ISSN 2347-4289

Building A Secure System For Patient Data Transmission And Bug Indication In Sensor Networks

Vidhyasagar, NulynPunitha J

Student, IFET College of Engineering, Tamil Nadu, India
M.Tech., Senior Assistant Professor, IFET College of Engineering, Tamil Nadu, India,
vidhyamohan92@gmail.com, mailnulyn@gmail.com

Abstract: Wireless medical sensor networks is a key enabling technology in e-healthcare that allows the data of a patient's vital body parameters and used in indicating the bug 's of patient.

Keywords: sensor; patient; bug; wearable

I. Introduction

Wireless medical sensor networks have emerged as a promising technique which will revolutionize the way of seeking healthcare at home, hospital, or large medical facilities. Instead of being measured face-to-face, with MSNs, patient's health related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. There are many other applications too e.g. body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body-area networks can collect information about an individual's health, fitness, and energy expenditure.

II. Related Work

Wearable biosensors

Wearable biosensor systems for health monitoring are an emerging trend and are expected to enable proactive personal health management and better treatment of various medical conditions. These systems, comprising various types of small physiological sensors, transmission modules and processing capabilities, promise to change the future of health care, by providing low-cost wearable unobtrusive solutions for continuous all-day and any-place health, mental and activity status monitoring.

Implantable sensors

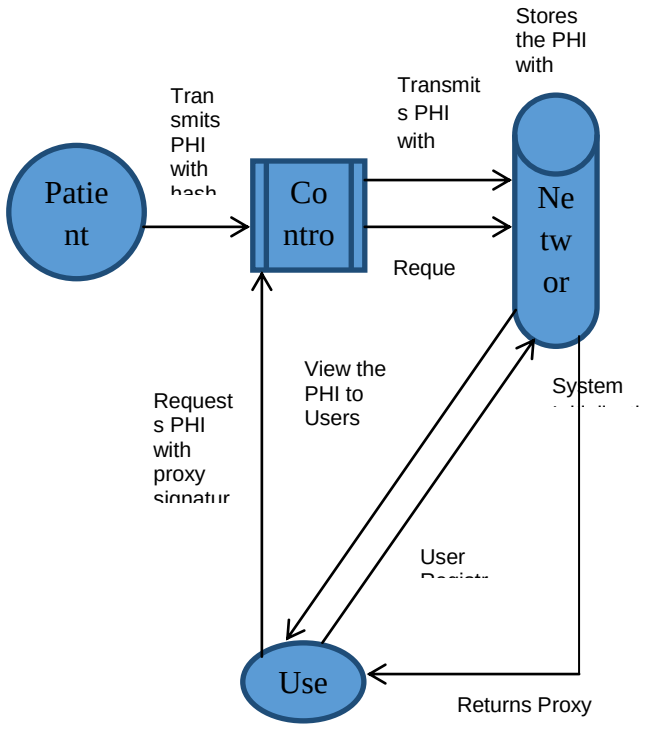
Implantable sensor systems offer great potential for enhanced medical care and improved quality of life, consequently leading to vast investment in this exciting field. Implantable sensor systems for medical applications provides a wide-ranging overview of the core technologies, key challenges.

Symmetric-key encryption and decryption

III. Equations

Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plain text and decryption of cipher text. n=p*q; p-1; q-1;e.d mod pi. In wireless medical sensor networks the patient's health information are collected by sensor. It is essential to strictly limit the access of these data to authorized users only in order to ensure the security of these data and preserve the patient's privacy.

IV. Figures



V. Bug Indication in sensor networking

Strapless heart rate monitors now allow the user to use sensors on their body for a few seconds to view their heart rate. These are popular for their comfort and ease of use though they don't give as much detail as monitors which use a chest strap which determine the heart rate. It includes a microprocessor which is continuously monitoring and calculating the heart rate, and other parameters. This sensor allows you to measure body temperature. It is of great medical importance to measure body temperature.

The reason is that a number of diseases are accompanied by characteristic changes in body temperature. Likewise, the course of certain diseases can be monitored by measuring body temperature. Hence it is a non-invasive sensor designed to measure human blood pressure. It measures systolic, diastolic and mean arterial pressure utilizing the oscillometric technique. Pressure range: 0 mm Hg to 250 mm Hg. Response time: 100 microseconds. With Continuous Glucose Monitoring you get a more complete picture of your glucose levels, which can lead to better treatment decisions and better glucose control. Without diabetes, your body tracks glucose levels all day and night to ensure the right amount of insulin is released at the right time. To successfully manage diabetes, a monitoring system is needed to consistently check your glucose levels.

VI. Conclusion

Here we proposed a secure and lightweight system for wireless medical sensor network. In the proposed system we used a hash-chain based key mechanism .Because of this security technique the data transmission from sensor to medical server done in a secure manner. The user here it is a doctor wants to access the patient's health parameters i.e. body temperature, blood pressure, blood glucose level, heart beat rate which are periodically collected. In each and every transmission the hash key gets updated. The original key is known only to sender and receiver. The other security technique we used here is proxy protected signature technique. In this technique the user who wants to access the patient's medical data must contain a valid proxy key. The proxy key is generated during registration itself. Using that proxy key he/she can able to

VII REFERENCES

[1] K.Lorincz,D.Malan,T.Fulford-Jones,A.Nawoj,A.pp.1946-1956,May2012.

[2] V.Shnayder,B.-R.Chen,K.Lorincz,T.R.F.Fulford-Jones,andM.Welsh,"Sensornetworksformedicalcare,"TechnicalReportTR-08-05,HarvardUniversity,2005.

[3] CrossbowSolutionsNewsletter.Motesformobilecommunicationandtele-medicine.2005.

[4] K.MalasriandL.Wang,"Addressingsecurityinmedicalsensornetworks,"inProc.ACMHealthNet,pp.7-12,2007.

[5] R.Rajasekaran,V.Manjula,V.Kishore,T.Sridhar,andC.Jayakumar,"Anefficientandsecurekeyagreementschemeusing Clavel,V.Shnayder,G.Mainland,S.Moulton,andM.Welsh,"Sensornetworksforemergencyresponse:challengesandopportunities,"IEEEPervasiveComputing,vol.3,no.4,pp.16-23,Oct.2004.

[6] Choi,B.Ahmed,andR.Gutierrez-Osuna,"Developmentandevaluationofanambulatorystressmonitorbasedonwearablesensors,"IEEETrans.Inf.Technol.Biomed.,vol.16,no.2,pp.279-286,Mar.2012.

[7] D.He,C.Chen,S.Chan,andJ.Bu,"DiCode:DoS-resistantanddistributedcodedissemination inwirelesssensornetworks,"IEEETrans.WirelessCommun.,vol.11,no.5,physiologicalsignalsinbodyareanetworks,"in Proc.ICACCI,pp.1143-1147,2012.

[8] H.Wang,H.Fang,L.Xing,andM.Chen,"Anintegratedbiometric-basedsecurityframeworkusingwavelet-domainHMMinwirelessbodyareanetworks(WBAN),"inProc.IEEEICC,pp.1-5,2011.

[9] K.MalasriandL.Wang,"Designandimplementationofasecurewirelessmote-basedmedicalsensornetwork,"Sensors,vol.9,no.8,pp.6273-6297,Aug.2009.

[10] S.Keoh,"Efficientgroupkeymanagementandauthenticationforbodysensornetworks,"inProc.IEEEICC,pp.1-6,2011.

[11] C.C.Tan,H.Wang,S.Zhong,andQ.Li,"IBE-lite:Alightweightidentity-basedcryptographyforbodysensornetworks"IEEETrans.Inf.Technol.Biomed.,vol.13,no.6,pp.926-932,Nov.2009.

[12] X.Le,M.Khalid,R.Sankar,andS.Lee,"Anefficientmutualauthenticationandaccesscontrolschemeforwirelesssensornetworkinhealthcare,"JournalofNetworks,vol.6,no.3,355-364,2011.

[13] P.KumarandH.-J.Lee,"Securityissuesinhealthcareapplicationsusingwirelessmedicalsensornetworks:asurvey,"sensor,vol.12,pp.55-91,2012.

[14] D.He,J.Bu,S.Zhu,S.Chan,andC.Chen,"Distributedaccesscontrolwithprivacysupportinwirelesssensornetworks,"IEEETrans.WirelessCommunication.,vol.10,no.10,pp.3472-3481,Oct.2011.

[15] W.He,Y.Huang,R.Sathyam,K.Nahrstedt,andW.Lee,"SMOCK:Ascalablemethodofcryptographickeymanagementformission-criticalwirelessad-hocnetworks,"IEEETrans.InformationForensicsandSecurity,vol.4,no.1,pp.140-150,Mar.2009.

[16] S.Zhao,A.Aggarwal,R.Frost,andX.Bai,"Asurveyofapplicationsofidentity-basedcryptographyinmobilead-hocnetworks,"IEEECommun.Surveys&Tutorials,vol.14,no.2,pp.380-400,SecondQuarter2012.

[17] D.MaandG.Tsudik,"Securityandprivacyinemergingwirelessnetworks,"IEEEWirelessCommun.,vol.17,no.5,pp.12-21,Oct.2010.

[18] C.CordeiroandM.Patel,"Bodyareanetworkstandardization:presentandfuturedirections,"inProc.BodyNets'07,pp.1-2,2007.

[19] Z.Shao,"Provablysecureproxy-protectedsignatureschemesbasedonRSA,"Computers&ElectricalEngineering,vol.35,no.3,pp.497-

505,May2009.

[20] Z.Shao,"Proxysignatureschemesbasedonfactoring,"InformationProcessingLetters,vol.85,no.3,pp.137-143,2003.

[21] K.C.BarrandK.Asanovi,"Energyawarelosslessdatacompression,"ACMTrans.Comput.Syst.,vol.24,no.3,pp.250-291,Aug.2006.

[22] OpenSSL,http://www.openssl.org.

[23] TinyOS:Anopen-sourceOSforthenetworkedsensorregime.http://www.tinyos.net/.

[24] Kapitanova,andS.Son,"Thepriceofsecurityinwirelesssensornetworks,"ComputerNetworks,vol.54,no.17,pp.2967-2978,Dec.2010.

[25] A.LiuandP.Ning,"TinyECC:Aconfigurablelibraryforellipticcurvecryptographyinwirelesssensornetworks,"in Proc.IPSN,pp.245-256,2008.

[26] SoftwareAES,http://tinyos.cvs.sourceforge.net/viewvc/tinyos/tinyos-2.x-contrib/crypto/index.html

[27] A.Milenkovi,C.Otto,andE.Jovanov,"Wirelesssensornetworksforpersonalhealthmonitoring:Issuesandanimplementation,"ComputerCommunications,vol.29,no.13-14,pp.2521-2533,Aug.2006.