Integrated Authentication Based on CDMA Modulation for Physical Layer Security of Wireless Body Area Network

Venkatasubramanian Sivaprasatham
Faculty, Department of Information Technology, Nizwa College of Technology, Nizwa, Sultanate of Oman
venkatasubramanian.sivaprasatham@nct.edu.om
Jothi Venkateswaran
HOD, Department of Computer Science, Presidency
College, Chennai, TamilNadu, India
jothivenkateswaran@yahoo.co.in
and
Hafid Taher Ba Omar
Dean, Nizwa College of Technology, Nizwa, Sultanate of Oman
baomar@nct.edu.om

Abstract

In this paper, to prevent physical layer attacks like jamming in Wireless Body Area Networks (WBAN), we propose an authentication mechanism using the CDMA modulation technique and a secure key management technique. Initially, sensor nodes use a shared symmetric key. When a node wants to join a network, it forwards a request message protected by the message authentication code (MAC) to the intermediate control node. The intermediate control node sends the request to the master node. The master server verifies the MAC master key for the node and sends it to the intermediate control node. The encryption and decryption are done at two different levels which include the transmission level and the master server level. The proposed approach offers data confidentiality and integrity in WBANs in the data link layer and the physical layer. By simulation results, we show that the proposed approach provides more security with less delay and overhead.

Keywords: Wireless Body Area Networks, Server, Authentication, Intermediate node, Keying function, Transmission keys

1. Introduction

1.1 Wireless Body Area Network (WBAN)

WBAN is defined as a wireless body area network [1]. WBAN is the network that permits the combination of smart, small scale, minimum power, aggressive/discreet sensor nodes which monitor body activities and neighboring environments. Every intelligent node in the network has the potential to forward information to the base station after processing to obtain the diagnosis and prescription. [2] The application of WBANs is utilized in the medical field as well as in consumer electronics applications. [3] The features of WBAN are listed below. [1]

- It is a miniature wireless network for communicating within a 3 meter gap.
- The speed at which the data is transmitted varies from 10Kbps to 10Mbps.
- The star topology is the fundamental arrangement considered with WBANs, and BAN nodes (BNs) communicate with the BAN network controller (BNC) alone.
- BNs possess restricted power, calculation and communication capabilities.
- An Energy efficient security mechanism is required with reduced overhead and also such requirements as data integrity, authentication and encryption should be fulfilled.
- The network surrounds the body for implanting its communication system.
- WBAN mainly detects, collects and transmits biomedical information.

The key issues to take into account while designing WBAN are Physical layer limits, MACs, Power limitation and short RF transmission range, mobility, and the minimum and time-dependent quality of wireless links and Network size [4].

1.2 Security Risks in WBANs

The susceptible nature of wireless channel results in a wide range of security threats which inhibit the WBANs progress [6]. Depending on the network layers, attacks over the WBAN are categorized into the following classes.

A. Physical layer attacks - Some of the important responsibilities of physical layer include frequency selection and generation, signal detection, modulation, and encryption [9]. As the medium is radio-based, jamming the network is always possible. Two most common attacks are jamming and tampering. Jamming is defined as the interference with the radio frequencies of the nodes. The jamming source can be powerful enough to disrupt the entire network. Tampering is defined as a physical attack on the sensor nodes. Nodes in WBAN are deployed in close proximity to the human body, and this reduces the chances of physical tampering.

B. Data link layer attacks - The Data link layer is responsible for multiplexing, frame detection, channel access, and reliability. Attacks on this layer include creating collisions, unfairness in the allocation, and resource exhaustion. A collision occurs when two or more nodes attempt to transmit at the same time in the same medium. An adversary may strategically create extra collisions by sending repeated messages to the channel. Unfairness degrades the network performance by interrupting the MAC priority schemes. Exhaustion of battery resources may occur when a self-sacrificing node always keeps the channel busy.

C. Network layer attacks - The nodes in WBAN are not required to route packets to other nodes. Routing is possible when multiple WBANs communicate with each other through their coordinators. Possible attacks include spoofing, selective forwarding, Sybil, and hello floods; In spoofing, the attacker targets the routing information and alters it to disrupt the network. In selective forwarding, the attacker forwards selective messages and drops the others [11]. In Sybil, the attacker represents more than one identity in the network [12]. Hello flood attacks are used to fool the network, i.e., The sender is within the radio range of the receiver.

D. Transport layer attacks - The attacks involved in the transport layer are flooding and de-synchronization. In flooding, the attacker repeatedly places requests for connection until the required resources are exhausted or reach a maximum limit. In de-synchronization, the attacker forges messages between nodes causing them to request the transmission of missing frames.

1.3 Fundamental security requirements in a WBAN

This section presents the fundamental security requirements of WBANs [5]

- Data Confidentiality
- Data Authentication
- Data Integrity
- Data Freshness.
- Security Management
- Availability

This paper divides the network in a tree like structure. The modulation technique is enhanced to CDMA. For the reference and problem formulation we have considered some existing papers in Section 2. After that our method which is Integrated Authentication and Security Check with CDMA (IASC) is proposed. This proposal is further supported by its advantages and future works and concluded.

2. Related Work

In [15], the proposed architecture consists of a set of WBANs connected to the backend server. The backend server relays the information sought by the sensor node to the master server through the internet.

All the sensor nodes will discover the master server by using node id. It generates a unique secret key for each node. When a node enters a network, it sends a request message protected by the MAC to the master server via the backend server. The master server authenticates the MAC and generates a message key and master key for the node and sends it to the master server through the backend server.

Their proposed technique shows an improved packet delivery ratio with reduced delay and overhead. But this paper does not discuss long range transmission and some of the physical and MAC layer security checking.

The work in [9] explains the use of Guaranteed Time Slots in WSN communication. After introducing the communication sequences of GTS allocation and DE allocation schemes, the paper identifies a GTS attack through illustrating various scenarios. Besides the attacks stated in Section II, our GTS attack scenarios contribute to WSN attack literature as categorized by the MAC layer attack type.

This paper investigates WSN attacks including a brief survey of physical layer, MAC layer, routing layer, transport layer, and application layer attacks. Furthermore, a new IEEE 802.15.4 MAC layer attack, the GTS attack [1], is defined and evaluated with respect to intelligence and random attacker behavior scenarios.

Future work of this paper will focus on tuning different parameters in GTS attack scenarios. The detection probability should be investigated when there is a lack of fine-grained time synchronization between the PAN coordinator and the GTS attacker. Additionally, a GTS-based application will be simulated and analyzed under GTS attack conditions.

The authors of [11] show the possibility of hiding data in wireless sensor networks by using a PHY layer field of the 802.15.4 protocol. The authors describe different possibilities for hiding data in MAC layer fields of the 802.15.4 protocol. They [11] analyze the risks and limits of this kind of attack. The authors discuss solutions for protecting wireless sensor networks against steganography attacks in layers of the 802.15.4 protocol.

The proposed set of rules and the use of a watchdog limit the possibilities of steganographic attacks. However, steganography is a new research path in wireless sensor networks and the author acknowledge that some other possibilities of cover objects for steganographic attacks can be found.

Other solutions can be sought to detect hidden data using steganalysis and also finding energy-efficient solutions based on steganography in order to reinforce wireless sensor network security.

The author [12] considered a particular class of DoS attacks called jamming attacks using IEEE 802.15.4 based OPNET simulative model for WSN, under a constant and varying intensity of attacks. The effects of the number of attackers on SNR, BER, network throughput and PDR are inclusively evaluated for the simulated scenarios.

The impact of a constant and varying intensity jamming attack over WSNs has been studied using the OPNET simulation software. The presence of malicious nodes drastically compromises WSN performance as jamming attacks limit the amount of legitimate sensing data reaching the analyzer node. Under constant jamming attack, simulations revealed that average sink node PDR degrades.

The above described methods describe backend server, master server which is good for the fewest numbers of sensor nodes but when the number of sensor nodes increases the workload on the master server increases. Increase in work load may lead to an erroneous output. Giving time slots to different operations is not the best way for transmission of data packets in a wireless body area network as two separate transmissions need a time slot difference to avoid interference. There are some other types of physical issues like the full use of frequency bands present after solving a steganography problem. Some easier techniques exist to prohibit jamming. We have given a method to protect the method against this kind of erroneous operation.

3. Proposed Solution

3.1 Overview

In wireless body area network security is an important concern. Security attacks can be any layer of the network. In this paper we are basically focusing upon the physical layer and MAC. Physical layer attacks mainly consist of spoofing and warm-hole attacks. Other factors that affect security includes: frequency jamming, un-authentication use of data, deciphering of data from other nodes, and dropping of the message. The previous work [17] shows a key-authentication technique with two types of server which includes a master server. This technique shows a good result when the body area network has a smaller number of node sets. When the number of sensor nodes is increasing, there is always a chance of frequency jamming. The authentication check of a larger set of nodes at a single point increases the risk of late response to data. Other authors have offered different methods to apply the network in a binary tree structure. However, when the number of sensor nodes increases to an undefined value the problem remains. The greater the number of sensor nodes, the slower the process can become.

Considering all the above factors our abstract proposes a security checking method which includes the division of the network in to a tree like structure. The nodes are mainly divided into three levels. The first one is a network coordinator node which carries the master server; some control nodes which are the intermediate nodes are used for the enhancement of security and data processing, and another part is compromised at sensor nodes, which are capable of transmission of their data packets using CDMA technology. The sensor nodes cipher the data for transmission.

In the proposed method we first define some fundamental issues in the overview. In the second part this procedure moves to prove its use of CDMA technology and its advantages to the network. A clear idea of CDMA structure and its advantages in the network is given in this section. The next part the paper focuses on the architecture diagram of the solution. Following that, the method for detecting and avoiding frequency jamming is discussed. Then we proceed to the creating of keying and rekeying methods. Finally in this method, the overall algorithm is shown.

3.2 Using CDMA for Attack Detection

Basically jamming, unwanted transmission loss, and worm holes can be easily eliminated using this method. Sharing of keys and using CDMA technologies easily can prohibit the worm hole effect.

Physical attack refers to when an unwanted node tries to destroy the message package by using a high frequency. The high frequency can create a high level of interference which creates jamming and degrades the functionality of the receiver which is present at nodes of the WBN. Jamming can also occur when there are too many data packets at a node. Too many data packets at a node causes slow processing. Our proposed solution is to divide the power of selecting the correct data packet in to two different levels. For that purpose it carries intermediate levels.

For the avoidance of high frequency we have used a band pass filter and CDMA technology. CDMA technology shares a code among the network nodes. It is like having 4 people in a room, two of whom are speaking Hindi to each other, while the other two are conversing in English. The two pairs don’t interfere with each other, just as the receiver node ignores non pertinent messages.

Modulation technique is mainly of CDMA, TDMA, and FDMA. These modulation techniques can be applied to any type of network. The band pass filter cannot be applied to FDMA techniques because it varies in frequencies among different signals. Some authors have tried to apply TDMA in WBN but the presence of the high guard band makes the system inefficient. So CDMA is used.

CDMA is a modulation technique which uses a shared code between two more nodes so that no other node can understand it. In a certain frequency range, a number of CDMA coded signals can be passed. CDMA uses the frequency band fully. As the frequency band is always constant, we can use a constant band pass filter throughout the lifetime of the network. It can easily detect unwanted nodes and the band pass filter limits the frequency in a range. CDMA technique is always a complex and error free method. Now a day’s invention of high speed processor and Nano technology makes CDMA available from everywhere. In this method CDMA technology is used. The detail of CDMA technology is given in the papers [18] [19].

A simple structure of CDMA modulation is given by

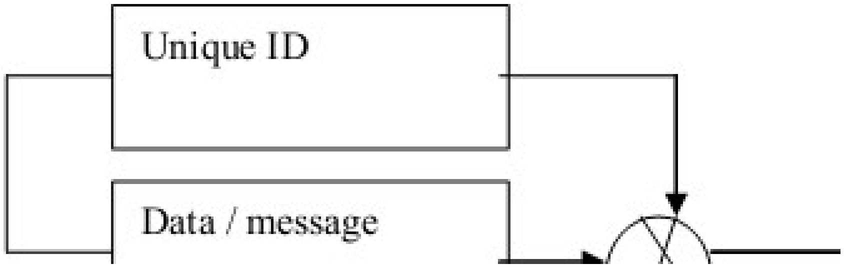

Fig-1. Showing an Architectural Diagram of CDMA Modulation

At the sensor node the signal is modulated with CDMA code to transfer the message to the intermediate control node.

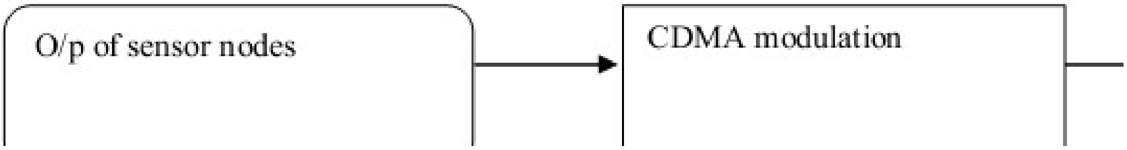

Fig-2. **A**rchitecture of CDMA Modulation at Sensor Node

3.3. System Architecture

Assumptions

There are three types of nodes present. The topmost type of node is a central control node. The central control node carries the master server. It is the coordinator of the network between the client server and the responding server. The second type of node is an intermediate control node. These nodes are capable of taking decisions, deciphering the data, ciphering data, and they are capable of two way communication which includes the connection to the sensor nodes and to the master node. The other type of node is the sensor node. Sensor nodes are capable of sensing data, converting it to the standard form for communication, and ciphering the data with two types of keys. The sensor node is also capable of communicating with other nodes with CDMA technology. Every sensor node has a timer. All types of nodes are authenticated statically or dynamically to send or receive from some specific nodes only. At the time of formation of sensor nodes, every node is given a symmetric key.

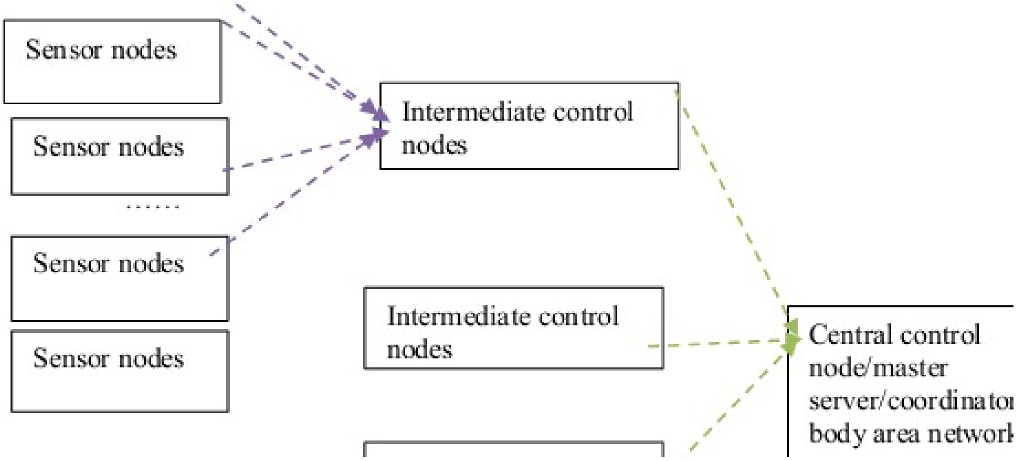
Sensor nodes
Sensor nodes
......
Sensor nodes
Sensor nodes
Intermediate control nodes
Intermediate control nodes
Central control node/master server/coordinator body area network

Fig-3 Showing the real scenario of Wireless Body Area Network

The above figure shows the central control system is not directly connected with the sensor nodes. The message packet travels through the intermediate control nodes. The security checking is in two phases. The first phase consists of a node authentication check of sender nodes and the second part consists of the generation of a security key for the cipher and deciphering the data packet. A method for the generation of a security key is given in the paper [17].

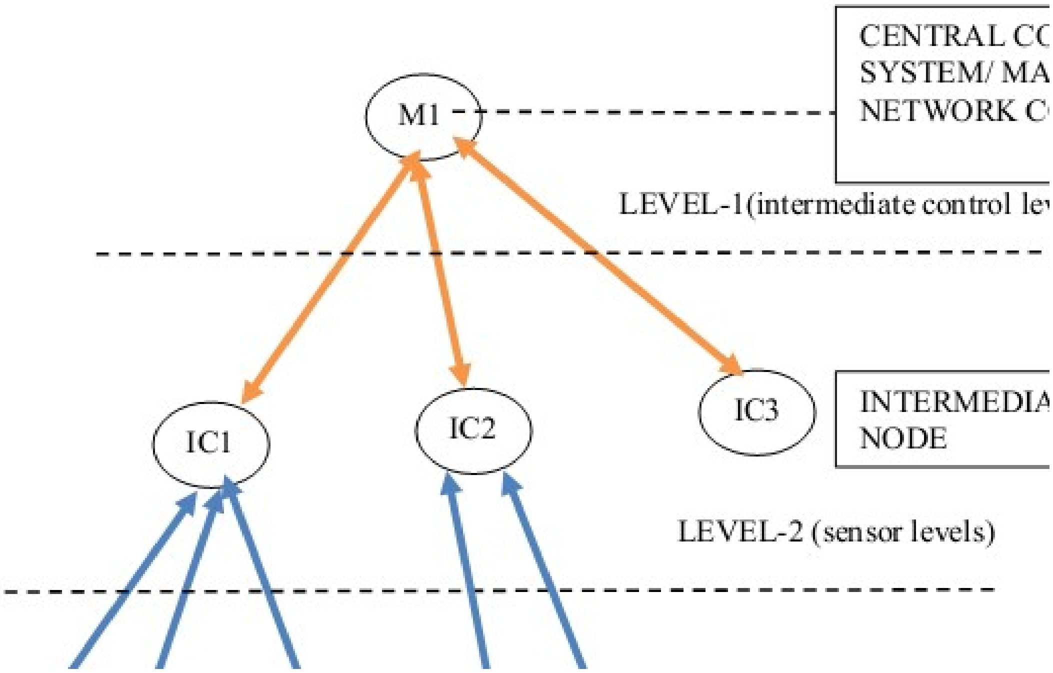

Fig-4. Showing the Communication from Sensor Nodes to Central Control System through a Tree Structure

Security checking at only the master-server level increases the time duration of the response, so we divided the architecture of the wireless body area network into three steps introducing intermediate control nodes. The whole architecture follows a tree like structure, so that authentication check is divided into multiple levels.

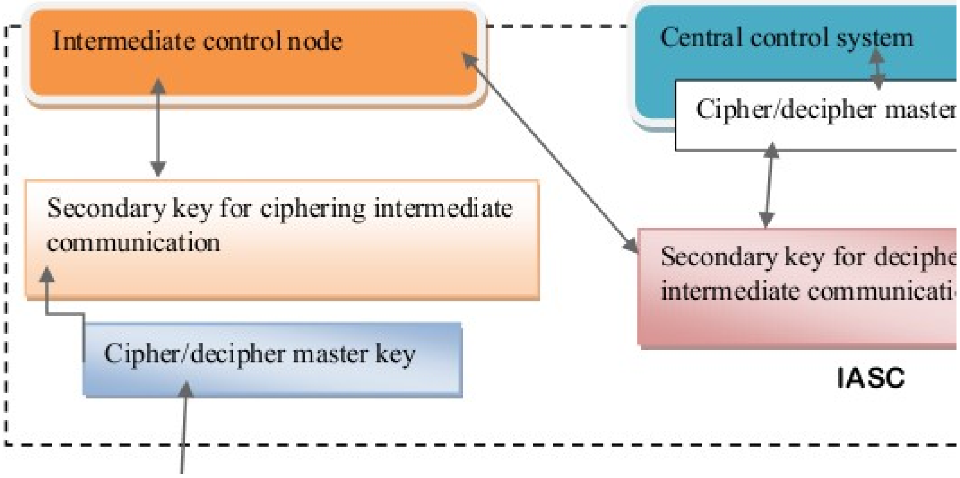
Intermediate control node
Central control system
Cipher/decipher master
Secondary key for ciphering intermediate communication
Secondary key for deciphe intermediate communicati
Cipher/decipher master key
IASC

Fig-5. Showing Architectural Diagram of the Proposed IASC Method

3.4 Mitigation of Frequency Jamming Attack

Frequency jamming can be easily avoided by using a band pass filter. The details of band pass filter are given in [20]. In CDMA a limited band of frequency is used.

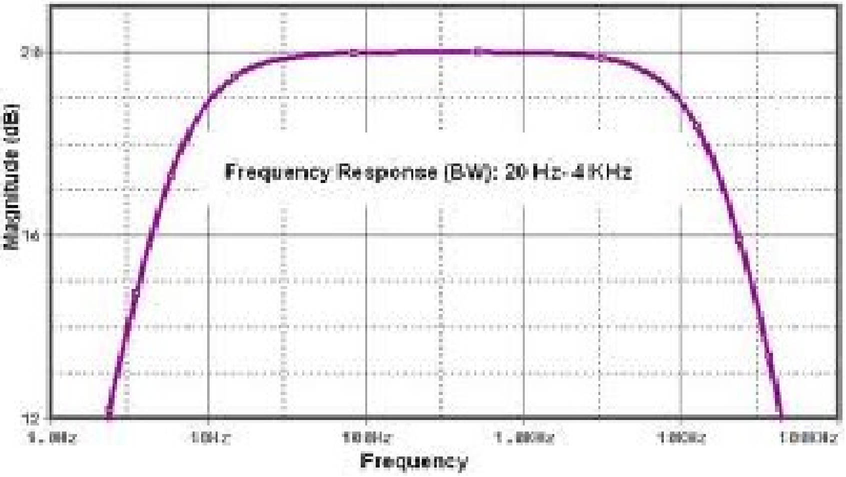

Fig-6. Showing Band-Pass Filter

The above figure clearly shows a response of a band-pass filter. The response diagram clearly shows which is allowing a single bandwidth signal to pass. It clearly shows it can avoid the frequency jamming. We have not considered the jamming detection as we first omitted the unwanted part of frequency range.

A frequency jammer or a band pass filter is used at the receiving point of the intermediate control nodes, the sensor nodes and at the master server.

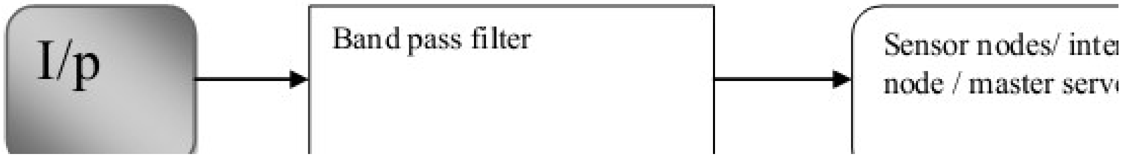

Fig -7. Showing the Architecture of Receiving at Nodes of Wireless Body Area Network

3.5 Key Generation and Key Updation

Master Key Generation

For any message transmitted in the network, encryption and authentication are required. Initially sensor nodes SNi share a master key with master node.

The symmetric key $k_{ms}^{SN_i}$ for a sensor node SNi is generated as follows.

$= \lambda m$ ksec(SNi)…………………………………………… …………………(1)

Where λ*m* = pseudo random function master keys generation of master key.
Ksec(SNi) = secret key of the node.

Intermediate transmission Key Generation

For any message transmitted in the network, encryption and authentication are required. Initially sensor nodes SNi share a symmetric key with MS.

The intermediate transmission key $k_{ms}^{SN_i}$ for a sensor node Ni is generated as follows.

$$k_{im}^{SN_i} = \lambda i \, \mathrm{k}_{\mathrm{sec}}(\mathrm{N}_\mathrm{i})\text{……..……..……………………… ……………………}(2)$$

Where λi = pseudo random function for intermediate transmission.

Ksec (Ni) = secret key of the node

Here the intermediate transfer key is of two types. One of is for down transmission that is for sensor node to intermediate control and vice versa. So it can be defined as $k_{im1}^{SN_i}$ which is built by the function $\lambda i1$. The second type is for up transmission that is for an intermediate control node to the master node. So we can define the intermediate key as $k_{im2}^{SN_i}$ which is built by a function λi 2.

The procedure of joining of a new node

For any message transmitted in the network, encryption and authentication are required. Initially sensor nodes SNi share a symmetric key with MS.

The symmetric key $k_{sy}^{SN_i}$ for a sensor node SNi is generated as follows.

$$k_{sy}^{SN_i} = \lambda\, k_{sec}(SN_i)\ldots \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(3)$$

Where λ = pseudo random function.

Ksec (SNi) = secret key of the sensor node.

With this code the newly entered sensor nodes send a request to the intermediate control node from sensor node to intermediate control node

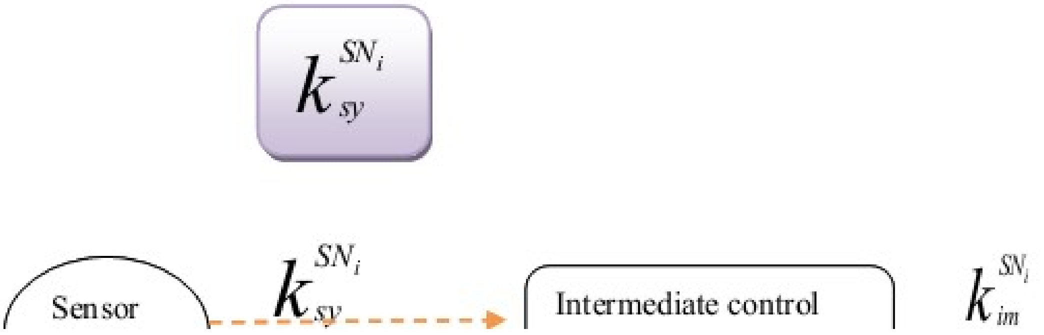

Fig-8. Showing Request of Attachment with the WBN

When a new node wants to join in the body area network, it first sends a request to the nearest intermediate control node with the symmetric key. The intermediate control node forwards this request to the master server with the symmetric key of the sensor node.

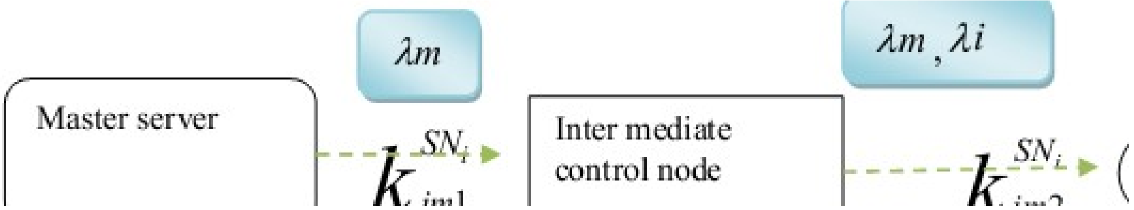

Fig-9. Showing Authentication given by the Master Server to the Sensor Nodes

After successful authentication, the master server (MS) supplies the unique master key function (λm) to each SNi through the intermediate control node. The intermediate control node also supplies the intermediate transmission function (λi) to each sensor node (SNi). The sensor node generates a message authentication code (MAC) key (kmac) which is the multiplication unique ID (UI) with the master key.

$$K_M = k_{ms}^{SN_i} *UI \text{ .... } (4)$$

When SNi wants to transmit the data to MS, the data is encrypted by the key $k_{ms}^{SN_i}$ and signed by the MAC key Kmac before transmission. Then the message is once again encrypted by $k_{im1}^{SN_i}$ and transmitted to an intermediate control node. The intermediate control node deciphers the message using of function ($k_{im1}^{SN_i}$). Then the intermediate control node ciphers the message using the intermediate transmission key ($k_{im2}^{SN_i}$). After getting the message, the master server first deciphers the message with the intermediate transmission key ($k_{im2}^{SN_i}$). After passing the authentication phase the message is deciphered by master key ($k_{ms}^{SN_i}$). After getting the data packet the master sends an acknowledgement to the sensor (SNi) node.

When a data packet is received at the intermediate control node it first goes through an authentication. The intermediate control node accepts only from some nodes and those nodes must be sensor nodes. The master server accepts only from the intermediate control node.

Table-1. showing authentication check table present at the intermediate node

Sensor Node-1	Sensor Node-2	Sensor Node-3	Sensor Node-4	Sensor Node-5	Sensor Node-6	Sensor Node-7	……	Sensor Node-n-1	Sensor Node n

Table-2. showing authentication check table present at the master server

Intermediate control node-1	Intermediate control node-2	Intermediate control node-3	……………………	Intermediate control node-n

3.6 Overall Algorithm

1. At the time of network design all the nodes in the network are identified by a unique ID.
2. The sensor node generates a data packet and ciphers it first using the master key ($k_{ms}^{SN_i}$) which is known to only the sensor node or central control node.
3. Then the sensor node once again ciphers the data using the intermediate ciphering key ($k_{im1}^{SN_i}$) for the intermediate control node.
4. The sensor node generates the MAC (message authentication check) as defined as above.
5. Then the data is modulated in CDMA technology and transferred to the corresponding intermediate control node which is pre-defined before the deployment of the network.
6. The sensor node starts the timer.
7. The intermediate relay node has a band pass filter which filters out a certain range of frequency.
8. Then the packet is processed to an authentication checking phase through the unique id. An intermediate control node is allowed to a certain number of nodes from where it accepts the data packet.
9. The intermediate control node deciphers the message using the key ($k_{im1}^{SN_i}$) and once again encrypts it with a new set of keys to communicate using the key ($k_{im2}^{SN_i}$) with the central control node/ master server.

10. The message is once again modulated with the CDMA technology and transferred to the master server/ central control system.
11. The master server when gets a data packet. It first collects the node's id and checks whether the intermediate control is an authenticated node. The master server is allowed to collect information only from an intermediate control node.
12. If the message is from an authenticated node then it deciphers the message by using the intermediate connection keys ($k_{im2}^{SN_i}$).
13. Then the message is deciphered with the master key ($k_{ms}^{SN_i}$). From this message the master server gets the data which has been sent by the sensor node.
14. After getting the data the master server sends an acknowledgement to the sensor node.
15. If the sensor does not get any acknowledgement from the master server before reaching 0, then the sensor node once again transmits the message.

4. Simulation Results

4.1. Simulation Parameters

To simulate the proposed Integrated Authentication based on CDMA Modulation for physical layer security (IACM) technique, NS-2 [16] is used. A network area of 50 X 50 m is considered. The IEEE 802.15.4 is used as the MAC layer since it provides reliable communication for the devices. For all types of communications, it provides access to the physical channel. It also supports security features. The IEEE 802.15.4 specification uses physical layer (PHY) options based on direct sequence spread spectrum (DSSS) which uses the frame structure for low-duty-cycle low-power operation containing a 32-bit preamble frame length.

4.2 Simulation Topology

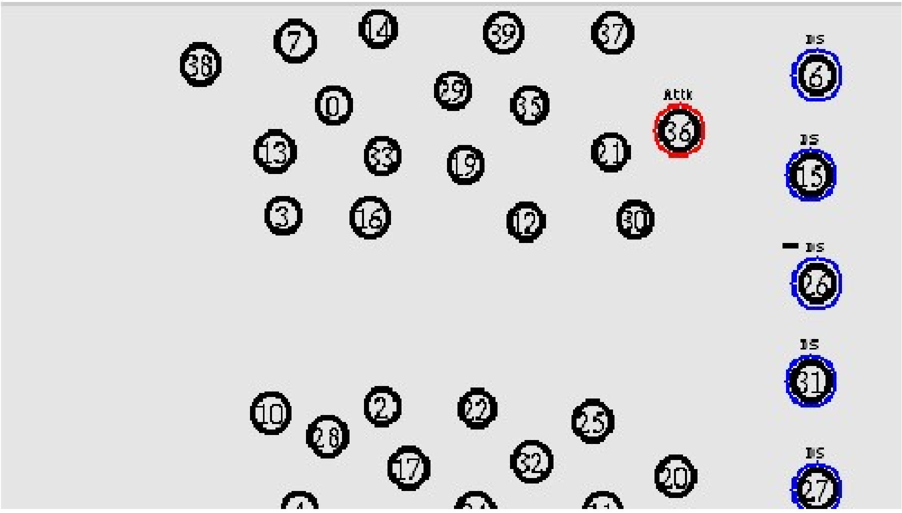

Fig 10. Simulation Topology

Table 3 summarizes the simulation parameters used.

Table 3. Simulation Parameters

Total Nodes	**20,30,40,50 and 60**
Area Size	50 X 50
MAC protocol	IEEE 802.15.4

Simulation Time	25 sec
Transmission Range	25m
Routing Protocol	IACM
Traffic Source	CBR,poisson
Packet Size	512
No. of Keys	50,100,150,200 and 250Kb.
Simulation Time	50 sec.

4.3. Performance Metrics

The SKM scheme [17] is considered for performance comparison. The performance is evaluated based on the following metrics; the Average end-to-end delay, the Average Packet Delivery ratio and the packet drop.

A. Based on Nodes

Case 1: (CBR)

In case-1, tThe number of nodes is varied as 20,30,40,50 and 60 and for the CBR traffic and performance is measured for the above metrics.

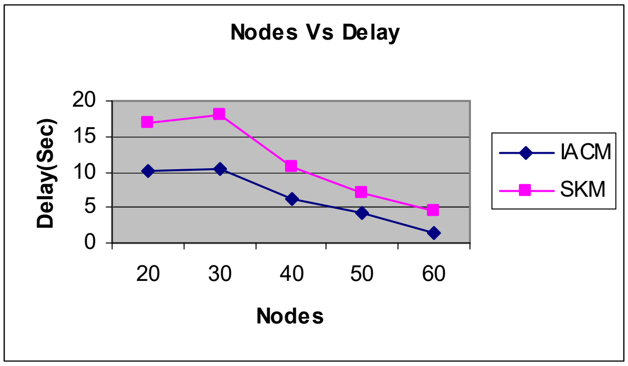

Fig 11. Nodes Vs Delay

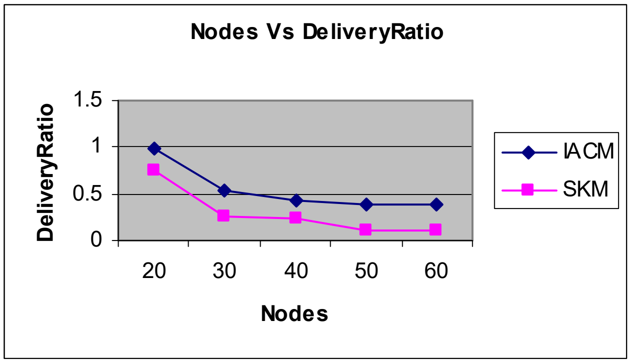

Fig 12. Nodes Vs Delivery Ratio

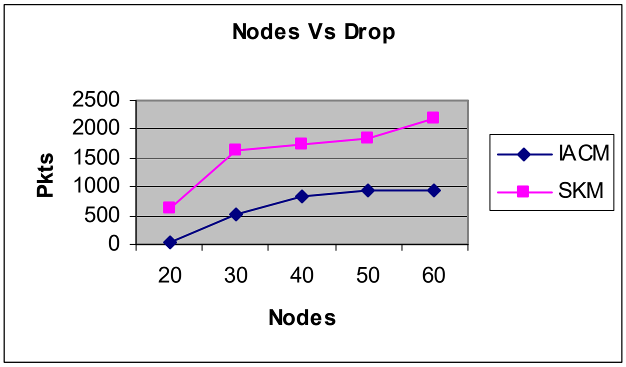

Fig 13. Nodes Vs Drop

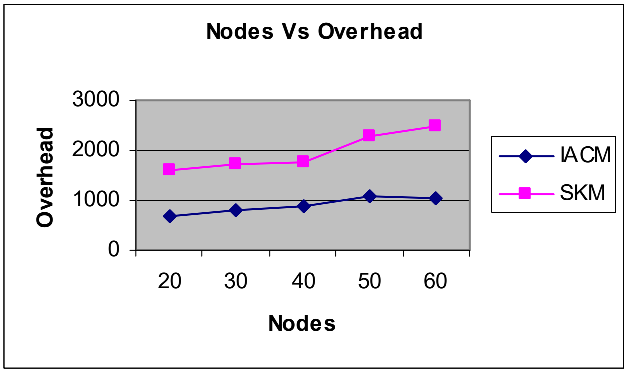

Fig 14. Nodes Vs Overhead

From Figure 11, we can see that the delay of our proposed IACM is less than the existing SKM technique.

From Figure 12, we can see that the delivery ratio of our proposed IACM is higher than the existing SKM technique.

From Figure 13, we can see that the packet drop of our proposed IACM is less than the existing SKM technique.

From Figure 14, we can see that the overhead of our proposed IACM is less than the existing SKM technique.

Case2: (Poisson)

In case-2, the number of nodes is varied as 20,30,40,50 and 60 and for the Poission traffic and performance is measured for the above metrics.

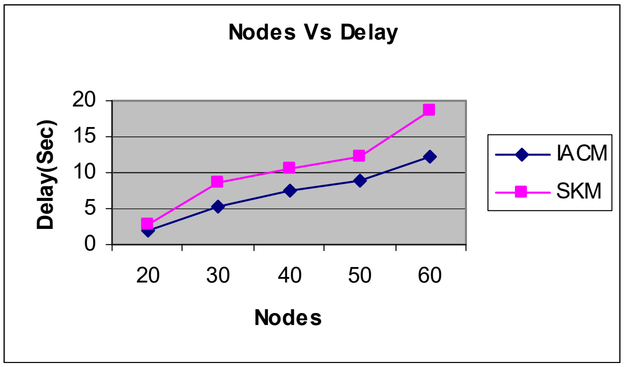

Fig 15. Node Vs Delay

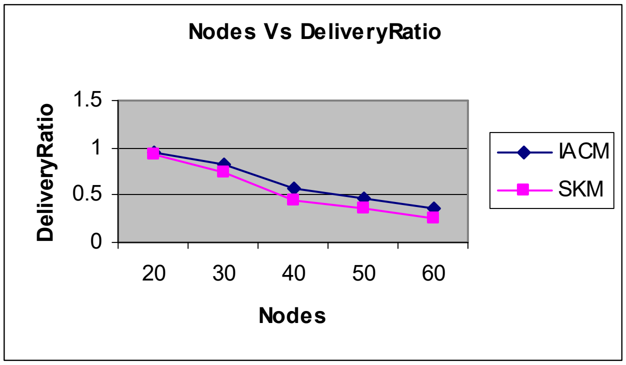

Fig 16. Nodes Vs Delivery Ratio

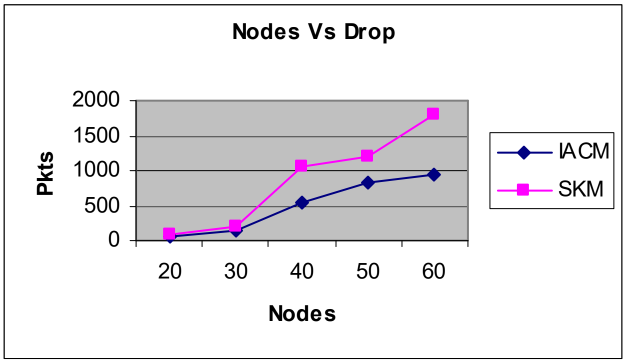

Fig 17. Nodes Vs Drop

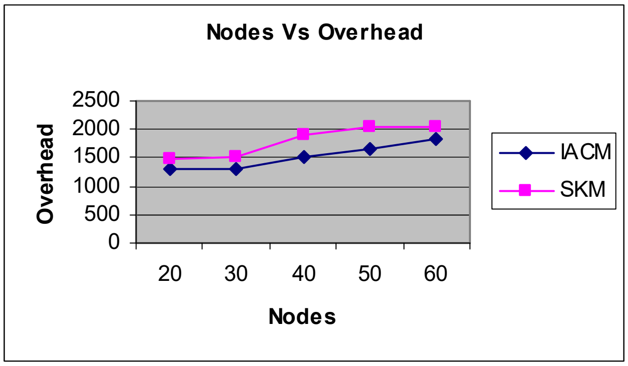

Fig 18. Nodes Vs Overhead

From Figure 15, we can see that the delay of our proposed IACM is less than the existing SKM technique.

From Figure 16, we can see that the delivery ratio of our proposed IACM is higher than the existing SKM technique.

From Figure 17, we can see that the packet drop of our proposed IACM is less than the existing SKM technique.

From Figure 18, we can see that the overhead of our proposed IACM is less than the existing SKM technique.

B. Based on Keys

Now we vary the number of keys as 50,100,150,200 and 250 for the 50 nodes scenerio.

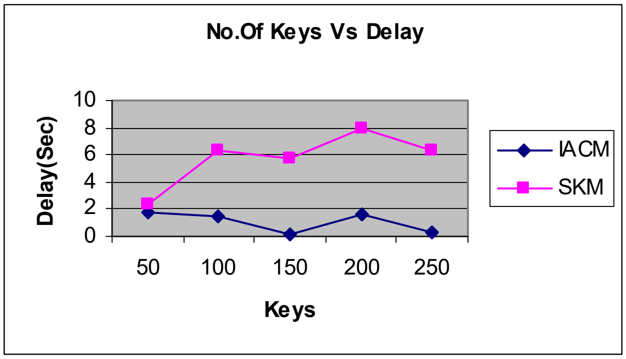

Fig 19. Keys Vs Delay

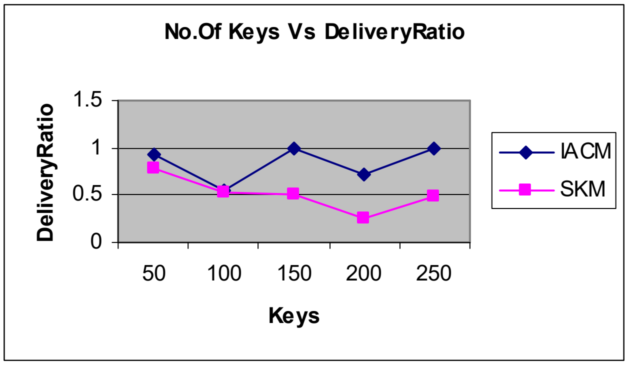

Fig 20. Keys Vs Delivery Ratio

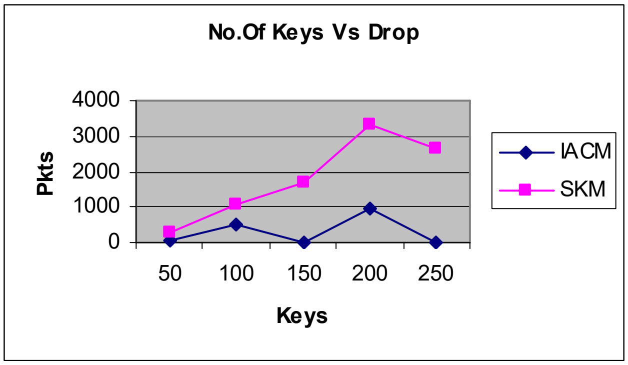

Fig 21. Keys Vs Drop

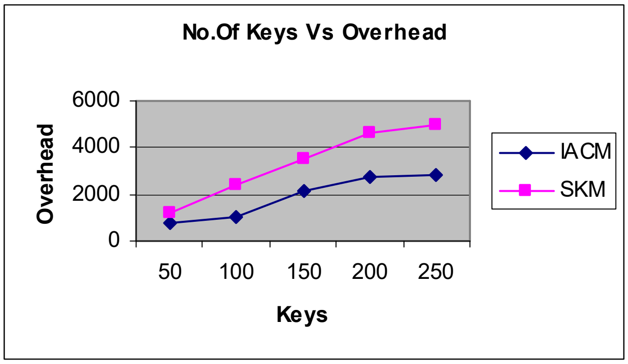

Fig 22. Keys Vs Overhead

From Figure 19, we can see that the delay of our proposed IACM is less than the existing SKM technique.

From Figure 20, we can see that the delivery ratio of our proposed IACM is higher than the existing SKM technique.

From Figure 21, we can see that the packet drop of our proposed IACM is less than the existing SKM technique.

From Figure 22, we can see that the overhead of our proposed IACM is less than the existing SKM technique.

5. Conclusion

In this paper, an integrated authentication mechanism using the CDMA modulation technique is proposed for physical layer security of WBAN. The mechanism can able to fight against frequency jamming attacks as it includes a band-pass filter of CDMA technology. Every node has authentication to receive only from specific nodes. No other unwanted node can make any variation in the software of another node. This method generates security keys in two levels of data transmission. No intermediate control node can create any problem for the data transmission. There is no direct connection between sensor nodes and the master server, so the sensor nodes cannot have any effect on the central control system. As a unique id is given to every node, it is easy to detect the faulty node in the network. The usage CDMA technology makes the transmission system faster and error free. Data is processed in only two steps, so it is comparatively faster than other networks. This paper can be extended by generating an intermediate key generation technique from the master key generation technique. By simulation results, we have shown that the proposed approach provides more security with less delay and overhead.

References

[1] Li, C., Li, J., Zhen, B., Li, H.B. & Kohno, R. "Hybrid Unified-slot Access protocol for wireless body area networks", International Journal of Wireless Information Networks vol-17, pp-1–12, 2010.

[2] Ullah, S. et al. "A Study of MAC Protocols for WBANs", Review Literature and Arts of the Americas, vol-10, pp-128-145, Sensors, 2009.

[3] Pervez Khan, Md.Asdaque Hussain and Kyung Sup Kwak, "Medical Applications of Wireless Body Area Networks", International Journal of Digital Content Technology and its applications, vol-3, 2009.

[4] Majid Nabi, Twan Basten, Marc Geilen, Milos Blagojevic and Teun Hendriks,"A Robust Protocol Stack for Multi-hop Wireless Body Area Networks with Transmit Power Adaptation", In 5th International Conference on Body Area Networks, Body Nets 2010, pp-10-12, 2010.

[5] Shahnaz Saleem, Sana Ullah and Hyeong Seon Yoo, "On the Security Issues in Wireless Body Area Networks", JDCTA, pp-178-184, 2009.

[6] Shahnaz Saleem, Sana Ullah, and Kyung Sup Kwak, "A Study of IEEE 802.15.4 Security Frame Work for Wireless Body Area Networks", Sensors, vol-11, pp-1383-1395, 2011.

[7] Chiu C. Tan, Haodong Wang, Sheng Zhong, and Qun Li, "IBE-Lite: A Light Weight Identity Based Cryptography for Wireless Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, vol-13, 2009.

[8] Krishna.K, Venkata Subramanian and Sandeep P.S Gupta, "Physiological Value Based Efficient Usable Security Solutions for Body Sensor Networks", ACM Transaction on Sensor Network, pp-1-77, 2010.

[9] S.S.Mohanavalli and Sheila Anand, "Security Architecture for At-home Medical Care Using Body Sensor Network", International Journal of Ad-hoc, Sensor, Ubiquitous Computing, vol-2, 2011.

[10] Neha Sharma and Er.Meenakshi Bansal, "Preventing Impersonate Attacks Using Digital Certificates in WBAN", International Journal of Advanced Engineering Sciences and technologies, vo-9, pp-31-35, 2011.

[11] Dave Singelee, Benot Latr, Bart Braem, Michael Peeters, Marijke De Soete, Peter De Cley Bart Preneel Ingrid Moerma and Chris Blondia, " A Secure Low Delay Protocol for Multihop Wireless Body Area Network", Ad Hoc & Sensor Wireless Networks, vol-9 , pp-953-72 ,2010.

[12] Syed Muhammad Khaliq-ur-Rahman Raazi and Heejo Lee, "BARI: A Distributed Key Management Approach for Wireless Body Area Networks", IEEE International Conference on Computational Intelligence and Security, pp-324-329, 2009.

[13] Christian Gehrmann, Chris J. Mitchell and Kaisa Nyberg, "Manual authentication for wireless devices", In: Cryptobytes, Vol. 7, No. 1, pp 29-37, 2004.

[14] Dave Singel´ee and Bart Preneel, "Key Establishment Using Secure Distance Bounding Protocols", 4th annual international conference on mobile and ubiquitous systems: Networking and services (MobiQuitous), pp 1 – 6, 2007.

[15] Yong Wang, Byrav Ramamurthy and Xukai Zou, "KeyRev: An Efficient Key Revocation Scheme for Wireless Sensor Networks", CSE Conference and Workshop, pp 1260-1265, 2007.

[16] Network Simulator: http:///www.isi.edu/ns/nam

[17] Venkatasubramanian Sivaprasatham and Jothi Venkateswaran," A Secure Key Management Technique for Wireless Body Area Networks", Journal of Computer Science 8 (11): 1780-1787, 2012, ISSN 1549-3636, Science publications

[18] Intuitive Guide to Principles of Communications, http://www.complextoreal.com

[19] "Introduction to CDMA," http://www.setyobudianto.com

[20] Thomas Kugelstadt," Active Filter Design Techniques" Chapter 16 Active Filter Design Techniques Literature Number SLOA088.

[21] Venkatasubramanian Sivaprasatham and Jothi Venkateswaran," Integrated Authentication and Security Check With CDMA Modulation Technique in Physical Layer of Wireless Body Area Network", IEEE International conference on Computational Intelligence and Computing Research,2012