International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

General Article

Issues in Transmitting Physical Health Information in m-Healthcare

Saikat Saha[a*] and Sanjeev Kumar Tomar[a]

[a]Computer Science, Amity University

Accepted 4 March 2013, Available online 1June 2013, **Vol.3, No.2 (June 2013)**

Abstract

With the advancement of wireless sensor network it allows critical patient to have a secure and advance Mobile healthcare solution. Mobile healthcare provides an extended monitoring of patients anywhere anytime. Although mobile healthcare solutions furnish a prominent commute in healthcare solutions there are some security issues in exchanging the Physical Health Information. In this paper some of the issues of physical health information are discussed.

Keywords: *Mobile Healthcare (m-Healthcare), Physical Health Information (PHI), Cellular Node, Body Sensor.*

Introduction

m-Healthcare Scenario

Let us first consider the mobile healthcare scenario (fig. 1). John is heart patient. He needs to be ceaselessly monitored to avoid the further health damage. Preciously he needs to monitor his blood pressure, heartbeat etc. So he subscribes for m-Healthcare solution which provides him various healthcare solutions including e-monitoring, e-assistance in case of emergency. As per the subscription terms and conditions he needs to equip wireless body sensors which will continuously check his medical condition and store the data to his medical record.

Medical data will be analysed by the consulted doctor remotely in the hospital and accordingly assistance will be provided to John. Except the regular work hour doctors can provide an assistance while he is on a go. In case of emergency if a specialist doctor is nearby while he is on a go, his device can discover the doctor and alert him for immediate medical assistance.

John can get help from other authorised medical centre and home based healthcare. m-Healthcare will also help John's family to locate him very easily.

Issues in m-Healthcare

Wireless monitoring of patients involves the wearable body sensors to measure heart rate, ECG, EEG etc. These body sensors further transfer the monitored data through Cellular Network. Although data transmission faces serious problem like:

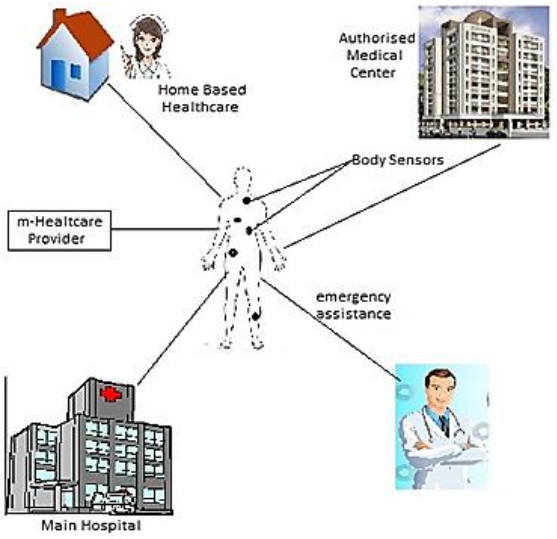

Fig. 1. m-Healthcare Scenario

- Quality of data
- Privacy of transferred data
- Power effectiveness of the transmitting device.

Physical Health Information (PHI) that are transmitted over the cellular network are highly sensitive to the individual person. Security of the PHI one of the biggest challenge in the context of mobile healthcare. Another major issue in mobile healthcare is power supply to the cell phone. These need other nodes to transmit the PHI to the healthcare centre.

Suppose a data need to be transmitted from source cellular node (C_s) to destination cellular node (C_d). Source will use the intermediate cellular node to transmit the PHI. Power consumption of the node depends on how many messages is being forwarded from a particular node. If the distance between C_s and C_d is D, and n intermediate node C_i help in transmitting the data,

*Saikat Saha is a M.Tech Student and Sanjeev Kumar Tomar is Asst Prof.

$$D = \sum_{i=s}^{d} d_i$$

Where d_i is the direct distance between the two neighbour nodes. If the power used to transmit over d_i is P_i, the total power $P = P_{s-1}(d_1) + P_{1-2}(d_2) + \ldots + P_{n-d}(d_n)$. According to this equation if the hop count minimizes power consumption will automatically minimizes.

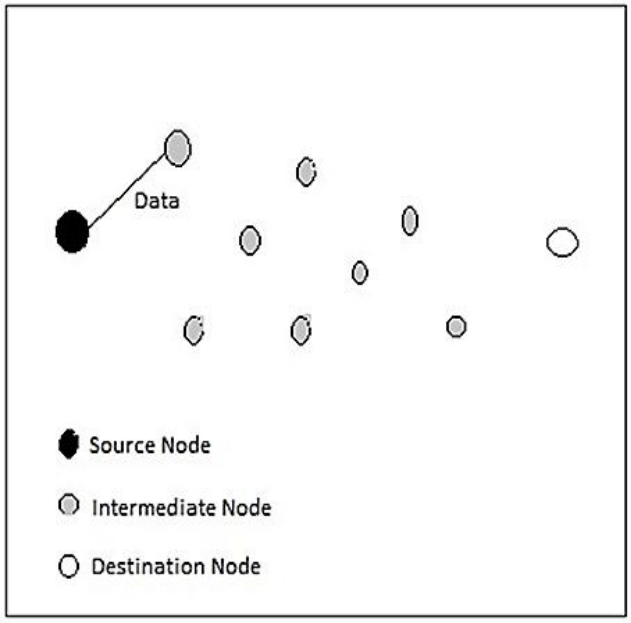

Fig. 2

Both the patient's node and the intermediate nodes must forward the message with the optimal power level so that message reaches the neighbour node. This will optimise the power consumption of cellular node.

Security of PHI in m-Healthcare

Although body sensors and wireless cellular node provide a significant advantage in mobile healthcare, there are some issues related to the security and privacy of medical user's physical health information in mobile healthcare solution. As the mobile healthcare system consist of wireless sensor and mobile node, the security of patient's private data at the time of transmission from one wireless cellular node to another wireless cellular node is the main concern. Security must provide a confidence to the user that the highly sensitive physical health information will not be disclose to the unauthorised third party, only authorised person should have access to the patient's physical health information.

Concealment of users' physical health information

One of the way to keep the data secure at the time of transition is to use key to encrypt and decrypt the highly sensitive data. A scenario of encryption and decryption of physical health information using key is shown in fig. 3.

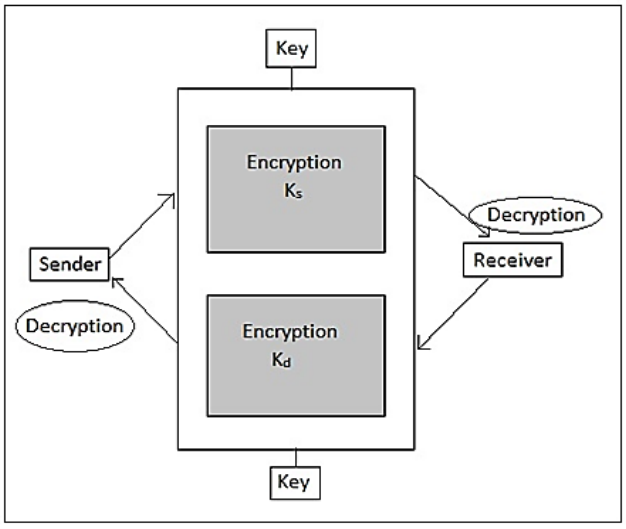

Fig. 3 PHI encryption/decryption

Encryption/decryption may be done using symmetric or asymmetric keys. Symmetric key includes secret key, session key or private key. Symmetric key is given to the user at the time of subscription to mobile healthcare solution. These keys are meant to be kept secret. User will share these keys with only the authorised person so that only authorised person have access to the patient's highly sensitive physical health information. Asymmetric key provides more confidentiality to the patient's health information and it reduces the computational cost of public key encryption. Data encryption and decryption process is depicted in fig 2.

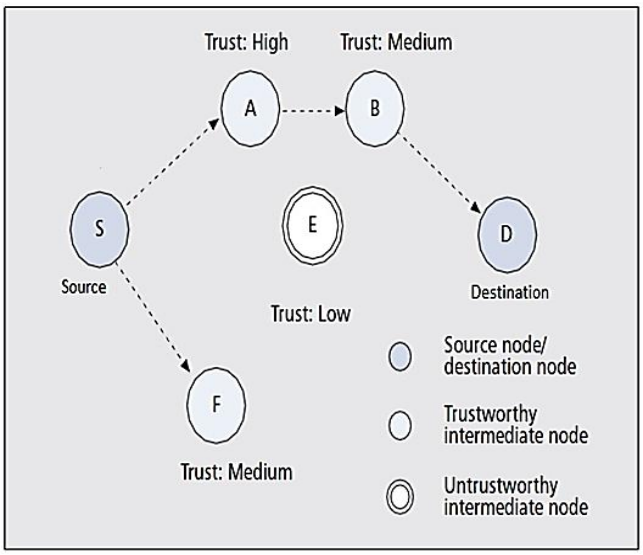

Fig. 4Time-serving trust based security

To optimise the power consumption, instead of sending the physical health information directly from the user's cellular node to the hospital, user's cellular node will use the neighbour cellular node to send the data. In this context trust based network can be formed to select the

opportunistic neighbour node. First the user's node will discover all the time-serving node for the further transmission of physical health information to minimize the power consumption. These time-serving nodes are categorized according to their trust. User's cellular node will always prefer the highly trusted node for the communication. Trust based time-serving security scenario is depicted in fig. 4.

According to the trust level cellular node will send the amount of highly sensitive data to the other cellular node. This will lead to minimum disclosure of physical health information and optimized power utilization.

Conclusion

Security and privacy of the patient's highly sensitive physical health information and optimized power utilization is the main issue to the mobile healthcare solution. A typical mobile healthcare scenario is shown here. In this paper power optimization and time-serving trust based security is discussed.

References

C.-C. Lin *et al.*(2008), A Healthcare Integration System for Disease Assessment and Safety Monitoring of Dementia Patients, *IEEE Trans. Info. Tech. Biomedicine*, vol. 12,pp. 579–86.

Rongxing Lu, *Member, IEEE,* Xiaodong Lin, *Member, IEEE,* and Xuemin (Sherman) Shen, *Fellow, IEEE* SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency

The Privacy and Security Gaps in Health Information Exchanges A White Paper by the AHIMA/HIMSS HIE Privacy & Security Joint Work Group.

Alessandra Toninelli, Rebecca Montanari, and Antonio Corradi (2009), University of Bologna, Enabling secure service discovery in mobile healthcare enterprise networks IEEE Wireless Communications.

U. Varshney (2006), Pervasive Healthcare and Wireless Health Monitoring, *Mobile Net. Apps.*, vol. 12,pp. 113–27.

W.-B. Lee and C.-D. Lee (2008), A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations, *IEEE Trans. Info. Tech. Biomedicine*, vol. 12, pp. 34–41.