A Generic Authentication Protocol for Wireless Body Area Networks

Mohammed Raza Kanjee
University of Massachusetts Dartmouth
North Dartmouth, MA 02747, U.S.A.
MKanjee@umassd.edu

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

ABSTRACT
This paper proposes a novel authentication protocol for wireless body area networks (WBAN). For the first time, the protocol adopts generic programming concept for cross-layer design of security in WBAN. By careful examination of various WBAN applications/systems and thorough research on physical-layer authentication mechanisms targeted for WBAN, a generic protocol is developed to authenticate entities in WBAN systems. Generic programming focuses on high-level functionality and component interface, leaving technical details for later development. This lightweight approach merits the deployment of emerging WBAN security technologies for a variety of applications. Generic authentication protocols bring academic laboratory results into real world products with practical implementation of WBAN security. The work is then validated with security analysis.

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

General Terms
Security, Design, Experimentation.

Keywords
Wireless Sensor Networks, Body Area Networks, Security and Trust Establishment, Authentication Protocol, Cross-Layer Security Design, Light-Weight Approaches, Practical Implementation of Security.

1. INTRODUCTION
Wireless body area networks (WBAN) originated from the projects of monitoring soldiers' mental/physical status in battlefield [1] and then extended to civilian healthcare applications such as patient monitoring in hospital and assistant living at home [2]. WBAN applications and systems are now blossoming beyond military/sports training and health/fitness remote monitoring [3]. The pervasiveness of WBAN systems poses serious security threats, partially inherited from the open air nature of WAN. The danger of counterfeit sensors affecting human life hinders the practical implementation of WBAN in real world.

WBAN is a special-purpose Wireless Sensor Network (WSN), where sensors are attached on or embedded in human body that communicate wirelessly among themselves and with processors nearby to form a WBAN system. In recent years, WBAN has drawn great interests of multidisciplinary research teams, solving issues of wearable/implantable sensors, wireless communication technologies, networking architectures, and signal processing. It reaches a consensus that many protocols and algorithms developed for traditional WSN no longer suit to the unique features and application requirements of WBAN. However, WBAN presents unique advantages, such as reliable and accurate physiological measures, to advance modern technologies and to benefit the global society [4].

Conventional authentication schemes based on cryptography, digital signature for example, no longer suitable for wirelessly distributed ad-hoc systems [5]. It is impractical in the open air to distribute, refresh, and revoke keys as required by cryptography-based authentication schemes. Ad-hoc networking features dynamics nodes' frequently joining/leaving the network, making key management extremely difficult. Miniaturization for practical WBAN applications constrains computation/storage resource to perform effective authentication based on resource-hungry cryptography. Though advancement in WSN security shows promise for non-cryptographic authentication and identification [6], many new authentication protocols are not directly applicable to WBAN. Some need additional hardware while others require skillful operation [7]. Channel/Location-Based Authentication is the most prominent approach to identify wireless users or detect identity-spoofing attacks in WSN. The theory behind this class of authentication schemes stems from the signals' location-specific characteristics due to path loss and channel fading. By exploiting the inherent defects or characteristics of sensing devices or wireless channels, an attacker at a different location will display a distinct profile from a genuine user's, hence detectable. However, it is difficult to obtain stable profiles for mobile nodes in WBAN.

On the bright side, WBAN presents great opportunities to advance security services. The unique features of human physiological information have been utilized in security. Various biometrics such as fingerprints are applied to thwart intruders, however, one can get a fingerprint lift kit to make a replica for identity theft. Fortunately, researchers have discovered that other biometrics, such as photoplethysmogram (PPG) [7] and electrocardiogram (EKG) [8], possess special channel characteristics suitable for WBAN security design.

Despite security advances in WBAN components at various layers mentioned above, the lack of integrated security in a WBAN

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

DOI 10.4108/icst.bodynets.2013.253681

system affects practical implementation and prohibits real world deployment. A system security is as weak as its weakest point. This paper addresses the issue of integrating security in WBAN systems with a novel authentication protocol. For the first time, the protocol adopts generic programming concept for cross-layer design of security in WBAN. By careful examination of various WBAN applications/systems and thorough research on physical-layer authentication mechanisms targeted for WBAN, a generic protocol is developed to authenticate entities in WBAN systems. Generic programming focuses on high-level functionality and component interface, leaving technical details for later development. This lightweight approach merits the deployment of emerging WBAN security technologies for a variety of applications. Generic authentication protocols bring academic laboratory results into real world products with practical implementation of WBAN security. The work is then validated with security analysis.

Major Contributions

Our major contributions have four folds. First, we discover the problem of integrating security in WBAN systems. Then, we define a high-level architecture of WBAN system. Third, we design a novel generic authentication protocol covering the two-tiers: intra-WBAN communications among the on-body nodes and inter-WBAN communications with off-body nodes and the remote processors/storages. The generic programming approach makes a WBAN system security modular so that a replacement of any component with a new technology keeps the entire system enacting. Last, we validate the authentication protocol with security analysis.

The remaining paper is organized as follows. Section 2 reviews the related work. The problem of integrating security in WBAN system and a solution with generic programming for two-tiered authentication for WBAN are presented in Sections 3 and 4, respectively. Section 5 conducts security analysis. Conclusion and future work are discussed in Section 6.

2. RELATED WORK

This work involves multidisciplinary research. Due to the page limit, we only discuss some notable works related.

Venkatasubramanian is among the first to discover biometric-based authentication in wireless networks of biosensors implanted in the human body [9]. The uniqueness and randomness of physiological signals have grown a new branch in WBAN security, namely non-cryptographic authentication and identification [6]. Some particular human body activities, like photoplethysmogram (PPG) [7] and electrocardiogram (EKG) [8], possess the temporal variant feature that advocate precious one-time key. It would be too hard to launch replay or man-in-the-middle attacks as one-time key renders it useless by copy.

The research team, largely at the University of Arkansas, revolutionized WBAN authentication without identification by exploiting channel characteristics [7]. Their novel non-cryptographic node authentication scheme, called BANA (Body Area Network Authentication), differentiates signals of a legitimate node and an attacker to form a cluster of good nodes and reject bad nodes from communications.

3. PROBLEM OF INTEGRATED SECURITY

We envision the need of robust and efficient authentication protocol for WBAN system, covering the entire communication protocol stack while withstanding ever-changing WBAN technologies and fast-growing WBAN applications. A system security is as weak as its weakest point. Any point of failure in the security of a WBAN system causes serious consequences, some life threatening as most WBAN applications relate to people's safety and health. WBAN usability demands light weight approach for efficient security service due to mission-critical nature and resource-constraint reality of WBAN applications.

Our past experience in designing mobile healthcare infrastructure with Quality-of-Service and Security Assurance exposed chaos [10]. A diverse array of specialized sensors is deployed to monitor, for instance, intensive-care patients with history of heart attacks or senior citizens living independently at home. A wide variety of wireless technologies are candidates for WBAN communication such as Zigbee, Bluetooth, Bluetooth Low Energy (previously calledWiBree), video surveillance systems, wireless personal area network, wireless local area networks, the Internet, and cellular networks. A broad range of WBAN applications becomes ubiquitous beyond imagination. In the case of medical emergency, any delay proves fatal for the patient. Security is instrumental as unauthorized sensors could invade patient's privacy and unauthenticated controllers could put patient's life in danger.

Integrating emerging WBAN technologies with effective and efficient authentication mechanisms remains a great challenge to WBAN development [4]. Complex but distinct physiological information provides a new direction to user authentication, yet it creates technical challenges. Different levels of security should be identified for various WBAN applications using suitable communication technologies and authentication mechanisms.

This work demonstrates the use of generic programming to design an authentication protocol for WBAN system. The design goals include modularity for component upgrade, flexibility to adopt emerging WBAN security technologies, robust to resisting point security failures from system malfunctioning, and efficiency with lightweight overhead for maximum security performance.

4. AUTHENTICATION PROTOCOL

4.1 High-Level Architecture

The architecture contains three types of nodes, each performing different well-defined functions at plug-and-play [11].

- *Data Collection Nodes (DCNs)* – on-body sensors to collect physiological signs such as oxygen level, electrocardiogram (EKG), and photoplethysmogram (PPG).
- *Aggregation Node (AGN)* – an on-body control unit to cumulate data from DCNs and to issue commands.
- *Base Station Node (BSN)/Local Authentication Server (LAS)* – an off-body device to communicate wirelessly with multiple AGNs in its vicinity. It also serves as a gateway between the Body Area Network (BAN) and the Master Authentication Server (MAS) for remote users to access the WBAN system.

In addition, a device called *Oracle* generates the public/private key pairs for AGN and BSN. Figure 1 depicts the high-level architecture.

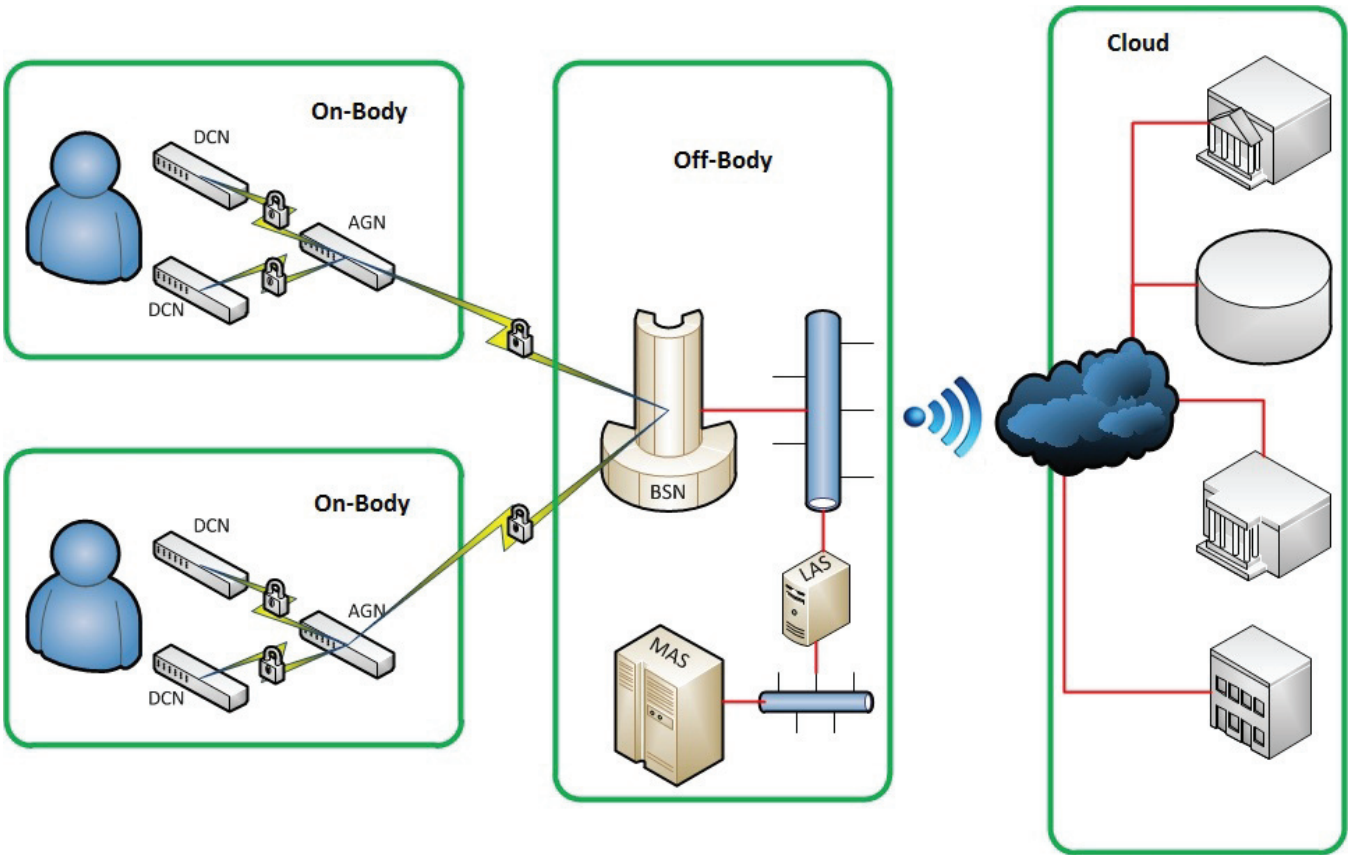

Figure 1. High-Level Architecture of WBAN System

4.2 Two-Tiered Authentication Protocol

This section describes the intricate workings of our proposed two-tiered authentication protocol for WBAN system. The solution utilizes physiological signals to implement a U-key authentication scheme. The physiological features of uniqueness and randomness facilitate strong security while offer convenient usability, robust reliability, and flexible applicability.

4.2.1 On-Body Nodes Physiological Authentication

The first tier gets the person's on-body nodes, i.e., several DCNs and one AGN, to authenticate among themselves [12]. They can utilize their shared physiological measures to agree upon a symmetric cryptographic key. This secret key is used for their mutual authentication. They also can conduct non-cryptographic authentication without using any key. Due to the large discrepancy between on-body and off-body channels Received Signal Strength (RSS) variation, the on-body nodes are able to accept each other while reject off-body nodes as malicious.

Various physiological signals have been demonstrated for key agreement. Venkatasubramanian et al takes photoplethysmogram (PPG), a measure of the volumetric change in the distention of arteries due to the perfusion of blood during a cardiac cycle [13]. A multidisciplinary cross-campus research team led by Honggang Wang chooses electrocardiogram (EKG), a recording of the heart's electrical activity in terms of the speed and rhythm of the heartbeat as well as the strength and timing of electrical signals passing through each part of the heart [8]. Key agreement among on-body nodes involves two processes. One is to hide the secret key by extracting the feature from the physiological signal measured and constructing its vault. The other is to reveal the secret key by unlocking the vault with the feature shared by its physiological signal measure. Experiments have confirmed that these physiological stimuli are universally measureable, the duration of their capture takes low latency, the values of individuals' physiology are distinct and vary by time [14]. Therefore, these kinds of physiological signals provide ideal media for authentication, much effective than traditional biometrics such as fingerprints that could be copied for impersonation.

4.2.2 Validating/Authenticating AGN

AGN features two states, reflecting two levels of security status [15]. The first state is valid when a person sets up his/her WBAN system. The validation procedure involves three automatic steps.

Step 1: AGN plugs to Oracle that matches the AGN's ID with its entry in MAS.

Step 2: Oracle generates a public/private key pair for AGN upon matching.

Step 3: AGN's public key is published to its BSN/LAS which updates the information to the MAS.

A valid AGN is now ready for authentication as the second part of the two-tier authenticating WBAN system.

4.2.3 Two-Tier Authenticating WBAN System

In a plug-and-play manner, the first tier involves three steps, using PPG to illustrate the authentication [13], after AGN validates itself with Oracle.

Step 1: AGN initiates authentication to DCNs, shown in Figure 2.

Step 2: AGN and DCNs generate their physiological features, depicted in Figure 3.

Step 3: AGN agrees with DCNs the shared keys or forms the communication cluster with DCNs, illustrated in Figure 4.

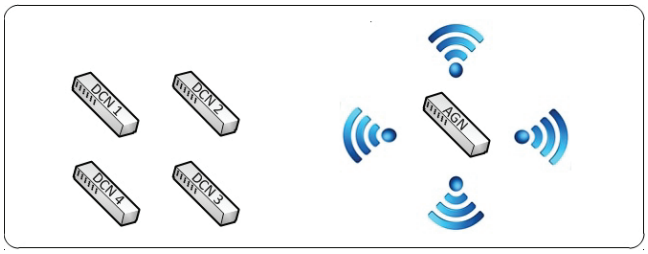

Figure 2. AGN→DCNs: broadcast(request)

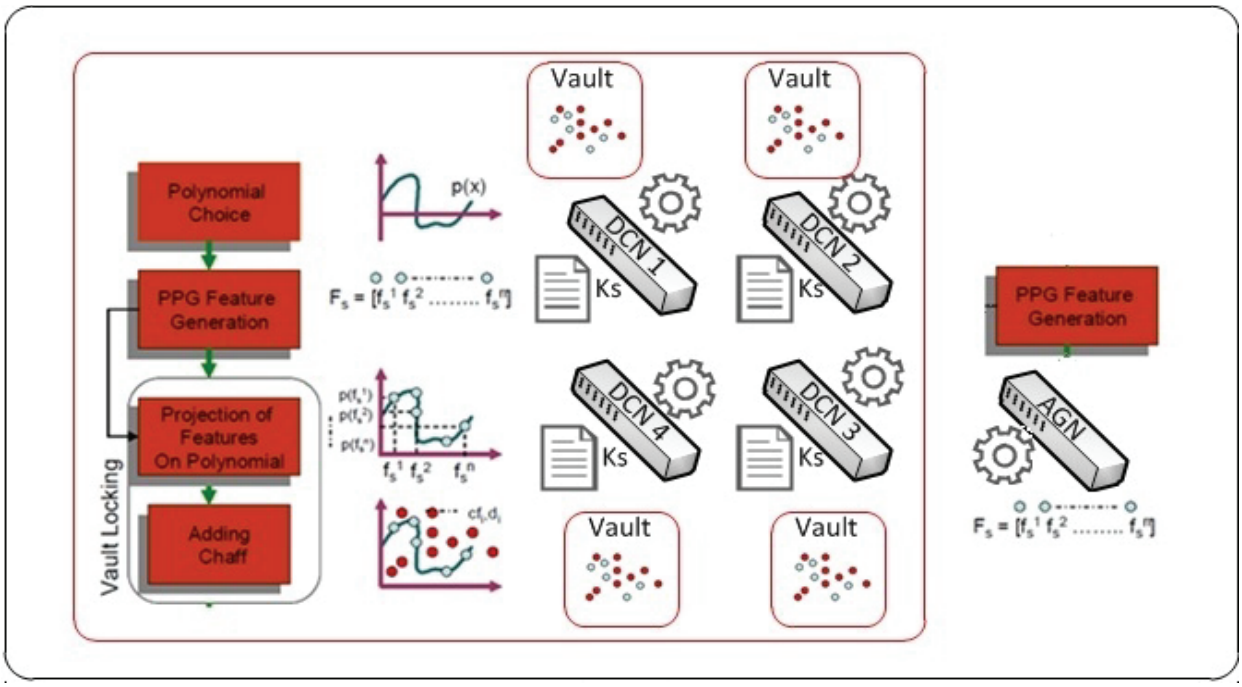

Figure 3. AGN & DCNs: generate Fs simultaneously

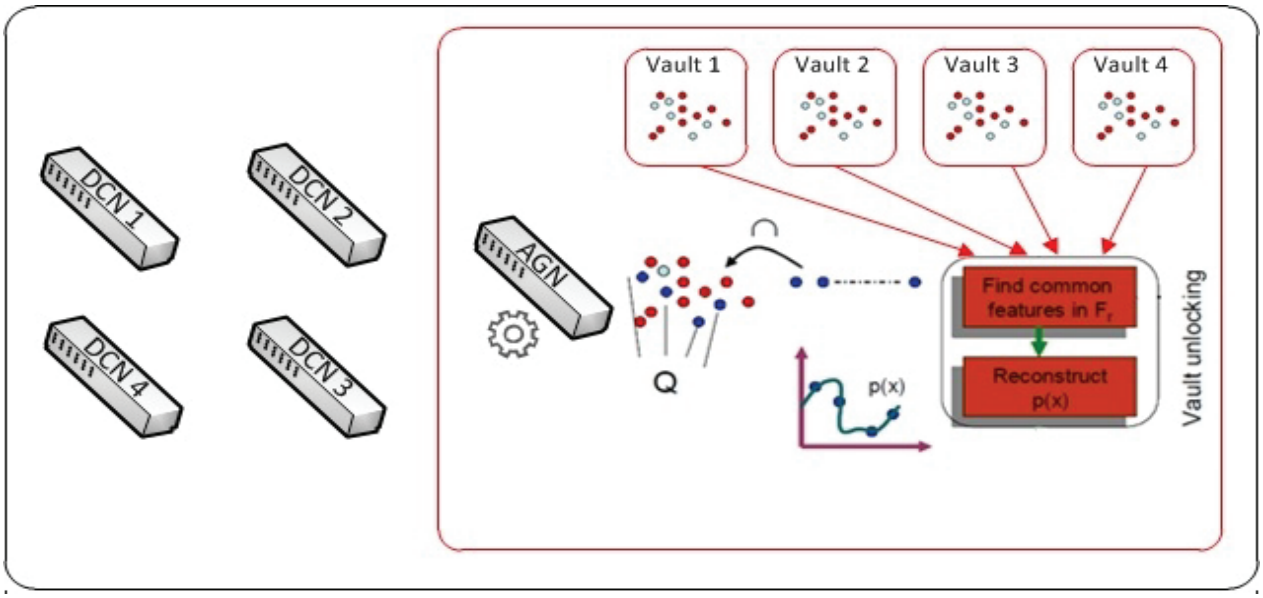

Figure 4. AGN: agree with DCNs

Seamlessly as plug-and-play, the second tier involves four steps for secure communications between AGN and BSN. AGN acts as the single access point between on-body and off-body of the WBAN system. BSN is the gateway for the WBAN and the remote processor/storage where traditional security services are provided.

Step 1: BSN broadcasts its public key to AGNs in its proximity as shown in Figure 5.

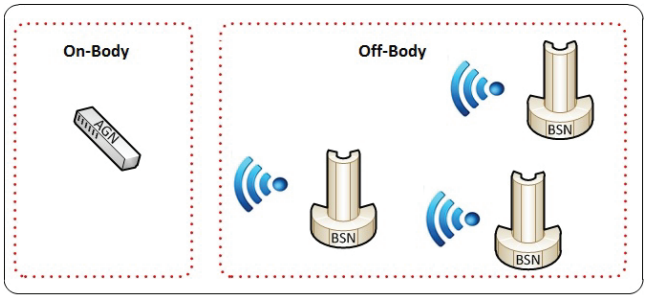

Figure 5. BSN→AGNs: broadcast($ID_B||PU_B$)

Step 2: AGN registers itself through a BSN that relays AGN's registration request to LAS which delegates MAS for the region, depicted in Figure 6.

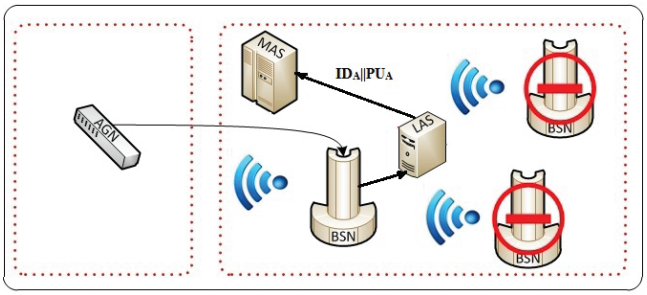

Figure 6. AGN→BSN: E($ID_A||PU_A$, PU_B)||register

Step 3: Upon successful registration, BSN initiates authentication to AGN, as shown in Figure 7.

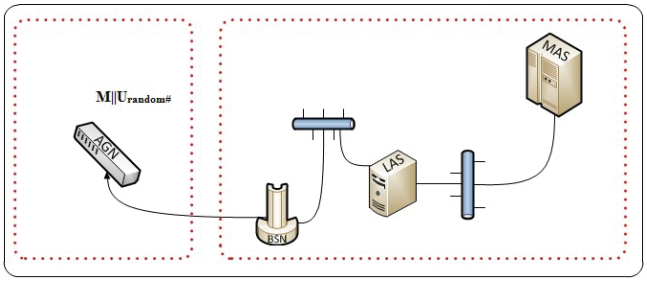

Figure 7. BSN→AGN: E(M||$U_{random\#}$, PU_A)||ID_A

Step 4: As illustrated in Figure 8, the mutual authentication for the entire WBAN system is completed by AGN responding to the authentication, BSN recognizing AGN as genuine, and AGN also recognizing BSN as genuine.

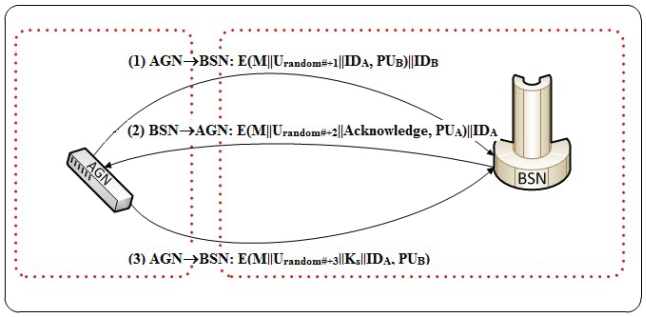

Figure 8. Mutual Authentication

5. SECURITY ANALYSIS

We conduct a credible analysis to our proposed two-tiered authentication protocol for WBAN systems.

5.1 Claims of the First Tier

Both teams have verified that the security strength of vault with respect to the order of polynomial varies drastically by the vault size [13] [8]. Hiding the legitimate feature points among a larger number of chaff points increases the vault size. Even if an attacker manages to find out the legitimate points, s/he would still face the daunting challenge of high-order polynomial reconstruction. Continuous efforts are being made to improve the performance of secret key generation for on-body nodes [16].

We especially assess the claims of distinctiveness and temporal variance featured in physiological signals. For example, PPG and EKG generated from two individuals are distinct. This feature ensures that the vault created by DCNs on one person cannot be unlocked by an AGN on the other person or an off-body device. The significance of the distinction is determined by the polynomial order. The polynomial order is chosen to minimize both false positive (the number of times the common features between two individuals exceeds the threshold) and false negative (the number of times the common features for the same person goes below the threshold). Figure 9 shows the percentage of false positives and false negatives with PPG and EKG. The minimum points for PPG and EKG are at the polynomial order of 6 and 14, respectively. Hence, EKG has greater potential in generating stronger vaults [8].

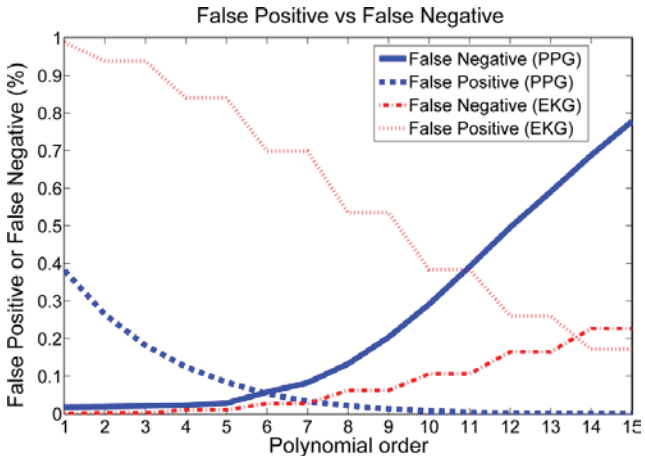

Figure 9. False Positive/Negative in PPG and EKG [13]

Temporal variance merits one-time key to prevent replay attacks. Figure 10 illustrates the time variance of PPG signals on an individual. The x-axis is the time duration between two cycles of key agreement. The y-axis is the polynomial order. The z-axis records the average violations (the percentage of times when the number of common features exceeds the polynomial order used). The shorter the duration, the higher the violations (towards the red spectrum) because the feature values would be similar between short cycles of key agreement. As time difference increases, violations fall drastically (towards the blue spectrum), reaching to zero in a few seconds for the polynomial order of 9 or above. The higher the polynomial order, the lower the violations as it is more difficult for an attacker to construct the vault.

5.2 Verification of the Second Tier

The second tier can be verified with a variety of formal methods to assess traditional authentication protocols. This kind of security analysis is out of the WBAN scope. We only brief some methods in this paper.

One method is by State Machine. A graph records each state where an attacker could reach by a poking message, becoming a machine for an attacker to go from total ignorance to fully knowledge. The security protocol is broken if an attacker can manipulate term-rewriting to find out a message meant to be secret.

Another formal method of cryptographic analysis is Modal Logic. Using belief or knowledge about messages in a distributed system, inference rules derive other beliefs to check if there is any contradiction in the protocol to be examined.

Cryptographic analysis also includes algebraic method. One can formulate the protocol in terms of an algebraic system, expressing the state of an attacker's knowledge about the protocol. The solution set leads to security breach.

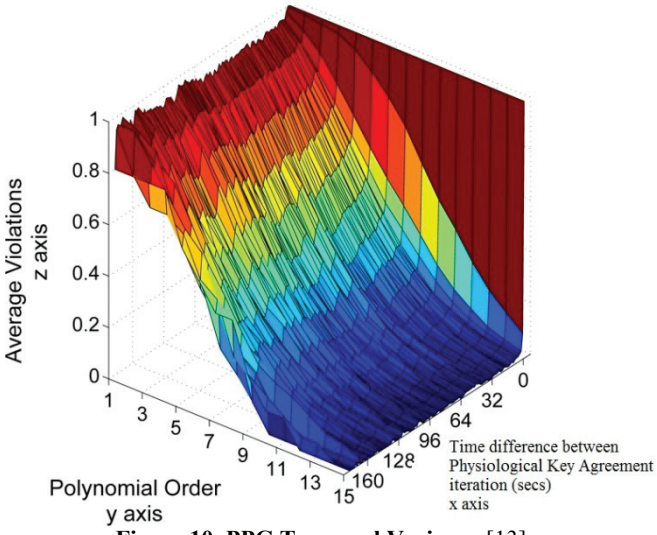

Figure 10. PPG Temporal Variance [13]

5.3 Analysis of the Authentication Protocol

Our proposed authentication protocol involves two tiers. The first tier authentication takes place on an individual's body. Each DCN hides a random but unique feature derived from the person's physiologic signals, which is to be reconstructed by the AGN on the same person's body. The DCNs and the AGN in the same WBAN authenticate each other via their shared physiological signals. A foreign node is unable to reproduce the unique feature since individuals' physiological signals distinct significantly and the same person's physiological signal varies randomly by time.

The second tier authentication utilizes a novel password-type authentication scheme. This scheme averts false AGNs from impersonating to the BSN off-body. Once the BSN receives the registration request from an AGN, it compares the message (decrypted with AGN's public key) with the content stored in LAS or MAS to ensure that the AGN is valid beforehand. This initial validation process serves the first level security. Once registered, BSN creates *Nonce* (a unique random number for transaction freshness), and the authentication procedure follows standard mutual entity authentication.

The tiered authentication adopts modular development. Any component can be substituted without affecting the entire WBAN system. Since nodes are authenticated pair-wisely, one broken link would not compromise the others. Session keys between AGN and BSN serve the purpose of data confidentiality and integrity for the users of WBAN system in addition to node authentication.

6. CONCLUSION

This paper is the first to bring in light the practical implementation issue of integrating security for WBAN systems. To address this issue, we propose a generic authentication protocol for WBAN that focuses on cross-layer security design without distractions by technical details. The polymorphic feature of generic programming advocates broader benefits of design reusability and efficiency, suitable to emerging WBAN security technologies. The two-tier architecture strategically allocates scare resources in WBAN and offloads communication/processing burden to remote processors/storages, making WBAN itself light weight without affecting performance of the entire WBAN system. We validate the generic authentication protocol with security analysis.

Future work includes developing domain-specific WBAN systems such as for ubiquitous healthcare and for vehicular safety application using the generic authentication protocol. Another research direction is to quantify the performance of security strength for various authentication schemes.

7. ACKNOWLEDGEMENTS

We thank the anonymous reviewers of BodyNets 2013, Special Track on Privacy, Security and Trust in Body Area Networks (PSTBAN), for their valuable comments and insightful suggestions that improve the paper.

8. REFERENCES

[1] Venkatasubramanian, K.K., A. Banerjee and S. K. S. Gupta, "Plethysmogram-Based Secure Inter-Sensor Communication in Body Area Networks," in *IEEE Military Communications Conference*, San Diego, CA, 2008.

[2] 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.

[3] 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.

[4] Chen, M., S. Gonzalez, A. Vasilakos, H. Cao and V. C. Leung, "Body Area Networks: A Survey," *Mobile Networks and Applications,* vol. 16, no. 2, pp. 171-193, April 2011.

[5] Lin, X., X. Ling, H. Zhu, P.-H. Ho and X. S. Shen, "A Novel Localized Authentication Scheme in IEEE 802.11 based Wireless Mesh Networks," *International Journal of Security and Networks,* vol. 3, no. 2, pp. 122-132, 2008.

[6] 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.

[7] Shi, L., M. Li, S. Yu and J. Yuan, "BANA: Body Area Network Authentication Exploiting Channel Characteristics," *IEEE Journal on Selected Areas in Communications (JSAC), Special Issue on Signal Processing Techniques for Wireless Physical Layer Security,* 2013.

[8] Zhang, Z., H. Wang, A. V. Vasilakos and H. Fang, "ECG-Cryptography and Authentication in Body Area Networks," *IEEE Transactions on Information Technology in Biomedicine,* vol. 16, no. 6, pp. 1070-1078, 26 June 2012.

[9] Cherukuri, S., K. K. Venkatasubramanian and S. K. S. Gupta, "BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body," in *Proceedings of the 2003 International Conference on Parallel Processing Workshops (ICPPW 2003)*, Kaohsiung, Taiwan, October 6-9, 2003.

[10] Mughal, A., M. R. Kanjee and H. Liu, "Mobile Healthcare Infrastructure with QoS and Security," in *Proceedings of the 1st International Workshop on Mobile Multimedia Networking in conjunction with Mobilware (ICST IWMMN 2010)*, Chicago, IL, 2010.

[11] 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.

[12] Kanjee, M.R., K. Divi and H. Liu, "A Physiological Authentication Scheme in Secure Healthcare Sensor Networks," in *Proceedings of the 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (IEEE SECON 2010)*, Boston, MA, 2010.

[13] Venkatasubramanian, K.K., S. K. Gupta and A. Banerjee, "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks," *In IEEE Transactions on Information Technology in Biomedicine,* vol. 14, no. 1, pp. 60 - 68, 2010.

[14] Venkatasubramanian, K.K. and S. K. S. Gupta, "Physiological value-based efficient usable security solutions for body sensor networks," *ACM Transactions on Sensor Networks (TOSN),* vol. 6, no. 4, pp. 1-36, July 2010.

[15] Kanjee, M.R., K. Divi and H. Liu, "Hierarchical Healthcare Sensor Network Security Protocol for a Forest Topology Three Tier (FTTT) Secure Architecture," *IEEE & ITSS Journal of Information Assurance and Security (JIAS),* vol. 6, no. 3, pp. 232-239, March 2011.

[16] Yao, L., S. T. Ali, V. Sivaraman and D. Ostry, "Improving Secret Key Generation Performance for On-Body Devices," in *Proceedings of the 6th International Conference on Body Area Networks (BodyNets 2011)*, Beijing, China, 2011.

[17] 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.

[18] Lu, R., X. Lin, X. Liang and X. Shen, "A secure handshake scheme with symptoms-matching for mHealthcare social network," *Mobile Networks and Applications - Special issue on Wireless and Personal Communications,* vol. 16, no. 6, pp. 683-694, December 2011.

[19] Dam, M. and R. Stadler, "A Generic Protocol for Network State Aggregation," in *Radiovetenskap och Kommunikation (RVK 2005)*, Linköping, Sweden, 2005.

[20] Reis, G.D. and J. Järvi, "What is Generic Programming?," in *Object-Oriented Programming, Systems, Languages and Applications (OOPSLA 2005) - Workshop on Library-Centric Software Design (LCSD 2005)*, San Diego, CA, October 16-20, 2005.