Efficient End to End Data Communication Protocol for Wireless Body Area Networks

T.Santhi Vandanna, S.Venkateshwarlu

Abstract**:** ***In recent years wireless body area network (WBAN) technology has been accelerated due to the demands that arise to provide solutions to the problems such as population aging, various chronic diseases monitoring and to facilitate data collection. This increasing demands and WBAN deployments always comes with the cost of various security and privacy related problems. Designing an efficient framework to ensure both security protection and reliability in all critical events with considerable energy efficiency is a difficult task to accomplish, due to the multi modal dynamics of the WBAN network topology. The performance of security mechanism and authentication measures has a direct impact on the attainable system performance. In this paper, we briefly introduce unique transformation and data protection schemes for end-to end secured WBAN systems. Here, we first present color variant and key driven QR pattern generation techniques, how they utilized and meets the requirements of security and privacy in WBAN and validated the performance metrics and efficiency of proposed pattern generation and analyzes in providing solution of security and privacy in WBAN.***

Index Terms**:** ***Body sensors, security, privacy, Biometric, Quick response (QR) code, data protection, Wireless network etc.***

I. INTRODUCTION

In recent years wireless body area networks (WBAN) is steadily emerged as prominent methodology in real-time patient monitoring which helps to detect many chronic diseases well early for appropriate medical treatment (Celić, Luka, et al., (2013)). In general sensor network based healthcare monitoring system automatically collects the patient report using tiny sensor nodes that can analyzed by any remote personnel's through some wireless networking technology. The wireless technology used and sensor nodes integration differ over wide range of WBAN applications such as Telemedecine (Chakraborty et al., (2013)), Rehabilitation (Jovanov, Emil, et al., (2005)) and Biofeedback etc. This will leads some critical issues like accessibility and privacy of a person's sensitive medical information data in wireless environments. The statistical analyzes and security measures carried by the US Food and Drug Administration (FDA) explores that the potential risks to the public and problems need to be addressed in medical devices and hospital networks.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author

T.Santhi Vandanna*, Research Scholar, KLEF Deemed to be University, Vaddeswaram, Guntur (Dt), A.P, India.

S.Venkateshwarlu, Professor, KLEF Deemed to be University, Vaddeswaram, Guntur (Dt), A.P, India.

Several Cryptography and authentication models are investigated in many works which can offer secure data transmission via wireless communications. In many cases numerous key management and sharing schemes are noted as major concern for security in any wireless sensor networks (He et al., (2013)). Moreover, formulating an efficient key management and security scheme in WBANs is also difficult task to accomplish due to the limitations that arises within sensor nodes such as less memory space, resource constraints and energy consumption etc. These requirements may differ depends on environments and sensor characteristics of WBAN network (Mehfuz et al., (2015)). In most cases WBAN mostly deals with medical information that needs to be processed and analyzed within given time bound. The security and privacy measures included for reliable WBAN system should not degrade the actual system performance. Li et al., (2010) proposed fine-grained distributed data access control unit to mitigate security problems and accessibility issues in dependable distributed medical data storage. It is also explored various practical issues that may arises in WBAM network and major security and privacy requirements for real time applications. In real time WBAN system should provide security and privacy in all stages such as data gathering from sensor nodes , data transmission, data storage and finally to extract correct medical information to appropriate medical personals.

In some cases WBANs should equipped with significant memory space and massive server based data storage for real-time medical data processing and data accessibility/ analysis in both online and offline. Due to the open access of the any cloud computing environment, the protection against attacks is the difficult task to accomplish to ensure privacy. In Wan, Jiafu, et al., (2013) Mobile cloud computing unit is integrated with wireless body area networks to accomplish cost-effective, scalable, and real time health WBAN healthcare systems. Negra et al., (2016) presented architecture deployments and appropriate radio technology requirements for WBAN application and investigated remotely access patients health information by means of the Internet. He, Debiao, et al.(2016) developed anonymous authentication scheme for data's confidentiality and patients' privacy in WBAN healthcare system and proved its performance metrics against impersonation attacks.

However health monitoring assisted by cloud computing need to be designed with appropriate control over data gathering and should provide very strong privacy and security protection. Li, Xiong, et al. (2017) developed mutual data validation and key agreement method for centralized WBANs which is connected with the local server/hub node and used unique session key for an anonymous access.

Shen, Jian, et al. (2018) proposed low complexity authentication protocol to obtain user's real identity in Cloud-aided WBANs. Wang et al., (2019) analyzed the security and privacy issues of the mobile cloud computing in various healthcare applications and presented optimization methods to meet the desired quality rate while achieving the optimal trade off among multiple data-intensive tasks. Bhatia et al., (2019) developed pairing-free incremental proxy re-encryption which generates hash value for each scratch. This incremental encryption method offers significant performance improvement with reduced energy consumption and computational time.

Due to its simplicity, QR patterns have emerged tremendously in the authentication of different commercial commodities including cloud data. Due to its simplified code generation methods and the readily available QR code readers in smart phones let them to use in wide range of application from entertainment to healthcare. K.-C. Liao and W.-H. Lee (2010) proposed QR code based authentication as a potential alternative to one-time password based authentication for a remote database to client access services.

To narrow down and solve the security issues we discussed above more explicitly, we proposed a novel WBAN communication architecture as shown in Figure 2. The proposed WBAN covers two aspects; secured sensor node communication using highly optimized cryptographic algorithm and privacy enabled communication between WBAN system and internet of things. This paper is organized as follows. In Section 2 we discuss security measures and key management goals for sensor node communication. Key issues such as data alterations and unauthorized access between WBAN and remote links are discussed in Section 3, and configurable QR pattern enabled data protection and access control is elaborated in Section 4. Finally, in Section 5, includes summary and probable research extensions.

II. SECURED INTER NODE COMMUNICATION IN WBAN

Sensor nodes in WBAN provides a compact and user-friendly patient's health care monitoring which can update the status for periods of time as per time bound given and also avoids highly complex wire connections around the patient. Though it has high potential for outdoor and remote patient monitoring it requires appropriate cipher transformations to incorporate adequate levels of security. Here these problems are mitigated using biometric key generation and optimized cryptographic measures. Here data confidentiality is achieved by utilizing RR-interval extracted from ECG signal features as encryption key which gives complete randomness and reliability. And simplified cipher transformations process is used which consists of XOR and permutation operations. The permutation and cyclic shifting process is applied to enable randomized transformation level called diffusion in the cipher, whereas the substitution block is used to accomplish confusion as discussed in (Karimian, Nima, et al., (2016)).

III. AUTHENTICITY AND PRIVACY PRIVILEGES

Authenticity in WBAN means the data transformation from access point to the legitimate entities and appropriate claim for each decomposed sub groups. The system requirements and security measures need to be solved for reliable data communication in WBAN are given below:

Data authenticity: intended attacks may carry out using malicious nodes during multi path data propagation and they may inject bogus sensor into the WBAN system; thus the end devices need to verify the validity of source of data transformation.

Data confidentiality: In general WBAN channel is open access will leads easy passive attacks which can explore sensor data collection and all other patient information to unauthorized users. This can be mitigated using some cryptographic cipher transformation during data transmission.

Data integrity: This deal with the eavesdropped information which is transmit back to sensor nodes to carry out some unintended tasks, which causes failure and disaster to the clients. This can be solved using appropriate data verification and valid integration.

Data availability: This comes under denial-of-service (Dos) kind of attacks to the server where patient's data stored leading to the services denials which causes complete health care failure. This can be solved with some unique detection methodologies to identify DOS attacks.

In order to minimize the human intervention, it is essential to incorporate an end-to-end security protocol between wireless body sensor integration and the back-end cloud database followed by authenticated data accessibility by medical personals. The solution suggested for fully integrated and automated security measures in WBAN need to full fill all above mentioned demands.

IV. ACCESS CONTROL AND PROTECTION USING QR PATTERNS

Here we consider both access control and protection as a primary concern WBAN healthcare monitoring systems. To ensure both privacy and safety for patients, unique key driven QR pattern generation and parametric driven QR pattern color selection users based on its legitimacy and end functionality. Here all kind of external attackers can be easily prevented from accessing the information's gathers in cloud using QR pattern analyzes. This key compound QR pattern privileges all medical personnel which include clients, doctors and pharmacist.As a one-to-many data transmission is essential in WBAN, key bounded QR pattern analyzes is an effective methodology to achieve finite data access control, where the information's are revealed only to a group of valid terminals that meets a certain access policy. As shown in Fig. 1. In the proposed system, we introduce a unique approach for generation of color variant QR codes for each sensor data collection. During data validation at access point this WBAN generated color pattern is used as validation key to avoid malicious attacks. Here, by applying a unique Number Generator (TNG) function which can select various pattern generations which will be act as a Master Share to protect server data. During data access unique sequence are forwarded to sever which is validated at server side and assessments were carried out accordingly.

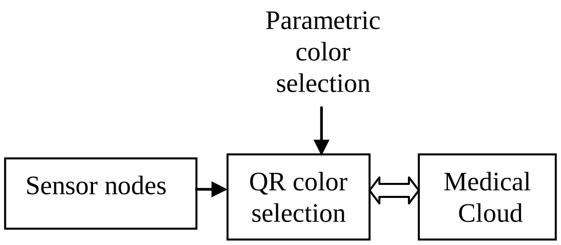


Figure 1. QR pattern variant driven WBAN access control and data protection

Table 1. Color variant QR patterns fordata validation and attack prevention over heterogeneous WBAN sensor network.

Signal measures	QR pattern
ECG	
EEG	
Pulse	

Table 2. QR pattern analyzes for authentication and medicalpersonal accessibility.

Key bound used:	Coded QR pattern
Valid key (decidable QR pattern)	
Randomized key (In valid pattern)	

V. Protection level and Efficiency

Due to uniqueness and randomized colour and pattern selection this moderate QR pattern matching solutions can tolerate any kind of attack; that is, any set of malicious users will not be able to assume or reproduce the patterns assigned for each entity. Meanwhile, quality metrics is also improved with salient error correction capabilities of QR pattern generation. Since the QR patterns are easily to handle and robust against erroneous wireless transmission, it is well suitable for any type of resource-constrained and high traffic – complicated WBAN network.

VI. EXPERIMENTAL RESULTS

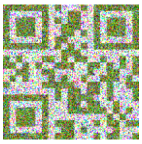
We have implemented the proposed color variant QR pattern generation and key driven pattern selection algorithms for WBAN data validation and authentication. The algorithms are tested with three different bio-signal measures and that can be extended for any number of heterogeneous information by simply applying appropriate colors during pattern generation.

Here we were considered the server is equipped with QR pattern analyzer. With this assumption, all session keys and authentication keys all are transformed into patterns and mapped as Master Share. In addition to this: This Master key is combined with the session based color QR models to generate the Secret key. The extracted QR shares are robust against path loss during propagation that is validated with Error Rate measures, variance coefficient, Structural Similarity Index Measure (SSIM) measures as shown in table 3.

VII. CONCLUSION

Wireless Body Area Networks supporting wide range of applications and offers significant contributions towards patient monitoring, clinical diagnostic measurements. Sensor data gathered in WBAN devices are highly sensitive and possibly need to store and accessed in remote places located at different places and situations, they require highly secured data transmission, storage medium and accessibility. Here simplified biometric cryptosystem technique is used secured for sensor data transmission with no chance of passive attacks. It was seen that the color variants and different types of pattern generation methodologies QR patterns plays an vital role in the design of reliable end-to-end security measures in WBANs. Based on system requirements and targeted application different QR patterns were developed for security solution such as data privacy, integrity, data freshness, valid medical personal authentication etc.

Table 2. QR pattern robustness analyzes for reliability measures

Key bound used:	Input QR pattern	Interfered QR pattern (Noise tolerance level-variance= 0.4)	Nominal Color variations (SSIM lower bound = 0 .345)
Non linearity measure			

REFERENCE

1. Celić, Luka, et al. "WBAN for physical activity monitoring in health care and wellness." World Congress on Medical Physics and Biomedical Engineering May 26-31, 2012, Beijing, China. Springer, Berlin, Heidelberg, 2013.
2. Chakraborty, Chinmay, Bharat Gupta, and Soumya K. Ghosh. "A review on telemedicine-based WBAN framework for patient monitoring." Telemedicine and e-Health 19.8 (2013): 619-626
3. Jovanov, Emil, et al. "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation." Journal of NeuroEngineering and rehabilitation 2.1 (2005): 6
4. Li, Ming, Wenjing Lou, and Kui Ren. "Data security and privacy in wireless body area networks." IEEE Wireless communications 17.1 (2010): 51-58.
5. He, Xiaobing, Michael Niedermeier, and Hermann De Meer. "Dynamic key management in wireless sensor networks: A survey." Journal of Network and Computer Applications 36.2 (2013): 611-622.
6. Mehfuz, Shabana, Shabana Urooj, and Shivaji Sinha. "Wireless body area networks: a review with intelligent sensor network-based emerging technology." Information Systems Design and Intelligent Applications. Springer, New Delhi, 2015. 813-821.
7. He, Debiao, et al. "Anonymous authentication for wireless body area networks with provable security." IEEE Systems Journal 11.4 (2016): 2590-2601.
8. Wan, Jiafu, et al. "Cloud-enabled wireless body area networks for pervasive healthcare." IEEE Network 27.5 (2013): 56-61.
9. Karimian, Nima, et al. "Highly reliable key generation from electrocardiogram (ECG)." IEEE Transactions on Biomedical Engineering 64.6 (2016): 1400-1411
10. K.-C. Liao and W.-H. Lee, "A novel user authentication scheme based on QR-code," Journal of Networks, vol. 5, no. 8, pp. 937– 941, 2010
11. Negra, Rim, Imen Jemili, and Abdelfettah Belghith. "Wireless body area networks: Applications and technologies." Procedia Computer Science 83 (2016): 1274-1281
12. Li, Xiong, et al. "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks." Computer Networks 129 (2017): 429-443.
13. Shen, Jian, et al. "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks." Journal of Network and Computer Applications 106 (2018): 117-123.
14. Wang, Xiaoliang, and Zhanpeng Jin. "An Overview of Mobile Cloud Computing for Pervasive Healthcare." IEEE Access (2019).
15. Bhatia, Tarunpreet, A. K. Verma, and Gaurav Sharma. "Towards a secure incremental proxy reencryption for e-healthcare data sharing in mobile cloud computing." Concurrency and Computation: Practice and Experience (2019): e5520.