Modeling of WBAN and Cloud Integration for Secure and Reliable Healthcare

Kalyani Divi and Hong Liu
University of Massachusetts Dartmouth
North Dartmouth, MA 02747, U.S.A.
HLiu@umassd.edu

ABSTRACT
Wireless Body Area Network (WBAN) becomes an emerging technology for ubiquitous healthcare. On-body or implanted sensors continuously collect patients' vital signs that are delivered wirelessly and automatically to caregivers. Humongous data need efficient process and storage with Cloud as it evolves from the Internet and distributed process/storage. Integrating WBAN and Cloud, WBAN-cloud, promises effective healthcare. However, security to resist malicious attacks and reliability to tolerate natural frays should be addressed due to its high stake. This paper proposes a WBAN-cloud architecture targeted at monitoring a variety of biomedical conditions. The design considers security and reliability requirements in the entire process, resulting in a unique structure of Forest Topology Three Tier (FTTT). By introducing a security gate, extended dynamic fault tree models *FTTT Secure Architecture* to analyze its resilience against security failures besides tolerance of component failures to ensure quality-of-service. FaultyTree+ package confirms the architecture's satisfactory level of security and reliability.

Categories and Subject Descriptors
C.2.0 [**COMPUTER-COMMUNICATION NETWORKS**]: General-Security and protection.

General Terms
Security, Reliability, Design, Verification.

Keywords
Wireless Body Area Networks (WBAN), integration of WBAN and Cloud (WBAN-cloud), security/reliability/quality-of-service (QoS), modeling and simulation.

1. INTRODUCTION
Recent advances in wireless body area networks (WBAN) pose threats beyond conventional security services [1]. The public cautions about severe consequences of both accidental misusages and malicious attacks. Other applications with wireless sensor networks, such as animal habitat monitoring, may not concern security, but energy consumption sets the first priority due to the difficulty in changing batteries. Therefore, we should design security solutions in application-specific context.

Cloud takes computing as a utility like water and electricity, transforming the information age into a new era [2]. Some pioneer medical projects promise grant opportunities to Cloud. However, security concerns of Cloud escalate due to the life-threatening situations related to healthcare applications.

Healthcare infrastructure deploys both WBAN and Cloud to achieve mobility and efficiency in monitoring patient conditions [3]. Miniature sensor nodes have constraints in computation, memory, and power resources. Most security mechanisms utilize cryptography, requiring high computation power. Cloud can offset critical resources to WBAN security services.

This paper addresses the application-specific security in healthcare context and provides an architecture that integrates WBAN and Cloud. The architectural design process takes into account the security/reliability requirements. We then validate the architecture for its fault-tolerance to component security failures.

Major Contributions

Firstly, we demonstrate the benefits and feasibility of integrating WBAN and Cloud, proposing WBAN-cloud architecture for healthcare applications. Second, we are the first to consider security requirements during the architectural design, resulting in a unique Forest Topology Three Tier (FTTT) structure resilient to security attacks. This approach departs from the usual way of patching security after the system is developed. Third, we analyze the system tolerance to security failures.

2. RELATED WORK
Breakthrough has recently achieved in programming complexity of WBAN applications. SPINE (signal processing in node environment) represents the most notable work [4]. SPINE is an open-source programming platform supporting rapid and flexible prototype and effective management of WBAN applications. By integrating WBAN with Cloud, quality-of-service (QoS) issues are adequately addressed with self-adaptive services to reliably deliver efficient data process [5].

It comes to a consensus that most security schemes proposed for general wireless sensor networks are not applicable to WBAN [6]. A new class of non-cryptographic authentication schemes shows the promise in WBAN [7]. In particular, group device pairing (GDP) scheme establishes initial ad-hoc trust with zero prior security context. With user aid, GDP authenticates key agreement among multiple sensor devices for their subsequent secure communications. GDP supports fast batch deployment of sensor devices, suitable to WBAN [8].

Divi et al, among the first, brought the attention to secure WBAN-cloud applications at architectural level. They propose a novel forest topology three tier (FTTT) structure for secure and reliable healthcare services, called *FTTT Secure Architecture* [9]. Its effectiveness to secure faults is subject to formal analysis.

BODYNETS 2013, September 30-October 02, Boston, United States

DOI 10.4108/icst.bodynets.2013.253706

3. FTTT SECURE ATCHITECTURE

Figure 1 illustrates a typical architecture for WBAN in healthcare. Sensor nodes are deployed on a patient in clusters to save energy consumption. Cluster nodes transmit data to a gateway, and the gateway relays data to a database through the Internet, accessed by hospital staff, system administrators, and the patient.

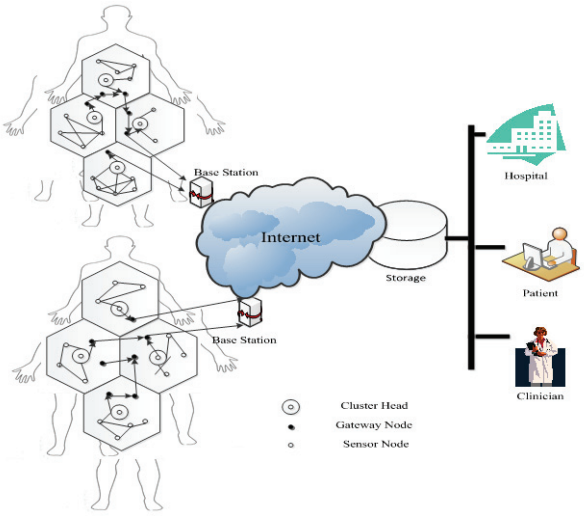


Figure 1. General WBAN in Healthcare

Much work provides secure communication for WBAN, however, as add-on feature, limited by the inherit WBAN vulnerability. Our research places security in the center of the architectural design.

3.1 Forest Topology Three Tier (FTTT)

General patient monitoring possesses forest topology, a choice by Microsoft exchange server 2007, an outer boundary of directory service. As shown in Figure 2, the Patient Monitoring System forms a forest at the base station with each aggregation node as a tree root and sensor nodes as leaves. WBAN-cloud requires security at three tiers: WBAN for patient monitoring, Cloud for process and storage, and Access Control with multiple facets.

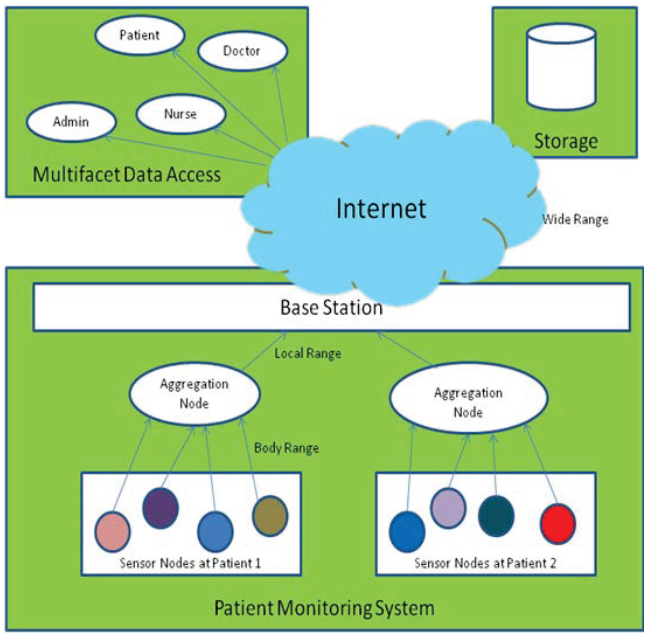


Figure 2. FTTT Architecture

The first tier (WBAN) needs strong authentication protocol for registering/authenticating on-body sensors and interacting with the other tiers. The second tier (Cloud) stores data with password protection. The third tier controls remote access with desktops, laptops, PDAs, or smart phones.

3.2 WBAN: Patient Monitoring (Tier 1)

Figure 3 depicts the functional overview of Patient Monitoring System with WBAN for mobility. Sensor nodes collect patients' vital information, aggregation nodes consolidates the data for efficient transmission, and base station relays mobile devices.

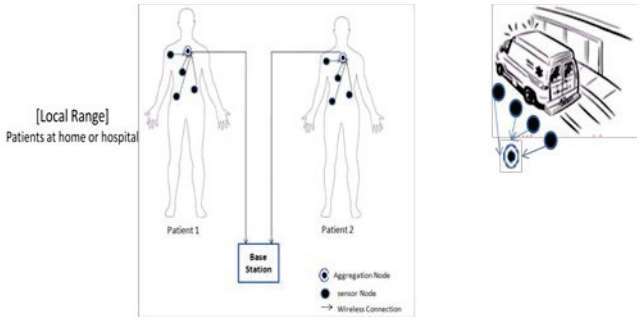


Figure 3. WBAN: Patient Monitoring

3.3 Cloud: Process and Storage (Tier 2)

Cloud stores the patient records. A patient registers in Cloud with his/her unique feature such as DNA sample. Sensors and aggregation nodes are also identified with Cloud. Both patients and medical devices are authenticated at each time of accessing Cloud via the Internet.

3.4 Access Control (Tier 3)

Multifaceted access to both Cloud and WBAN by caregivers, administrators, and patients via a variety of devices such as laptops and smart phones needs authentication.

4. DYNAMIC FAULT TREE MODELING

Modeling is a technique to analyze a system's behavior. One such technique to model the possible failure of a system is fault tree, from which we can calculate the reliability of wireless sensor networks [10]. Reliability is a measure of fault-tolerance, system's resistance to faults that the system continues to perform correctly in spite of hardware/software failures.

There are two types of fault trees, static and dynamic. Static fault tree models functional behavior. Dynamic fault tree models the sequence of functions or operational behavior. For FTTT Secure Architecture, dynamic fault tree is chosen to examine WBAN-cloud security services.

4.1 Security Model

Failures in WBAN-cloud are unique, compared to traditional network failures. The stake is high as human lives are in danger should WBAN-cloud fail to function properly. WBAN failures can be classified into two types: one is *operational failures* caused by malfunctions of the system's constituent components, and the other is *security failures* due to malicious intrusive events. Current dynamic fault tree only covers operational failures. Therefore, we introduce a new gate to model security failures of WBAN-cloud components.

Figure 4 on the next page represents the *Security Module (SM)*. *Component Dependency* is triggered by *Protocol Failure* that deems it *Unavailability* to serve. Internally as a dynamic fault

tree, a PAND of Key Compromise or Intrusion Attack leads Protocol Failure. A Functional Dependency (FDEP) gate relates Protocol Failure to Denial-of-Service affect. An OR of Protocol Failure triggered and direct Denial-of-Service attack causes Component Unavailability, security failure.

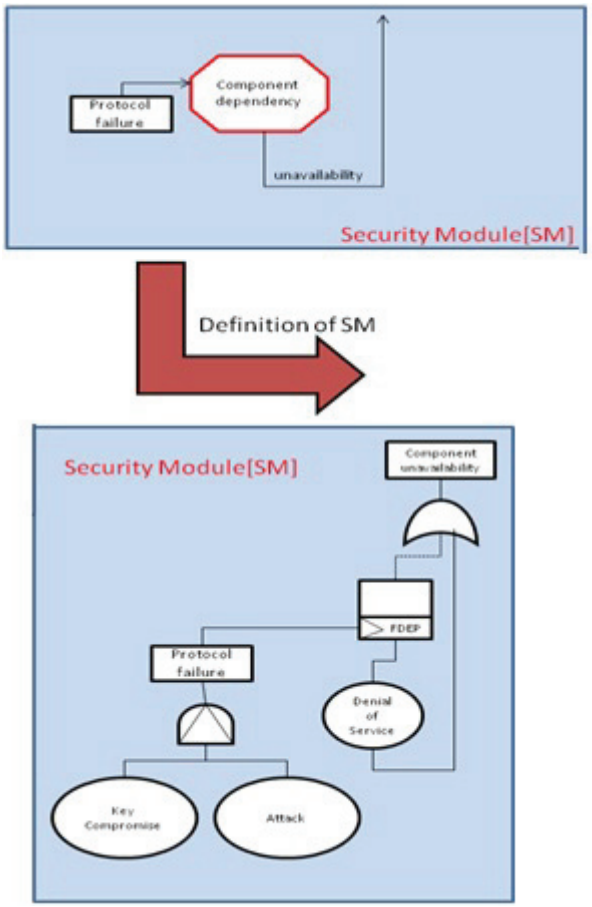


Figure 4. Security Gate to Model Security Failures

4.2 Dynamic Fault Tree

With Security Module (SM) in dynamic fault tree vocabulary, we model security failures in addition to malfunction failures in the form of basic events. A fault tree for a single patient is modeled with a K/N gate, where K represents the number of failed nodes among N nodes deployed on the patient. A patient's WBAN (Tier 1) fails if all the sensor nodes or the aggregation node experience either security failure or malfunction failure. A base station, having a spare part, is considered failure by its own or when all the patients under which fail. Therefore, an OR gate models each base station. Cloud (Tier 2) and Access Control (Tier 3) are modeled accordingly. Failure of WBAN-cloud is represented with an OR gate. Figure 5 represents a model of two base stations, each supporting three patients each with three sensor nodes and one aggregation node.

4.3 Security/Reliability Analysis

Reliability is calculated by dividing a fault tree into blocks and then using Reliable Block Diagram (RBD) model to compute the reliability of the entire system [10]. A fault tree is divided into the following blocks:

- Security Module (SM)
- Warm Spare Part (WSP)
- Sensor Node
- Aggregation Node
- Base Station
- System

We have blocks with static gates and blocks with dynamic gates. The reliability of static gate blocks can be calculated with RBD model or reliability equation. The reliability of dynamic gate blocks can be calculated using Markov chains.

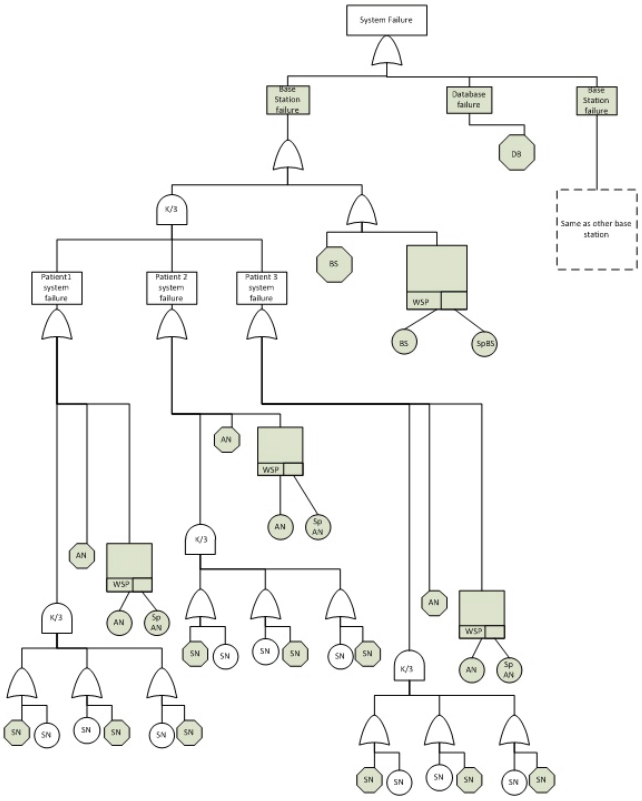


Figure 5. Dynamic Fault Tree of FTTT Secure Architecture

Steps to calculate the reliability using Markov chains are as follows:

Step 1. Convert fault tree model to Markov chain
Step 2. Find the state equations of the Markov chain
Step 3. Find state probabilities by solving the state equations
Step 4. Find the system reliability

Assume the failure rates of the components and then calculate the reliability of the system. Reliability expressions for dynamic modules are as follows:

Reliability of the K/N gate above sensor nodes:

$$\mathbf{R_{SMSN}} = e^{-(\lambda_{DSN} + \lambda_{ASN})t} + (\lambda_{ASN}/[\lambda_{ASN} + \lambda_{KSN}])*(e^{-\lambda_{DSN} t} - e^{-[\lambda_{ASN} + \lambda_{DSN} + \lambda_{KSN}]t})$$

Reliability of the patient subsystem at the aggregation node:

$$\mathbf{R_p} = (R_{SMAN})*(R_{WAN})*(R_{K/4})$$

Reliability of base station:

$$R_{BS} = (R_{SMBS})*(R_{WBS})*(R_{KNP})$$

Reliability of the system:

$$R_{SYS} = (R_{SMDB})*(R_{BS})^2$$

4.4 Evaluation Results

Using FaultTree+ package downloaded from:

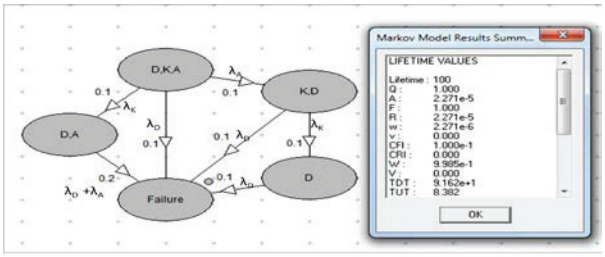
http://www.isograph-software.com/download.php?src=isoswr

We compute the system reliability of security. We consider the scenario of two base stations with three patients each, and each patient with three sensors nodes and one aggregation node.

The system reliability is evaluated by trail values. For the trail values, we consider two scenarios one with low failure rate and the other with high failure rates. The evaluation of reliability is cross-verified with manual calculations and Fault Tree+ software package.

Figure 6 shows a sample of the computation with Fault Tree+:

R_{SM}=0.00002271



RSM for high failure rates

Figure 6. Sample

5. CONCLUSION

This paper proposes a secure and reliable WBAN-cloud for healthcare, called *FTTT Secure Architecture*. It provides a platform to fulfill security goals for various medical services. This architecture deviates from general wireless sensor networks with a forest topology, suitable for patient monitoring with mobility and scalability. Three-tier structure breaks security into patient level and system level, taking advantage of the mature security mechanisms developed for computer networks and systems. The work directs a new research field on security protocols for forest topology WBAN-cloud at patient level. This accomplishment would not be possible with the traditional approaches of add-on security features after the architecture is designed.

We validate our architecture's tolerance to security faults with formal analysis. Current dynamic fault tree models FTTT naturally for QoS reliability but cannot represent security. We introduce Security Module. With this new vocabulary in dynamic fault tree, we model FTTT Secure Architecture. Using FaultyTree+ package, the system's failure rates are computed from components' faults. The results direct us where to deploy redundancy for efficient provision of security.

Future work includes demonstrating the effectiveness of FTTT Secure Architecture with simulation. Next, we will prototype the architecture and develop multi-facet Browser User Interface to securely access patient information. Privacy should also be considered abiding the medical regulations.

6. ACKNOWLEDGEMENTS

We thank the anonymous reviewers of BodyNets 2013 for their valuable comments that improve the paper.

7. REFERENCES

[1] Ullah, S., H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman and K. S. Kwak, "A Comprehensive Survey of Wireless Body Area Networks," *Journal of Medical Systems,* vol. 36, no. 3, pp. 1065-1094, June 2012.

[2] Armbrust, M., A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. i. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A view of cloud computing," *Communications of the ACM,* vol. 53, no. 4, pp. 50-58, April 2010.

[3] Fortino, G., M. Pathan and G. D. Fatta, "BodyCloud: Integration of Cloud Computing and Body Sensor Networks," in *2012 IEEE 4th International Conference on Cloud Computing Technology and Science*, Taipei, Taiwan, December 3-6, 2012.

[4] Fortino, G., R. Giannantonio, R. Gravina, P. Kuryloski and R. Jafari, "Enabling Effective Programming and Flexible Management of Efficient Body Sensor Network Applications," *IEEE Transactions on Human-Machine Systems,* vol. 43, no. 1, pp. 115-133, January 2013.

[5] Lai, C., H. Wang, H.-C. Chao and G. Nan, "A Network and Device Aware QoS Approach for Cloud-Based Mobile Streaming," *IEEE Transactions on Multimedia,* vol. 15, no. 4, pp. 747-757, 2013.

[6] Rong, C. and H. Cheng, "Authenticated Health Monitoring Scheme for Wireless Body Sensor Networks," in *Proceedings of the 7th International Conference on Body Area Networks (BodyNets 2012)*, Oslo, Norway, 2012.

[7] Zeng, K., K. Govindan and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Communications - Security and Privacy in Emerging Wireless Networks,* vol. 17, no. 5, pp. 56-62, October 2010.

[8] Li, M., S. Yu, J. D. Guttman, W. Lou and K. Ren, "Secure Ad Hoc Trust Initialization and Key Management in Wireless Body Area Networks," *ACM Transactions on Sensor Networks (TOSN),* vol. 9, no. 2, pp. 18-52, March 2013.

[9] Divi, K., M. R. Kanjee and H. Liu, "Secure FTTT Architecture for Healthcare Wireless Sensor Networks," *IEEE & ITSS Journal of Information Assurance and Security (JIAS),* vol. 6, no. 2, pp. 157-166, February 2011.

[10] Shrestha, A., L. Xing and H. Liu, "Modeling and evaluating the reliability of wireless sensor networks," in *2007 Annual Reliability and Maintainability Symposium (RAMS)*, January 22-25, 2007.