ASN.1-XML Based Optimized Exchange Protocol For Health Information

Mruga Parikh[1] Mr. Basavaraj Hooli[2]
[1]Department of Wireless and Mobile Computing[2]Founder Director
[1]GTU PG-School, BISAGGandhinagar, India[2]Graceful Growth Consulting (India) Private Limited Pune.

Abstract— In healthcare, the importance of obtaining the right information, at the right time is very critical. Healthcare personnel need to access the real-time medical data such as patient's observation readings. Reliable, secure and optimized exchange protocol is developed over unreliable 3G network using TCP/IP protocol stack for Health information exchange. Security algorithm will be developed considering the criticality of Medical data. Improved QoS (Quality of service) over unreliable network by handling packet loss and reliability at application layer. And the exchange of Health Information will be in a data format that will be legible to read. Encoding standards will be used to provide compact transfer of medical data over the network.

Key Words: Quality of service, reliable,optmiized,secure.

I. INTRODUCTION

Nowadays, in our country the emergency services provided by the ambulance services, is such that while the patient is in transit to the hospital, the patient's observation readings are manually written. Which means that the staff at the hospital comes to know when the patients reaches the hospital. Now this is a big problem which results in worsening the patient's life or sometimes may be death. So, there is a need to develop such a system where patient is being give premedical health care [4]. Nowadays there are many new technologies being increasing at hospitals and labs at ever increasing rate, and many of these new technologies have the potential to interact cooperatively if they can be integrated properly. So, there is a need for an interoperability solution that has the ability to make the medical device work along with other applications and devices. EMR Gateway provides such software solution that automates the process of data capture by connecting simultaneously to various health, fitness, laboratory, and medical device's enabling flexible connectivity with any clinical systems in the hospital IT Infrastructure [1]. In healthcare the importance of obtaining the right information at right time, irrespective of time and location is very critical. Mostly the exchange of medical data lacks optimization over the network. Today the market situation is such that only 16 to 20 percent of hospital are using the gateway facility [1]. With such low rate adaption of m-health gateway, in emergency situations like in ambulance sending sensitive real time medical data to hospital server, without using m-health gateway or we can say a middleware or transport, will be facing problems like improperaggregation of medical data, improper structure format, lack of optimization during transport of data, lack of security. This all factors makes it time consuming for the hospital staff to identify and reorganize the information from the hospital server. Delay in such kind of situation can put the patient's life in danger which is not appropriate. Emergency services requires real time data of patient at appropriate time rather than delaying it. With large scale wireless networks and mobile computing solutions like 3G network, Wi-Fi mesh, Wimax, Bluetooth can tap into vital information anywhere and at any time within the healthcare network. Nowadays 3G technology is one of the emerging technology for demanding m-health services. MobiHealth is a European project that has explored the capabilities of 3G wireless network to support emergency m-health services. GE(General Electric) Healthcare is a unit of General Electric Company headquartered in United Kingdom is working on new medical technologies and services that are shaping new age of patient care [7]. It takes patient data access to an innovative level by helping enable hospitals access the patient data. Carescape Gateway is GE's excellent patient monitoring solutions which gathers data from multiple devices and systems and delivers real time patient data to nearby all hospitals. The Carescape gateway provides safe access to patient data by protecting the integrity and performance of the patient monitoring system. It uses HL7 data integration healthcare standard for exchange of medical data. Patient's health records are very sensitive data so secure access to medical record and secure transmission of medical data to hospital server needs to be implemented. Security in terms of Confidentiality, Integrity and authenticity should be provided.

While deciding which security algorithm to be implemented in our system, the most important thing to be considered like if the encryption and decryption process is time consuming due to large volume of data. As, we know that mobile devices have less memory ,so choosing such an algorithm which uses small key size so that on other side when receiving medical data the private keys can be get easily stored onto the device and decryption can be done faster [4].

Nowadays the most commonly used security protocol is SSL (Secure socket layer) protocol which ensures secure communication between two machines. Japanese governments are using SSL protocol for secure medical transmission within the hospital .Automatic implementation of algorithm, whichmeans we don't need to write any algorithm .But one needs to regularly renew the SSL certificate.

II. OVERVIEW OF PROPOSED SYSTEM

Our proposed solution is to develop a reliable protocol over unreliable 3G network using TCP/IP as an underlying protocol for communication which implements a strong security algorithm for exchange of medical data, handling packet loss and applying encoding standards over the data for compact transfer of medical data so that proper

All rights reserved by www.ijsrd.com

bandwidth utilization happens. The medical data will be exchanged XML format over http. A communication platform is provide for the exchange of medical data in an optimized and secure way, where the exchanged data format will be XML which will be legible for the hospital staff to observe the medical data.

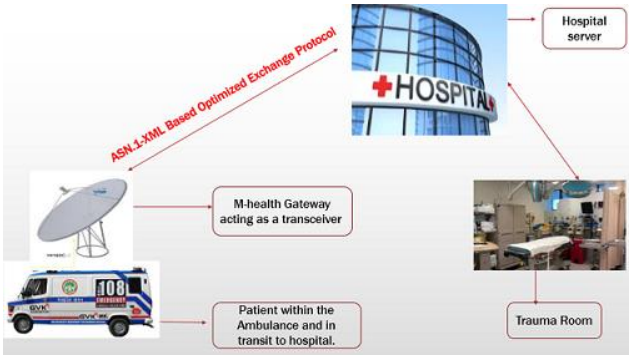


Fig. 1: Visual representation of Proposed System

The above figure depicts the Visual representation of the proposed system. When the patient is in transit to the hospital in ambulance, a transceiver acting as M-health gateway will be exchanging the Health information with the hospital server using Optimized Exchange protocol. And then the Health information will be provided from the hospital server to the Trauma room. The medical data will be exchanged in XML format. Here in the above figure, ASN.1 stands for Abstract Syntax Notation. A language for describing structured information, typically, information intended to be conveyed across some interface or communication medium.ASN.1 has been standardized internationally [2]. It is widely used in the specification of communication protocols.

III. Architecture Of Propsed System

The architecture of proposed system is designed in such a way that the medical information is exchanged in an optimized and secured way. Packet loss and reliability issues is be handled. TCP/IP protocol stack is used as an underlying communication for exchange of medical data. The different layers of TCP/IP protocol stack will be providing different functionality to the transferred data. As shown in Figure-2 at the Gateway and server side TCP/IP protocol suite is used and underlying 3G network is used as a communication medium.

At network layer, TCP protocol is used as underlying connection as it is a reliable protocol and in my case medical data is critical. Data will be encoded at network layer to provide optimized transfer of data. For handling Packet loss an intelligent acknowledgement algorithm is designed at transport layer so that no need for unnecessary retransmission of data packets. According to the TCP/IP protocol stack at application layer the data will be transmitted in XML format over HTTP (Hyper Text Transfer protocol). At application layer HTTP protocol acts as a transport protocol and the data is transferred in XML format which is legible and easily readable.3G network used as the underlying connectivity, upon which WAP (Wireless application protocol) protocol stack will be used.

WAP is an open specification which enables mobile users to access the internet. This protocol is independent of the underlying network which means that it can operate upon every network whether wireless or wired network. Each layer of WAP protocol stack is described below:

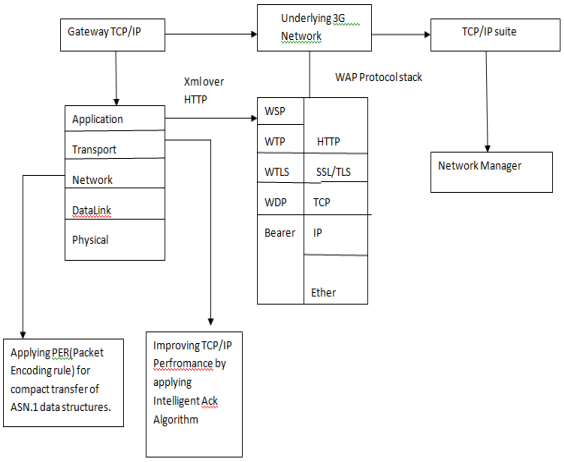


Fig. 2: Architecture of proposed system

- WSP (Wireless session protocol)
  This protocol is similar to HTTP protocol and provides data transmissions with small sizes so that clients can process data with less complexity.
- WTP (Wireless transaction protocol)
  This protocol is responsible for reliability.
- WTLS (Wireless transport layer security)
  This protocol provides security features such as authentication, confidentiality and integrity. This protocol uses SSL (Secure socket layer).
- WDP (Wireless datagram protocol)
  This protocol provides the underlying transport service.
- Bearer protocol
  This is the lowest level protocol and can be any wireless technique such as GSM, CDMA etc.

At network layer, PER encoding standard is applied to the ASN.1 file. PER stands for Packet encoding rule. It Optimizes the flow of information by applying packet encoding rules (PER) onto the ASN.1 file [9]. Provides a compact transfer syntax for the data structures like BOOLEAN, CHOICE, SEQUENCE, INTEGER described in ASN.1 file [10]. Provides more compact encoding then BER (Basic encoding rule).It is Bit Oriented. PER Encoding rule provides constraints to the data structure of ASN.1 file which limits the size of message and provides compactness during transmission of message [10]. If the given specification is not within a particular range it is not PER-Visible constraint. There can be extensibility while representing data in ASN.1 notation, which does not make it PER-Visible constraint. It extensibility is not applied, then the following specification is PER-Visible.
For example:

A ::= IA5String(SIZE(1..4))(FROM("ABCD",...))

The above expression is representation of ASN.1 notation. Now to apply PER encoding standard onto the above expression, PER visibility constraints comes into picture which has effective's size constraint of 1... 4 but the alphabet constraint is not visible because it is extensible.

All rights reserved by www.ijsrd.com

IV. Design Of Security Algorithm

In Healthcare sectors, medical data is very vital. So the security algorithm is designed considering the criticality of medical data. The designed algorithm uses one asymmetric and two symmetric key concept. For providing two layer security, concept of digital envelope is used. Digital signature is used for authenticity of client. The working of security algorithm is described as below:

- The client takes as input any file format.SHA-1 stands for secure hash algorithm is used.SHA-1 is applied onto the file.
- Now, the hashed file is encrypted using Triple DES (Data Encryption Standard) algorithm and key for encrypting the hashed file is the unique session id generated by the server.
- The encrypted hashed file is signed using clients private key (RSA(Rivest Shamir Adelman) generated keys)
- Now the concept of digital envelope is used upon the signed file, the normal input file and the Hash Encrypted file.
- To encrypt the data a random key is generated, and using that random key the signed file, normal input file and the Hash Encrypted file are encrypted.
- The randomly generated key is encrypted using server public key which is generated through RSA algorithm.
- Here, by using the concept of digital envelope two layer security has been provided which makes it a stronger algorithm.
- Same way at the server side, the signature file will be verified to check if it is an authenticated client or not.
- At the server side, integrity is also checked by the comparing the two hash files.

The designed security algorithm is providing authenticity, integrity and two layer security (Digital Envelope) which makes it stronger.

V. QoS Parameters

QoS (Quality of Service) includes parameters like delay, jitter, reliability, packet loss. Improved quality of Service helps over unreliable network.

Nowadays, 3G wireless connectivity provides pervasive internet access, good performance of TCP over wireless connectivity. Wireless link losses results in poor TCP throughput since losses are due to congestion by TCP. In order to mitigate the wireless loss effect, 3G wireless links are designed in such a way that local retransmission mechanisms are implemented. Local retransmission mechanisms ensure packet loss probability of less than 1% which ultimately reduces the impact of loss on TCP.No matter this mechanism reduces the effect of loss on TCP, but increases delay variability. Now, to increase the throughput, channel state based scheduling is used which increases delay and rate variability. This rate and delay variability translates to burst yack arrivals at the TCP source. Since TCP uses ack clocking to probe for more bandwidth, burst yack arrival leads to release of a burst of packets from the TCP source. When this burst arrives at a link with variable rate or delay, it could result in multiple packet losses [13].

3G networks are not so reliable so, Quality of service parameters needs to be handled in such a way that the network provides good quality of service. Some QoS parameters like reliability, delay, packet loss handling needs to be considered for improving quality of service over unreliable network.

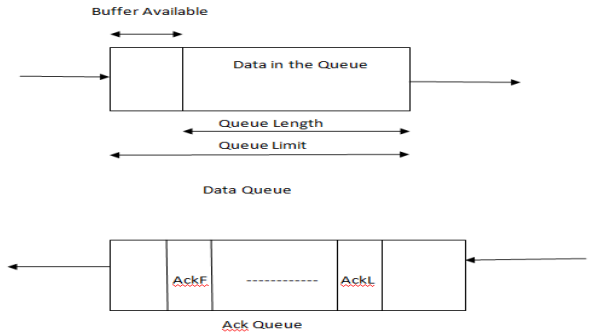


Fig. 3: Per-Flow of Data packets

For handling packet loss, algorithm has been designed. The working of the proposed algorithm is as follows:

- Firstly to check if there is buffer available in the data queue.
- If there is at least one buffer space available and if the number of acknowledgments present in the Ack queue is lesser than buffer available, all those acknowledgements are sent to the source.
- Otherwise only buffer available number of acknowledgements are sent to the source.

TCP/IP protocol is a transport layer protocol which provides reliability at transport layer. ARQ (Automatic Repeat Request) protocol delivers the packet to the intended users successfully even though they have got it, thus unnecessarily wasting bandwidth. So a Conceptual design of handling reliability is provided at application layer. Reliability is provided by replicating the data within the packet. Suppose packet contains data like Blood pressure, pulse oximeter and heart rate, the data is replicated within the packet five times. Concept of replication reduces the level of retransmission and multicasting becomes easier.

VI. Implementation

The proposed security algorithm has been implemented using SSL (Secure Socket layer) Protocol and the encoding data has been posted to the server over HTTPS (Hyper Text transfer Protocol Secure).

VII. Conclusion

In this paper, we designed and implemented a strong security algorithm for critical data such that our proposed system will effectively exchange the health Information. For improving Qos (Quality of service) algorithms have been designed in such a way that packet loss has been handled and unnecessary retransmission is avoided. The reliable protocol developed over unreliable network is providing optimization of Health Information.

References

[1] Mohan S., "EMR Gateway: An Interoperability solution for medical devices," White paper:Wipro Technologies.

All rights reserved by *www.ijsrd.com*

[2] O. Nokalva, ASN.1 Today and Tomorrow.

[3] P. Camacho, "An Introduction to the OpenSSL command line tool," [Online].

[4] G. R. Sudha G, "Secure transmission Medical data for pervasive healthcare system using android," in International conference on Communication and Signal Processing, April 3-5, 2013.

[5] R. B. H. Katarazyna Wac, "Measurement Based performance Evaluation of 3G Wireless network supporting m-health services.," IEEE.

[6] "XML Based DICOM Format," [Online]. Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3043771.

[7] GE Healthcare Innovations, "CARESCAPE Gateway :An innovation in patient data access".

[8] hl7.org, "HL7CDA," [Online]. Available: http://www.hl7.org.

[9] G. ADAMIS, ASN.1 Encoding.

[10] I. T. Union, "Information technology – ASN.1 encoding rules:Specifications of Packed Encoding rules," 07/2002.

[11] A. G. Abdurakhmanov, "BinaryNotes Developers Guide".

[12] P. j. Larmouth, ASN.1 Complete.

[13] M. C. C. a. R. Ramjee, "TCP/IP Performance over 3G Wireless Links with Rate and Delay variation".

All rights reserved by *www.ijsrd.com*