

CRYPTOGRAPHY BASED SECURED LIFI FOR PATIENT PRIVACY AND EMERGENCY HEALTHCARE SERVICE

*M. Sindhu, M. Priyanka, A.K. Swedha, RA. Ranjana,
Dept of Electronics and Communication Engineering,
Velammal Engineering College Chennai, India.*

sujathar@velammal.edu.in, smeanssindhu@yahoo.com, priyankaforpassion@gmail.com

Mrs.R.Sujatha ,M.E,(PhD)

Asst. Professor-III,

*Dept of Electronics and Communication Engineering,
Velammal Engineering College Chennai, India*

Abstract: Health care is one such area, where WIFI is still not used as the electromagnetic waves affects patients with diseases like neurological disorders, cancers etc. Hence LIFI can be considered the next big technology which causes no harm to patients and also provides more additional features like greater speed and wider spectrum than WIFI. The only problem while transmitting data through it, in hospitals is to make sure that it ensures confidentiality. As a solution for this problem, the model proposed here uses Elliptic Curve Diffie Hellman and Secure Hash Algorithms to provide utmost security. Elliptic Curve Diffie Hellman is used as an asymmetric function that is, it uses two keys which in turn makes it difficult to hack. Secure Hash Algorithm works as an added advantage used mainly for authentication purpose.

Keywords: LIFI, Elliptic Curve Diffie Hellman algorithm, Secure Hash algorithm, Confidentiality.

1.Introduction

In Hospitals, the excess paper work generated while monitoring patients and the labor power wasted in shuffling between doctors with reports can be reduced by using “LIFI” as the network with cryptography technique brought in to ensure confidentiality. The concept of using LIFI rather than WIFI (in hospitals) is due to its wide spectrum and the speed at which the control packets are transmitted. Also it has very low implementation cost as it uses the normal LED light bulbs for transmission, hence maintenance is cheaper.

Cryptography technique is brought in by using Elliptic Curve Diffie Hellman which is an asymmetric key encryption which uses Public and Private keys for key exchange, and next Secure Hash Algorithm which is used for data encryption/decryption as well as authentication, the main advantage of this is that it can take a huge file and compute HASH, which is a one-way process. Hence, it provides utmost privacy, the need of the hour. Almost all the health care parameters can be transmitted as control packets with various medical data sets in it. The data such as heart rate, EEG, pulse rate and blood pressure which are some important basic details can be transmitted way too fast in case of patients whose health demands continuous monitoring and quick actions that is, patients with FITS or cardiac disorders have to be treated quickly once a change is observed. Thus it saves time.

Thus LIFI technique has been used with Cryptography to provide a better network in restricted field like Hospitals. We have used Elliptic Curve Diffie Hellman Algorithm over

others because it allows both the user and destination to independently calculate the private keys without transmitting the private keys as such.

2. Related Work

Harald Hass, Liang Yin, Yunlu Wang, Cheng Chen and Yunlu Wang were the people who introduced lifi to the world, that is, data transmission through lights by modulating its intensity. Rahul. R. Sharma has compared how LIFI works better than WIFI mainly focuses on how WIFI restricted fields can also use LIFI. Shubham Chatterjee explains how LED bulbs, can be exploited completely, not just using it simply as light bulbs but also for data transmission in between computers. Jay. H. Bhut discusses the issues faced with WIFI when the amount of users increases, the speed decreases proportionally and the use of LIFI as our future technology. Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts and Mahendra Srivatsava explains the efficiency of ad-hoc on demand distance vector algorithm, The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks.

Neha Tirthani and Ganesan enlightens us about using Elliptic Curve Diffie Hellman Algorithm for providing security for Cloud architecture. Ram Ratna Ahirwal explains how Diffie Hellman key agreement protocol is used to provide forward secrecy for web browser applications. Xing Jhang describes about using Diffie Hellman on IRIS nodes for key agreement and pair-wise key creation between the sensors amidst the network composed of IRIS nodes. In Local Session Initiation Protocol(SIP) environment, Jinhee Seo proposes an idea to reduce the execution time of Transport Layer Service(TLS) handshake authentication mechanism, Diffie Hellman based password authentication method can be used as replacement. Snigdha Soni and Sandeep Pratap Singh explains security is based on three parameters i.e. integrity, confidentiality and authenticity. This paper focuses on integrity. Many cryptographic hash functions are designed to provide integrity over data. Hash function generates message digest of fixed length.

3. Proposed Approach

In this paper, we have proposed the idea of combining the next big technology LIFI with confidentiality through a series of algorithms. The Ad-Hoc On Demand Vector algorithm helps in expanding the network by configuring node characteristics with that of its network. The Greedy Algorithm used here finds the best possible path to send the data to the destination node, better than other algorithms. Elliptic Curve Diffie Hellman provides an asymmetric function of using public and private keys and finally Secure Hash Algorithm provides data security and Authentication.

1.Lifi Overview

The new age wireless technology that's ready to create an impact is termed LIFI, which accesses internet through light instead of using the traditional radio frequencies. Here, every light bulb (LED) can be made a hotspot. Since the future of radio frequencies is very congested(2.5Ghz- 5Ghz), we are in the need of technologies like LIFI, whose spectrum is 10,000 times wider than radio frequencies. Considering the speed of approximately 220gbps is much better than WIFI's current highest speed 1.3gbps. Other main point to be taken note of is its use in WIFI restricted areas like Medical health care and aviation industries

2. Requirements Of A Lifi System

- 1) Data conversion module: Acquires medical data of an individual, the analog data is then converted into digital data and passed to LIFI module through UART.
- 2) Transmitter module: It is possible to encode data in the light by changing the intensity at which the LED's flicker to pass 1's and 0's. The modulation is pretty fast such that the human eye doesn't notice.
- 3) Receiver module: Here, photodiodes are used to capture the optic signals and convert them back into original data.
- 4) Display module: The received data can be displayed via Personal computer using various existing software like Real term etc.
- 5)

3. Lifi System Performance Metrics

These are some of the most important parameters that help us analyze the system performance.

- (1)Signal to Noise ratio
- (2)Type of light panels used
- (3)Coverage area of Access point (LED)

Based on these parameters, a system's performance can be judged and these parameters performance depends on the application field and differs accordingly.

4. Fusion of Lifi and Cryptography

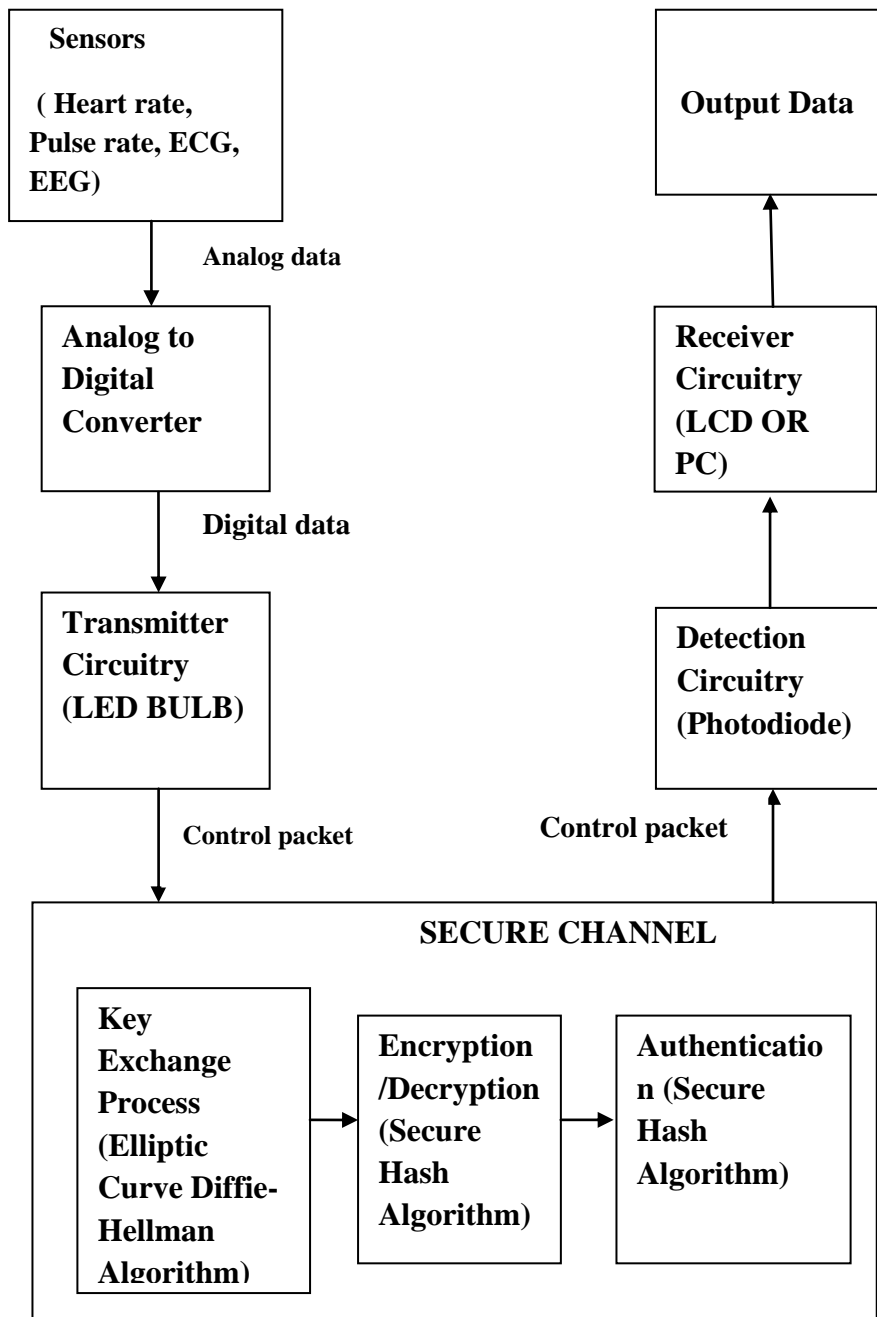
As discussed earlier LIFI is already secure if it is used within a very short range just like Bluetooth, but to increase its coverage area we need to concentrate on its security. To provide utmost confidentiality we follow five modules, which are as follows,

- 1) Node Configuration: This mainly deals with the node characteristics based on the network.
- 2) Route Finding: Ad-Hoc On Demand Vector protocol is used for finding all possible paths between the user and destination, while Greedy Algorithm helps to find the shortest path.
- 3) Key Exchange: Elliptic Curve Diffie Hellman Algorithm is used for exchanging the private and public key in encrypted format as it would be more secure than regular exchange.
- 4) Encryption/Decryption and Authentication: The Secure Hash Algorithm used here provides data security as well as authentication feature.
- 5) Performance Analysis: This final module shows the performance, on how well the data reaches the user in a secure manner.

Software used for simulation:

NS-2 is a packet level simulator and essentially a centric discrete event scheduler to schedule the events such as packets and timer expiration. NS-2 implements a variety of network components and protocols.

5. General Block Diagram



4. Modules involved in simulation process:

Node configuration

The first task in the simulation process is to configure a node for a set of parameters involved in the process. A node can be configured using the network components like link layer, MAC layer, the wireless channel nodes that transmit and receive the data packets, the type of ad-hoc routing protocol. In this process the source node will be patient, the destination node will be the doctor and the control packets will be the medical parameters of the patient.

Route finding

Here we use AODV routing protocol and Greedy algorithm for finding the shortest path between the source node and the destination node.

Aodv protocol

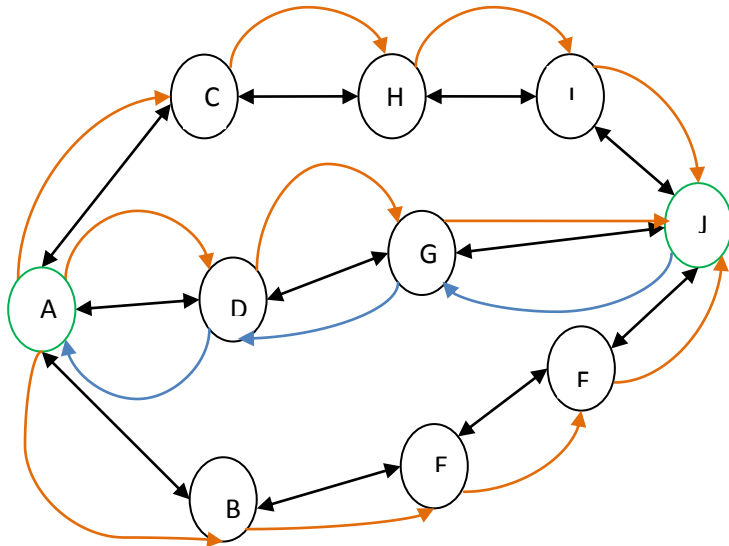
AODV is a reactive protocol which transmits the topology information by the nodes on demand. The difference between the AODV and other routing protocols is ensuring the freshness of the route and route timestamp by the use of sequence number in AODV routing protocol. The two mechanisms involved in this protocol is route discovery and route maintenance.




Route discovery

The term route discovery details identifying all the paths between the sender (patient) and receiver (doctor) and choosing the route with less number of hops. When a host wishes to transmit the data traffic (medical parameters) to another host to which it has no direct route it floods a RREQ packet to the network. The header fields of RREQ packet contains request ID, source ID, destination ID, sequence number of the source and the destination, hop counts, time to live. If the RREQ packet is received by an intermediate node it checks whether it is the desired destination. If not it rechecks status of the RREQ that has been received already by verifying the request ID and source node ID. If this condition is true then the RREQ packet is dropped. Otherwise the packet is forwarded further. Thus the loops are being avoided. If there exists an active route to the destination RREP will be sent with its route entity. Otherwise RREQ will be rebroadcasted. If the desired node received the RREQ, RREP will be unicasted back to the source node. After the route discovery the data packets which are waiting transmitted using First In First Out principle.

Route maintenance

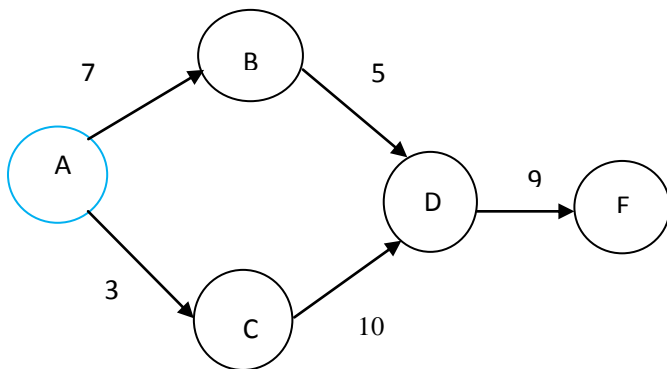
The routes are maintained up to date by the use of the sequence number. If the intermediate node receives either RREQ or RREP updates the information of the route in its routing table. By this mechanism a node can decide which next node can be used to reach the destination. While forwarding a packet if a node detects there is a link breakage RRER will be broadcasted to the source such that again the route discovery process will begin



	RREP
	RREQ
	LINKS
A	SOURCE NODE
J	DESTINATION NODE

Greedy algorithm

Greedy algorithm is a paradigm which renders solution piece by piece, always opting the next piece that offers most apparent and immediate benefit. This algorithm is mostly used for optimization of a problem. At each step the best choice is taken to obtain a best and optimized solution. The obtained result will be more efficient. We make use of Dijkstra’s algorithm which follows the greedy approach. This algorithm calculates the shortest path between the single source and the other hosts but works under the constraint that it must not contain the negative weighted values in the graph.



A	→	SOURCE NODE
A	→	B → 7
A	→	C → 3
A	→	B → D → 12
A	→	B → D → E →

VISITED NODE (FROM A)	B	C	D	E
A	7	3	∞	∞
C	7	3	13	∞
B	7	3	12	∞
D	7	3	12	21
E	7	3	12	21

Key exchange mechanism:

The purpose of key exchange mechanism is to enable the sender and the receiver for the subsequent encryption of the messages. The algorithm used is Elliptic Curve Diffie-Hellman.

Elliptic Curve Diffie-Hellman Algorithm:

Elliptical Curve Diffie-Hellman is one of the public-key cryptosystem. It requires low computational power, less communication bandwidth and less memory requirements. The important aspects of this algorithm are computation time of this algorithm is faster, high security with smaller key size and supports forward secrecy for web browser applications. It is a non authenticated key-agreement protocol and provides bidirectional encryption of communication between the client and the server which protects against eavesdropping. An elliptic curve E , over a finite field F is given by the equation, $Y^2 = X^3 + aX + b$ Where $a, b \in F$ and $-(4a^3 + 27b^2) \neq 0$. The secret key between A and B is generated by agreeing upon the EC domain parameters. A and B consists of pair of keys, private key say d (a randomly selected integer which is less than n , where n is the order of the curve) and public key say $Q = d * G$ (where G is the generator point). The private, public pair of key for A is (d_A, Q_A) and for B is (d_B, Q_B) .

- i. A computes $K_A = (X_A, Y_A) = d_A * Q_B$
- ii. B computes $K_B = (X_B, Y_B) = d_B * Q_A$
- iii. Since $d_A * Q_B = d_A d_B G = d_B d_A G = d_B * Q_A$
Therefore $K_A = K_B$ and hence $X_A = X_B$
 K_A is the shared key.

It is practically impossible to find the private key d_A or d_B from the public key K_A .

5.Encryption, Decryption and Authentication of the Messages

Secured Hash Algorithm is abbreviated as SHA. The SHA algorithm is based on the concept of hash function. The fundamental notion of the hash function is the input is taken as variable length measure and the output is produced as fixed length message. Hash function is a mathematical function which converts numerical input to a compressed one. The hash cryptographic function is similar to that of MD family exempting the fact that MD uses more number of bits while SHA uses less number of bits. This makes SHA more secure. The values processed by the hash functions are called as message digest or simply hash values. The paradigm of the SHA algorithm is closely similar to that of MD5. MD5 generates the message digest of 128 bits where SHA produces the message digest of 160 bits. The input text is divided into 512 bit blocks after initial processing and it is further divide into 16 32-bit blocks. The output is 5 32-bit blocks of message digest. Steps involved in SHA algorithm are:

Message Padding: In this step the extra bits are padded to the original message with the objective of achieving the length of the message 64 bits less than 1024.

Append Length: Before adding the extra bits the exact length of the original message is calculated. After padding the extra bits the length of the message is appended.

Dividing The Input Into 512 Bit Blocks: The input message is divided equally into 512 bit blocks.

Initialize The Chaining Variables: The chaining variables are from A through E. These variables are initialized.

A	HEX	01	23	45	67
B	HEX	89	AB	CD	EF
C	HEX	FE	DC	BA	98
D	HEX	76	54	32	10
E	HEX	C3	D2	E1	F0

Process the blocks: The actual process begins here. The values of the chaining variables ‘A-E’ are copied to another set of registers ‘a-e’ results in a combined register ‘abcde’. These registers are used for storing the temporary or intermediate results. SHA algorithm process the data in four rounds each having 20 steps. The input for each step is one 512 bit block and each round having 20 iterations total of 80 iterations are involved.

Authenticity and macs:

The integrity and authenticity of the information is essential in computer networks. If sender transmits the information to the receiver in an insecure channel, the data received at another end must remain unaltered. For this case authentication is required. Most common prevailing techniques are sharing the secret keys between the parties and take the form of message authentication code (MAC). A appends the authentication tag with original message and it is transmitted to B which is computed by MAC algorithm along as a function of the transmitted function and shared secret key. At the reception, the authentication tag is recomputed by B in the received message using the same mechanism and checks whether the value obtained equals the tag appended to the received message. If both values are same then the message is unaltered on its way from A to B. Thus authentication is achieved. SHA algorithm is affirmed to be secure because it is infeasible to compute the message corresponding to the message digest.

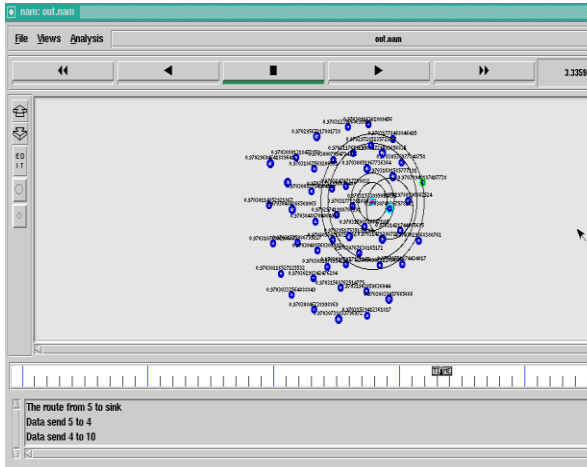
6. Simulation Results

PERFORMANCE ANALYSIS: These graphs capture the performance of the system and how well it helps the data to be secure.

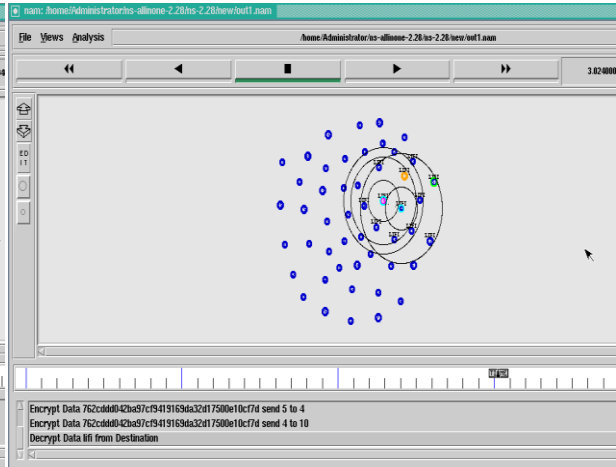
- 1. EXISTING MODEL OUTPUT:** The existing model is using radio waves so, there will be electromagnetic interference. So, there will be more delay in delivering the data traffic. The accuracy of the data will be affected.
- 2. PROPOSED MODEL OUTPUT:** The proposed model is with light nodes so there will not be any interference. The accuracy of the data will be maintained. The data traffic will be efficiently transmitted with high speed. Authentication will be provided between the sender and the receiver.
- 3. PACKET RECEIVED:** The packet transmission process will be without any loss in proposed system.
- 4. THROUGHPUT:** The throughput in the proposed model is high when compared to that of the existing model.
- 5. DELAY:** The delay in the proposed model is less when compared to the existing model as there is less interference.

- RESIDUAL ENERGY:** The power used for the proposed model is less when compared to that of the existing model and hence some of the energy will be unused.

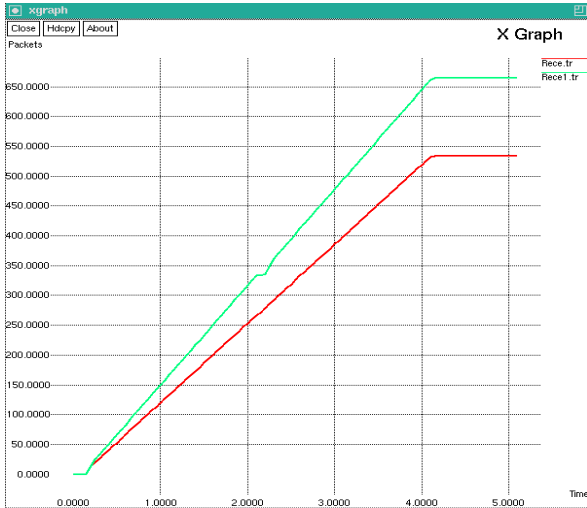
EXISTING SYSTEM



PROPOSED SYSTEM



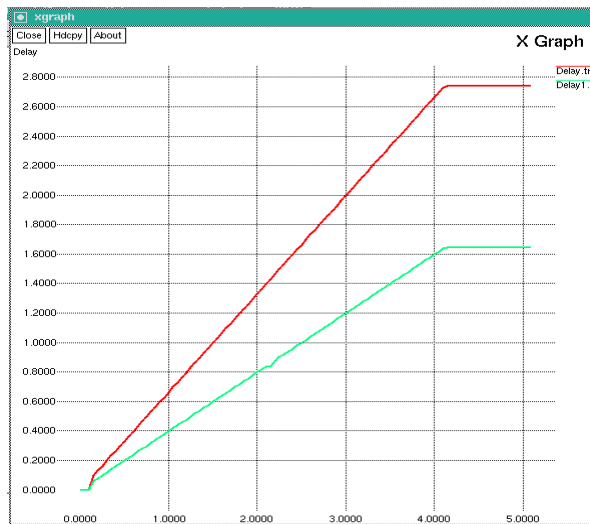
PACKET RECEIVED



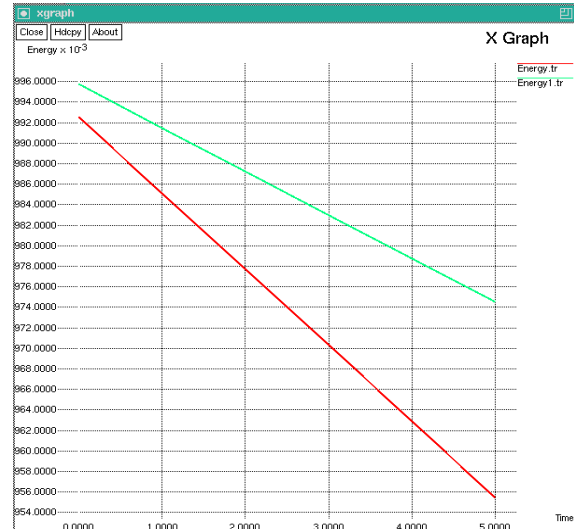
THROUGHPUT



DELAY



RESIDUAL ENERGY



7. Conclusion

The proposed idea of using LIFI in Medical Health Care arose solely because WIFI is still restricted in such fields as its considered harmful and insecure. Thus eventually, it leads to extra Labor force and Paper work. Another striking feature implemented in LIFI is Security through Elliptic Curve Diffie Hellman and Secure Hash Algorithms, thus making it reliable. The future of WIFI is highly uncertain with very little spectrum of radio frequencies left, hence LIFI remains to be the next generation wireless technology which can also be used in another WIFI restricted domain that is, Aviation industry.

References

1. Annu Malik, Anju Sharma (2013) "Greedy Algorithm", International Journal of Scientific and Research Publications, Vol.3, pp.1-5.
2. Anurag Sarkar, Prof. Shalabh Agarwal, Dr. Ashoke Nath (2015) "Li- Fi Technology: Data Transmission through Visible Light", International Journal of Advance Research in Computer Science and Management Studies, Vol.3, pp.153-159.
3. Ayaz Ahmad, Mahfuzul Huda, Mohd Atif Kaleem, Rajendra Kr Maurya (2015) "Mobile Ad-Hoc Networks: AODV Routing Protocol Perspective", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, pp.514-517.
4. Balajee Maram, Sravanthi Dangani, "Group Key Exchange Analysis in Sensor Networks", International Journal of Distributed Sensor Networks, Vol.10, pp.1-12.
5. Balaram Ghosal, Asim Kumar (2014), "Li-Fi a Green Energy Initiative", International Journal of Computer Applications, Vol.95, No.11, pp.1-3.
6. Chaitya B Shah, Drashti R Panchal (2014) "Secured Hash Algorithm-1: review Paper", International Journal For Advance Research In Engineering And Technology, Vol.2, pp.26-30.
7. Cheng Chen, Harald Hass, Liang Yin, Yunlu Wang "What is LIFI?", Journal of Lightwave Technology, Volume: 34, pp.1533 – 1544.

8. Christian Lederer, Roland Mader, Manuel Koschuch, Johann Grobsch ad, Alexander Szekely, Stefan Tilich (2009) “Energy-Efficient Implementation of ECDH Key Exchange Algorithm for Wireless Sensor Networks”, Information Security Theory and Practice, Vol.5746, pp.112-127.
9. Ganesan R and Neha Trithani (2014) “Data Security in Cloud Architecture based on Diffie-Hellman and Elliptical Curve Cryptography”, International Association for Cryptologic Research.
10. John Justin Thangaraj . S and A. Rengarajan (2016) “Unreliable Node Detection by Elliptical Curve Diffie-Hellman Algorithm in MANET”, Indian Journal of Science and Technology, Vol.9, pp.1-6

