IJCTA, 10(01), 2017, pp. 1-11

A Study on Security for Adaptive Periodic Threshold Sensitive Energy Efficient Protocol Based on Elliptic Curve Cryptology in Wireless Sensor Network

N. Sathish kumar* and K. Rajakumar**

Abstract : The Wireless sensor network is playing amajor role in *e*-health monitoring, military, video surveillance, agriculture activities and vehicle monitoring. Particularly in *e*-health monitoring system in hospital patient data is very important to protect from the attacker. The data will capture from the sensor and it will send in the wireless network. There are many security issues based on existing research. At present attacker using high version software and hardware to attack the system. Still need the high security of patient data while it is present in the inside node or send in the wireless network. In this paper, we have discussed various security issues and proposed new encryption method for the Adaptive periodic threshold-sensitive wireless protocol based on elliptic curve cryptography and use shorter keys for encryption and decryption for protecting the data. The proposed system will produce the more energy-efficient and high security for medical data.

Keywords : Wireless Sensor Network, Elliptic curve cryptography, Encryption and Decryption.

1. INTRODUCTION

The Wireless Sensor Network is becoming a ubiquitous in various applications. Wireless sensor made up of 35mm with sensor, radio and base station. It is used to capture the data from one place and it will transmit the data from one place to anywhere in the world using wireless network. In 2020 more than 4.1 billion awaited to join the world Internet gathering. The application such as parking, transport system, electricity ,machine surveillance, waste management, military, e-health, smart cities are creating new networks and all the application wireless sensor is needed, nearly in 2020 the Internet of object to Internet of object nearly 12.2 billion. The connected e-health monitoring segment will have the over growth and of machine to machine 729 million in 2020.The wireless sensor network particularly in e-health is an emerging area. Many researchers used elliptic curve cryptography for medical data protection [1,2].The energy-saving also playing a vital role, according to the earlier research [3,4].The safety of patient data while it is transferred from one node to another node must be very important factor according to 2016 and in the future. The medium access control protocol is one of the important access mechanism in wireless sensor network. It is divided into two type’s allocations. One is Static Channel Allocation and other one is Changing Channel Allocation. The frequency is divided into four types according to bandwidth. First one is the Rate division multiple access and second one is the Case division multiple access and third one is the Code section multiple access and fourth one is an Infinite Division Multiple Access or Orthogonal Rate Division Complex. There is no determinate information measure are used here. All the frequency is

* Research Scholar, School of Computer Science and Engineering, VIT University, Vellore. *sathishkumar.n2016@vitstudent.ac.in*

** Associate Professor School Of Computer Science and Engineering, VIT University, Vellore. *rajakumar.krishnan@vit.ac.in*

dynamically allocated. The Wireless sensor network classified into two types one is proactive networks is based on the sensor continuously sense the medium. If the medium is free it sends the data otherwise it will take random of time and it will send if the medium is free and the second one is reactive. The data will send according to sudden changes by the sensor in the network. The requirements of wireless sensor network should be small and low power consumption and usage of the network is always high and it should be always low-cost and high Security is needed. In this model senor node is formed in the form of cluster [5]. From the figure 1 the data will be collected from the various sources using sensor node. After collecting the data, it will send to the base station and from the base station to internet service user and data center. In data center all captured data is stored and stored data is viewed by the internet user. During transmission from one to another end the attacker can modify or corrupt the data in the network. At present day by data the equipment and the software is growing by way ofupdate version releasing in every year.

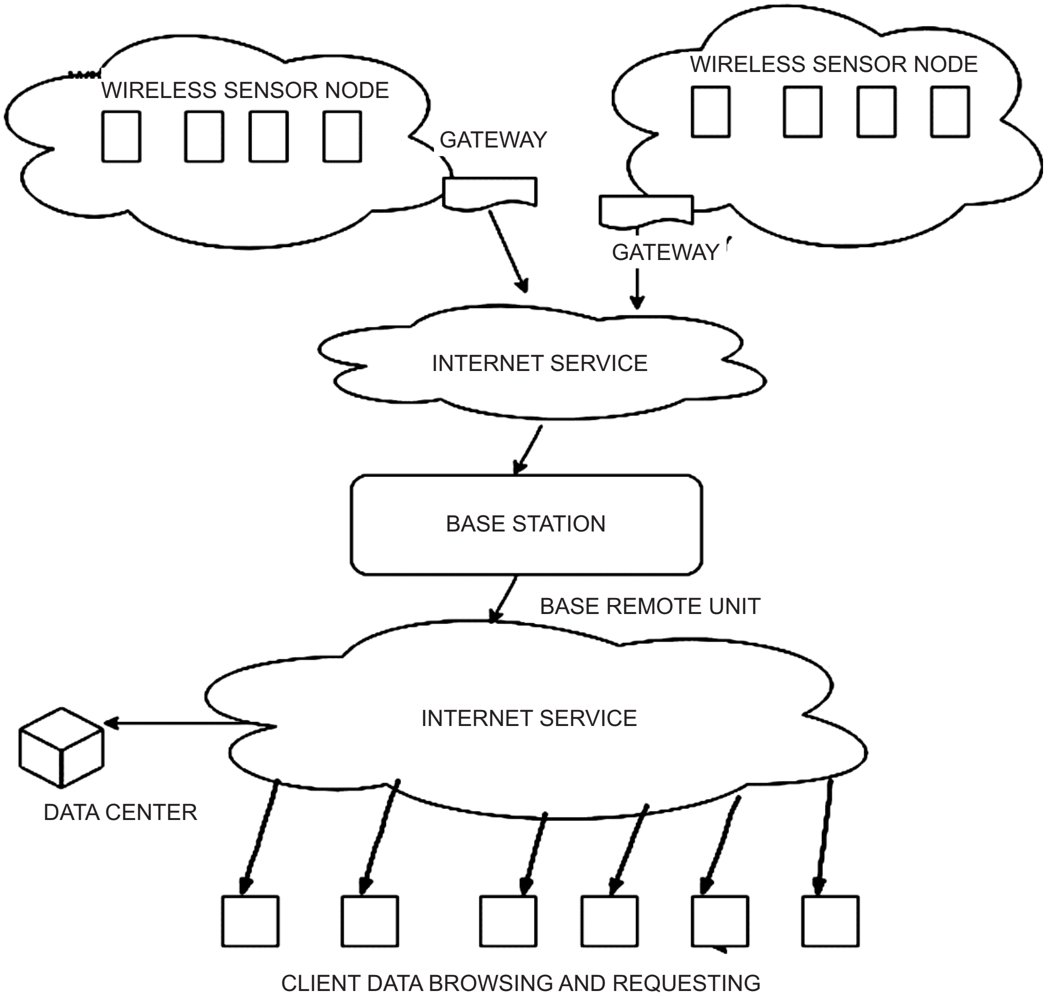

Figure 1: Layout of wireless model

The attacker used high end technology and software to attack the data in the network. Always we need to protect the data in an electronic health monitoring system with more protection is needed. The safety of medical data is a vital role for all the people. The data will be encrypted while the data's are present inside any node based on data privacy and also encrypted while sending the request, reply and acknowledgement. The data will be collected from various sources based on the application domain. In this proposed model seven levels of handshaking security mechanism will be following.

2. RELATED WORK

This section introduces literature review on security for wireless sensor network based on elliptic curve cryptography with focus on energy efficiency, low battery power and more authentications. Mohamed said

SALAH et al [6]states that the Elliptic curve cryptography used for encryption and decryption with shorter keys. The elliptic curve cryptography is purely based on the mathematical model. It was developed by diffie-hellman. The AVL tree key management used for key exchange and also used for the GPSR wireless sensor protocol in wireless routing. Leinharn et al[7] illustrated that the wireless sensor end to end routing protocol used for routing in the network and adopted group key pre-distribution scheme used for the design and also used group key for entire path called unique key. Di Lin et al[8] presents a concept of a captious content by using wireless communication nether a wellness care by electromagnetic interference(EMI) caused by radio malfunction of medical sensor. They had proposed new algorithm for surgical information and also analyzed about the disconnect user in the sensor network. Jun Zhou et al[9] proposed the privacy conserving dynamical medical text mining and also discussed about the image extraction in the cloud based system. First they analyzed about protect the data aggregation and it was used for correlation matching and characteristic extraction method. Chia-Mu Yu et al [10] proposed the strategy for grouping, anomaly sending, and compressive detection to cut down the elevated of wireless transmission, storing, and encrypting and attests the information and demonstrated about the result in three order improvement according to energy and storage requirements. Arsalan Mohsen Nia et al [11] investigated about the eight medicine sensorsbased upon this they had analyzed energy and storage requirements in the device and analyzed about the reduce overheads in the wireless network. Di Tang et al [12] investigated about the energy deployment, energy resource and security in the message delivery in the network. The have been discussed about the new system in routing method and energy balance for the sensor network. Seung-Hyun Seo et al [13] investigated about the secure connection in wireless sensor network and also discussed about the key modification and key privacy. They had analyzed about the various attacks using changing less effective key management method and it has been implemented in a contiki operating system. LeinHarn and Ching-Fang Hsu[14] investigated about the group key distribution in the sensor network system and also discussed about the polynomial system and also analyzed about multivariate polynomial. Finally discussed about the security and procedure complexity is efficient. Kyung-Ah Shim et al [15] illustrated about the public key cryptography in wireless sensor network consider refer bases cryptography and also discussed about the open research issues and also analyzed about the public cardinal cryptanalytic early in footing of executing clip, force intake and asset activity on constrained wireless devices .Finally discussed about the mixture to find commerce offs, according to outgo, public presentation and safety. Donglai Fu and Xinguang Peng [16] investigated about sensor node is equipped with a Sure Horizontal surface Module and also analyzed about the single-hop and multi-hop testimony according to effective, businesslike and secure. Chunsheng Zhu Set et al [17] investigated about the hallmark, computation andorganized according to three functions. 1) Attest CSP and SNP 2) service of CSP and SNP and 3) Helping CSU.Daojing et al [18]investigated about the vulnerabilities of the protocol and discussed about the security function more efficient. The protocols are important for transfer the message between one and to another end. Security is playing a major role in all type of wireless protocol.

3. MODEL FOR SECURE END TO END PROTOCOL

In this protocol the sensor will sense the medium continues in the network, the data will transmit only if the value changes in soft threshold value and hard threshold value and if the value is not sending in the medium it is forced to send the data in the network. It is used in time division access mechanism to send the data according to the time slot.

A. Functioning Of Protocol

It combines both retroactive and activated policies in the sensor network and users are allowed according to count time and value based on property. The physical Phenomenon intake can be dynamical the number of times as well as the first values. The Disadvantage of the network is required the number of times using the sensor network. The proposed model based on a secure end to end protocol, and it is sensitive energy efficient because the sending of data through sensor is based on the hard threshold value and soft threshold value.

B. Main Features of the Protocol

It combines both retroactive and activated policies in the sensor network and in this method user are allowed according to count time and value based on property. The physical Phenomenon intake can be dynamical the number of times as well as the first values and the Disadvantage of the network is required the number of times in the sensor network.

4. ATTACKS IN THE WIRELESS SENSOR NETWORK AND IT IS DIFFERENT TYPES

The Wireless Sensor Network Attack classified into two types one is the attack against the safety node in the network and the second one is against the basic routing execution in the system and its different types are followed.

A. Denial-Of-Resource

In a network, a denial of resource attack is an attempt to make data unavailable in network or make resource unavailable in network or suspend service to the node connected to the network or make a bottleneck from figure 2 in the network.

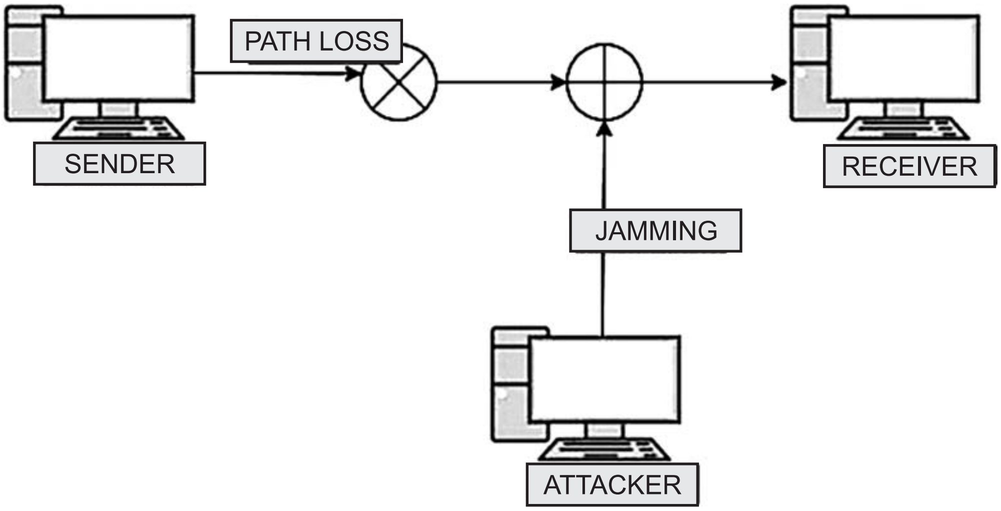

Figure 2: Diagram of the Jamming in the network. The attacker makes overcrowding on the network

B. Parody, Adjusted, Or Replayed Routing Info

In this attack, the routing information can be altered/twist in the network and also modify the data content or generate false error or Traffic redirection.

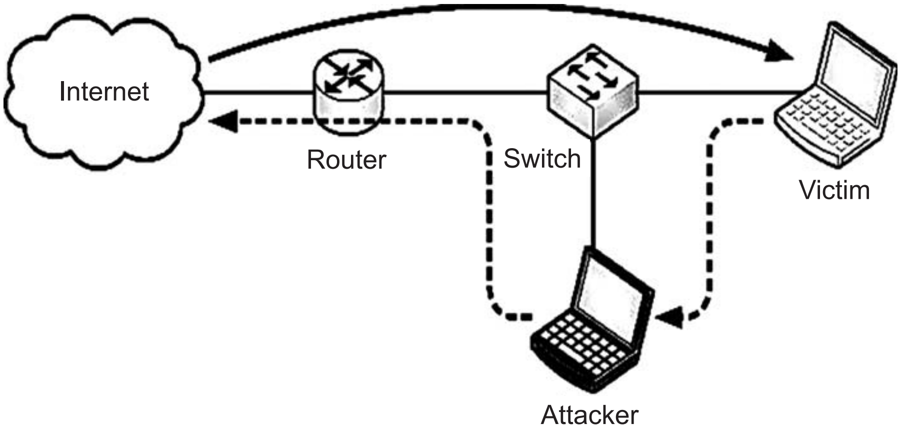

Figure 3: Diagram of the alter data in the network. The attacker changing the route and alter the message in the network

C. Exclusive transmission

The dummy node like black hole can compromise the other node in the network by creating an appearance that it is still active by forwarding only exclusive packets and that data can be routed via it.

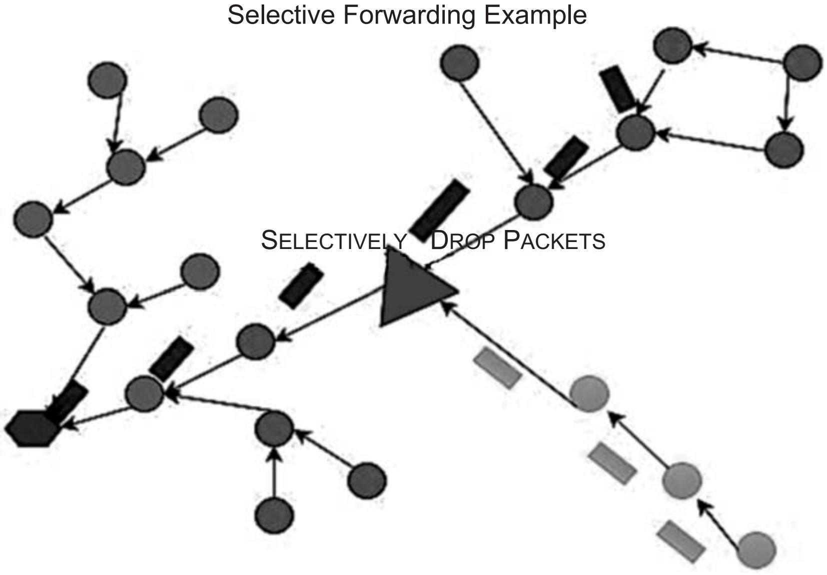

Figure 4: Diagram of the changing transmission route in the network by the attacker

D. Sybil Onslaught

In this model of attack a network with break attitude each node(C, D, E) sends data to multiple intermediate nodes and after Sybil attack the Adversary intermediate node (A) from fig:5 assumes multiple identity, removing the fault tolerance requirement in the network.

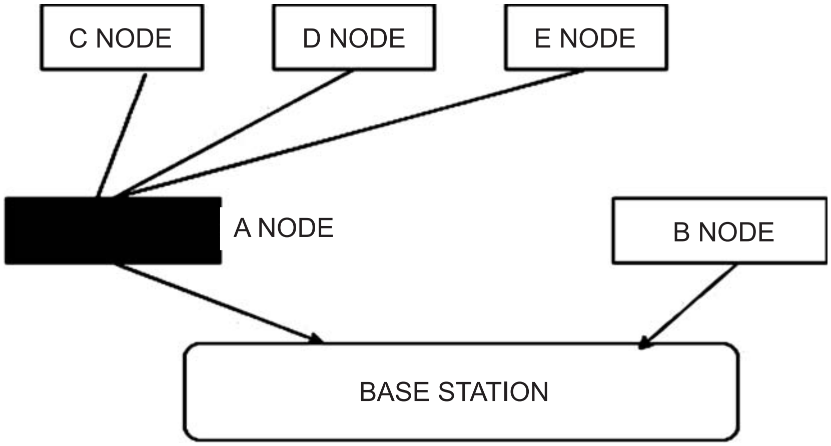

Figure 5: Diagram of the attack in the particular node in the network by the attacker

E. Sinkhole Onslaught

In this model corrupt node close to base advertise attractive routing information and issuesin this model corrupt node close to base announce attractive routing message. A force node in the region to route data forwards it and creates a ‘sphere of influence.

F. Wormhole Onslaught

In this attack Hard to detect because the connection environment between the two bad nodes are unknown. This limits the self-organizing criteria of an ad-hoc network. The use of rule that is not based on hop count. In magnetic routing, a route is based on equality of intermediate nodes. But if opponent nodes can copy its location, this doesn’t work.

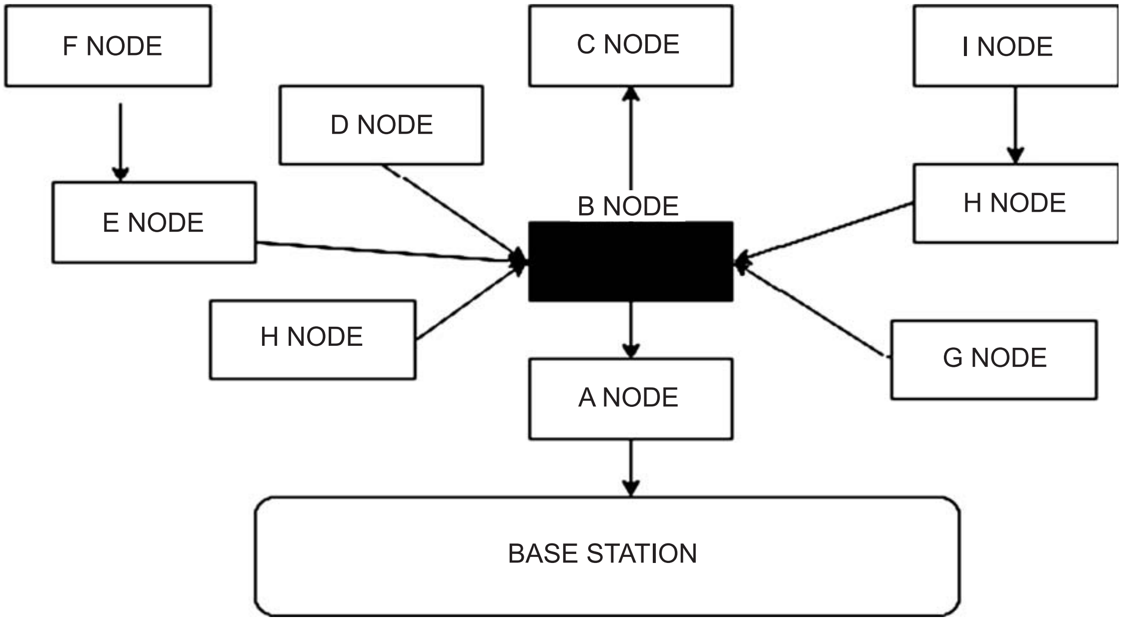

Figure 6: Diagram of the attack in the particular node in the network by the attacker. Node B generates the duplicates routing information in the network and also attract the data for themselves and also neighboring node in the network

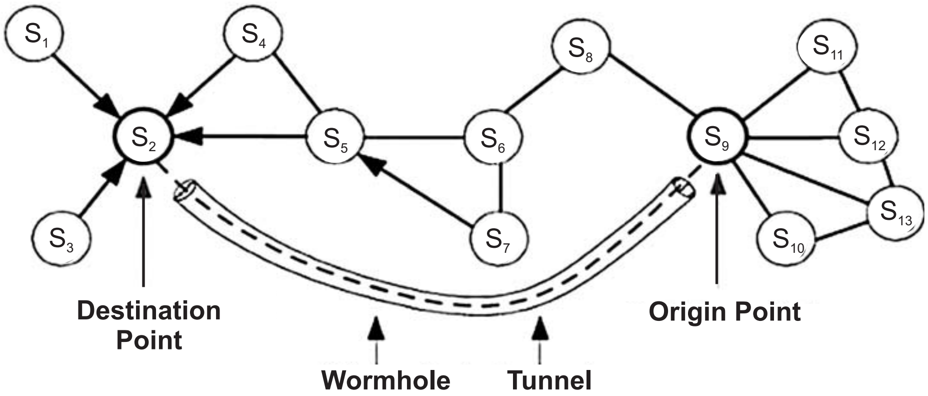

Figure 7: Diagram of the attack in the particular node in the network by the attacker. The attacker creates a tunnel between s2 and s9 after that the attackers modify the data in the network

G. Hello Flood Onslaught

In this model new sensor send a hello message to all neighbors and also broadcast the hello message through its route to the base station. Another node in the network chooses a route through this new node. Opposing node communicates a small message to the base station. Attack node attempt to reply in the network, but the opposing node is becoming out of range. This attack is used by three way handshake protocol model and any node in the network sending a hello message and randomly any system in the network reply this message. The new system in the model must resend the reviving message using bi-directional link.

H. Acknowledgement Parody

In this attack, the aggressor can easily point message between two nodes leaving and acknowledge to the transmitter and the attacker can easily change the message between two nodes leaving and acknowledge of information to the Receiver. The goal is to convert the transmitter that a weak link is strong in the network, or a deadline is still active in the network. The counters of the affliction by attach a random number to the message and encrypt the whole thing. Admit by sending the decrypted random number.

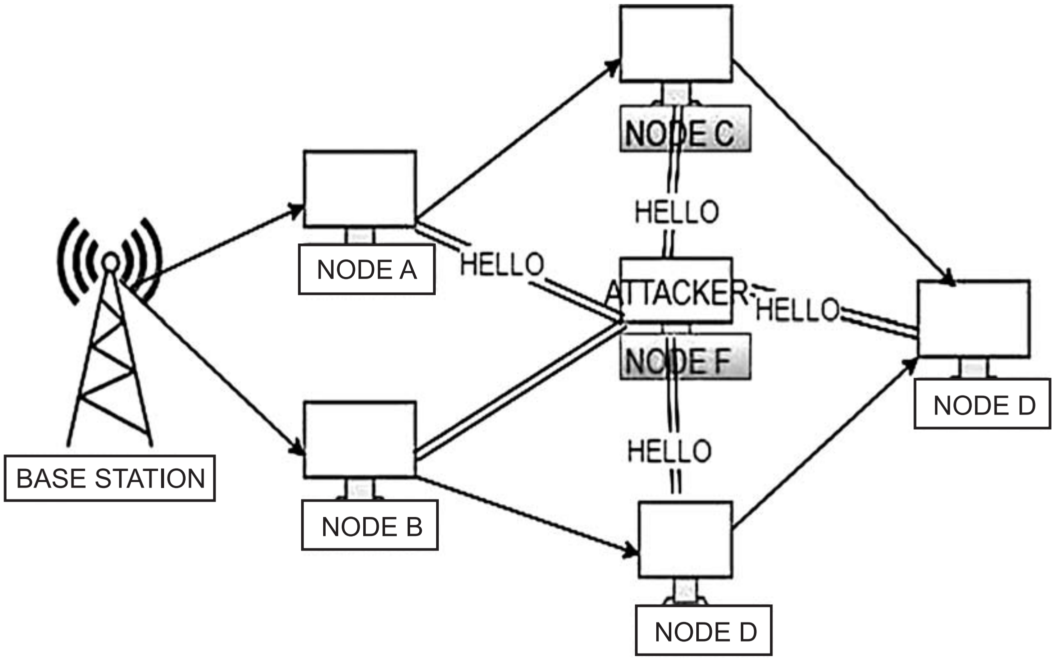

Figure 8: Diagram of the HELLO Flood in the network by the attacker. The attacker sends hello message to all nodes in the network

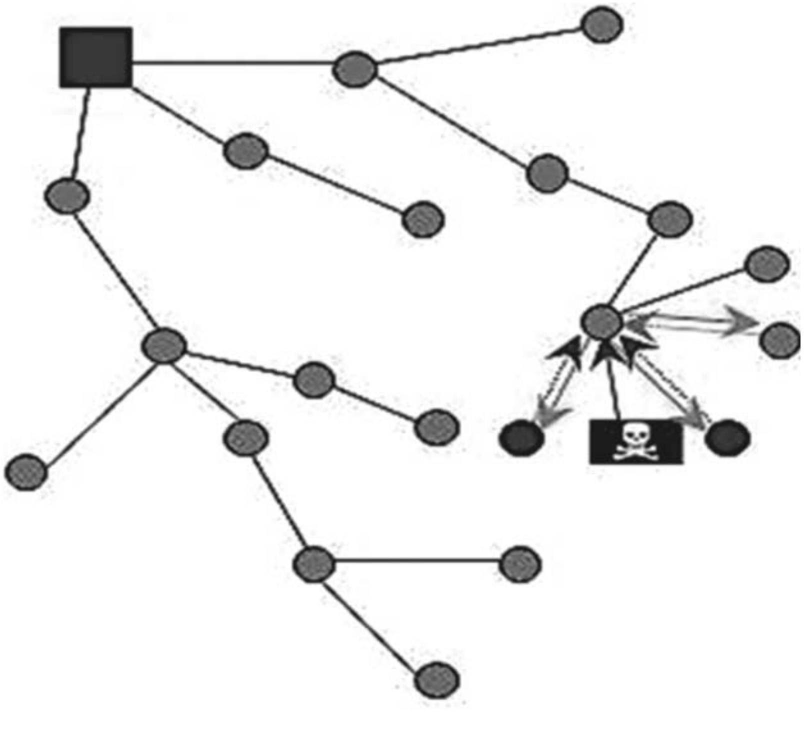

Figure 9: Diagram of the acknowledgement spoofing in the network. The attacker made trick other node in the network to believe that a node or link in the network is either dead condition or a live condition

5. MAIN SAFETY MEASURE IN WIRELESS SENSING ELEMENT NETWORKS

In a wireless sensor network he communication between two ends could be eavesdropping. So security is very much important while transferring the message between two ends. The attacker can be any type and they are very powerful than the owner of the data. The attacker types are classified into three types. One is mote-class in this attacker uses analogous identifying toattack the data and the second one is laptop-class in this attacker uses more powerful device to attack the data and the third one is Outside/inside attack in this attacker hold some sum of nodes in the network.

6. APPROACHES BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

Simple elliptic curve cryptography is a public key encryption and it is utilized to faster encryption and decryption. It generates keys from the elliptic curve equation as product of very large prime numbers and it is used with small keys to encrypt and decrypt. It is proposed by Diffie-Hellman in 1970. The benefit of ECC is used smaller keys it reduce storage and transmission requirements. In this proposed model mathematical object are used to encrypt with shorter key and decrypt with shorter key than those of public cryptography. The shorter key produces the fast processing, less memory power and battery power will be very long.

A. Description about Routing Protocol

Simple elliptic curve cryptography based on a secure end to end Energy Efficient telecommunication sensor Network protocol. Encryption based on an end to end system wireless sensor routing protocol. .In this paper the proposed system will be protecting inside and outside attack in end to end system. The keys will be shared based on a binary tree. It has three orders to manage the key for all the nodes. Any new node wants to add and delete in this model. After adding or deleting any new node in the network, it will be automatically update the key based on a binary tree key management.

B. Elliptic Curve Cryptography Key Management

In this paper the key management done in binary tree. These trees are used to manage the key of the all the node in the network. The tree represents nodes connected by edges. A binary tree has the benefits of insertion or deletion operation in a very fast mode**.**

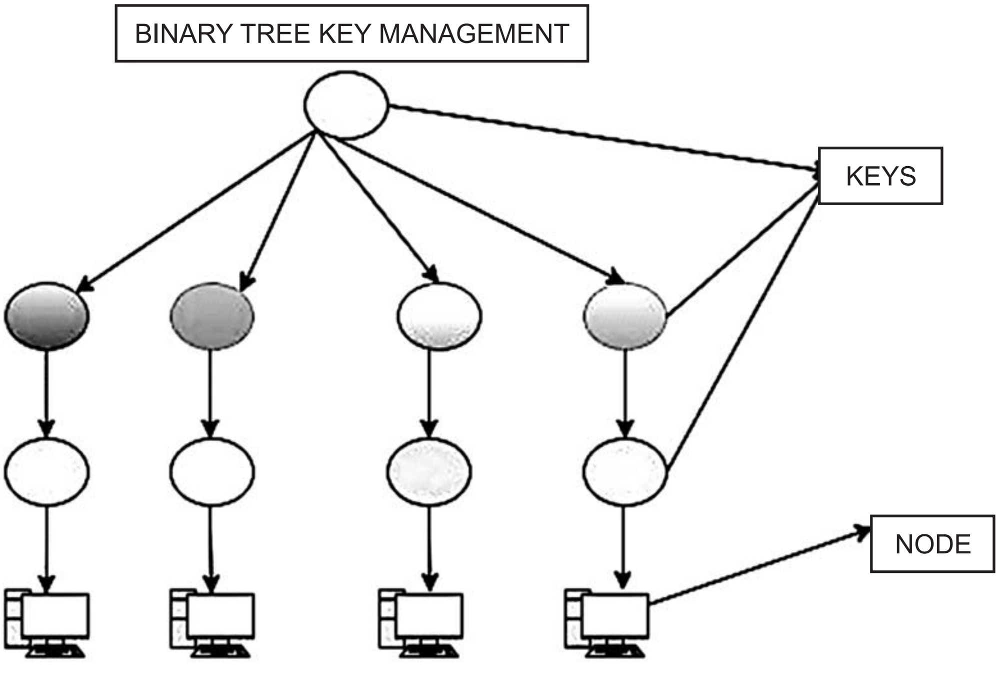

Figure 10: Diagram of the Binary tree in data structure

According to this the encryption and decryption key will be managed in the network. The key management done by from figure-8 Binary tree and also secure end to end energy efficient telecommunication sensor network.Here threshold based protocol used for communication and elliptic curve cryptography mathematical model used for encryption and decryption. The key will be automatically shared by all the nodes. The basic operations are insert and search. The first operation is used to insert an element in a node or to create a node in a network and search is used to search an element in a node.

7. SEVEN LEVEL OF SECURITY SYSTEM MODEL

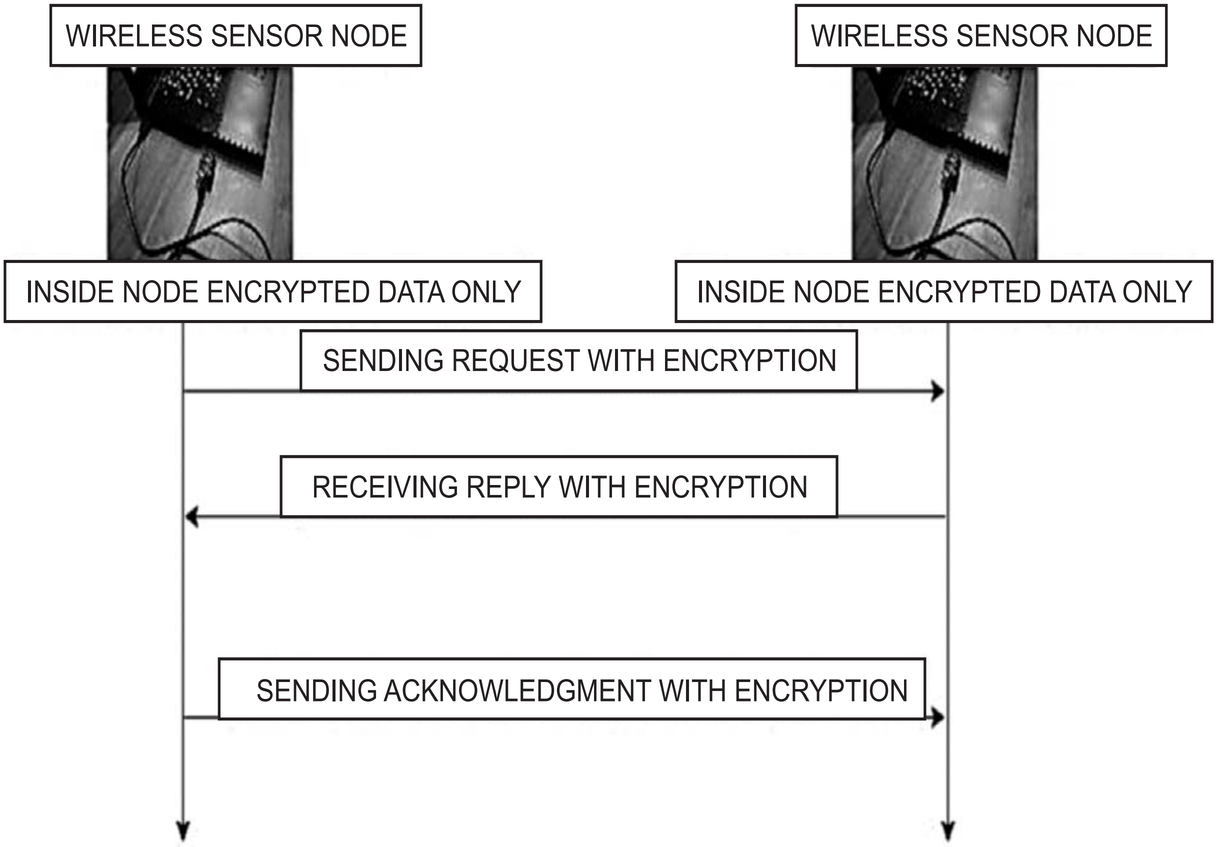
WIRELESS SENSOR NODE
WIRELESS SENSOR NODE
INSIDE NODE ENCRYPTED DATA ONLY
INSIDE NODE ENCRYPTED DATA ONLY
SENDING REQUEST WITH ENCRYPTION
RECEIVING REPLY WITH ENCRYPTION
SENDING ACKNOWLEDGMENT WITH ENCRYPTION

Figure 11: Diagram of the seven levels security model for wireless sensor network.

8. RESULT

In this proposed system we have used seven level of security system for medical data protection using wireless sensor and communication protocol. The First level is data will be encrypted/decrypted inside any node. The Second level is data will be again encrypted/decrypted during transmit any data and receiving any data. The Third level is data acknowledgement also encrypted/ decrypted. The Fourth level is Reply also encrypted/ decrypted. The Fifth level is elliptic curve cryptography used for encryption and decryption with shorter keys bit size which is less than 80 bits. The Sixth level is Wireless sensor protocol based on soft threshold and hard threshold. The Seventh level is key management. Here key management done by a binary tree. For any node the key management will be dynamically configured during insert in the network and delete in the network.

9. COMPARISON OF DIFFERENT TYPES OF WIRELESS SENSOR NETWORK SECURITY AND PROPOSED SYSTEM

From Table 1 : Comparison model shows the security of wireless network sensor. We have used eight types of attack and based on proposed seven levels of security model the solution will be given. The data will be completely encrypted in complete network and also encrypted acknowledgement and reply from one end to another.

10. CONCLUSION

There are many existing systems used for protecting that data. But in this paper the proposed system used for seven levels of security system. The data will be encrypted in complete network and also in any system in the network. Any type of attack discussed above not possible to attack any node in the network because the data will be fully protected by seven level of security mechanism. The wireless sensor protocol discussed above works based on threshold values. If the value of the threshold change, then only sensor will be activated and data will be send in the network. So the proposed system gives complete solution for the safety of medical data and the sensor battery power will be very high and processing time from one end to another end will be vey low.

Table 1
Comparison model for seven levels of security

Wireless Network Security	*Problem*	*Proposed System Solution*
Denial of resource	Data unavailable	Not possible inside node and outside node all data are encrypted. Reply also encrypted. Acknowledgement also Encrypted.
Parody, adjusted or replayed routing information	Modified data	
Exclusive transmission	Black hole attack	
Sinkhole onslaught	Corrupt any node	
Sybil onslaught	Corrupt any node	
Wormhole onslaught	Corrupt any node	
Hello flood onslaught	Send hello message to neighbors	
Acknowledgement parody	Change the message between two odes	

11. REFERENCE

1. Chinyang Henry Tseng Member, IEEE, Shiau-Huey and Woei-JiunnTsaur.Member, IEEE, “hierarchical and Dynamic Elliptic Curve Cryptosysem Based self-Certified Public key Scheme for Medical Data Protection system.”, IEEE Transactions On Reliability, Vol 64, No,3 SEPTEMPER, 2015.
2. Xun Yi, AthmanBouguettaya, Fellow, IEEE, DimitriosGeorgakopoulos, Andy Song, and Jan Willemson ,“Privacy Protection for Wireless Medical Sensor Data ”, IEEE transactions on dependable and secure computing, vol. 13, no. 3, June 2016.
3. Sanay Abdollahzadeh, and NimaJafari Navimipour,”Deployment strategies in the wireless sensor network: A comprehensive review”,Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran, Computer Communications 91– 92 (2016) 1.16 ,2016 Elsevier B.V.
4. Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Member, IEEE, and Mohsen Guizani, Fellow, IEEE ,”An Efficient Distributed Trust Model for Wireless Sensor” IEEE transactions on parallel and distributed systems, vol. 26, no. 5, May 2015.
5. Daojing He, Member, IEEE, Sammy Chan, Member, IEEE, Mohsen Guizani, Fellow, IEEE, Haomiao Yang, Member, IEEE, and Boyang Zhou ,”Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks ”,IEEE transactions on parallel and distributed systems, vol. 26, no. 4, April 2015.
6. Mohamed said SALAH, AbderrahimMaizate, Mohammed QUZZH,”Security approaches based elliptic curve management in wireless sensor network”, 201527thinternational conference on microelectronics.
7. Leinharn, ching-Fang hou, OuRuan and Mao-Yuan Zhang, “Novel Design for secure end to end routing protocol in wireless sensor network”, IEEE Sensors Journal VOL 16,No.6 March 15,2016.
8. Di Lin ,FabriceLabeau, Yuanzhe Yao, Athanasios.V, Vasilakos, and Yu Tang, “Admission Control over the internet of vehicles attached with medical Sensor for ubiquitous Healthcare application”, IEEE journal of biomedical and health informatics ,Vol 20, no 4, July 2016.
9. Jun Zhou, Zhenfu Cao, Senior Member, IEEE, Xiaolei Dong, and Xiaodong Lin, Senior Member, IEEE “PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems ”, ieee journal of selected topics in signal processing, vol. 9, no. 7, October 2015.
10. Chia-Mu Yu, Chi-Yuan Chen, and Han-Chieh Chao, “Verifiable, Privacy-Assured, and Accurate Signal Collection for Cloud-Assisted Wireless Sensor Networks” IEEE Communications Magazine , August 2015.
11. Arsalan Mohsen Nia, Student Member, IEEE, Mehran Mozaffari-Kermani, Member, IEEE, Susmita Sur-Kolay, Senior Member, IEEE, AnandRaghunathan, Fellow, IEEE, and Niraj K. Jha, Fellow, IEEE ,“Energy-Efficient Long-term Continuous Personal Health Monitoring”, IEEE transactions on multi-scale computing systems, vol. 1, no. 2, June 2015.

12. Di Tang, Tongtong Li, Jian Ren, Senior Member, IEEE, and Jie Wu, Fellow, IEEE ,”Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks ”,IEEE transactions on parallel and distributed systems, vol. 26, no. 4, april2015. Networks”, IEEE transactions on parallel and distributed Systems, Vol. 26, no. 5, may 2015.

13. Seung-Hyun Seo, Member, IEEE, Jongho Won, Student Member, IEEE, Salmin Sultana, Member, IEEE, and Elisa Bertino, Fellow, IEEE.”Effective Key Management in Dynamic Wireless Sensor Networks”, IEEE transactions on information for ensics and security”, vol. 10, no. 2, February 2015.

14. LeinHarn and Ching-Fang ,”Predistribution Scheme for Establishing Group Keys in Wireless Sensor Networks”,IEEE sensors journal, vol. 15, no. 9, September 2015.

15. Kyung-Ah Shim, Member, IEEE,”A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks”,IEEE communication surveys & tutorials, vol. 18, no. 1, first quarter 2016

16. Donglai Fu and XinguangPeng,”TPM-Based Remote Attestation for Wireless Sensor Networks”,tsinghua science and technology 11llpp312–321 Volume 21, Number 3, June 2016

17. Chunsheng Zhu, Student Member, IEEE, HasenNicanfar, Student Member, IEEE,Victor C. M. Leung, Fellow, IEEE, and Laurence T. Yang, Member, IEEE,”An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration”,IEEE transactions on information forensics and security, vol. 10, no. 1, January 2015.

18. Daojing He, Sammy Chan, Mohsen Guizani,”Small Data Dissemination for Wireless Sensor Networks: The Security Aspect”,IEEE Wireless Communications • June 2014.