Protect your BSN: No Handshakes, just *Namaste*![*]

Priyanka Bagade, Ayan Banerjee, Joseph Milazzo and Sandeep K.S. Gupta
IMPACT Lab (http://impact.asu.edu/)
School of Computing Informatics and Decision Systems Engineering
Arizona State University, Tempe, Arizona
Email: {pbagade, abanerj3, joseph.milazzo, sandeep.gupta}@asu.edu

***Abstract*—Privacy of physiological data collected by a network of embedded sensors on human body is an important issue to be considered. Physiological signal-based security is a light weight solution which eliminates the need for security key storage and complex exponentiation computation in sensors. An important concern is whether such security measures are vulnerable to attacks, where the attacker is in close proximity to a Body Sensor Network (BSN) and senses physiological signals through non-contact processes such as electromagnetic coupling. Recent studies show that when two individuals are in close proximity, the electrocardiogram (ECG) of one person gets coupled to the electroencephalogram (EEG) of the other, thus indicating a possibility of proximity-based security attacks. This paper proposes a model-driven approach to proximity-based attacks on security using physiological signals and evaluates its feasibility. Results show that a proximity-based attack can be successful even without the exact reconstruction of the physiological data sensed by the attacked BSN. Our results show that with a 30 second handshake we can break PSKA with an average probability of 0.3 (0.24 minimum and 0.5 maximum).**

***Keywords*—Model based, Security in Body Sensor Network**

I. Introduction

The usage of miniature sensors with the capability of wireless communication for pervasive health monitoring are prone to security vulnerabilities and hence may jeopardize the privacy of patient data [1]–[3]. Wireless sensors in Body Sensor Networks (BSNs) thus employ some form of cryptography to encrypt physiological data while sending it to a base station over the insecure wireless channel [4]. Recently researchers have proposed the usage of physiological data collected by the sensors to generate cryptographic keys to be used for secure communication as a lightweight and usable alternative to traditional elliptic key or shared secret key cryptography [1]–[3], [5]–[8]. Physiological signal based security have two working principles: a) time variance, the features used for generation of cryptographic keys vary over time and hence replay attacks are not possible, and b) variance among individuals, where physiological features of one individual is very different from those of the other. Hence, an implicit assumption is that to break the physiological signal based security the attacker has to posses the sample by sample physiological data, which was used to generate the key. In this paper, we show that these two assumptions may not hold and physiological signal based security can be violated using generative models, which only need certain features as opposed to sample by sample physiological measurements. Further, the paper also shows that the features required for developing these models can be obtained by an adversary who is in close proximity of the attacked BSN. On a lighter note, we propose to use the Indian tradition of greeting with a *Namaste*, without physical contact and from a distance, instead of shaking hands just to keep your BSN secure.

Physiological signal based security such as the Inter-pulse-Interval (IPI) based key generation [2] or the physiological value based key agreement (PSKA) [1] depend on some common feature sensed by physiological sensors on the same human body [7]. The assumption is that the common feature can be extracted by any two sensors at different parts of the body and cannot be obtained by any sensor not deployed on the body. The operation of PSKA as an example is shown in Figure 1 and discussed in more detail in Section III. When two sensors on body need to communicate securely they consider their current buffer of the physiological signal and extract features, peaks of fast Fourier transforms in case of PSKA. These features are similar if not exactly same between the two sensors on the same body. A cryptographic key is then generated at the sender and each of the features are transformed using a function of the key. For PSKA it is a polynomial transformation where the coefficients are derived from the key. The transformed features are then obfuscated and transferred to the receiver; fuzzy vault is used for PSKA. At the receiver end all the features need not match. Only a few exactly matching features, their number being a polynomial order with respect to the key size, are needed to regenerate the key. Any person with access to the extracted features can regenerate the cryptographic key in polynomial time w.r.t. the key size. While an attacker without access will need exponential time.

The attacker however may not need the timely physiological features. Representation of physiological signals using *generative models* has been studied thoroughly [9] for quite some time. Such models allow regeneration of diagnostically equivalent current physiological signals from past data [10]. Approaches for electrocardiogram (ECG) and photoplethysmogram (PPG) signals have been exhaustively tested for robustness [10], [11]. Thus, if an attacker can obtain a generative model of the physiological signal using past data then it can regenerate diagnostically equivalent present signals and can potentially use it to obtain *timely features*. However, these generative models provide signals which are not sample by sample equivalent to the current signal. Instead they are equivalent in some key parameters such as heart rate, standard deviation of heart rate, low frequency to high frequency (lfhf) ratio, and morphological patterns of the signal. In this paper, we show that diagnostic equivalence is sufficient to generate timely features so that an attacker can break PSKA.

To generate timely features using the generative model the attacker however needs current values of the diagnostic features. Research in ECG artifacts reduction from electroen-

[*]This research is funded by NSF grant CNS-0831544 and IIS-1116385.

cephalogram (EEG) measurements show that when two individuals are in close proximity (less than four feet), the ECG of one person gets reflected or coupled with the EEG of the other person [12], [13]. However, exact re-construction of the ECG from other person's EEG may not be successfully achieved unless actual physiological data for ECG is available [14]. We use ECG artifact reduction algorithms proposed in recent literature and modify them to extract diagnostic parameters such as R-R intervals, and R peak locations. These diagnostic parameters are used by the generative models to extract timely features to break PSKA. Specifically this paper makes the following contributions: it a) provides a security attack on PSKA using generative models of ECG and PPG, b) analyzes the feasibility of the attack based on experiments on real data obtained from MIT PhysioNet data base as well as data collected at the IMPACT Lab, and c) proposes a methodology for the attacker to extract diagnostic features from close proximity which makes the security attack non-invasive.

II. Related Work

Using models to analyze the system security has become a focused area of research. Attack models of known threats and real vulnerabilities are injected in the systems to test the security flaws [15]. Using only known threats model to check system security might give false alarms due to unusual legitimate input traffic. Thus adaptive attack model which learns traffic data behavior is used along with known threats model [16]. Attack models are executed on system models to define system security metrics [17]. These attack models are created by considering attack preferences, goals and methodology of attacking the system. Network vulnerabilities play an important role in securing the system. Model checker are created to check these vulnerability [18]. These results are further used to create attack models to test the system security in such a susceptible environment. Further, application specific query modeling technique is used to detect web server and web-based attacks [19]. All these techniques are focused on creating models of the attack to test the system security. However this paper focuses on a methodology where system models are used to break the system.

III. System Model for BSN Security

In a BSN, wearable sensors are communicating with each other through the wireless channel. The wireless channel is under continuous surveillance by an attacker who has access to all the information that a sensor sends to a base station. In this scenario the sensor has to transfer a secret information to the base station without the attacker knowing it. Secure communication between sensors can be achieved by generating secure key using physiological signals. Figure 1 shows the generic system model for establishing security in BSN. Let S_1 and S_2 be the physiological signals collected by body wearable sensors in a BSN. The sensed signals are processed further to extract features, $A_1 = f(S_1)$ and $A_2 = f(S_2)$ respectively. Each sensor uses these features to generate security key k, by using signal processing algorithms. The extracted set of features A_1 and A_2 are not equal as they are not time synchronized. However, there exists some correlation between them, $A_1 \cap A_2 = A$. The signal S_1 is further processed to obtain k. The signal transformation, $T_k(a_{1i})$ is done on A_1 set using k, where a_{1i} is the i^{th} feature value in set A_1. The number of such pairs are equal to the size of set A_1. Set C

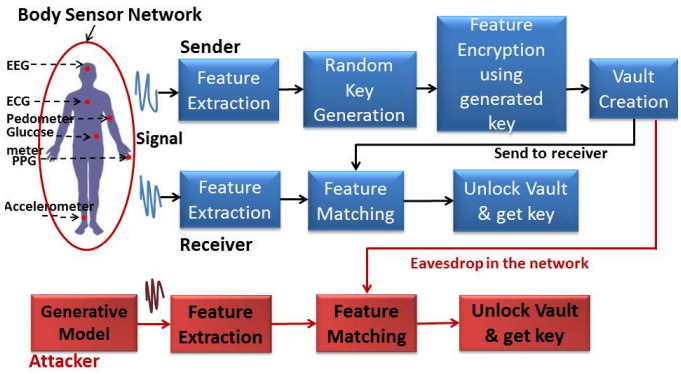

Fig. 1. **BSN model, physiological value based security, and threat model.**

contains the obfuscation of pairs $[T_k(a_{1i}), a_{1i}]$ which is to be sent to other sensor over the wireless channel. Before sending C, large number of randomly generated pairs are added to C to enhance security of the legitimate pairs. These extra chaff pairs are of the form (b_1, b_2), where $b_1 \neq T_k(b_2)$. This is called a vault. The secret k is stored in this vault and receiver needs to unlock it to know the secret. Once the receiver gets the vault C, it first calculates set D such that it tries to match values from set A_2 with second value in the pair from each pair in set C. The signal transformation algorithm T is known to all sensors in the BSN. Thus the value of k is easily obtained by using pairs in set D and transformation algorithm T, which unlocks the vault.

This method of establishing secure communication in BSNs using physiological value-based signals is presented in [1], [2], [5]. PSKA [1] shows the usefulness of this method using two sensors, ECG (Electrocardiography) and PPG (Photoplenthysymogram). It uses Fast Fourier Transform (FFT) and peak detection techniques to extract features from physiological signals, $f = peakDetect(FFT(S_2))$. The sender generates a random key, which is used as the coefficients of a secret polynomial. A fuzzy vault is created using ordered pairs of feature values and their secret polynomial evaluations, (x, y). The vault is obfuscated using large number of chaff points, which are randomly generated ordered pairs such that y is not a polynomial evaluation of x. On the receiver end, the set of extracted features using peak detection algorithm is used to match vault pairs. If the feature value of receiver sensor signal matches with feature values with sender, then those pairs are is used to find the coefficients of the polynomial, which unlocks the secret from the vault.

Physiological signal based key agreement has two basic assumptions: trust model and threat model.

A. Trust Model

Sensors, in a BSN, communicate over insecure wireless channel. While securing a BSN over untrusted wireless channel, it is assumed that there are no jamming and denial of service attacks, where the wireless channels are blocked so that legitimate devices can not communicate with each other. This is done by tuning the transmitting frequency of adversary sensor to that of legal receiver sensor. We have also assumed that, no malicious sensor is implanted in BSN user's body as this can not be done unknowingly to the user and doctors, who

are able to do this during surgery, are considered as trusted entities in BSN health services.

Although, we have assumed that there are no such attacks or there is no adversary sensor in contact with the user, still communication between sensors in a BSN can be interrupted. To save energy and avoid network congestion, a *pilot* sensor is selected among the sensors in the BSN. All *non-pilot* sensors send sensed data to the pilot sensor, assuming it is a legitimate sensor, which then sends redundancy-free data to the base station in the BSN. Base station is also considered as non tamper-able entity in BSN. If the adversary entity becomes successful in establishing itself as a pilot sensor, the data privacy, in the BSN, is easily compromised to attacks by injecting malicious information into the system. Attacker can tamper non-pilot sensor also, as the pilot sensor assumes that it is receiving information from a legal sensor in the network. These loopholes in the BSN security allows adversary to break into an system's security.

B. Threat Model

Generative models are developed to regenerate physiological signals by using morphology and signal variations from raw data. These models are trained using raw data so that they can replicate the diagnostic features for a particular person. Generative models use clinically important features from physiological signals such as R-R interval, high frequency and low frequency ratio, and heart rate for ECG signal. The signal obtained from sensor and synthetic signal obtained from generative model are not time synchronized. However, they are highly correlated in frequency domain because of the same diagnostic features. Currently available BSN security methods, such as PSKA, relies on diagnostic features of human physiology. Generative models also use these features to generate physiological signals which do not vary over time. Thus the original signal features used in PSKA are similar to that extracted from synthetic signal. This regenerated signal can be used for breaking the security protocol between sensors in BSN (Figure 1). This section will focus on how the secure communication protocol used in previous section can be breached by an attacker using generative models.

Algorithm 1 illustrates the attack model for BSNs using synthetic signal. It has been observed that physiological signals are periodic in nature and have typical temporal variations. With the help of physiological signal nature, the model is formed by extracting peculiar features from signal S_2 which is used in Section III, to unlock the vault sent by signal S_1. These features are sufficient for reproducing signal S_2 using a generative function. S_{m2} is the modeled signal. Henceforth, variables subscripted with m will be used for the attacker who has access to a model and all other variables will be for the BSN user. Attacker will perform similar signal processing on the synthetic signal which would have been done on the receiver end. Now attacker has got the set of extracted feature, A_{m2}, from physiological signal similar to valid receiver. By eavesdropping in a BSN, attackers can get vault from one of the sensor. The attacker algorithm uses the synthetic signal and received vault to reveal the shared secret. A_1 and A_{m2} are raw and modeled features, respectively for the same physiological signals of the same person. Thus there should be some commonality between them, i.e. $I_m = A_1 \cap A_{m2} \neq$. Using I_m, the secret shared by sender will be revealed by the attacker. Thus, if the attacker gets hold of physiological signal model and raw data, security key can be obtained to breach the BSN system. Here, our hypothesis is that, $A_{m2} \cap A_1 \neq$, and $||I_m|| \geq ||k||$. We will support this hypothesis using two physiological signals, ECG and PPG, in following sections.

Algorithm 1 Attacker Algorithm

1: Extract signal parameters using signal model M and raw data S_2, $P = M(S_2)$.
2: Use generative model G to generate synthetic signal, $S_{m2} = G(P)$.
3: Apply feature extraction algorithms f on modeled signal, $A_{m2} = f(S_{m2})$.
4: Get $vault$ from BSN = $\{T_k(a_1), a_1\} \forall a_1 \in A_1$ + chaff points.
5: Call PSKA decryption algorithm with ($vault$, A_{m2}) as argument.

IV. Model-based attack on PSKA

Model based attack on physiological value based security assumes that the attacker has access to a generative model of the signal. The attacker generates a signal sample that is diagnostically equivalent to the original signal. The attacker then extracts timely features from the diagnostically equivalent signal and uses the features to break the vault. In this section, we discuss the generative models of ECG and PPG that the attacker can use. We also show how the PSKA features extracted from the original signal and the synthesized diagnostically equivalent signal match to a level that it is sufficient for the attacker to break the vault.

A. Generative Models of ECG and PPG

A generative model is essentially a function of time and physiological parameters of the signal, $G = f(t, a, b, c, \ldots)$. The parameters a, b, c and so on can be of two types: a) temporal, which represent time properties of the signal for example average heart rate, standard deviation and b) morphological, which represent the shape of the signal for example, relative height of R peak with respect to Q peak for ECG. The temporal features are often used for diagnosis. The morphological parameters are obtained through a training phase. In this phase an interval of the physiological signal is taken and a mathematical model is fitted to it. The parameters of the mathematical model capture the morphology of the signal. In this paper we have considered PSKA for PPG as well as ECG signals. Hence we need generative models for both PPG and ECG signals.

For ECG signals, the ECGSYN generative model is used [9]. The ECG signal has five peaks: P, Q, R, S and T. Each peak is represented using a Gaussian function with parameters a, b, and θ, which determine its height, width and distance to R peak, respectively. The inter-beat features of ECG (mean and standard deviation of heart rate and LF/HF ratio) are modeled using three parameters: hrmean, hrstd and lfhf ratio respectively. Two generative models for PPG are proposed [11], one of which considered modeling the pumping process of the heart using and electric circuit, while the other one used templates of PPG waves as models. In this paper, we use both the models for PPG.

B. Feature Extraction from Original and Synthetic signal

PSKA processes ECG and PPG signals in frequency domain which gives better idea about the physiology of the

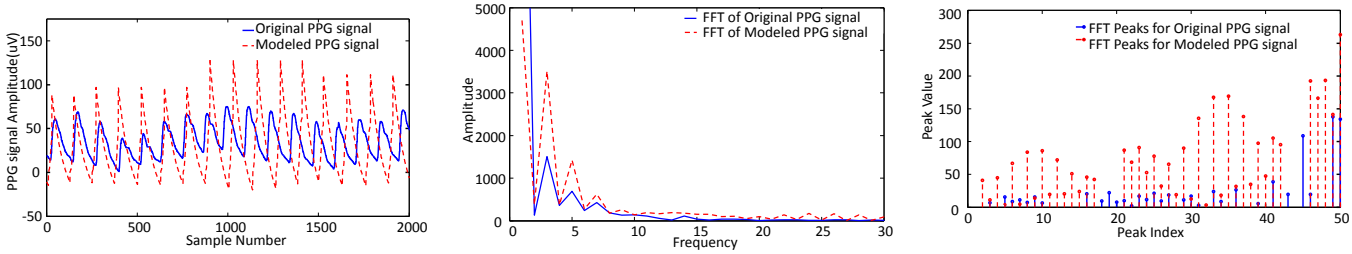

Fig. 2. **(a) Original and Modeled PPG signal (b) Original and Modeled PPG signals in frequency domain (c) Peak detection on FFT processed Original and Modeled PPG signals.**

patient as compared to time domain. In feature extraction process, FFT algorithm is applied on both ECG and PPG. Peak detection algorithm is then applied on these processed signals to get peak values p_v and the locations of the peaks p_i. For every peak, the feature is calculated as concatenation of location of peak and its value, $p_v p_i$. The set of all calculated features for every peak in FFT processed signal forms extracted feature set for that signal. This set of calculation is done for each sensor in the BSN. In this section, we demonstrate that features extracted from signals obtained using generative model gives maximum matching with that of original signal features. This makes our hypothesis of breaking security using models stronger.

We have obtained original ECG and PPG signals for 10 subjects from the PhysioBank database (http://www.physionet.org/physiobank). Generative models discussed in the previous section are used to generate synthetic signals using these original physiological signals. Figure 2 shows similarity between the original and modeled signals of PPG after processing them with FFT and peak detection algorithm. At every processing level, they show maximum correlation. Equivalent results for ECG were also obtained. This increases the possibility of generating same key from both the signals.

As the original and modeled signal are highly correlated, false positive and false negative results will give us the maximum possible polynomial order for which the security protocol can be broken. False positive means when the number of common features between original and generated signal are more for a given polynomial order where as false negative means the number of common features for the modeled signal are less than given polynomial order. Figure 3 shows that for polynomial order 7 the values of false positive and false negative are minimum. It implies that up to polynomial order 7, the vault can be broken using model based attack.

V. Feasibility of Model-Based Attack

Previous sections of the paper talks about model based attack on BSN security is possible if attacker gets the model of the physiological signal for the person irrespective of time when the reading has been taken. However, feasibility of the attack depends on getting access to physiological model of the person. We focus on how to obtain the physiological model in this section.

The attacker needs the generative model of the physiological signal and the current values of the temporal diagnostic

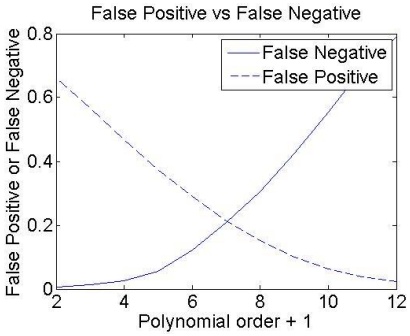

Fig. 3. **False positive and False negative Results for PPG.**

features to regenerate timely physiological features for breaking PSKA. The generative model can be obtained in two ways:

From old physiological data: Physiological signals such as ECG and PPG do not change in their morphology over time [10], [11]. Thus, old physiological data can be used to learn the morphological features of the generative model.

From sniffed network data: An attacker can sniff the network and get access to the secure data. A brute force algorithm to break the security can be employed to obtain physiological signals. These signals can be used to train a generative model on morphological features. The assumption is that the morphology of physiological signals do not change over time.

However, the temporal features are hard to obtain and without them timely physiological features cannot be generated and the attacker cannot break the BSN security. To obtain temporal features we propose to use the principle of electricity touch as explained in [12]. The electromagnetic field generated by heart is much stronger than that of brain electrical signals. It has been experimentally proven that, due to the stronger electromagnetic field generated by heart, whenever people come in contact with each other or even if they are in proximity with each other, the heart signal of one person gets reflected in the brain signal of other person. It is observed that if ECG and EEG for different people in contact by touch or in proximity are over-layed then they show similar wave form. Also, particularly alpha wave in EEG signal of one person has a strong relation with R-waves in the ECG signal of other person in contact. Using this result, the attacker can potentially get access to temporal features by only holding hands or staying in proximity with that person while wearing an EEG

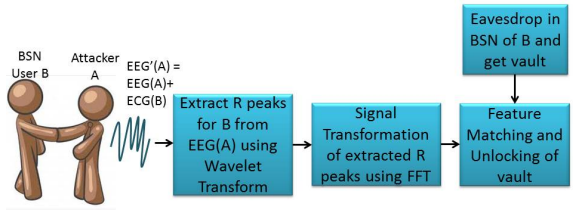

Fig. 4. **Step-wise execution of proximity-based attack using models.**

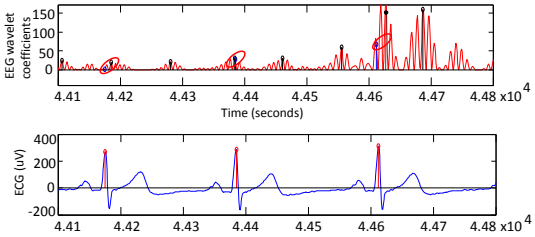

Fig. 5. **R peaks from ECG data and wavelet transform of EEG.**

sensor. Wavelet transform can be used to extract temporal features such as heart rate, standard deviation of heart rate and low frequency top high frequency ration (Section IV-A) from EEG without using ECG as the reference signal [14].

We explore this possibility of obtaining physiological signal of the person using proximity-based technique in the following sections. Figure 4 shows the step-wise execution of this attack. The attacker wears an EEG sensor, sensing $EEG(A)$, and comes in close proximity of a BSN user with an ECG monitor sensing $ECG(B)$. The BSN is using PSKA to secure inter sensor communication. The attacker shakes hand with the BSN user and his EEG, $EEG'(A)$ contains $EEG(A)$ plus the ECG R waves of the BSN user ($ECG(B)$). The attacker then samples the EEG signals and performs a windowed wavelet transform on $EEG'(A)$. For each upward wave of $ECG(B)$ there exists a corresponding "oscillation" in the wavelet transform. The oscillations are localized and converted to peaks using an adaptive thresholding technique as discussed in [13]. The R peaks from $ECG(B)$ and the peaks of wavelet coefficients of $EEG'(A)$ are shown in Figure 5. The peaks obtained from $EEG'(A)$ are then used to determine the heart rate, standard deviation, and lfhf ratio of $ECG(B)$. This also involves removing the EEG peaks corresponding to P, Q, S, and T waves in the ECG. For this we run peak detection in the ECG and map them to EEG peaks. The temporal features thus obtained combined with the morphology features can be used to generate the ECG signals of the BSN user. The generated ECG signals are used to break the vault in PSKA.

A. Experimental Setup and Data Collection

We collected three physiological signals from the subject. The first is EEG in which we used Emotiv Epoch Neuroheadset Model 1.0 (http://www.emotiv.com/). It contains 14 channels (AF3, F7, F3, FC5, T7, P7, O1, O2, P8, FC6, F4, F8, AF4) with numbers indicative of the specific position of the lead and a sampling rate of 128 Hz. The data is run through a built-in digital 5th order Sinc filter and a notch filters at 50 and 60 Hz to remove noise from power lines. The ECG sensor is a Wireless Shimmer2r device. The sensor has 3 leads (LA, RA, NL) and a sampling frequency of

Algorithm 2 Algorithm for Extracting ECG from EEG using Wavelet Transform

1: Filter the EEG signal to remove DC offset.
2: Use Coiflet-1 wavelet to perform CWT on EEG signal.
3: Extract the scale 4 data from the CWT processed EEG signal.
4: Set window length to detect peaks in CWT processed EEG signal such that threshold y-values in the window length should represent R-peak.
5: Update window length after every 5 seconds by averaging the distance between R-peaks obtained in last 5 seconds.
6: Repeat step 5 to detect all R-peaks in the EEG.

125 Hz. Smith Medical pulse-oximeters (http://ww.smithsoem.com/applications/oxiboards) were used for PPG sensing.

B. Extracting ECG from EEG using Wavelet Transform

Continuous Wavelet Transform (CWT) can capture temporal and morphological features in the signal which enable it to be used for analyzing physiological signals [20]. CWT gives information about the available frequencies in the signal at a particular time, where as Fourier transform (FT) can only illustrate frequency content in overall signal. Thus to detect ECG in EEG, CWT is preferred over FT as both temporal and morphological information are required. CWT uses a basic signal function which is scaled according to the frequency and time shift allowing specific shape properties of the signal to be analyzed. CWT for $x(t)$ signal is expressed as:

$$x(t) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} x(t)\psi^* \left(\frac{t-b}{a} \right) dt, \quad (1)$$

where, $a > 0$ is a scaling parameter, b is a shift parameter and ψ is a wavelet function. The scale parameter a, is used to denote how much the wavelet is stretched or compressed. Smaller the value of a, more the compressed wavelet. The shape of wavelet becomes stretched with increase in value of a. R-peaks in ECG from EEG signal are correctly obtained using Coiflet-1 wavelet with scale parameter 4 [14]. Algorithm 2 gives the steps for extracting ECG R-peaks from EEG using CWT. These R-peaks are further used to create model for ECG signal for the particular person. Algorithm 2 was applied to a 10 minute data sample obtained from two volunteers in the IMPACT Lab (Figure 7). The data collection protocol included an initial period of separation of the two individuals J and S and then a period of holding hands. Each period was 30 seconds in length. The window length of Algorithm 2 was varied from 1 sample to 128 samples. The inter peak interval of the peaks obtained from EEG signals is obtained. It is observed that when J was away from S, the average inter peak interval of the wavelet of J's EEG at a window length equal to the average R-R interval of J, is equal to the average R-R interval of J. However, when J and S were in proximity the average inter peak interval of the wavelet transform of J's EEG at a window length equal to average R-R interval of J's ECG

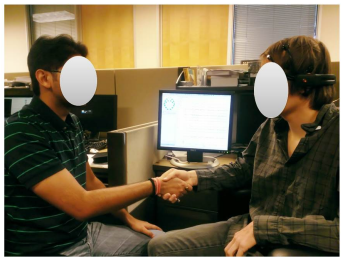

Fig. 7. **Experimental setup for collecting data from subjects at the IMPACT Lab.**

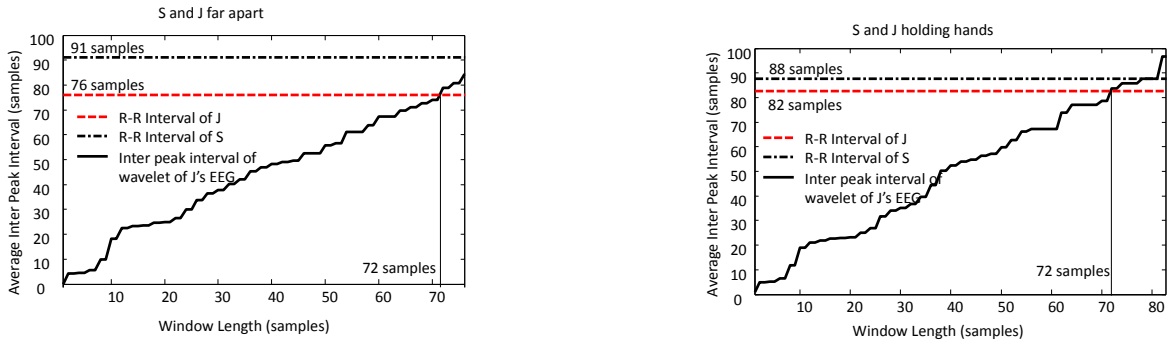

Fig. 6. **Comparison of R-R intervals of J and S with average inter peak interval of the wavelet transform of J's EEG.**

reduced considerably indicating overlap of S's and J's R peaks in J's ECG. This fact is shown in Figure 6. S's R peaks can then be obtained by removing J's R peaks from the peaks obtained from J's EEG's wavelet transform. This shows how we can obtain the diagnostic parameters of S from J's EEG. This makes model based attack on PSKA feasible. This attack was tested on 30 mins EEG and ECG data obtained from different pairs of individuals shaking hands for 30 seconds at regular time intervals and we found a 30% average accuracy of ECG R peak detection from EEG. This implies that with a 30 second handshake we can break PSKA with an average probability of 0.3. The minimum and maximum probabilities were 0.24 and 0.5, respectively.

VI. Conclusions

In this paper, we have shown how models can be used to breach the security in Body Sensor Networks. To demonstrate the possible model-based attack using generative models, PPG and ECG signals for multiple users are used. This paper identifies methods for retrieving private physiological signals from a BSN user through a non-invasive method. The proximity based attack is accomplished by extracting ECG of a BSN user from EEG of an adversary entity, when these two subjects were holding hands. We could break PSKA with an average probability of 0.3 with 30 second handshakes.

References

[1] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 14, no. 1, pp. 60 –68, Jan. 2010.

[2] C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *Communications Magazine, IEEE*, vol. 44, no. 4, pp. 73 – 81, April 2006.

[3] K. K. Venkatasubramanian and S. K. S. Gupta, "Physiological value-based efficient usable security solutions for body sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 4, p. 31, 2010.

[4] O. Morchon, H. Baldus, and D. Sanchez, "Resource-efficient security for medical body sensor networks," in *Wearable and Implantable Body Sensor Networks, BSN Intl. Workshop on*, April 2006, pp. 4 pp. –83.

[5] S. J. Kim and S. K. S. Gupta, "Audio-based self-organizing authentication for pervasive computing: A cyber-physical approach," in *Parallel Processing Workshops, ICPPW. International Conference on*, Sept. 2009, pp. 362 –369.

[6] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Ekg-based key agreement in body sensor networks," in *INFOCOM Workshops 2008, IEEE*, 2008, pp. 1–6.

[7] S. Cherukuri, 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 *Parallel Processing Workshops, Proceedings International Conference on*, Oct. 2003, pp. 432–439.

[8] A. Banerjee, K. Venkatasubramanian, and S. K. S. Gupta, "Challenges of implementing cyber-physical security solutions in body area networks," in *Proceedings of the Fourth International Conference on Body Area Networks*, ser. BodyNets '09. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, pp. 18:1–18:8.

[9] P. E. McSharry, G. D. Clifford, L. Tarassenko, and L. A. Smith, "A dynamical model for generating synthetic electrocardiogram signals," *Biomedical Engineering, IEEE Transactions on*, vol. 50, no. 3, pp. 289–294, 2003.

[10] S. Nabar, A. Banerjee, S. K. S. Gupta, and R. Poovendran, "GeM-REM: Generative model-driven resource efficient ecg monitoring in body sensor networks," in *Body Sensor Networks (BSN), 2011 International Conference on*. IEEE, 2011, pp. 1–6.

[11] ——, "Resource-efficient and reliable long term wireless monitoring of the photoplethysmographic signal," in *Proceedings of the 2nd Conference on Wireless Health*, ser. WH '11. New York, NY, USA: ACM, 2011, pp. 9:1–9:10.

[12] R. McCraty, M. Atkinson, D. Tomasino, and W. Tiller, "The electricity of touch: Detection and measurement of cardiac energy exchange between people," *Brain and Values: Is a Biological Science of Values Possible. Mahwah, NJ: Lawrence Erlbaum Associates, Publishers*, vol. 1998, pp. 359–379, 1998.

[13] S. Firoozabadi, N. Jafarnia Dabanlo, F. Mohammadi, and S. Koozehgari, "Effect of physical contact (hand-holding) on heart rate variability," *International Journal of Advanced Computer Science*, vol. 2, no. 12, 2012.

[14] J.-A. Jiang, C.-F. Chao, M.-J. Chiu, R.-G. Lee, C.-L. Tseng, and R. Lin, "An automatic analysis method for detecting and eliminating ECG artifacts in EEG," *Computers in biology and medicine*, vol. 37, no. 11, pp. 1660–1671, 2007.

[15] A. Morais, A. Cavalli, and E. Martins, "A model-based attack injection approach for security validation," in *Proceedings of the 4th international conference on Security of information and networks*, ser. SIN '11. New York, NY, USA: ACM, 2011, pp. 103–110.

[16] A. Valdes and K. Skinner, "Adaptive, model-based monitoring for cyber attack detection," in *Recent Advances in Intrusion Detection*. Springer, 2000, pp. 80–93.

[17] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based security metrics using adversary view security evaluation (advise)," in *Quantitative Evaluation of Systems 8th International Conference on*. IEEE, 2011, pp. 191–200.

[18] R. W. Ritchey and P. Ammann, "Using model checking to analyze network vulnerabilities," in *Security and Privacy, Proceedings. IEEE Symposium on*. IEEE, 2000, pp. 156–165.

[19] C. Kruegel, G. Vigna, and W. Robertson, "A multi-model approach to the detection of web-based attacks," *Computer Networks*, vol. 48, no. 5, pp. 717–738, 2005.

[20] M. Unser and A. Aldroubi, "A review of wavelets in biomedical applications," *Proc. of the IEEE*, vol. 84, no. 4, pp. 626–638, 1996.