelligent homes. These networks consist of distributed sensor nodes that operate independently or collaboratively to collect environmental data and transmit it to a base station or remote server for further analysis. WSNs are characterized by their wireless sensors that support mobility, reliability, and broad dispersion, making them suitable for various scenarios.

Wireless body area networks (WBANs) have also gained immense popularity due to their potential to monitor a patient's health remotely using wireless sensor nodes on their body. WBANs can measure physiological parameters such as blood pressure, body temperature, heart rate, and blood sugar level. They can be either wearable or implantable, making them an ideal option for patients. The primary objective of WBANs is to ensure people's well-being by providing medical servers with physiological information from sensors on the body, allowing doctors to analyze the patient's health status.

However, as the use of WBANs becomes more prevalent, there is a growing concern about the security of the data collected. Patients' health data are very sensitive, and it is crucial to prevent unauthorized access to them. To ensure the data's protection, it is necessary to use encryption, secure communication protocols, and access control mechanisms. These measures help to make sure that only authorized individuals can access the data, and that the data remains confidential and secure.

Security issues and data protection:

The primary objective of my thesis was to identify security issues in wireless sensor networks in healthcare (WMSNs) and propose secure ways to protect them from unauthenticated access. Specifically, the unique features of WBANs, such as their star topology architecture with a sinkhole located in the body to collect information from nodes, present unique security challenges, such as the potential for unauthorized access to the sinkhole. These challenges must be addressed to ensure the confidentiality, integrity, and availability of the data. Moreover, the limited infrastructure and power of WBAN systems make it challenging to implement security measures, especially those related to authentication. Therefore, my work focused on proposing an automatic and user-friendly authentication process that relies minimally on cryptography. To achieve this, I conducted a comprehensive literature review to identify potential security threats and evaluated the effectiveness of existing security mechanisms. Additionally, I proposed a security protocol to enhance the security of WMSNs and tested their effectiveness using security verification tools such as Scyther and AVISPA. Moreover, I conducted simulations to test the proposed security protocols. This involved searching, learning, and writing the code to simulate the protocols and evaluate their effectiveness. The simulations were performed using a variety of scenarios to validate the proposed protocols in a controlled environment.

Structure of the thesis:

Chapter 1 provides an introduction to wireless medical sensor networks, including their architecture and various tiers. It also discusses the different types of medical sensors used in these networks and their constraints and limitations, such as memory, bandwidth, energy capacity, and computation capacity. Furthermore, it discusses the security requirements for wireless medical sensor networks, including data originality, confidentiality, integrity, availability, freshness, authentication, secure management, dependability, safe positioning, accountability, flexibility, privacy, and compliance. Finally, it outlines the different types of security threats and attacks faced by wireless medical sensor networks, along with the various security mechanisms used to mitigate these threats, such as cryptography, key management, secure routing, trust management, and blockchain technology.

Chapter 2 focuses on data protection during transmission, building on the concepts introduced in Chapter 1. It provides an overview of previous studies conducted in this area and discusses the different security methods used to protect wireless body area networks (WBANs). In particular, it examines cryptographic authentication methods, including those that rely on biometric data and unique characteristics. It then goes on to propose a new security protocol for wireless medical sensor networks and provides a detailed specification of the protocol, including cryptographic primitives election.

Chapter 3 discusses the testing and outcomes of the proposed security protocol. It provides an overview of two popular protocol verification tools, Scyther and AVISPA, and discusses the results of the security analysis conducted using these tools. The chapter then concludes by summarizing the main findings of the study and discussing their implications for future research.

Chapter 1:

Wireless Medical Sensor Networks :

Wireless Body Sensor Networks (WBSNs) are a type of wireless network that involve tiny biomedical nodes distributed on the body surface, underneath the skin, inside the body, or in the vicinity of the body. These networks are also known as WBANs, and they are specifically designed for healthcare applications. WBSNs are made up of small sensors that capture physiological signals, which can include vital signs, movement, and location data. The sensors in WBSNs communicate with each other and with a central device or gateway that is connected to a hospital or healthcare provider's network. This allows physicians and other medical professionals to remotely monitor patients and receive alerts in real-time, improving their ability to provide timely and effective medical interventions. The ability to monitor patients continuously, even when they are at home or on the move, can be especially valuable in managing chronic conditions, such as diabetes or heart disease.

WBSN nodes, due to their small size and low power consumption, are a promising technology for use in wearable devices. These sensors can be easily integrated into clothing, jewelry, or other accessories, enabling patients to track their own health and activity levels, and share this data with their healthcare providers. Additionally, WBSNs have the potential to be utilized in healthcare facilities to monitor the health and safety of patients and staff, as well as improve the overall quality of patient care.

The design of WBSNs is a challenging task due to the limited energy resources of the sensor nodes, the need for reliable and secure data communication, and the need for high accuracy and precision in capturing physiological data. Researchers and engineers have addressed these challenges by developing advanced algorithms, protocols, and hardware components, such as low-power radio transceivers, energy-harvesting techniques, and efficient data compression and encryption schemes.

WBSNs have significant potential in the healthcare sector, with remote patient monitoring being a critical application. Patients with chronic illnesses can be monitored from home, reducing the need for frequent hospital visits. In emergencies, WBSNs can provide timely and accurate medical information to first responders, improving their ability to provide life-saving interventions. By enabling continuous monitoring and management of patient health, WBSNs have the potential to transform healthcare, improving patient outcomes, reducing costs, and increasing the effectiveness of medical interventions. However, certain challenges must be overcome, including ensuring data security and privacy, developing interoperability standards, and addressing data ownership and sharing issues.

In today's world, sensor networks are revolutionizing healthcare by monitoring physical well-being and identifying disease occurrence. These networks can help reduce costs and risks throughout the therapeutic process. Sophisticated medical facilities currently employ basic sensor technology to oversee patient vital signs, monitor drug regimens, and track interactions between doctors and patients on-site. By integrating sensor networks, it is possible to remotely monitor patients' health in some instances. Although remote monitoring systems are still in their early stages of development, they hold great potential for accurately determining one's physical condition, especially as technology continues to advance and broadband technology is increasingly utilized.

An essential area where sensor networks are proving to be useful in the healthcare industry is in elderly care. A sophisticated system of sensor cameras can identify muscle movements, falls, unconsciousness, vital signs, dietary habits, and physical activity levels. The real-time health assessments provided by this technology can potentially compensate for delays in detecting

degenerative diseases, resulting in saved lives and reduced healthcare expenses. Despite their compact size, surveillance sensors equipped with ultrawideband technology can transmit large amounts of information that can greatly enhance medical services, improve healthcare outcomes, minimize treatment expenses, and aid in the prevention of illnesses.
In summary, WBSNs represent a highly promising technology with the potential to revolutionize healthcare. They provide patients with greater convenience, flexibility, and accuracy in monitoring their health, while also enabling new forms of medical interventions and treatments. As further advancements are made in this area, we can anticipate even more innovative and groundbreaking applications of WBSNs in healthcare and beyond.

Architecture

The literature reveals various architectures of WMSNs in IoT environments, depending on the application domain and approach. However, all the works in the literature share a common three-tier architecture that is present in every WMSN implementation. This fundamental architecture is a prerequisite for any e-health application based on WMSN under an IoT environment.
The architecture of wireless medical sensor networks is depicted in Fig. 1, which comprises three primary tiers:

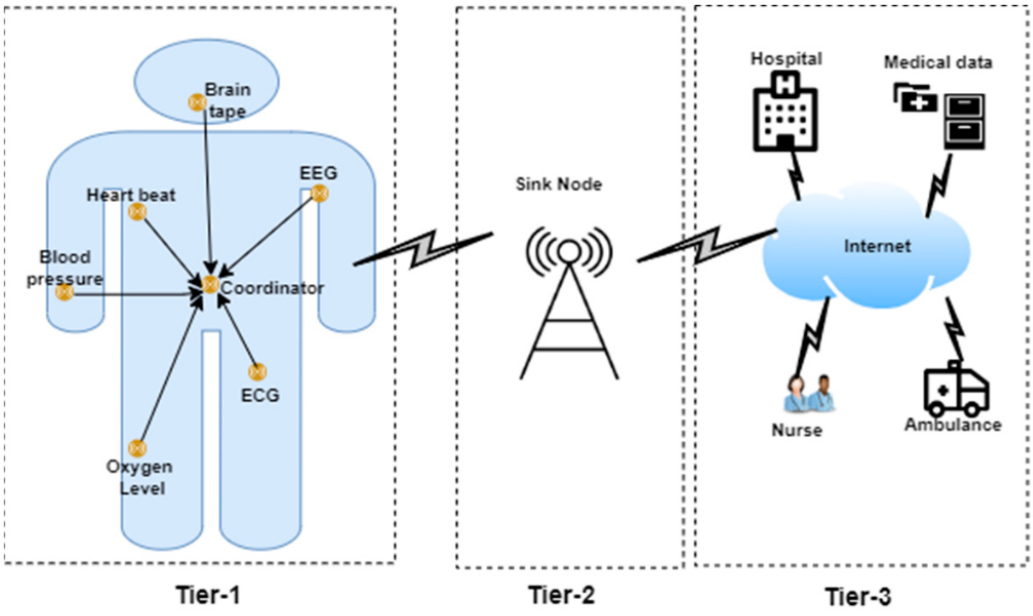

Figure 1: The architecture of WBSN [17]

Tier 1:
This tier consists of medical sensors, which can continuously measure, monitor and collect specific biological signals. The data collected by these sensors are then transmitted to level 2 devices.

Tier 2:
This tier is represented by gateways, such as personal digital assistants (PDAs), computers, smartphones, etc., that serve as the intermediary between level 1 and level 3 devices. They are responsible for transmitting the collected data from level 1 nodes to end-users in level 3 via open channels.

Tier 3:
At this tier, the received data and information from tier 2 devices are transmitted to end-users via the Internet. The type of end-users can vary depending on the WMSN design, such as cloud servers, emergency physicians, professionals, service providers, data analysts, family members, or even the patients themselves.

Wireless Communication Technologies :
Communication network technology has a crucial role in body sensor networks as it deals with sensitive data related to the vital signs of the human body. Maintaining interference-free communication channels is essential to ensure accurate monitoring of the human health condition. Here, is several wireless technologies utilized in body sensor networks:

Bluetooth Technology :
Bluetooth is a widely adopted standardized protocol used for short-range communication that is cost-effective, low energy-consuming, and does not require wires. The primary technology behind Bluetooth is radio waves, which makes it an excellent choice for body sensor networks. Fig. 2 has demonstrated that Bluetooth is an optimal technology that facilitates the monitoring of human body information. With the installation of a small Bluetooth chip in systems, a personal wireless network is created, allowing for seamless communication with other nearby user devices.

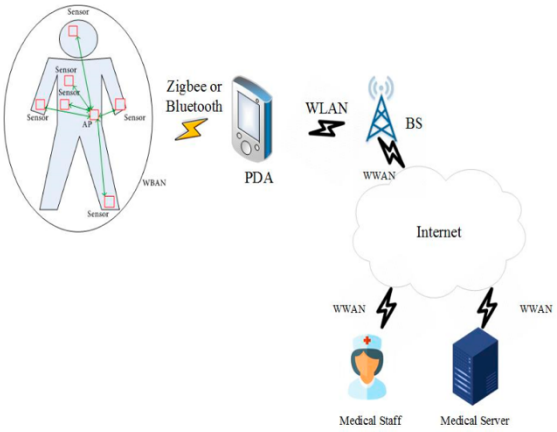

Figure 2: Bluetooth technology in WBSN[17]

ZigBee technology:
This technology is well-suited for use in WBANs due to its low power consumption, ability to support multiple devices, and low data rate. This technology enables long battery life in body-worn sensor devices, which is beneficial in reducing the need for frequent battery replacements or recharging. The low data rate is appropriate for transmitting vital signs and health-related data that do not require high bandwidth. ZigBee's mesh networking allows for self-organizing and self-healing networks, making it perfect for dynamic environments. The encryption in the ZigBee protocol provides security to sensitive data transmitted within the network, making it a suitable option for medical and healthcare applications.

Ultrawideband (UWB) :
UWB is another wireless technology that can be used in WBANs. It is well-suited for transmitting large amounts of data quickly and reliably, such as real-time physiological signals from body-worn sensors. However, its implementation in WBANs may be limited due to the lack of widely available UWB wireless components.

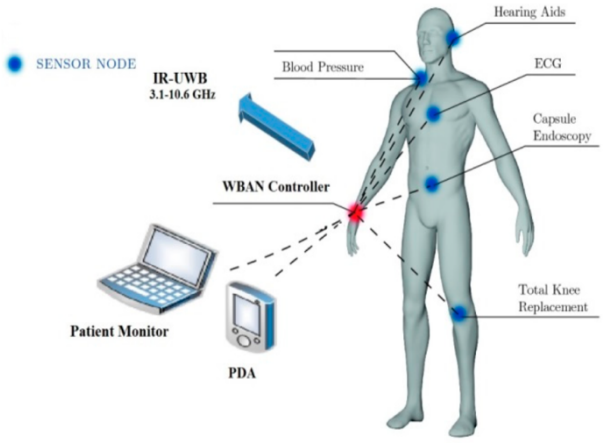

Figure 3: UWB technology in WBSN[17]

Medical Sensors:

Medical IoT sensors are specialized sensors utilized to measure and monitor physiological metrics like body temperature, blood pressure, heart rate, electroencephalogram (EEG), and electrocardiogram (ECG). These sensors transfer the recorded biological information to a wearable control device placed on the body or in an accessible location. Medical sensors can be categorized as implanted nodes, clothes-attached, or body surface nodes (wearables) and have varied uses. As it pertains to the human body, medical IoT sensors are predominantly utilized in healthcare and medical applications. Various types of medical sensors exist based on their intended functions, such as Electrocardiogram (ECG) sensors: These sensors measure the electrical activity of the heart and can help diagnose heart conditions such as arrhythmia and heart attack.
Pulse oximeters: These sensors measure the oxygen saturation level in the blood and are commonly used to monitor patients with respiratory conditions such as COPD.
Blood glucose sensors: These sensors are used to monitor blood glucose levels in patients with diabetes.
Blood pressure sensors: These sensors are used to measure blood pressure and can help diagnose hypertension and other cardiovascular conditions.
Temperature sensors**:** These sensors can be used to monitor body temperature and can help diagnose fever and other conditions.
Respiratory rate sensors: These sensors can be used to monitor the breathing rate of patients with respiratory conditions such as asthma and COPD.
Motion sensors: These sensors can be used to monitor patient movement and activity levels, and can help assess mobility and rehabilitation progress.

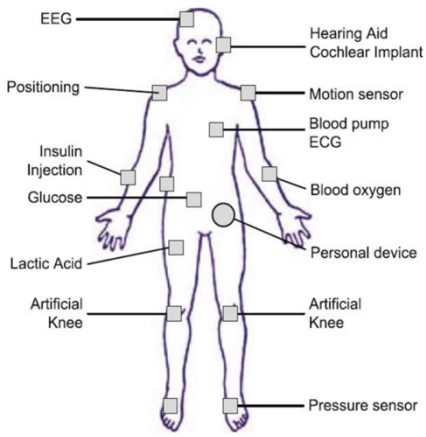

Figure 4: Patient monitoring[22]

Constraints and limitations:

Medical sensors have several constraints and limitations. It is important to consider these limitations when developing or using medical sensor systems. Some of the primary limitations of medical sensors include:

Memory: The memory capacity of medical sensors is limited and typically ranges from a few to several kilobytes. Similarly, the storage capacity of these devices is also limited, requiring only essential data to be stored for implementing communication and security protocols.

Bandwidth: the limited bandwidth of medical IoT devices restricts the amount of data that can be transmitted and the speed of transmission. This can be a significant challenge when dealing with large amounts of data, such as high-resolution images or video. Therefore, it is essential to optimize the communication protocols and the amount of data transmitted to ensure efficient use of the available bandwidth.

Energy capacity: energy capacity is a critical limitation of medical sensors as they rely on batteries with limited energy. The sensors need to operate for extended periods without recharging or replacing the batteries. Therefore, energy efficiency is a significant concern for these devices, and the design of these sensors should take into account the power consumption to extend their battery life.

Computation capacity: this is an important limitation to consider for medical IoT sensors. These sensors typically have limited computing power, which can affect their ability to process data efficiently. As a result, it is important to use lightweight communication and security protocols that can operate on these devices without consuming too many computational resources. Additionally, the data collected by these sensors should be pre-processed on the device itself to reduce the amount of data that needs to be transmitted, thus conserving energy and bandwidth.
Taking into account the aforementioned restrictions, medical IoT sensors can be classified based on their functionalities. The Internet Engineering Task Force (IETF) has developed a system for categorizing resource-limited IoT devices, including medical sensors. We concentrate our attention on medical sensors that fall under class 1 and class 2 since they are

the only ones that provide security features and possess adequate power to operate a protocol stack specially designed for medical sensors.

Security in WMSN :

The physiological signals of patients are captured by sensor nodes through the body control unit (BCU), making message transmission among network members a crucial factor in ensuring patients' physical well-being. However, without a robust security mechanism, the system may be vulnerable to hacking attempts. Attackers have the ability to intercept and tamper with the information exchanged between the sensors and the Patient's Digital Assistant (PDA), creating a breach in the system's security. Therefore, it is imperative to incorporate measures that give the utmost importance to data authenticity, privacy, confidentiality, and integrity during the system's development phase.

WMSN security requirement:

The following are some of the critical security needs that must be addressed to safeguard the integrity, privacy, and confidentiality of patient data:

Data originality: Is essential for WMSNs to ensure the integrity and reliability of the data being transmitted. Verification and licensing services are necessary to achieve this. In WMSNs, authentication mechanisms must be employed for each sensor and base station to verify the authenticity of the data transmitted. This guarantees that the data is accurate and reliable, preventing incorrect diagnoses and inappropriate treatment decisions. By using authentication mechanisms, the confidentiality and privacy of patient data can also be safeguarded, ensuring that it is not compromised during transmission.

Data confidentiality: In WMSNs, the wireless channel is susceptible to eavesdropping by attackers, who can intercept sensitive information being transmitted between nodes. This can lead to the unauthorized disclosure of patient information to unauthorized parties. To prevent this, it is crucial to encrypt the data before transmission to ensure that only authorized parties can access and understand the data. Encryption techniques are used to protect patient confidentiality by keeping the data secure during transmission, preventing it from being accessed by potential attackers.

Data integrity: It is crucial in ensuring that patient data is not tampered with during transmission. When data is intercepted and modified by attackers, it can lead to system failures and put patients at risk of injury. Therefore, it is important to implement measures that can prevent data tampering during transmission. One way to achieve this is by using data integrity checks that verify the authenticity of the data received at the destination. These checks compare the data received with the data that was originally transmitted to ensure that no modifications or alterations have been made to the data. By implementing data integrity measures, healthcare providers can ensure that the patient data they receive is accurate and trustworthy, allowing them to make informed decisions about patient care.

Data availability: The availability of medical sensor nodes is essential in ensuring that health data is continuously accessible for medical care purposes. However, if an unauthorized individual captures a sensor node, data access may be lost, leading to significant challenges in

providing medical care services. Therefore, it is necessary to maintain accessibility in medical care applications to guarantee that medical professionals have uninterrupted access to critical patient data.
Data freshness: The freshness technique prevents attackers from recycling old data by implementing measures that prevent data recording, replaying, and publishing by the attacker node. By ensuring that the data being transmitted is fresh and has not been tampered with, WMSNs can guarantee the accuracy and reliability of the data, leading to improved patient care outcomes. In medical care applications, fresh and accurate data is necessary for healthcare professionals to provide timely and effective treatment decisions to patients.

Data authentication: By implementing an authentication system, every node has the capability to recognize and verify the identity of the nodes that provide it with data, ensuring that the data is legitimate and not tampered with by unauthorized parties. By implementing data authentication, WMSNs can ensure that sensitive patient data is accessed and exchanged only by authorized nodes, leading to improved patient privacy and security.

Secure management: The coordinator can use various methods to securely distribute keys, such as the use of encryption, secure communication channels, and secure authentication protocols. Additionally, the coordinator can ensure that the keys are revoked when necessary to prevent unauthorized access to the network and its data. By utilizing a coordinator and implementing secure key management practices, WBANs can help ensure that the sensitive data transmitted and received by the network remains secure and protected from unauthorized access.

Dependability: Error coding is a technique that involves adding redundant data to the transmitted data, allowing the receiver to detect and correct any errors that may have occurred during transmission. This technique can be particularly useful in WMSNs where the data being transmitted may be subject to noise or interference from the wireless medium. By implementing error coding, WMSNs can help ensure the accuracy and reliability of the data transmitted and received by the network, which is particularly important in applications such as medical monitoring, where errors in the data could have serious consequences. Additionally, error coding can help improve the dependability of the network by reducing the likelihood of data loss or corruption due to errors in transmission.

Safe positioning: movements and updates to the patient's location can also provide an opportunity for attackers to enter fake signals and information into the location registration system, compromising patient privacy and security. To prevent this, secure authentication and encryption protocols can be implemented to ensure that only authorized devices are able to update the patient's location information. Additionally, regular monitoring and detection mechanisms can be put in place to identify any suspicious activity or attempts at unauthorized access to the location registration system. Ensuring the safe positioning of patients in WBANs is crucial for maintaining the privacy and security of the patient's data and preventing unauthorized access or manipulation of the location information. By implementing appropriate security measures, WBANs can help to ensure the safe and reliable tracking of patient location data.

Accountability: Healthcare providers and staff must recognize the importance of safeguarding patient information and take appropriate measures to ensure its protection. Any unauthorized use or disclosure of patient information can have serious consequences, and those responsible for such breaches must be held accountable. Therefore, it is essential to establish clear policies

and procedures for the management and protection of patient data and to regularly monitor and review these measures to ensure their effectiveness.

Flexibility: In emergencies, patients may require their information to be shared with a second person or hospital. Therefore, the system must provide a secure and efficient means of sharing this information with authorized parties while ensuring the confidentiality and integrity of the data. It is crucial to establish clear policies and procedures for sharing patient information, as well as mechanisms for obtaining patient consent and controlling access to their data.

Privacy and Compliance: Protecting the personal and sensitive data of patients is of utmost importance. To ensure this, international regulations and guidelines have been established, including the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Non-compliance with these regulations can result in serious civil and criminal consequences, including fines and imprisonment. It is the responsibility of healthcare providers to adhere to these guidelines and safeguard the privacy of patient information.

Data authenticity: In wireless medical sensor networks, it is important to verify the authenticity of data and ensure it comes from a trustworthy source. Authentication techniques like public and private keys can be used to achieve this. Public keys encrypt the data while private keys decrypt it, ensuring that only authorized entities can access the data and that the data hasn't been altered by unauthorized sources. Authenticating the data is critical to ensuring the reliability and accuracy of medical information, which is crucial for patient care and treatment.

Data authorization: To control user access to network resources and services, the authorization method is essential. A combination of an access control list (ACL) and an access policy can enable precise control of user access to network resources and services. This is particularly important in healthcare settings where sensitive patient data must be protected from unauthorized access.

Security Threats :

Patient privacy is a paramount concern in the surveillance and monitoring of vital signs in body sensor networks. Attackers can engage in eavesdropping on communication channels, resulting in the unauthorized disclosure of sensitive patient information. By utilizing powerful receiver antennas, attackers can intercept network communications and obtain critical details such as message IDs, time tags, source and destination addresses, and even the physical location of the patient. This information can then be maliciously manipulated to cause physical harm. Such eavesdropping activities pose significant threats to the privacy and security of patients. Furthermore, wireless networks, which are commonly used for communication in medical IoT sensor systems, are not inherently limited in their communication range and are susceptible to vulnerabilities during transmission. This leaves room for potential information threats. Attackers could intercept and modify patient and environmental data being transmitted from medical IoT sensors to the physician and hospital server. This unauthorized manipulation of data could include altering physiological information, which could then be directed to a server, posing a grave risk to the patient's life. Hence, it is of utmost importance to implement robust security measures to ensure the confidentiality, integrity, authenticity, and privacy of patients' data throughout the entire transmission process.

Different Types of Attacks :

Interception: an attacker gains access to the wireless communication channel used to transmit vital signs data between a patient and a healthcare provider. The attacker can then intercept this data, which may include sensitive information such as the patient's medical history, location, or other personal information.
Message change: It is a type of attack in which an unauthorized entity intercepts a message and alters its content before delivering it to the intended recipient. This type of attack is particularly concerning in healthcare settings, as it can lead to the delivery of incorrect medical information or instructions, which can be harmful to the patient's health. For instance, an attacker may alter a prescription for medication, leading to adverse health effects. Therefore, it is essential to employ measures such as encryption and digital signatures to ensure the integrity and authenticity of messages in healthcare communication.
Wireless sensor routing threats: These refer to malicious activities that occur at the network layer of wireless sensor networks. These threats can involve actions such as stealing or modifying packets and forwarding them to the remote control center, potentially triggering false alarms. Attackers may also manipulate the address field of captured packets to disrupt the correct routing path or create routing loops, which can disrupt the entire network. These attacks can compromise the integrity and confidentiality of the transmitted data. Therefore, it is crucial to implement effective security measures to safeguard against routing threats in wireless sensor networks.

Security Mechanisms

Cryptography:

Cryptography is a critical aspect of ensuring the security and privacy of sensitive information in WBANs. It involves using mathematical algorithms to encode data, preventing unauthorized access and manipulation of data transmitted between network nodes. Selecting the appropriate encryption method for WBANs requires consideration of factors such as energy and memory requirements, runtime, and sensor node capabilities. Asymmetric cryptography methods are generally more secure but computationally expensive, while symmetric cryptography methods are more efficient but less secure. Hybrid approaches and lightweight encryption algorithms may provide a balance between security and resource consumption. Proper implementation of cryptography can ensure the confidentiality, integrity, and authenticity of data transmitted and received by the network. Cryptography can also be used for secure key distribution and management, preventing unauthorized access to sensitive data. Overall, cryptography plays a vital role in the security of WBANs, and its proper implementation is crucial to protecting sensitive patient data.

Key management :

Key management is an essential part of any encryption system, and it involves all aspects of key generation, distribution, storage, and revocation. The effectiveness of a cryptographic system can be significantly impacted if key management is not done correctly. If keys are not properly managed, it can result in vulnerabilities and weaknesses in the system, even if the cryptographic algorithms and protocols used are strong. An attacker may be able to exploit

these weaknesses to compromise the security of the system. Therefore, it is crucial to ensure that keys are generated securely, exchanged only with authorized parties, and stored securely. The design of key management systems should also take into account the potential risks and threats to the system. This includes the risks associated with the loss or theft of keys, as well as the risks associated with the compromise of keys due to attacks on the key management system itself.
Overall, a robust and reliable key management system is essential to ensure the security of information exchanges in any cryptographic system, including those used in WBANs.

Secure routing:
Secure routing is an essential aspect of wireless sensor networks, including WBANs, as it ensures that data is transmitted to the correct destination and is not intercepted or manipulated by malicious nodes. Routing protocols that are designed with security in mind should be used to prevent attacks such as denial-of-service attacks and malicious routing data insertion. In the case of WBANs, mobility, and dynamism must also be taken into account when designing routing protocols, as the requirements of real-time medical applications may add additional complexity. It is important to consider the security requirements of the specific application when selecting a routing protocol for a WBAN, as the level of security needed may vary depending on the sensitivity of the data being transmitted.

Trust management: This is a crucial aspect of wireless sensor networks, including WBANs. Trust refers to the level of confidence and reliability that one node has in another node's behavior, which is crucial for establishing collaborative relationships between nodes. Trust management systems aim to evaluate the trustworthiness of nodes based on their past behavior and interactions with other nodes. In WBANs, where patient health data is transmitted, trust management systems can help ensure the privacy and security of sensitive information.
Trust management systems can use various mechanisms such as reputation-based systems, trust-based access control, and trust evaluation models to evaluate a node's trustworthiness. Reputation-based systems evaluate the reputation of a node based on its past behavior and the feedback received from other nodes. Trust-based access control allows only trusted nodes to access sensitive information. Trust evaluation models consider several factors, such as the node's behavior, its location, and its communication patterns, to assess its trustworthiness.
Effective trust management systems can enhance the security and reliability of wireless sensor networks, including WBANs. They can help detect and isolate malicious nodes, prevent unauthorized access to sensitive information, and maintain the integrity and availability of the network.

Blockchain technology:
Blockchain technology has been proposed as a solution to security and privacy issues in various applications, including WBANs. In the context of smart grids and WBANs, blockchain can provide secure and efficient management of data transactions and communications between different nodes. Blockchain's decentralized nature and use of cryptographic techniques make it resistant to malicious attacks and tampering, which enhances the security and privacy of WBANs. Additionally, the use of private and public keys in blockchain technology ensures secure and authentic communication between different nodes in the network. However, it is important to note that blockchain technology also requires significant computational resources, which may be a challenge for resource-constrained sensor nodes in WBANs.

Security Attacks on Wireless Sensor Networks:

The wireless sensor network is susceptible to various types of attacks due to the spreading nature of the transmission medium. These attacks can be categorized into two types, active and passive attacks.

Active attacks :
Active attacks are a serious concern in wireless sensor networks, including WBSNs, as they can compromise the integrity, authenticity, and confidentiality of the data. The attacker can modify the data, inject false data, or replay previously recorded data to create confusion and harm. Moreover, the attacker can compromise the entire network by impersonating a legitimate node and gaining access to sensitive information, which can lead to unauthorized control over the network.

Active Attacks on WSNs :

DoS Attack: A denial-of-service (DoS) attack is a type of cyber attack in which an attacker attempts to prevent legitimate users from accessing a network or system by overwhelming it with a flood of traffic or other malicious activity. In the context of wireless body area networks (WBANs), DoS attacks can disrupt the normal functioning of the network, preventing medical data from being transmitted, and potentially causing harm to the patient.
One type of DoS attack in WBANs is called the "jamming" attack. In this attack, the attacker floods the wireless spectrum with much noise or interference, making it difficult or impossible for legitimate data transmissions to occur. As a result, vital signs or other medical data from a patient's sensors may not be transmitted to the medical staff monitoring the patient, which can lead to serious medical consequences.
Another type of DoS attack in WBANs is the "sleep deprivation" attack. In this attack, the attacker targets the battery-powered sensors worn by the patient and continuously sends them wake-up signals, preventing them from entering low-power sleep modes and conserving energy. This can quickly drain the batteries and render the sensors useless, preventing the transmission of vital medical data. Overall, DoS attacks in WBANs pose a serious threat to the security and reliability of medical monitoring systems.

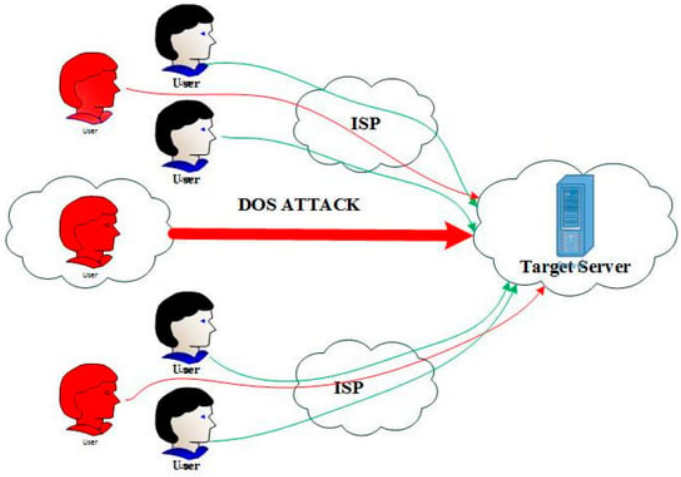

Figure 5:DOS attack[17]

Physical attacks:
Physical attacks are a serious threat to outdoor wireless networks due to their unsecured and scattered nature. Such attacks are more common in these networks than in wired ones. We can see that sensor node are frequently targeted and damaged by physical attacks, causing irreparable damage. An attacker can take advantage of physical access to steal sensitive data or manipulate software code to cause further harm.

Routing attacks:

Deceptive routing information :
This attack aims to divert the network traffic to a different path, which could lead to the creation of routing loops or suboptimal paths that degrade the network's performance.
The attacker can create false routing information by modifying the header information of the data packets that are being transmitted in the network. This can be done by altering the source or destination addresses, the hop counts, or other routing metrics. When other nodes receive this false routing information, they may use it to route their packets, leading to the propagation of the attack throughout the network.

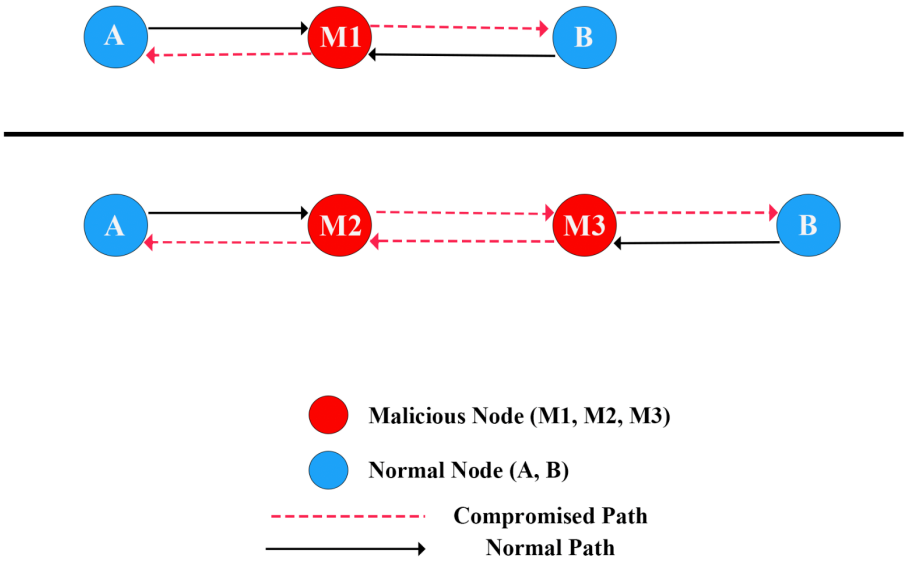

Figure 6: Deceptive routing information on WSN[17]

Blackhole attack :
In this scenario, a malicious node in the network falsely claims to have the shortest path to the sink node, which is the ultimate destination for the data collected by the network. Once the attacker convinces other nodes in the network that it has the shortest path, it begins dropping or discarding all data packets forwarded to it. As a result, all packets sent toward the sink node are lost, which can cause significant damage to the network.
The blackhole attacker can use a variety of techniques to convince other nodes that it has the shortest path. For example, it can spoof routing messages, forge the hop count or sequence number of routing messages, or exploit the weaknesses in the routing protocols used by the network.

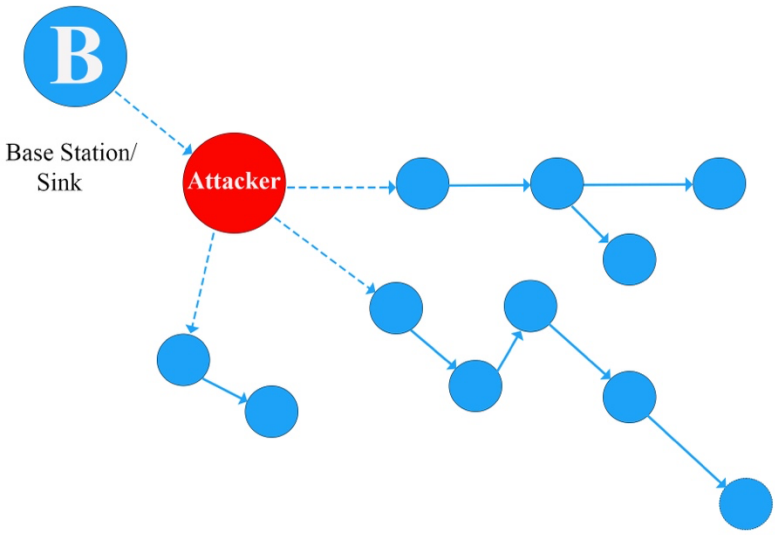

Figure 7: Blackhole attack[17].

Sybil attack :

Sybil attack is a security threat that can occur in WSN where a malicious node impersonates multiple identities in the network. The attacker creates several fake identities, called Sybil nodes, and uses them to manipulate the network's operations and data. These Sybil nodes can send false routing information, flood the network with false messages, or launch a Denial of Service (DoS) attack.

The Sybil attack can compromise the security and functionality of the WSN as the attacker can use multiple fake identities to gain control of the network or disrupt its operation. For instance, the attacker can use Sybil nodes to convince other nodes to route traffic through them, thereby intercepting and modifying the network traffic. The attacker can also use Sybil nodes to create a false view of the network topology, leading to incorrect routing decisions by legitimate nodes.

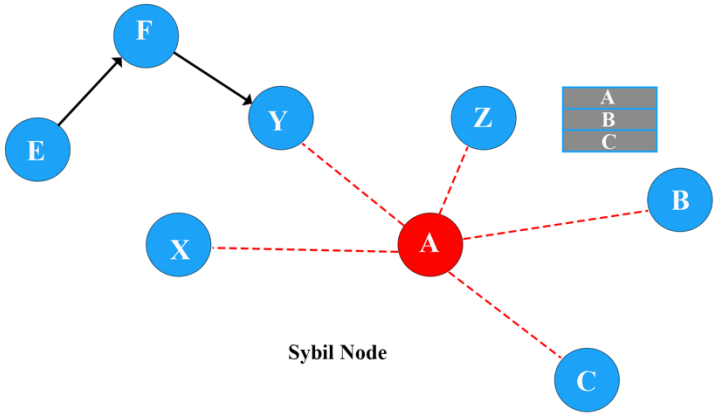

Figure 8: Sybil attack[17].

Wormhole attack:
A wormhole attack is a form of attack that can be carried out in wireless sensor networks (WSNs) by an attacker who captures and redirects packets from one part of the network to another. In this type of attack, the attacker creates a tunnel or a virtual link between two separate areas of the network, allowing them to bypass normal network routing mechanisms. By doing this, the attacker can compromise the network by disrupting the transmission of data, causing information to be lost, or even injecting malicious data into the network.

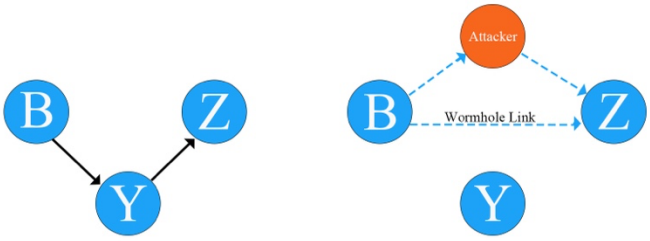

Figure 9: Wormhole attack[17].

Hello flood :
The Hello Flood attack is a simple yet effective attack on a WSN. The attacker uses a high-power Hello packet to flood the network and convince sensor nodes to extend their reach to a wider area. As a result, victim nodes may try to transmit their data through the attacker, mistaking it for a neighbor, leading to compromised node behavior and communication. This can ultimately result in the node being deceived by the attacker and cause further network vulnerabilities.

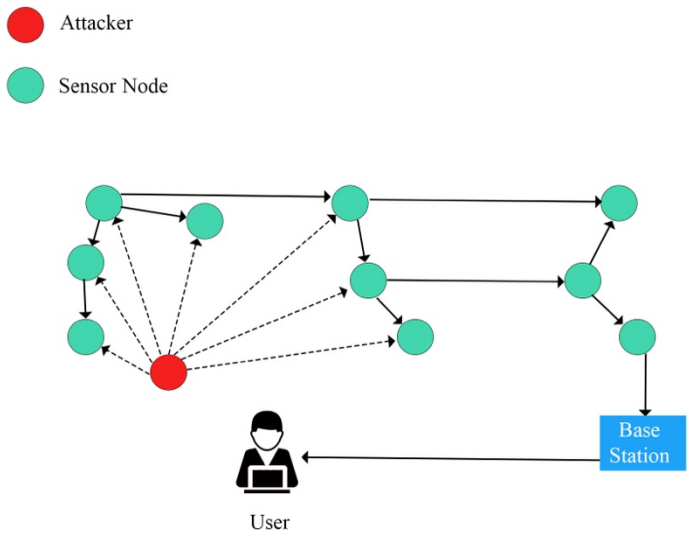

Figure 10: Hello flood attack[17].

Acknowledgment Spoofing:
Another type of attack in wireless sensor networks is where an attacker intercepts an acknowledgment message sent by a node and modifies its content before sending it back to the original sender. The attacker might use this technique to deceive the sender into believing that its message was successfully delivered to the destination node when in reality, it was not.

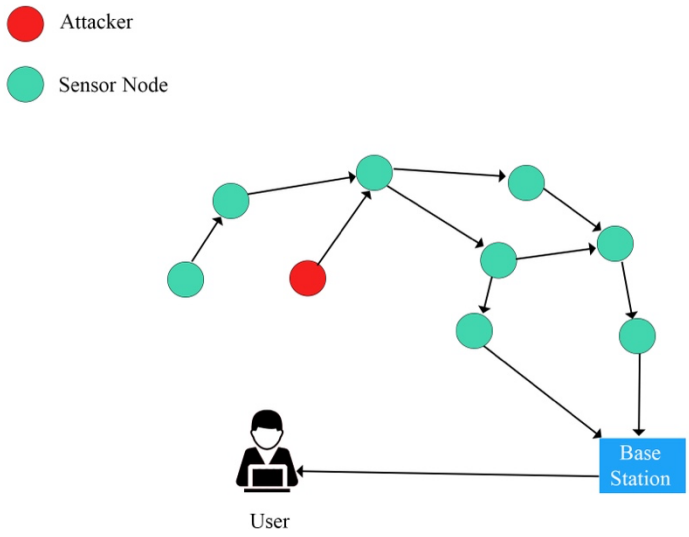

Figure 11:Acknowledgment spoofing attack[17].

Node reflection:
Node reflection attacks are a type of attack that targets the communication between nodes in a wireless sensor network. In this type of attack, an attacker creates a fake node that impersonates a legitimate node in the network. The attacker then sends a message to a legitimate node, making it appear as if the message is coming from another legitimate node in the network. The legitimate node receives the message and sends a response, but the response is sent back to the fake node instead of the legitimate node that originated the message. This allows the attacker to intercept and manipulate the communication between nodes, potentially leading to further attacks such as message interception, modification, or insertion.

Node Malfunction:
Node malfunction is a significant issue that can impact the reliability and availability of wireless sensor networks. When a node fails to function correctly, it can disrupt the network's operations, leading to data loss or interruption of communication links. Moreover, it can also cause network congestion, leading to increased latency and decreased throughput.
There are several reasons why a node may malfunction. It may be due to hardware or software failure, power outages, or physical damage to the node. These issues can cause the node to stop functioning, leading to the loss of critical data and network failure. Moreover, a malfunctioning node can also introduce vulnerabilities into the network, which can be exploited by attackers to launch further attacks.

Collecting Passive Information:
It refers to an attack where an unauthorized person can eavesdrop on the wireless sensor network's communication without actively participating in the transmission. They can analyze the captured data to gain insight into the specific content of messages, including physiological data, location, and other personal identifying information, without affecting the communication's propagation or location of the sensor nodes.

artificial node:
An artificial node (or false node) is a type of attack in wireless sensor networks where a malicious node falsely claims to be a part of the network and tries to perform malicious actions. This node may pretend to have sensor readings, send fake messages or even alter legitimate messages. Such nodes can disrupt the network operations by misguiding other nodes and causing wrong decisions to be made, leading to the failure of the intended task. Artificial nodes are a significant threat to wireless sensor networks, and various countermeasures, such as authentication and secure communication protocols, have been proposed to mitigate this type of attack.

Passive attacks:

Passive attacks are a type of cyber attack where the attacker monitors and eavesdrops on the network traffic to obtain sensitive information, without altering or modifying the data in any way. The attacker's goal is to intercept the information being transferred, which may include passwords, credit card numbers, or other confidential data. Passive attacks can be carried out using various methods, such as packet sniffing, network scanning, or traffic analysis. Packet sniffing involves intercepting and analyzing the network packets that contain the data being transmitted. Network scanning involves identifying and mapping the devices and services on the network, which can help the attacker identify potential vulnerabilities. Traffic analysis involves analyzing the patterns of data transfer to infer information about the communication patterns and the content being transmitted.
Passive attacks are difficult to detect since they do not alter the data, but they can be prevented by using encryption and authentication mechanisms to secure the data being transferred.

Attacks on The Physical Layer:

Congestion:
congestion attacks on the physical layer refer to a type of attack where an attacker intentionally causes congestion in the radio frequency (RF) spectrum used by the network, resulting in degraded network performance or even network failure. In a congestion attack, an attacker can generate high levels of interference that prevent the WBAN nodes from communicating with each other effectively. This interference can be created by transmitting high-power signals on the same channel used by the WBAN, or by jamming the channel with noise or other types of signals that degrade the signal-to-noise ratio (SNR) and reduce the effective range of the wireless communication. As a result of this attack, the sensor nodes may experience increased latency, dropped packets, reduced throughput, or complete communication breakdown, which can compromise the reliability and effectiveness of the WBAN. Additionally, congestion

attacks can cause additional power consumption and affect battery life, as the sensor nodes attempt to retransmit lost or corrupted packets.

Frequency transmission:
This attack is a technique used to combat unexpected congestion or interferences in wireless sensor networks. It involves using a sequence to change the transmission frequency, which is then reconstructed by the receiver to obtain the original message. This technique is resistant to noisy environments that can cause damage to the sensor network. However, the use of broad-spectrum systems in frequency transmission can be complex and expensive for the sensor nodes. Despite these challenges, frequency transmission remains an effective method for maintaining reliable communication in wireless sensor networks.

Frequency Jump:
This involves rapidly changing the frequency of transmission to evade detection or disrupt communication. This attack requires a high power source and is often associated with a high financial cost. It can be particularly effective in single-frequency networks, which are commonly used in wireless body area networks.
Preventing frequency jump attacks can be a difficult task, as many sensor networks cannot quickly adapt to changes in frequency. One approach to mitigating the effects of frequency jump attacks is through the use of jammed-area mapping, as proposed by Wood, Stankovic, and Son. This technique involves identifying and mapping the areas where congestion or interference is likely to occur, and then taking steps to minimize its impact. This may include using wider frequency ranges, more advanced encryption techniques, or other methods to increase the security of the network.

Tapping:
Tapping is a security threat that poses a risk to the physical layer of WBANs. This attack involves unauthorized access to network devices, which can create various issues. Attackers can potentially abduct or trap nodes, which can be challenging to identify due to the large number of nodes in the network. Additionally, the small and portable nature of the nodes makes them an easy target for attackers.
To address this issue, one potential solution is to regulate the physical temperature of the devices. This can help remove sensitive cryptographic information in response to tapping attempts. However, this approach can be costly and may not be suitable for all types of WBANs. Alternatively, using algorithms that reduce the impact of a single key factor on the network can be helpful. For instance, if each node has a key with its agents and neighbors, only a small part of the network will be affected if a single node is compromised.

Chapter 2:

Data protection during transmission:

For a WBAN to be considered secure, it must ensure secure transmission, authenticity, confidentiality, and data integrity. However, due to the inherent constraints and limitations of WBAN systems, implementing such measures can be a challenge. Authentication is a crucial feature of a network's security that involves communication between devices. In the past, the authentication process relied on pre-shared secret keys between nodes in a network. However, WBAN users typically lack security experience, which requires a highly usable authentication process, minimizes key distribution and management, and requires minimal user involvement, and is easy to use. The authentication approach for nodes in a WBAN shouldn't rely heavily on cryptography to ensure minimal dependence on it. Low-end medical sensors have limited resources, making it challenging to implement authentication mechanisms that rely on advanced hardware or cryptographic techniques. Therefore, non-cryptographic authentication mechanisms are often used, but they may require significant changes to the software of the system to ensure compatibility and usability.

Authentication of nodes in a WBAN is a critical issue that could potentially put the preservation of the privacy of the data transmitted between nodes in the network at risk. Therefore, this thesis uses a protocol that provides the necessary security features, including authentication, data protection, and data integrity, to safeguard a WBAN. The protocol offers an approach to WBAN node authentication that eliminates the need for pre-shared secrets between nodes. Instead, it utilizes a non-cryptographic method for sensor authentication protocol that employs cryptographic primitives as a means of ensuring the security of the data being transmitted, including digital signatures, hash functions, and the key encapsulation mechanism. This combination of non-cryptographic and cryptographic techniques enables the protocol to provide identity verification, privacy, and data integrity services to the WBAN network. Current protocols implemented in wireless body area networks (WBANs) rely heavily on cryptographic algorithms to provide protection against unauthorized access and data tampering. The most commonly used cryptographic algorithms in WBANs include digital signatures and encryption, key encapsulation mechanism (KEM), and hash functions. Cryptographic protocols offer a level of protection to the sensitive data being transmitted in WBANs, minimize the need for mutual trust, and improve the security posture of the network. Without these security services, WBANs can be vulnerable to attacks and compromise the privacy and confidentiality of the entire network.

Security verification tools play a crucial role in ensuring that protocols are capable of withstanding various types of attacks. These tools are designed to identify security or semantic vulnerabilities in the protocol design. There are different types of security verification tools available to formally verify a protocol's security properties. These tools check the use of cryptographic primitives in the protocol and assess the level of security they offer in different scenarios. By subjecting protocols to rigorous testing and verification, it is possible to detect and address any weaknesses or vulnerabilities, and thereby enhance the overall security of the protocol.

Previous Studies:

The security of medical devices is of utmost importance considering the private and sensitive nature of the data transmitted by these devices. The level of security required varies depending on the function of each device. Many medical devices are embedded and designed to be physically secure, but this can make them vulnerable to targeted cyberattacks. Attackers may attempt to access sensitive information by exploiting vulnerabilities such as sharing of secrets by someone who wants to attack or by saving or sharing private certificates, weak passwords, or putting them in a place that is easy to access, cryptography, and finally authentication that's weak. It is therefore necessary to implement strong security measures to protect these devices and the information they transmit. Various approaches have been suggested to ensure the security of Implantable Medical Devices (IMDs) through the use of protocols, systems, or cryptographic schemes. Security solutions for sensor network architecture in medical settings come in different forms. There are two main categories of studies on security techniques for authentication in WBAN: the first mechanism is cryptographic and the second one is non-cryptographic.
Mechanisms 1: Cryptographic authentication have been developed to meet the security requirements of medical scenarios within a sensor network architecture. These mechanisms use lightweight traditional cryptographic schemes.
Mechanism 2: Non-cryptographic authentication, on the other hand, uses non-cryptographic techniques to authenticate the devices in the WBAN. Non-cryptographic authentication approaches include physical authentication, such as fingerprint recognition, voice recognition, or face recognition, or context-aware authentication, such as location-based authentication or behavior-based authentication. Non-cryptographic authentication is less complex than cryptographic authentication, and it does not require the exchange of secret keys between devices, which reduces the computational overhead of the network. However, non-cryptographic authentication approaches are generally considered to be less secure than cryptographic authentication because they are susceptible to various types of attacks, such as spoofing attacks and replay attacks.

The authors of [1] proposed an authentication method that builds upon the scheme developed by Hwang and Li [2]. Their approach employs smart cards and one-way functions to achieve efficient and practical authentication. By replacing the original discrete logarithm-based security with hash functions, the proposed solution addresses a potential security vulnerability in Hwang's scheme. The authors conducted both security and efficiency analyses on their method, which demonstrated that the substitution of the problem does not compromise the security of the protocol.

The authors of [3] proposed a lightweight authentication protocol for WBAN by making use of the public key algorithms and Rabin scheme, suitable for compact devices that have limitations in resources. The system is designed for a medical scenario where sensors and actuators are placed in patients' bodies with different diseases. There are four entities involved in the system, namely, actuators, a doctor, sensors, and a node coordinator. These nodes interact with each other in the system to ensure secure communication.

The paper [4] presents an upgraded version of a protocol that is used for authentication in Telecare Medic Information Systems (TMIS), based on the work done by Lu et al. [5]. The authors found that the original protocol was vulnerable to various attacks that could violate patient anonymity, lead to identity theft, and attacks the TMIS server. To address these vulnerabilities, they developed a new protocol that provides better security but at a higher

computational cost. The protocol was tested using the ProVerif tool to ensure its resistance to attacks.

A secure key management protocol for e-health applications to ensure the confidentiality, integrity, and availability of sensitive health information is discussed in [6]. The protocol uses a hybrid approach that combines both symmetric and asymmetric cryptography to handle the key distribution and management process efficiently. The protocol utilizes a trusted third-party authority (TPA) to handle the key establishment and management between the sensors and the server. The authors also proposed a secure session key establishment algorithm that uses a one-time password for mutual authentication and key establishment between the sensor and the server. The proposed protocol was evaluated through simulation, and the results show that it is efficient, secure, and can effectively handle the key management process for e-health applications.

A new protocol was introduced in [7] for use in Telecare Medic Information Systems. The work proposes a protocol for authenticating a medical server in a telecare medical information system while preserving the anonymity of the patient. The protocol involves four entities: the patient, the medical sensor node, the medical server, and the trusted authority. The protocol uses a hash function, symmetric key cryptography, and message authentication codes to provide confidentiality, integrity, and authentication of the exchanged messages. The protocol ensures the anonymity of the patient by using a pseudonym instead of the actual identity. The protocol has been tested using the widely accepted AVISPA tool and showed that it is secure against various types of attacks, such as replay attacks, impersonation attacks, and man-in-the-middle attacks. The authors also compared their protocol with other existing protocols and demonstrated that their protocol is more lightweight and efficient in terms of computation and communication overhead. Overall, the proposed protocol provides an effective solution for authenticating medical servers in telecare medical information systems while preserving patient anonymity and ensuring security.

In 2020, a protocol for IMD was proposed in [8]. The paper proposes a secure protocol for implantable medical devices, addressing the need for secure communication in the context of healthcare applications. The proposed protocol, called Imdfence, is designed to ensure the confidentiality, integrity, authentication, and freshness of communication in implantable medical devices. The authors use a lightweight and efficient approach to meet the resource constraints of such devices. The protocol involves two modes of operation, a setup mode and a normal operation mode. In the setup mode, a secure key establishment process is performed between the medical device and the external device, which serves as a trusted authority. The normal operation mode involves secure communication using symmetric cryptography-based algorithms, digital signatures for authentication, and hash functions with Message Authentication Code (MAC) to ensure integrity. The authors evaluated the protocol using the AVISPA verification tool and simulation-based evaluations using the NS3 simulator. The simulation results showed low overhead in terms of computation and communication, making the protocol suitable for resource-constrained implantable medical devices. The AVISPA analysis revealed that the protocol meets the security goals of confidentiality, integrity, authentication, and freshness, but identified a potential vulnerability related to the key establishment process. Based on the evaluation results, the authors concluded that the proposed Imdfence protocol provides a secure and efficient solution for implantable medical devices, ensuring patient privacy and protection against various security threats. They also suggested the use of physical layer security mechanisms, such as channel characteristics, to further enhance the security of the key establishment process.

In 2020, researchers presented a privacy-preserving protocol [9] and proposes a new privacy-preserving mutual authentication protocol for WBANs. The protocol aims to provide efficient and secure communication between a user's body sensors and a remote server while preserving user privacy. The proposed protocol is based on three entities: the user, the proxy node, and the remote server. The protocol is designed to ensure the anonymity of the user by allowing the user to remain anonymous to the proxy node and remote server. It uses a unique encryption and decryption scheme based on elliptic curve cryptography and hash functions for secure communication between entities. The proposed protocol consists of four main steps, including registration, authentication, session key establishment, and message exchange. In the registration phase, the user is authenticated and the session key is generated. In the authentication phase, the user and proxy node authenticate each other using the session key, while the proxy node also authenticates the remote server. In the session key establishment phase, the session key is established between the user and the remote server. In the message exchange phase, encrypted messages are exchanged between the user and the remote server using the established session key. The paper presents a comprehensive analysis of the proposed protocol's security and efficiency by conducting simulation-based experiments using NS-2. The results show that the proposed protocol provides secure and efficient communication with low communication overhead, latency, and computation cost compared to existing protocols. the proposed EPAW protocol provides a secure and efficient privacy-preserving mutual authentication scheme for WBANs. The protocol ensures user anonymity while providing secure communication between the user's body sensors and the remote server. The simulation-based experiments show that the proposed protocol has low overhead and computation costs and can be implemented in resource-constrained WBANs.

In 2020, a novel key agreement and authentication protocol for wireless sensor networks was proposed [10]. The proposed scheme involves three entities: the user node (UN), the gateway node (GN), and the remote healthcare server (RHS). The scheme uses symmetric key encryption and hash functions to provide secure communication between entities. The key agreement process is performed in two phases, where initially, UN and GN establish a session key and then GN and RHS share the same key using the previous session key. The authentication process involves the use of message authentication codes (MACs) to verify the authenticity of messages transmitted between entities. The proposed scheme provides mutual authentication between entities, ensures the confidentiality and integrity of data, and prevents various attacks such as impersonation, replay, and man-in-the-middle attacks. The scheme has been tested using the AVISPA tool to ensure its security and correctness. The results of the security analysis demonstrate that the proposed scheme is secure and efficient, making it suitable for use in WBANs. The proposed scheme offers better performance in terms of communication overhead, computation time, and memory consumption than other existing schemes.
In another paper in 2020, a new protocol was proposed in [11]. This paper suggests an enhanced anonymous authentication protocol based on elliptic curve cryptography (ECC) to provide efficient and secure authentication for wearable health monitoring systems. The protocol introduces improved features over the Li et al. protocol, utilizing ECC-based cryptographic algorithms for authentication, confidentiality, and integrity. The proposed protocol involves three main entities: the wearable device (WD), the gateway (GW), and the health server (HS). The protocol includes registration, authentication, and data transmission phases, where WD securely registers with GW, authenticates itself using ECC-based session key exchange, and securely transmits health data to HS. The proposed protocol aims to enhance the security and

privacy of wearable health monitoring systems, providing anonymous communication and protecting sensitive health information from unauthorized access.

Security Methods for WBAN

When it comes to ensuring security for WBAN, there are two main categories of authentication methods: cryptographic and non-cryptographic. Cryptographic methods rely on lightweight cryptographic schemes to provide authentication, confidentiality, and integrity services. Meanwhile, non-cryptographic approaches make use of authentication systems based on biometrics, channels, or proximity.

Cryptographic Authentication Methods

Cryptographic authentication techniques demand significant computational resources, which makes them impractical for WBAN sensors with limited power. While elliptic curve cryptography makes them effectively utilized in the security of WSN, these systems still consume more energy compared to symmetric cryptosystems. TinySec [13] offers a solution for authentication in WBAN. In this approach, prior to network deployment, each sensor is pre-configured with a mutually shared key. This key is then utilized for subsequent communication in the network, including message and packet encryption. However, a significant drawback of this method is that if a sensor is compromised, it can result in complete information leakage from the sensor network, posing a risk to the entire system. Consequently, conventional authentication methods discussed above are insufficiently secure and computationally intensive, which makes them impractical for WBANs.

Authentication methods that rely on biometric data:

Biometric authentication is a method of verifying the identity of a user based on their unique physical or behavioral traits. It can provide a secure and convenient way to authenticate users and protect their personal health data. There are several biometric authentication techniques that can be used in WBANs, including fingerprint recognition, iris recognition, face recognition, and voice recognition. These techniques require sensors to capture biometric data and algorithms to process and compare the data with stored templates. Compared to other authentication methods, biometric-based systems do not require the distribution of pre-shared keys. Academics have studied various bodily functions such as heartbeat patterns, ECG signals, PPG readings, and fingerprints to evaluate their potential for use in authentication[14,15]. The effectiveness of these systems relies on the correlation coefficient of physiological parameters calculated at the sender and receiver. However, different physiological signals may occur due to the position of sensors at different parts of the human body. The drawback of biometric-based systems is the need for specialized sensing hardware, which can place an additional load on small on-body sensors.

Authentication methods based on unique characteristics:

These methods utilize the channel response of the communication channel between the nodes for authentication purposes. This approach takes advantage of the unique channel characteristics of the human body, which can be used to identify and authenticate different nodes in the network. Channel characteristic-based authentication methods have the advantage of being lightweight and not requiring additional hardware or sensors. They are also less susceptible to attacks compared to biometric-based authentication methods. However, they are sensitive to environmental changes, such as body posture and movement, which can affect the

channel response and accuracy of the authentication. One popular approach for channel characteristic-based authentication in WBANs is the received signal strength indicator (RSSI)-based method. This method utilizes the RSSI value of the received signal to identify the node and verify its authenticity. Another approach is the time-of-flight (ToF)-based method, which measures the time taken for a signal to travel from the transmitter to the receiver and back, which is unique for different nodes and can be used for authentication. Overall, channel characteristic-based authentication methods offer a promising solution for authentication in WBANs, with their lightweight and low-cost nature. However, they require further investigation and optimization to address their limitations and improve their accuracy and reliability in different environmental conditions.

Design and Specification of the Protocol

In the preceding section, various strategies were discussed for safeguarding WBASNs and TMIS. The central goal of these protocols is to authenticate the involved entities. In contrast, the protocol described below is focused on assuring both entity authentication and data confidentiality and integrity. This is accomplished by employing four cryptographic fundamental components that guarantee safe communication among the WBASN participants, resulting in the protection of transmitted sensitive information between nodes. Furthermore, the protocol implements a method of non-cryptographic authentication for the nodes, enabling the differentiation of on-body sensors.

Cryptographic Primitives Election

Once the security services and techniques that ensure them have been examined, the next step is to identify the cryptographic methods that will be employed in the future. The goal is to maintain data confidentiality, data integrity, and data authentication, which are essential security services, using a set of four cryptographic techniques. Encryption is used to protect the information during transmission and to provide confidentiality. A digital signature guarantees authentication by enabling the recipient to identify the sender. Key encapsulation mechanism (KEM) employs asymmetric algorithms to secure the keys of symmetric cryptography and encrypt the information for transmission. Hash functions are used to map binary strings of arbitrary length to binary strings of fixed length, making it easy to obtain any output from any input, but difficult to obtain any input from a hash value. These techniques are chosen to maximize the capabilities of each device involved in the protocol. Before deciding on the specific location of each technique, it is critical to assess the minimum capabilities required for the equipment in use, including data handling range, working frequency, and data range presented by each device.

Proposed security protocol:

The proposed method for ensuring security involves the participation of four different entities, each with a specific purpose and abilities. Entity A, referred to as the Medical server, carries out complex cryptographic operations and is typically under the control of the patient's physician. A personal computer or laptop is usually employed for this entity. Entity B, known as the Coordinator node, is expected to be in constant proximity to the patient and has limited resources when compared to the server. Smartphones, embedded systems, or ARM processor-equipped devices may be utilized for this entity. The Coordinator node performs cryptographic operations as required by the protocol and is in constant communication with the sensors, actuators, and server. The Sensors, or entity C, are affixed to the patient's body and collect measurements, securely transmitting them to the Coordinator node (entity B). Lastly, the Actuators (entity D) are also placed on the patient's body and operate based on instructions from A via B. The entities need to be low-cost and have the ability to complete their regular operations while fulfilling their assigned roles in the protocol.

The diagram depicted in Fig. 12 illustrates the protocol's sequence of actions, showcasing the order in which each entity will perform its functions and the messages that will be exchanged among them. The protocol is composed of four major steps.

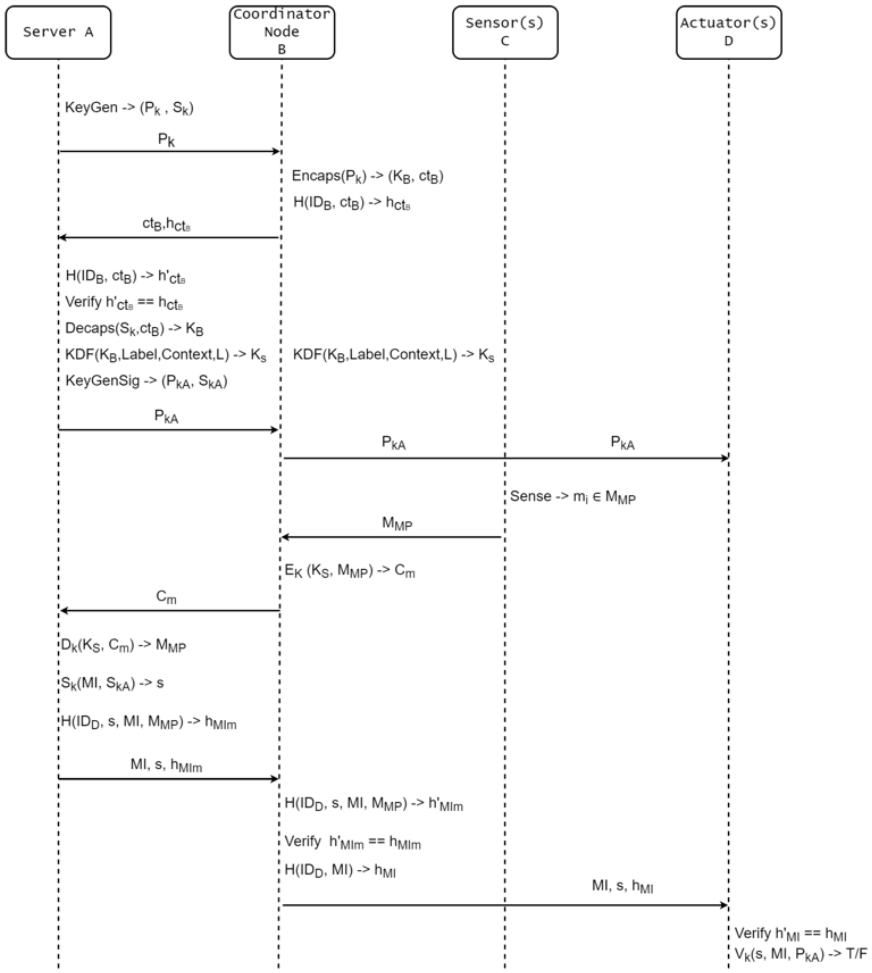

Figure 12: Protocol entities interact and function [23].

Step 0 in the protocol aims to set up and authenticate the sensors. In this stage, the sensors B (accelerometer and gyroscope), C (accelerometer and gyroscope), and D (accelerometer and gyroscope) generate movement data. Based on this data, the system either grants or denies access to the WBAN.
Step 1, the protocol generates a public key(P_{KA}), and a secret key(S_{KA}), and transmits P_{KA} to entities B and D.
Step 2 of the protocol involves the sensing, encryption, and transmission of information. The sensors on Entity C detect the necessary data, encrypt it, and send it securely to Entity B.
Step 3, B receives the encrypted information from C, decrypts it using its private key, and generates instructions based on the decrypted data. B then signs the instructions with its digital signature and sends them, along with the signature, to D.
In Step 4, a verification function is applied to ensure that the received instructions are safe to apply. This is done by checking the digital signature that came with the instructions. If the signature is valid, the instructions are applied; otherwise, they are rejected.

Step 0: Authentication

The first step of the protocol involves agreeing on security levels and parameters. To ensure secure communication, Before participating in the protocol, it is necessary to register all sensors and actuators with the coordinator node and the server. A's communication with C and D must go via B, but wireless communication poses a risk of unauthorized third-party entities accessing information transmitted via legitimate sensors. To solve this issue, an authentication method based on the correlation between acceleration vectors and gyroscopes is proposed[20]. The technique employs a central node as a coordinator and a sensor node equipped with 3D-axis accelerometers and gyroscopes, located on various regions of the patient's body. The correlation between the new sensor's accelerometer data stream and the coordinator node is computed by analyzing the received data by the coordinator node. If the correlation value is high, the connection is approved, and if not, it is rejected. Fig. 13 shows the flow diagram of this method of authentication.

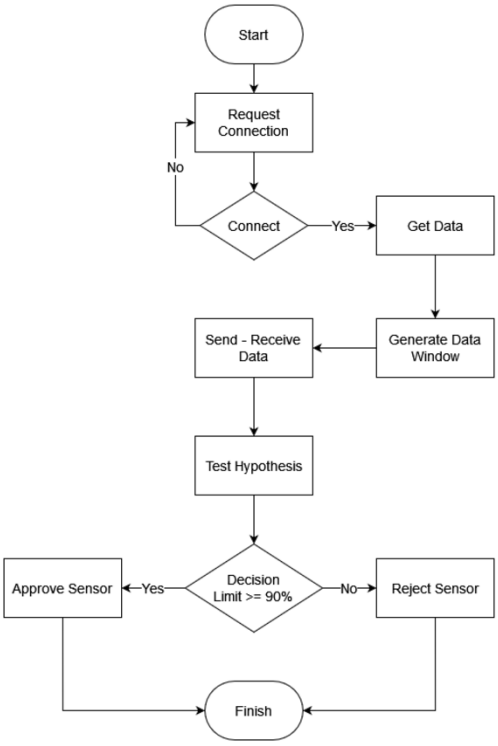

Figure 13: Authentication method's data transmission[23].

The below algorithm is a process for authenticating sensors. The algorithm takes as input the newly detected sensor, b, as well as the accelerometer and gyroscope readings of the coordinator node (A_{CN}, G_{CN}) and the new sensor (Ab, Gb). The correlation between the measurements of the accelerometer and gyroscope of the sensor and the CN are calculated and stored as C_{ACC} and C_{GYR}, respectively. The algorithm then compares C_{ACC} and C_{GYR} with a decision limit, LD, to determine whether the sensor should be accepted or rejected. If the correlation value is above the decision limit, the sensor is approved, and data can be transmitted to the CN. If the correlation value is below the decision limit, the sensor will be denied access, and network access will not be granted.

```
while True:
   if  b = newSensorDetected():
      markSensorAsUnauthenticated(b)
      A_CN = readData(d)
      A_b = readData(d)
      G_CN = readData(d)
      G_b = readData(d)
      C_ACC = computeCorrelation(A_CN, b)
      C_GYR = computeCorrelation(G_CN, b)
      if computeConditionalAverage(C_ACC, C_GYR) >= LD:
         markSensorAsAuthenticated(b)
         sendDataToCN(b)
      else:
         deleteSensor(b)
```

During the initial step of the protocol, The registration of all nodes and actuators in the WBAN with the coordinator node is a necessary step to ensure secure communication with the server. This ensures that the server is aware of all the participants in the network. After this registration process, communication between C and D with A occurs through B. Each entity is assigned a unique identifier (IDx) during this step, which is stored by the server. The diagram presented in Fig. 14 depicts the registration and identification process that occurs in step 1 of the protocol.

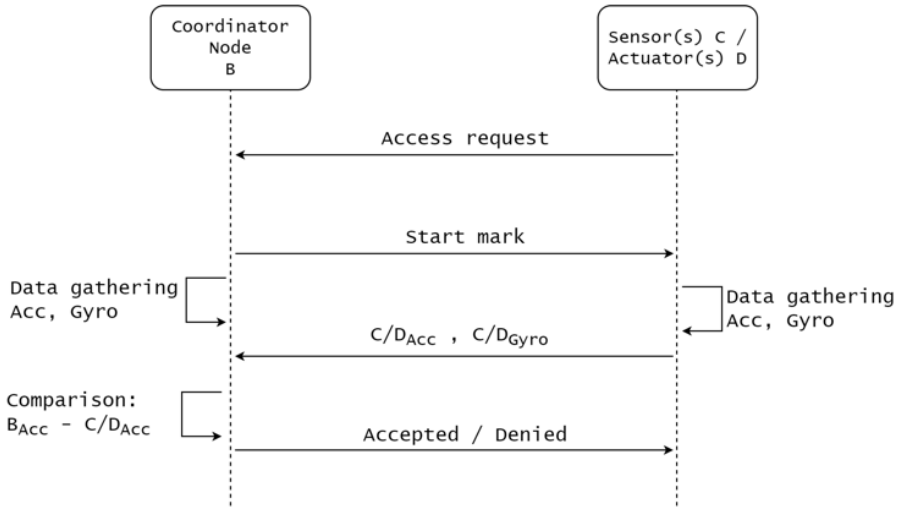

Figure 14:keyless Authentication[23].

Step 1: Generation a new key

Depending on the selected scheme, the input variables used may vary. Typically, generating keys involves selecting prime numbers p and q, as well as a generator g, in step 0. The initial key to be created is the symmetric key, which is generated using asymmetric cryptography, where the KEM acts as the key agreement protocol. The KeyGen algorithm is executed by the server to generate a key pair (P_k, S_k), which is used to derive K_B through the Encaps algorithm. The values K_B and ctB are returned by Encaps and ctB is hashed with the identifier of B, ID_B, using the hash function to produce hctB. A receives hctB and ctB and verifies that hctB is an integer, then executes the Decaps algorithm to obtain K_B. A symmetric key Ks is derived by applying the Key Derivation Function (KDF) to K_B, Label, Context, and L. A new key pair (P_{kA}, S_{kA}) is generated by the server using KeyGen from the digital signature scheme to get the key that will sign subsequent steps. Once P_{kA} is obtained, it is sent to B and D. The diagram in Fig. 15 corresponds to step 1 of the protocol.

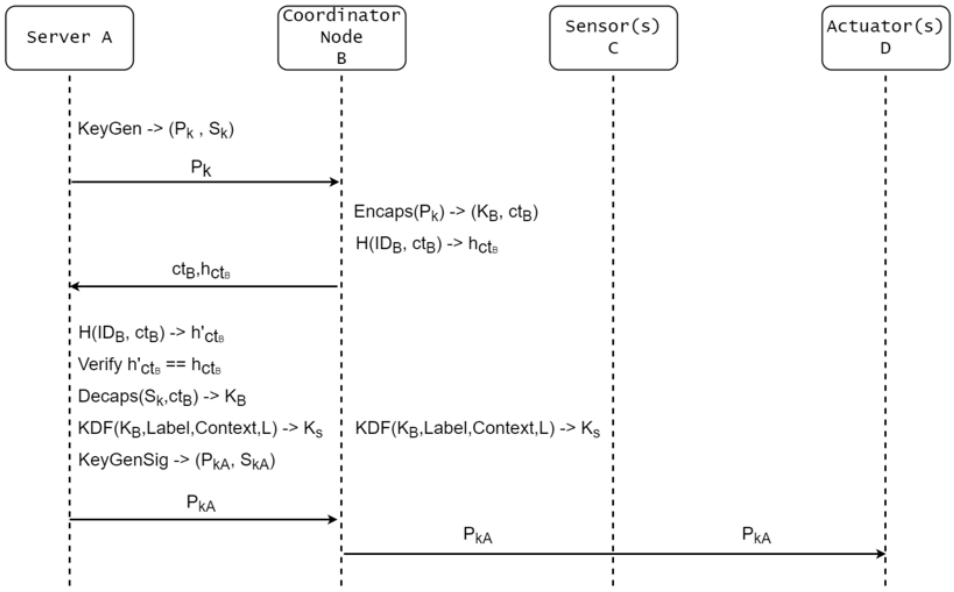

Figure 15:Symmetric key generation between A and B. Asymmetric keys generation from A for subsequent distribution to B and D[23].

Step 2: Sending of Information from Sensors and encryption by Coordinator Node

When the nodes in the WBAN have been registered and communication initiated, the sensors will start collecting data at regular time intervals to form a final message called M_{MP}, which is a dataset containing information for each time unit. Once the M_{MP} is done, it will be sent to Coordinator. The symmetric key K_s will be used to encrypt the data in M_{MP} by using the encryption algorithm E_k, which produces a message that is encrypted called C_m. This encrypted message is then sent from the coordinator to the server. Fig. 16 illustrates the information flow and the functions used in step 2 of the protocol.

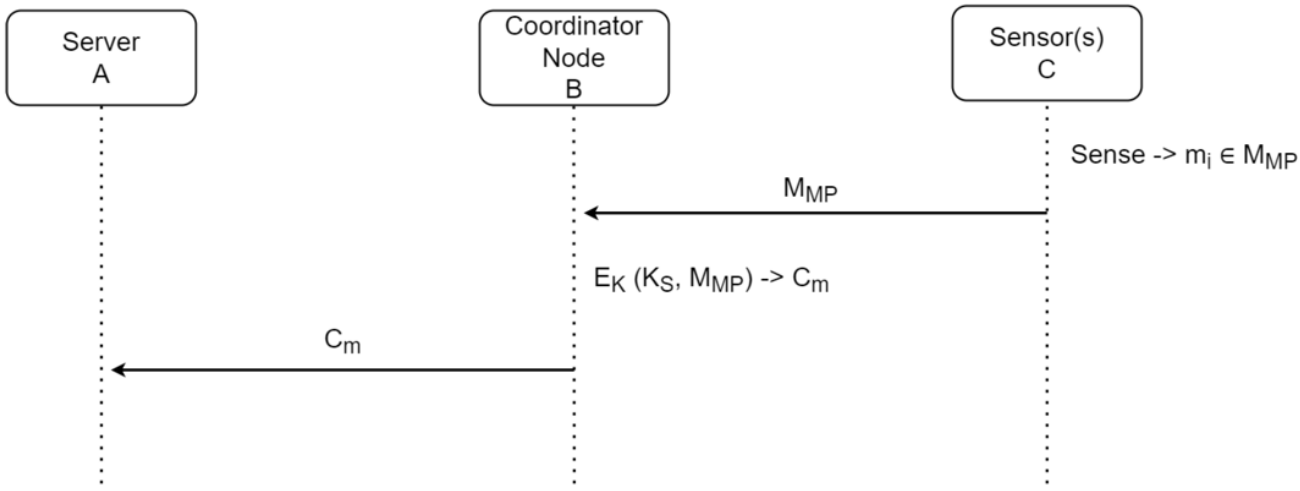

Figure 16: Symmetric key generation between A and B. Asymmetric keys generation from A for subsequent distribution to B and D [23].

Step 3: Verification confirmation of the signature and implementation of the directions

In step 3 of the protocol, shown in Fig. 8, the entities involved use the inputs K_s, S_{KA}, C_m, and a message that contains the instruction called MI, which is formed based on the physician's interpretation. A decrypts C_m using the decryption function $D_k(K_s, C_m) \rightarrow M_{MP}$ to obtain the data that were gathered by sensors. A then generates and signs MI using the S_k function of the cryptographic method for generating a digital signature s. The ID_D identifier, the message MI, the message M_{MP}, and the signature s are input into a hash function, $H(ID_D, s, MI, M_{MP}) \rightarrow$ hMIm. The resulting value is sent to entity B along with the message MI and the signature s. After receiving values from A, B verifies them using a hash function to ensure their completeness. If the values are complete, B can proceed with the next step and sends them to entity D, identified by ID_D. Upon successful verification of the received values, Entity B proceeds to apply the instructions using the derived symmetric key in Step 3. The process of Step 3 is completed once Entity B successfully applies the instructions.

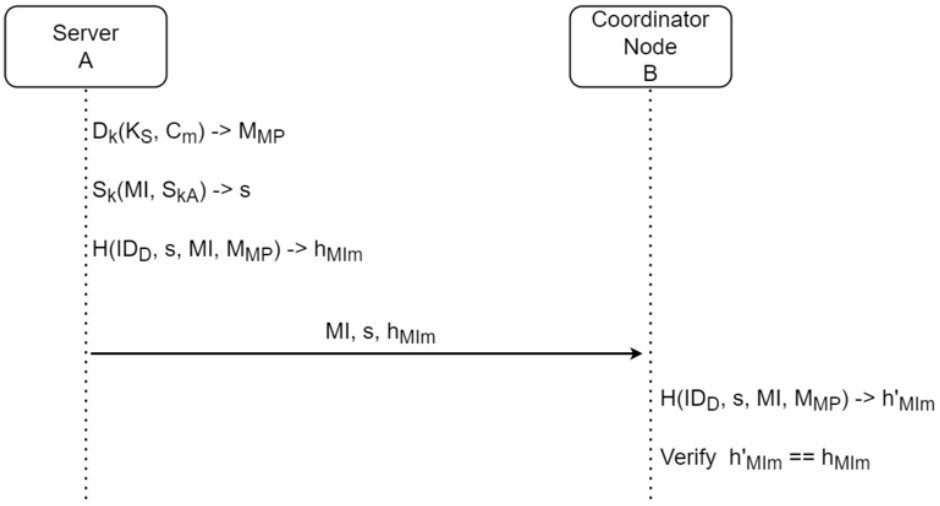

Figure 17:Decryption, signature generation, hash value generation[23].

Step 4: Verification Confirmation of the Signature and Implementation of the Directions

In the final step of the protocol, entity B uses a hash function to generate a value based on the identifier of entity D(ID_D) and the message MI. The hash value is then appended with the signature and the message MI, and the resulting packet is sent to entity D. Upon receiving the packet, entity D performs two important verifications. Firstly, it verifies the received hash value to ensure the integrity of the message. This step is crucial because any tampering with the message can result in the patient being harmed. Secondly, entity D checks the authenticity of the signature using a verification function. This function takes s, P_{kA}, and MI as inputs and outputs a Boolean value (True/False) that determines whether the signature is authentic or not. The verification function ensures that the instructions received by the actuators are legitimate and have not been tampered with. This step is important because it guarantees that the actuators can safely apply the instructions to the patient's body without any risk of harm. Fig. 18 provides a visual representation of all the functions performed by each entity in this step.

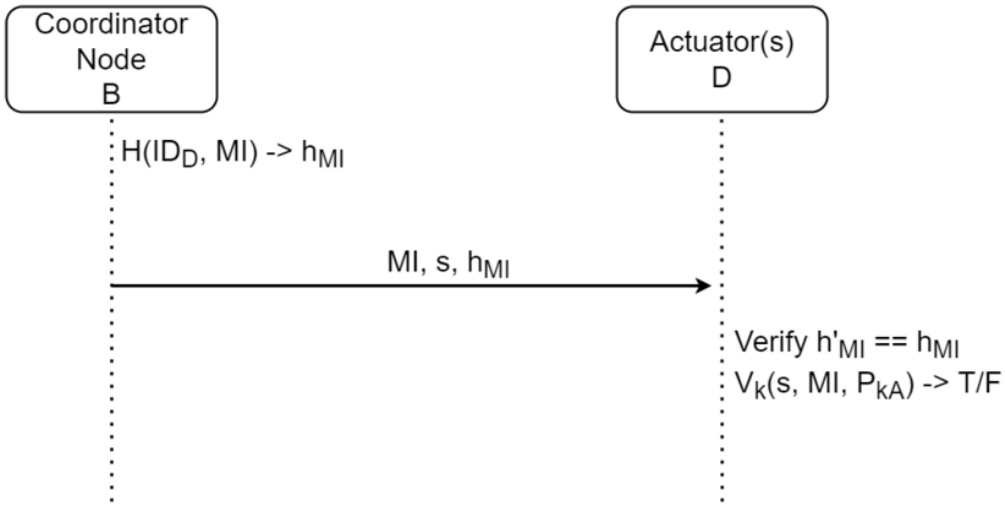

Figure 18:Transferring MI data from coordinator B to D[23].

Chapter 3:

Testing and Outcomes

A series of procedures and rules, known as cryptographic protocols, are implemented to establish secure communication between different entities involved in a transaction or data exchange. These protocols protect the information using cryptographic techniques to provide confidentiality, authentication, data integrity, and irrefutability. However, protocols may still be vulnerable to security or semantic issues, which is why formal Verification instruments are employed to authenticate. the cryptographic properties of protocols. These tools use security services, the protocol's design, and a model of potential attackers to test the protocol's security and semantics. This allows for the detection of any security breaches or attacks that could be performed on the protocol. The verification tools provide proof of the protocol's security or descriptions of potential attacks, helping to identify and correct any security vulnerabilities. Fig. 10 illustrates this methodology. Additionally, some tools offer information on how to correct security breaches identified during the verification process.

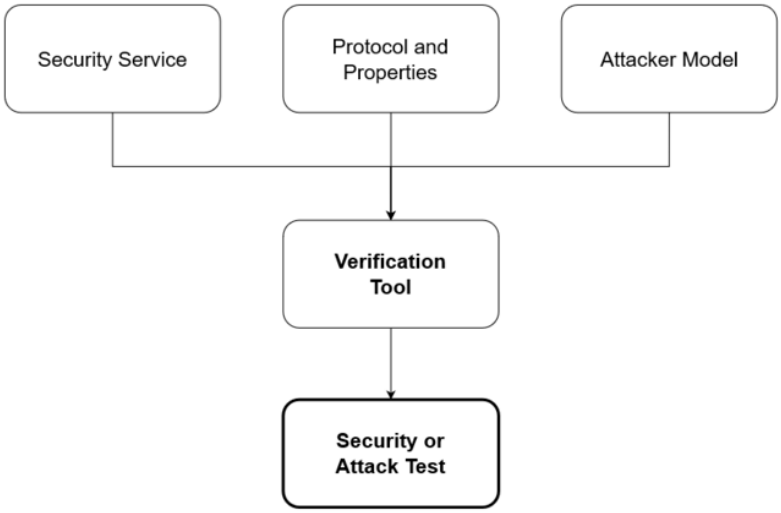

Figure 19: Protocol verification [23]

Various tools are available for verifying the security of protocols, with some being automatic in nature. These tools analyze the cryptographic protocol and the security properties that must be met and perform attacks to assess their security and semantics. In case the protocol is found to be vulnerable, the tool detects the type of attacks executed, while secure protocols are identified as such. One such tool that performs these functions is Scyther. The results generated by these verification tools can be used to improve the protocol itself. The process of automatic protocol verification is graphically represented in Fig. 20.

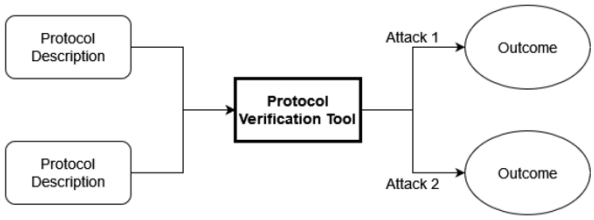

Figure 20: Block diagram illustrating the process of verifying a cryptographic[23].

Scyther:

Cas Cremers developed Scyther in 2006 as a powerful tool for verifying cryptographic protocols. Scyther is capable of verifying an unlimited number of protocol executions without requiring a specific scenario. It uses the Security Protocol Description Language (SPDL) to describe protocols and security parameters and offers a graphical user interface for ease of use. Scyther conducts a thorough analysis of the protocol and produces a report with a graph for each attack it detects. In the event that the verification uncovers one or more attacks, Scyther generates a tree diagram to show potential attacks. This makes it easier for users to visualize the different ways that an attacker could exploit a protocol's weaknesses. Scyther is capable of verifying man-in-the-middle attacks and performing protocol characterization analysis.
One of the strengths of Scyther is its ability to validate specific protocol aspects and evaluate the protocol from the perspective of each role involved. This allows users to gain a better understanding of the protocol's security posture and identify areas where improvements could be made. Scyther accepts four authentication claims, namely aliveness, Weakagree, Niagree, and Nisynch, as well as two confidentiality claims, Secret and Session Key Reveal (SKR). The aliveness claim ensures that a connection with the target goal is possible. Weakagree guarantees weak agreement between the source and destination entities, indicating that both entities are aware of the communication. Niagree requires non-injective agreement on the communicated data, in addition to weak agreement. Nisynch ensures non-injective synchronization by requiring the messages to be transmitted in a specific order.
The authentication claims are organized in a hierarchy, with Nisynch being the most stringent authentication claim. This means that if Nisynch is satisfied, then all other authentication claims are also met. This hierarchical organization allows users to specify the level of authentication required for their protocols and ensure that their protocols meet the necessary security requirements.

AVISPA:

AVISPA is a popular and powerful tool used for the verification of cryptographic protocols. It was developed in 2003 by a group of researchers from the University of Bologna in Italy. The name "AVISPA" stands for Automated Validation of Internet Security Protocols and Applications. AVISPA offers four different models for protocol verification: OFMC (On-the-fly Model-checker), SATMC (SAT-based Model-Checker), AtSe (CL-based Attack Searcher), and TA4SP (Tree Automata-based Protocol Analyzer). Each model has its own strengths and weaknesses, and users can choose the most appropriate model for their specific verification needs.
The OFMC model is a model-checking tool that checks a finite-state model of a protocol against a security property. It performs verification by exploring the state space of the model on-the-fly, which makes it more efficient than other model checkers.
The SATMC model is another model-checking tool that checks a finite-state model of a protocol against a security property. It uses Boolean satisfiability (SAT) solvers to efficiently search for a counterexample to the security property. This makes the SATMC particularly useful for verifying large and complex protocols.
The AtSe model is an attack-searching tool that searches for attacks on a protocol by encoding the search as a constraint logic problem (CLP). The tool then uses a CLP solver to search for attacks. AtSe is particularly useful for finding new attacks that are not covered by existing attack libraries.

Finally, the TA4SP model is a protocol analysis tool that uses tree automata to check a protocol against a security property. Tree automata are used to represent sets of trees and are used to model message exchanges in a protocol. TA4SP can check both the safety and liveness properties of a protocol.

Results of Security Analysis Conducted by Protocol Verification Tools:

For testing the security of the protocols, both Scyther and AVISPA were customized to match the testing environment in which the protocols were evaluated. Appendix 1 contains SPDL (Scyther Protocol Description Language) code related to the Scyther tool, while Appendix 2 contains Hspsl (High-level Security Protocol Specification Language) code related to the ASIPA (Automated Security Protocol Analysis) tool.
Scyther was run a minimum of five times to ensure consistency in the analysis results. The configuration of the tool was set to search for all potential attacks on the protocol, limited to a maximum of ten patterns per claim. During the analysis, Scyther generated several attack graphs, which represent potential attacks on the protocol. The attack graphs included various attack paths that could exploit weaknesses in the protocol to achieve unauthorized access, disclosure of sensitive information, or other security breaches. Scyther also generated several counterexamples, which represent possible executions of the protocol that violate the security properties specified in the protocol claims.
After reviewing the generated attack graphs and counterexamples, the protocol was modified to address the detected security weaknesses. The modified protocol was then reanalyzed using Scyther to ensure that the changes did not introduce new security vulnerabilities.
On the other hand, AVISPA permits the user to select from the different models available to test the protocol, and the protocol was executed under each of these modes. The models available in AVISPA are the OFMC (On-the-fly Model-checker), SATMC (SAT-based Model-Checker), AtSe (CL-based Attack Searcher), and TA4SP (Tree Automata-based Protocol Analyzer). Fig. 21 presents some of the outcomes of Scyther. The outcomes are arranged in columns. The first column indicates the protocol name, which in this case is an abbreviation for "New Cryptographic Protocol for Medical Devices." The second column specifies the entity under review, while the third indicates the communication side between entities. The following column specifies the claim being verified. In the case of confidentiality, the information being protected is also shown, such as the symmetric key derived through a KDF function, as well as the value ctb and the message. The final two columns present the result of the claim and the feedback regarding the claims. The results only show "Ok," showing that the demonstrated property has been confirmed. The comments indicate that there are "No attacks within bounds," suggesting that the tool did not detect any attacks within the specified limits.

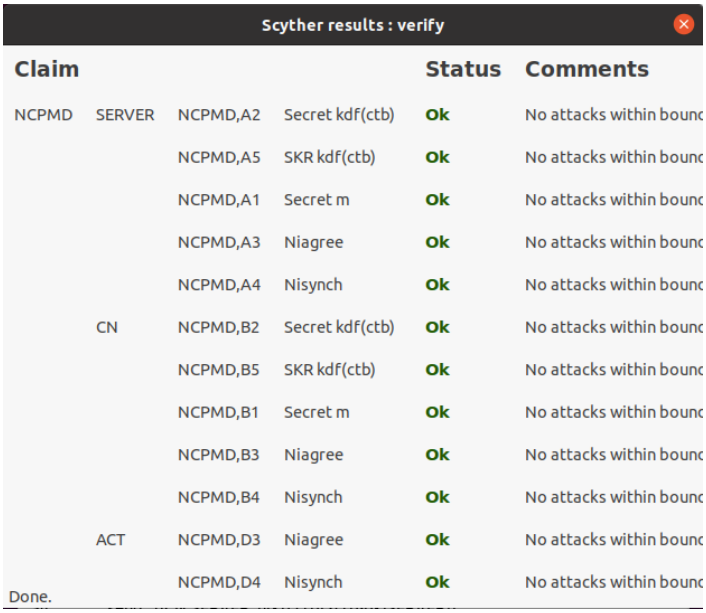

Figure 21: Outcome achieved by SCYTHER

The results indicate that the protocol ensures security by providing authentication, confidentiality, and integrity services. To achieve this, the protocol uses encrypted primitives, digital signatures, Key Encapsulation Mechanisms (KEM), and hash functions.
Based on the analysis performed using the AVISPA tool, it can be concluded that the protocol under study is secure and meets the defined security objectives. The results of the analysis are shown in Figs. 22-24, which confirms that the protocol is secure when tested under the specified mode. The findings from this analysis suggest that the protocol is effective in protecting information and ensuring the confidentiality, integrity, and authenticity of data transmissions.

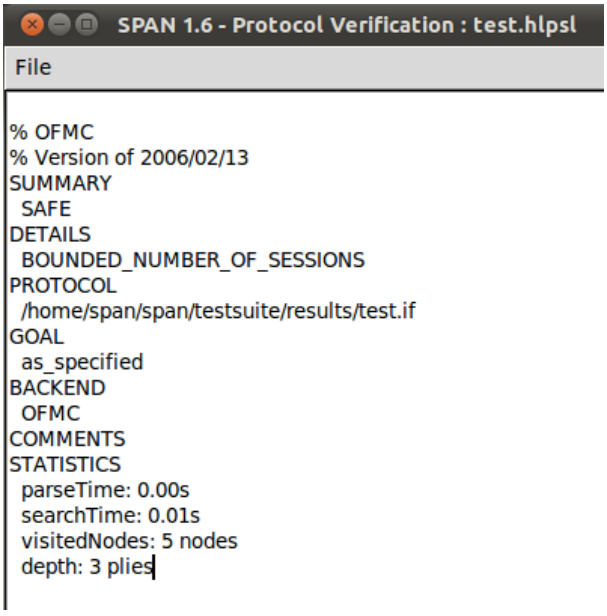

Figure 22:Protocol verification by AVISPA of the OFMC model

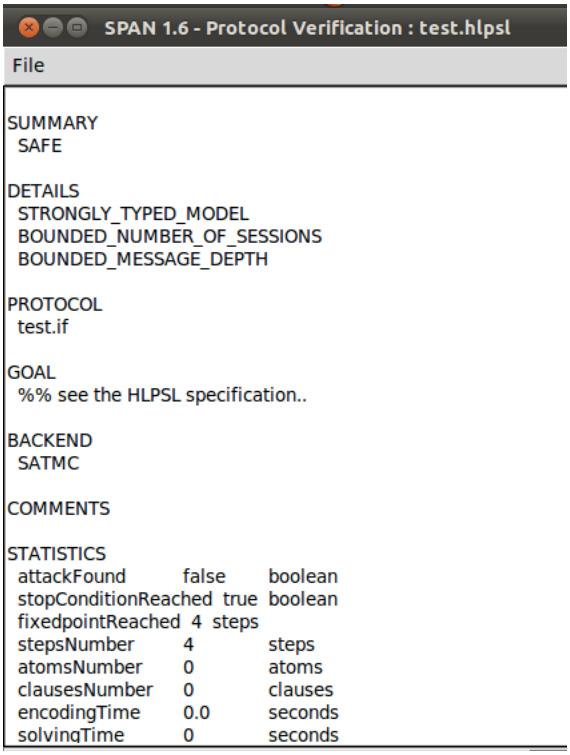

Figure 23: Protocol verification by AVISPA of the SATMC model

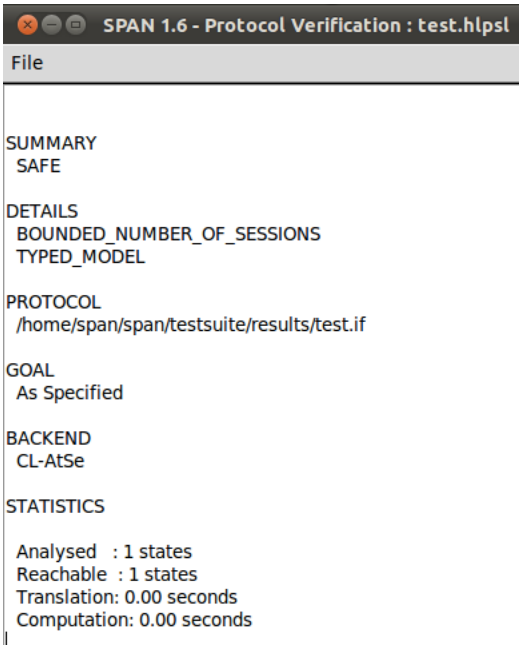

Figure 24: Protocol verification by AVISPA of the AtSe model

Conclusion:

The proposed protocol is designed to provide confidentiality, authentication, and integrity for data that traveled through a WBAN in healthcare-related scenarios. The protocol uses a range of cryptographic primitives to achieve these security services, with its security verified using automated cryptographic protocol verification tools. A key advantage of this protocol is its use of a keyless authentication method, eliminating the need for additional cryptographic key pairs.

The protocol prioritizes the confidentiality and integrity of patient data, ensuring authenticated and complete communication between entities. Authentication between sensors is based on the same human body, while the protocol design avoids exposing data during key generation to protect against unauthorized access to sensitive information for spoofing attacks, which were identified in previous protocols. Overall, the protocol has been verified to be secure in terms of the three security services, and the message sending process is free from errors.

References

1. *Sun, H.M. An efficient remote use authentication scheme using smart cards. IEEE Trans. Consum. Electron. 2000.*
2. *Hwang, M.S.; Li, L.H. A new remote user authentication scheme using smart cards. IEEE Trans. Consum. Electron. 2000.*
3. *Hayajneh, T.; Vasilakos, A.V.; Almashaqbeh, G.; Mohd, B.J.; Imran, M.A.; Shakir, M.Z.; Qaraqe, K.A. Public-key authentication for cloud-based WBANs. In Proceedings of the 9th International Conference on Body Area Networks, London, UK, 29 September–1 October 2014.*
4. *Chaudhry, S.A.; Mahmood, K.; Naqvi, H.; Khan, M.K. An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. J. Med. Syst. 2015.*
5. *Lu, Y.; Li, L.; Peng, H.; Yang, Y. An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. J. Med. Syst. 2015.*
6. *Abdmeziem, M.R.; Tandjaoui, D. An end-to-end secure key management protocol for e-health applications. Comput. Electr. Eng. 2015.*
7. *Chaudhry, S.A.; Mahmood, K.; Naqvi, H.; Khan, M.K. An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. J. Med. Syst. 2015.*
8. *Siddiqi, M.A.; Doerr, C.; Strydis, C. Imdfence: Architecting a secure protocol for implantable medical devices. IEEE Access 2020.*
9. *Jegadeesan, S.; Azees, M.; Babu, N.R.; Subramaniam, U.; Almakhles, J.D. EPAW: Efficient privacy-preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). IEEE Access 2020.*
10. *Rehman, Z.U.; Altaf, S.; Iqbal, S. An efficient lightweight key agreement and authentication scheme for WBAN. IEEE Access 2020.*
11. *Sowjanya, K.; Dasgupta, M.; Ray, S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. Int. J. Inf. Secure. 2020.*
12. *Li, X.; Peng, J.; Kumari, S.; Wu, F.; Karuppiah, M.; Choo, K.K.R. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. Comput. Electr. Eng. 2017.*
13. *Karlof, C.; Sastry, N.; Wagner, D. TinySec: A link layer security architecture for wireless sensor networks. In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, India, 3–4 November 2004.*
14. *Venkatasubramanian, K.; Gupta, S. Physiological value-based efficient usable security solutions for body sensor networks. ACM Trans. Sens. Netw. (TOSN) 2010.*
15. *Xu, F.; Qin, Z.; Tan, C.; Wang, B.; Li, Q. IMDGuard: Securing implantable medical devices with the external wearable guardian. In Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM 2011), Shanghai, China, 10–15 April 2011; pp. 1862–1870. 16. Formal Methods in Security Protocols Analysis. (accessed on 5 January 2022).*
16. *Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges 2022.*

17. *Yaghoubi, M.; Ahmed, K.; Miao, Y. Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges. J. Sens. ActuatorNetw.2022.*
18. *Mainanwal, V.; Gupta, M.; Upadhayay, S.K. A survey on wireless body area network: Security technology and its design methodology issue. In Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 201.*
19. *Zeng, K.; Govindan, K.; Mohapatra, P. Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]. IEEE Wirel. Commun 2010.*
20. *Cai, L.; Zeng, K.; Chen, H.; Mohapatra, P. Good Neighbor: Ad hoc Pairing of Nearby Wireless Devices by Multiple Antennas. In Proceedings of the 18th Annual Network and Distributed System Security Symposium, San Diego, CA, USA 2011.*
21. *Elyazidi, S.; Escamilla-Ambrosio, P.J.; Gallegos-Garcia, G.; Rodríguez-Mota, A. Accelerometer-based body area network sensor authentication. In Smart Technology; Springer: Cham, Switzerland, 2018.*
22. *Mile, A.; Okeyo, G.; Kibe, A. Hybrid IEEE 802.15. 6 wireless body area networks interference mitigation model for high mobility interference scenarios 2018.*
23. *Kevin Andrae Delgado.; Gina Gallegos-Garcia.; Ponciano Jorge.; Cryptographic Protocol with Keyless Sensors Authentication for WBAN in Healthcare Applications 2023.*

Appendix 1:

```
hashfunction h, kdf;
const Concat: Function;
usertype SessionKey;
protocol NCPMD(A,B,D)
{
	role A
	{
		var ctb: Nonce;
		const kb :Nonce;
		fresh s, Mi: Nonce;
		var m;
		var kab: SessionKey;
		recv_1(B,A, h(kb,ctb),{ctb}pk(A));
		macro kab = kdf(ctb);
		recv_3(B,A,{m}kab);
		send_4(A,B,h(Concat(s,Mi,m)),{Mi}sk(A),s);

		claim_A2(A,Secret,kab);
		claim_A5(A,SKR,kab);
		claim_A1(A,Secret,m);
		claim_A3(A,Niagree);
		claim_A4(A,Nisynch);
	}

	role B
	{

		fresh ctb: Nonce;
		fresh m;
		const kb :Nonce;
		var s, Mi,m;
		var kab: SessionKey;
		send_1(B,A, h(kb,ctb),{ctb}pk(A));
		macro kab = kdf(ctb);
		send_3(B,A,{m}kab);
		recv_4(A,B,h(Concat(s,Mi,m)),{Mi}sk(A),s);
		send_5(B,D,{Mi}sk(A),s);

		claim_B2(B,Secret,kab);
		claim_B5(B,SKR,kab);
		claim_B1(B,Secret,m);
		claim_B3(B,Niagree);
		claim_B4(B,Nisynch);
	}

	role D
	{
		var s, Mi;
```

```
                recv_5(B,D,{Mi}sk(A),s);
                claim_D3(D,Niagree);
                claim_D4(D,Nisynch);
        }
}
```

Appendix 2:

HSPSL File :

```
role
role_A(A:agent,B:agent,C:agent,D:agent,PkA:public_key,IDA:text,IDB:text,IDC:text,IDD:te
xt,SND,RCV:channel(dy))
played_by A
def=
        local

        State:nat,Ctb:text,Ks:public_key,S:text,M:text,Concat:hash_func,H:hash_func,Mi:text
,SkA:public_key
        init
                State := 0
        transition
                1. State=0 /\ RCV(H(Concat(IDB.Ctb')).{Ctb'}_inv(PkA)) =|> State':=1
                3. State=1 /\ RCV({M'}_inv(Ks')) =|> State':=2 /\ S':=new() /\ SkA':=new() /\
Mi':=new() /\ SND(H(Concat(IDD.S'.Mi'.M')).{Mi'}_inv(SkA').S')

end role

role
role_B(A:agent,B:agent,C:agent,D:agent,SkA:public_key,IDA:text,IDB:text,IDC:text,IDD:te
xt,SND,RCV:channel(dy))
played_by B
def=
        local

        State:nat,PkA:public_key,Ctb:text,Ks:public_key,M:text,Concat:hash_func,S:text,H:h
ash_func,Mi:text
        init
                State := 0
        transition
                1. State=0 /\ RCV(start) =|> State':=1 /\ PkA':=new() /\ Ctb':=new() /\
SND(H(Concat(IDB.Ctb')).{Ctb'}_inv(PkA'))
                2. State=1 /\ RCV(IDC.M') =|> State':=2 /\ Ks':=new() /\ SND({M'}_inv(Ks'))
                4. State=2 /\ RCV(H(Concat(IDD.S'.Mi'.M)).{Mi'}_inv(SkA).S') =|> State':=3
/\ SND(H(IDD.Mi').{Mi'}_inv(SkA).S')
end role
```

```
role
role_C(A:agent,B:agent,C:agent,D:agent,PkA:public_key,IDA:text,IDB:text,IDC:text,IDD:te
xt,SND,RCV:channel(dy))
played_by C
def=
        local
                State:nat,M:text
        init
                State := 0
        transition
                2. State=0 /\ RCV(start) =|> State':=1 /\ M':=new() /\ SND(IDC.M')
end role

role
role_D(A:agent,B:agent,C:agent,D:agent,PkA:public_key,IDA:text,IDB:text,IDC:text,IDD:te
xt,SND,RCV:channel(dy))
played_by D
def=
        local
                State:nat,S:text,H:hash_func,Mi:text,SkA:public_key
        init
                State := 0
        transition
                5. State=0 /\ RCV(H(IDD.Mi').{Mi'}_inv(SkA').S') =|> State':=1
end role

role
session1(SkA:public_key,A:agent,B:agent,C:agent,D:agent,PkA:public_key,IDA:text,IDB:te
xt,IDC:text,IDD:text)
def=
        local
                SND4,RCV4,SND3,RCV3,SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                role_D(A,B,C,D,PkA,IDA,IDB,IDC,IDD,SND4,RCV4) /\
role_C(A,B,C,D,PkA,IDA,IDB,IDC,IDD,SND3,RCV3) /\
role_B(A,B,C,D,SkA,IDA,IDB,IDC,IDD,SND2,RCV2) /\
role_A(A,B,C,D,PkA,IDA,IDB,IDC,IDD,SND1,RCV1)
end role

role environment()
def=
        const

        hash_0:hash_func,actuator:agent,bob:agent,pa:public_key,alice:agent,sensor:agent,ka:
public_key,const_1:text,const_1:text,const_1:text,const_1:text
        intruder_knowledge = {}
        composition
                session1(pa,alice,bob,sensor,actuator,ka,const_1,const_1,const_1,const_1)
end role
 goal
```

secrecy_of pa
end goal

environment()

Cas File :

protocol Autent;
identifiers
A,B,C,D : user;
Ctb,IDA,IDB,IDC,IDD,Mi,S,M : number;
PkA,SkA, Ks : public_key;
H,Concat,AES,KDF,Sign : function;

messages
1. B -> A : H(Concat(IDB,Ctb)), {ctb}PkA'
2. C -> B : IDC,M
3. B -> A : {M}Ks'
4. A -> B : H(Concat(IDD,S,Mi,M)), {Mi}SkA', S
5. B -> D : H(IDD,Mi), {Mi}SkA', S

knowledge

A : A,B,C,D, PkA,IDA,IDB,IDC,IDD;
B : A,B,C,D, SkA,IDA,IDB,IDC,IDD;
C : A,B,C,D, PkA,IDA,IDB,IDC,IDD;
D : A,B,C,D, PkA,IDA,IDB,IDC,IDD;

session_instances
[A: alice, B: bob, C: sensor, D: actuator, PkA:ka, SkA:pa, Ks:ks];

goal
secrecy_of ks;