DYNAMIC AND EFFICIENT AUTHENDICATION SCHEME FOR SECURE HEALTHCARE SYSTEM IN BODY AREA NETWORK

R.Maniyammal[1] | R.Sujitha[2]
[1](UG Student, Christ the King Engineering College, chitrabe97@gmail.com)
[2](Assistant Professor, Christ the King Engineering College, srisuji14@gmail.com)

Abstract— *The wireless body area network (WBAN) technology is one of the core technologies of developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes. However, development of this new technology in healthcare applications without considering security makes patient privacy vulnerable. In this article, at first we highlight the major security requirements in BAN based healthcare system. Subsequently, we propose Robust and Efficient Authentication Scheme based healthcare system using WBAN - HealthCare, which can efficiently accomplish those requirements. And then we used Lightweight Authentication Protocol for secure data sharing in WBAN. Using secure key management Scheme. WBANs not only bring us conveniences but also bring along the challenge of keeping data's confidentiality and preserving patients' privacy. In the past few years, several authentication schemes for WBANs were proposed to enhance security by protecting patients' identities and by encrypting medical data. However, many of these schemes are not secure enough. First, we review the most recent REAS scheme for WBANs and point out that it is not secure for medical applications by proposing an impersonation attack. After that, we propose a new scheme for WBANs and prove that it is provably secure. Our detailed analysis results demonstrate that our proposed scheme not only overcomes the security weaknesses in previous schemes but also has the same computation costs at a client side.*

1. INTRODUCTION

The different types of networks available today are Wired and Wireless networks. Wired are differentiated from wireless as being wired from point to point. Each of these types of networking has their advantages and disadvantages according to security. Wired networking has different hardware requirements and the range and benefits are different. Wireless networking takes into consideration the range, mobility and the several types of hardware components needed to establish a wireless network. There are different types of configurations of networks and the security measures that need to be taken to ensure a secure network.

Organizations rely heavily on the ability to share information throughout the organization in an efficient and productive manner. Computer networks have allowed for this technology and are now a part of almost every business. An organization has two options when it comes to setting up a network. They can use a completely wired network, which uses networking cable to connect computers, or they can use a wireless network, which uses radio frequencies to connect computer. Wireless networks have allowed organizations to become more therefore organizations are now using a combination of both wired and wireless networks.

1.2 WIRELESS SENSOR NETWORKS

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year, for example IPSN, Senses, and EWSN.

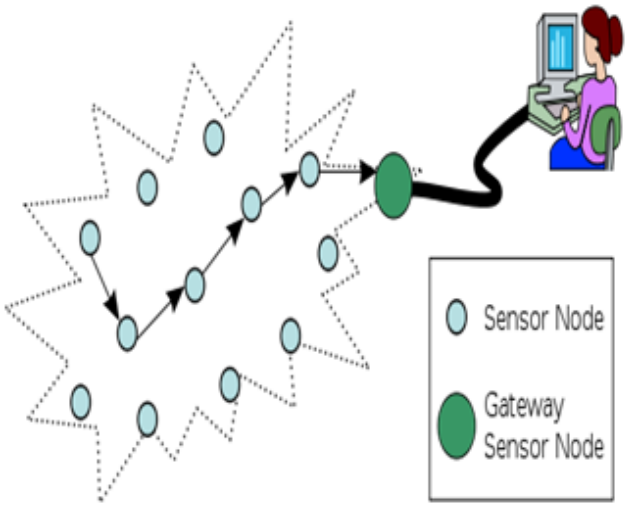

Figure.1.3 Wireless Sensor Network

1.2.1 APPLICATIONS

- Process Management
- Health care monitoring
- Environmental/Earth sensing
- Air pollution monitoring
- Forest fire detection
- Landslide detection

1.2.2 CHARACTERISTICS

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Cross-layer design

Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach presents three main problems:

1. Traditional layered approach cannot share different information among different layers which leads to each layer not having complete information. The traditional layered approach cannot guarantee the optimization of the entire network.
2. The traditional layered approach does not have the ability to adapt to the environmental change.
3. Because of the interference between the different users, access confliction, fading, and the change of environment in the wireless sensor networks, traditional layered approach for wired networks is not applicable to wireless networks.

So the cross-layer can be used to make the optimal modulation to improve the transmission performance, such as data rate, energy efficiency, QoS (Quality of Service), etc.. Sensor nodes can be imagined as small computers which are extremely basic in terms of their interfaces and their components. They usually consist of a processing unit with limited computational power and limited memory, sensors or MEMS (including specific conditioning circuitry), a communication device (usually radio transceivers or alternatively optical), and a power source usually in the form of a battery.

Other possible inclusions are energy harvesting modules, secondary ASICs, and possibly secondary communication interface (e.g. RS-232 or USB).The base stations are one or more components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables.

1.2.3 PLATFORMS

HARDWARE -One major challenge in a WSN is to produce low cost and tiny sensor nodes. There are an increasing number of small companies producing WSN hardware and the commercial situation can be compared to home computing in the 1970s. Many of the nodes are still in the research and development stage, particularly their software. Also inherent to sensor network adoption is the use of very low power methods for radio communication and data acquisition. In many applications, a WSN communicates with a Local Area Network or Wide Area Network through a gateway.

SOFTWARE- Energy is the scarcest resource of WSN nodes, and it determines the lifetime of WSNs. WSNs may be deployed in large numbers in various environments, including remote and hostile regions, where ad hoc communications are a key component. For this reason, algorithms and protocols need to address the following issues:

- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

Lifetime maximization: Energy/Power Consumption of the sensing device should be minimized and sensor nodes should be energy efficient since their limited energy resource determines their lifetime.

- Operating systems
- Security and Mobility
- Usability and maintenance

1.2.4 SIMULATION OF WSNS

At present, agent-based modeling and simulation is the only paradigm which allows the simulation of complex behavior in the environments of wireless sensors (such as flocking). Agent-based simulation of wireless sensor and ad hoc networks is a relatively new paradigm. Agent-based modeling was originally based on social simulation. Network simulators like OPNET, OMNeT++, NetSim, WSNet [12] and NS2 can be used to simulate a wireless sensor network.

1.3 BODY AREA NETWORKS (BAN)

A body area network (BAN), also referred to as a wireless body area network (WBAN) or a body area network (BAN), is a wireless network of wearable computing devices. BAN devices may be embedded inside the body, implants, may be surface-mounted on the body in a fixed position Wearable technology or may be accompanied devices which humans can carry in different positions, in clothes pockets, by hand or in various bags. Whilst there is a trend towards the miniaturization of devices, in

particular, networks consisting of several miniaturized body sensor units (BSUs) together with a single body central unit (BCU). Larger decimeter (tab and pad) sized smart devices, accompanied devices, still play an important role in terms of acting as a data hub, data gateway and providing a user interface to view and manage BAN applications, in-situ.

The development of WBAN technology started around 1995 around the idea of using wireless personal area network (WPAN) technologies to implement communications on, near, and around the human body. About six years later, the term "BAN" came to refer systems where communication is entirely within, on, and in the immediate proximity of a human body. A WBAN system can use WPAN wireless technologies as gateways to reach longer ranges. Through gateway devices, it is possible to connect the wearable devices on the human body to the internet. This way, medical professionals can access patient data online using the internet independent of the patient location.

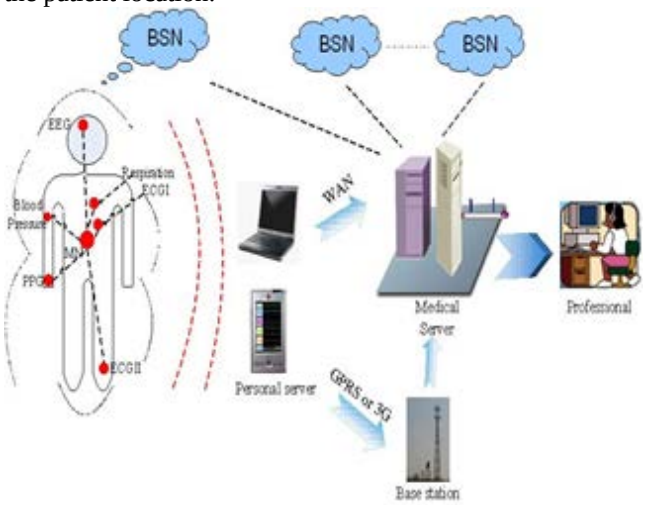

Figure.1.4BodyArea Network

This chapter outlines the Wireless BODY AREA NETWORKS (WBANs) component of the CAPSIL roadmap. The current state of the art in terms of technology, applications and research challenges and in particular body worn sensor networks for home monitoring of healthcare and ageing-in place applications are described.

BODY AREA NETWORKS are a specific category of wireless sensor networks intended to operate in a pervasive manner for on-body applications. Much of the theory relating to general wireless sensors relates also to BODY AREA NETWORKS (BNSs) and issues such as power optimization, battery life performance and radio design are key. These issues are examined in the first section of the chapter and key design considerations such as the correlation between Moore's Law (i.e. integration density) and power/battery performance are discussed.

Key to body worn sensors are issues such as usability, durability, robustness, how well the sensor 'fits' in with the application and reliability and security of the data. Sensor networks suffer from the so called 'reliability dilemma' which means that the more reliable and secure you want to make data transmission, the higher the data overhead and consequently the higher the power required, hence battery life is reduced. These issues are discussed and some of the techniques for overcoming this dilemma are discussed. System-On-Chip developments promise to significantly advance sensor integration (and reduce cost) and some of the current offerings in this area are presented. Notable research projects in this space are summarized and current research within the EU is also summarized.

This document also examines the software aspects of wireless sensor networks and presents a brief history of operating systems development from the original single thread, event-driven TinyOS to some of today's multithread systems such as Contiki and Mantis. As sensor networks have evolved from the domain of the programmer and scientist to general use, so have the means of developing solutions and rapid prototypes. No longer do users need to be proficient programmers and developers and environments such as Mote view, Lab VIEW and BioMOBIUS™ are presented as environments that facilitate non-programming users to build solutions and rapid prototypes.

A wireless sensor network is a collection of nodes organized into a cooperative network. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces. In particular, their application to healthcare areas received much attention recently. The design and development of wearable biomedical sensor systems for health monitoring has drawn particular attention from both academia and industry. As an extension to the WSN a body area network (BAN), also referred to as a wireless body area network (WBAN) or a body area network (BAN), is a wireless network of wearable computing devices. The development of WBAN technology started around 1995 around the idea of using wireless personal area network (WPAN) technologies to implement communications on, near, and around the human body.

The implanted sensors in the human body will collect various physiological changes in order to monitor the patient's health status no matter their location. The information will be transmitted wirelessly to an external processing unit. This device will instantly transmit all information in real time to the doctors throughout the world. If an emergency is detected, the physicians will immediately inform the patient through the computer system by sending appropriate messages or alarms. Currently the level of information provided and energy resources capable of powering the sensors are limiting factors.

WSN	BSN
Low level security	High security
Accessible power supply	Inaccessible power source
High power demand	Lower power availability
Solar,wind power	Thermal, piezoelectric energy
Replaceable/disposable	Biodegradeable
No biocompatibility needed	Biocompatible
Low context awareness	High context awareness
Wireless solutions available	Lower power wireless
Data loss less of an issue	Sensitive to data loss

WSN	BSN
Cover the environment	Cover the human body
Large number of nodes	Fewer sensor nodes
Multiple dedicated sensors	Single multitasking sensors
Lower accuracy	Robust & Accurate
Small size not limiting factor	Miniaturization
Resistant to weather,	Pervasive
Resistant to noise	Predictable environment
Resistant to asynchrony	Motion artefacts an issue
Early adverse event detection	Early adverse event detection
Failure reversible	Failure irreversible
Fixed structure	Variable structure

1.3.1 Vulnerability

Vulnerability is an important part of any system and it is a major area of research in general WSN. Wireless media is always more vulnerable than wired media for attackers. This is more important in healthcare applications since a security breach can result in life threatening situations. We can define security at several levels in healthcare applications. The security threats can occur during routing the data where intruders may change the destination, can make routing inconsistent or even steal the data by eavesdropping the wireless communication media. The attackers can steal or modify the data routing through GPRSor similar networks.

The criminal-minded attackers can track the user location or can keep an eye on user's activity. The attackers can fiddle with the data by forging alarms. They can also wage the Denial of Service (DoS) and Jamming attacks on the networks. Data Encryption and Authentication are major security techniques used for security provision. Data encryption techniques must be used for secured data transfer and legitimate devices must be allowed to create or inject data into the system. One of the solutions against security threats is to implement different encryption techniques.

1.3.2 Power Sources

No matter how intelligent the routing mechanism or how adaptive the network, if the sensor loses power the sensor is simply nonfunctional. Significantly more work is needed on alternative low cost power techniques such as solar, fuel cells and RF coupling.

1.3.3 Usability

Much of the work in this space has stopped at lab type prototype solutions. More commercial devices are needed and more studies needed on performance in real world applications.

Figure1.5 Applications of BAN

A. Sports and Fitness - In Sports WBAN can be used to examine the health of the athletes. Readings can be taken from the athletes without requiring them to exercise on a treadmill. Coaches can take a closer look at the strong and weak points of an athlete by measuring various body conditions like change in heartbeat, oxygen level etc.

B. Military - Uses of WBAN in defense are many. Examining the health condition of soldiers, checking level of hydration, tracking their location and body temperature monitoring are few of them. All the readings can be used for providing help to the soldiers when they get injured, to get an idea of when strength, precision, attention have to be enhanced and can also be used for reducing incidents of friendly fire due to misunderstanding in identity by telling them their exact location and identity time to time.

C. Emergency Services - WBAN can be used in providing emergency services to fire fighters. The readings of changes in body conditions of fire fighters like oxygen level, pulse etc. is taken and along with it the toxin level in the air are monitored and the fire fighters are warned in case of the emergency conditions or asked to leave the location or use some preventive measures like using gas mask.

E. Emotion Detection - Human emotions can also be monitored by WBAN. A chemical called serotonin is created in the human body by the brain and the intestine.

Decrease in level of serotonin causes sadness and increased level causes happiness or anxiety. Thus we can keep track of this chemical and know the mood of the person.

F. Personal Health Monitoring - Non-stop monitoring of critical parameters of the patients who suffer from chronic diseases such as heart attacks, asthma and diabetes can be done by WBAN Readings of ECG, EMG can be taken by patients on their own at home and can be checked by doctors.

G. Posture Detection - The posture of a person can be detected by using sensor nodes. Games can be played on computer by wearing sensors over body that gives a feel as if a person is playing on a real field. The motion of the player changes as per player's motion. Dance lessons can also be given by gesture detection and body movement.

H. Medical - BANs can prove to very helpful in monitoring the health of the patients from faraway places. The patient and doctor do not necessarily have to be at the hospital. Even when patients are at home they can be administered medicines and their body's vital signs like blood glucose level, heartbeat, blood pressure etc. can be checked.

I. Consumer Electronics - Devices like microphone, MP3 players and head mounted displays can form a part of BAN and play their respective roles. Like as per the mood of the person songs can be played etc.

1.4 THE INTERNET OF THINGS (IoT)

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT revolution"—from new market opportunities and business models to concerns about security, privacy, and technical interoperability.

The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home'', offering more security and energy efficiency. Other personal IoT devices like wearable fitness and health monitoring devices and network enabled medical devices are transforming the way healthcare services are delivered.

This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost.1 IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities'', which help minimize congestion and energy consumption. IoT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. However, IoT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized.

Fundamentally, the Internet Society cares about the IoT as it represents a growing aspect of how people and institutions are likely to interact with the Internet in their personal, social, and economic lives. If even modest projections are correct, an explosion of IoT applications could present a fundamental shift in how users engage with and are impacted by the Internet, raising new issues and different dimensions of existing challenges across user/consumer concerns, technology, policy and law. IoT also will likely have varying consequences in different economies and regions, bringing a diverse set of opportunities and challenges across the globe.

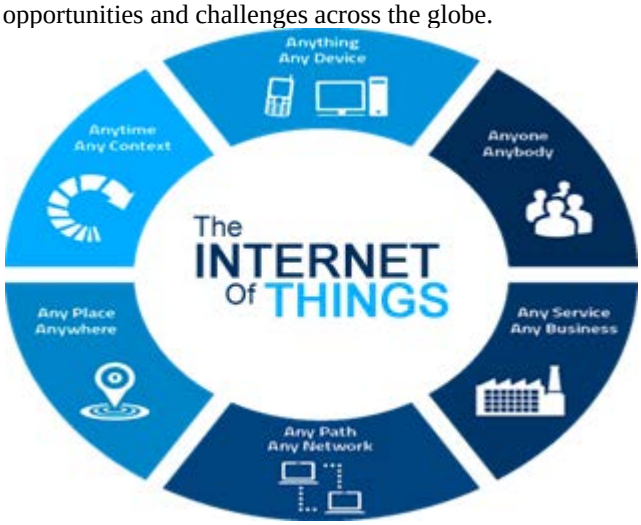

Figure.1.6 Internet of Things

Everyone, however, thinks of the IoT as billions of connections (a sort of "universal global neural network" in the cloud) that will encompass every aspect of our lives. All of this public discussion suggests the IoT is finally becoming a hot topic within the mainstream media. Many recent articles point to the IoT as the interaction and exchange of data (lots of it) between machines and objects, and now there are product definitions reflecting the same concept.

A quick Internet search highlighted the following example use cases/applications under consideration:

- Machine-to-machine communication
- Machine-to-infrastructure communication
- Tele health: remote or real-time pervasive monitoring of patients, diagnosis and drug delivery
- Continuous monitoring of, and firmware upgrades for, vehicles
- Asset tracking of goods on the move
- Automatic traffic management
- Remote security and control
- Environmental monitoring and control
- Home and industrial building automation
- "Smart" applications, including cities, water, agriculture, buildings, grid, meters, broadband, cars, appliances, tags, animal farming and the environment, to name a few.

The IoT is expected to transform how we live, work and play. From factory automation and automotive connectivity to wearable body sensors and home appliances, the IoT is set to touch every facet of our lives. We will "author" our life with networks around us that constantly change and evolve based on our surroundings and inputs from other systems

• Ubiquitous Connectivity—Low–cost, high–speed, pervasive network connectivity, especially through licensed and unlicensed wireless services and technology, makes almost everything "connectable''.
• Widespread adoption of IP–based networking— IP has become the dominant global standard for networking, providing a well–defined and widely implemented platform of software and tools that can be incorporated into a broad range of devices easily and inexpensively.
• Miniaturization— Manufacturing advances allow cutting-edge computing and communications technology to be incorporated into very small objects. Coupled with greater computing economics, this has fuelled the advancement of small and inexpensive sensor devices, which drive many IoT applications.
• Advances in Data Analytics— New algorithms and rapid increases in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; these large and dynamic datasets provide new opportunities for extracting information and knowledge.
• Rise of Cloud Computing– Cloud computing, which leverages remote, networked computing resources to process, manage, and store data, allows small and distributed devices to interact with powerful back-end analytic and control capabilities. From this perspective, the IoT represents the convergence of a variety of computing and connectivity trends that have been evolving for many decades.
IoT may force a shift in thinking if the most common interaction with the Internet and the data derived and exchanged from that interaction -- comes from passive engagement with connected objects in the broader environment. The potential realization of this outcome a "hyper connected world" is a testament to the general-purpose nature of the Internet architecture, which does not place inherent limitations on the applications or services that can make use of the technology.

2. CONCLUSION

To defend against code-reuse attacks increase the entropy by randomizing the function blocks. This randomization may be applied at various levels of block level. The level of granularity is to choose is a tradeoff between security and performance. In our implementation, we implemented the randomization at the function level which is the most coarse granularity amongst the three mentioned above. However, we show that even this coarse level of granularity provides substantial randomization to make brute force attacks infeasible.

Randomizing at basic block granularity will likely incur higher runtime overhead as it would break the principle of locality. DSA algorithm will have will have a great effect on all of our federal agencies because they are required to use this standard when transmitting information that is not declassified. This standard is also available to the private sector and commercial organizations. The DSA is necessary to make sure that our governments' communications are secure. The standard ensures that these federal agencies that may have not had a secure algorithm to transmit data will now have such a means to make sure communications are secure.

REFERENCES

[1] C. Lin, P. Wang, H. Song, Y. Zhou, Q. Liu, G. Wu, "A differential privacy protection scheme for sensitive big data in body sensor networks," Annals of Telecommunications, 2016, ISSN 0003-4347.
[2] A. Siva Sangari, J. Martin Leo Manickam, "Secure Communication over BSN Using Modified Feather Light Weight Block (MFLB) Cipher Encryption," Journal of Software, vol. 10, pp. 961, 2015, ISSN 1796217X.
[3] T. Hayajneh, B. Mohd, M. Imran, G. Almashaqbeh, A. Vasilakos. "Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks," Sensors, vol. 16, pp. 424, 2016, ISSN 1424-8220.
[4] Y. Zhou, B. Yang, W. Zhang, "Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing," Discrete Applied Mathematics, vol. 204, no. 5, pp. 185202, 2016.