IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 6, 2017, accepted May 18, 2017, date of publication June 9, 2017, date of current version August 8, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2714258

A Continuous Change Detection Mechanism to Identify Anomalies in ECG Signals for WBAN-Based Healthcare Environments

FARRUKH ASLAM KHAN[1], (Senior Member, IEEE), NUR AL HASAN HALDAR[1,2], AFTAB ALI[1], MOHSIN IFTIKHAR[4], TANVEER A. ZIA[3], (Senior Member, IEEE), AND ALBERT Y. ZOMAYA[4], (Fellow, IEEE)

[1]Center of Excellence in Information Assurance, King Saud University, Riyadh 11653, Saudi Arabia
[2]School of Computer Science and Software Engineering, The University of Western Australia, Perth, WA 6009, Australia
[3]School of Computing and Mathematics, Charles Sturt University, Wagga Wagga, NSW 2678, Australia
[4]Centre for Distributed and High Performance Computing, School of Information Technologies, The University of Sydney, Sydney, NSW 2006, Australia

Corresponding author: Farrukh Aslam Khan (fakhan@ksu.edu.sa)

ABSTRACT The developments and applications of wireless body area networks (WBANs) for healthcare and remote monitoring have brought a revolution in the medical research field. Numerous physiological sensors are integrated in a WBAN architecture in order to monitor any significant changes in normal health conditions. This monitored data are then wirelessly transferred to a centralized personal server (PS). However, this transferred information can be captured and altered by an adversary during communication between the physiological sensors and the PS. Another scenario where changes can occur in the physiological data is an emergency situation, when there is a sudden change in the physiological values, e.g., changes occur in electrocardiogram (ECG) values just before the occurrence of a heart attack. This paper presents a centralized approach for the detection of abnormalities, as well as intrusions, such as forgery, insertions, and modifications in the ECG data. A simplified Markov model-based detection mechanism is used to detect changes in the ECG data. The features are extracted from the ECG data to form a feature set, which is then divided into sequences. The probability of each sequence is calculated, and based on this probability, the system decides whether the change has occurred or not. Our experiments and analyses show that the proposed scheme has a high detection rate for 5% as well as 10% abnormalities in the data set. The proposed scheme also has a higher true negative rate with a significantly reduced running time for both 5% and 10% abnormalities. Similarly, the receiver operating characteristic (ROC) and ROC convex hull have very promising results.

INDEX TERMS Healthcare, wireless body area networks, change detection, intrusion detection, Markov model.

I. INTRODUCTION

THE number of elderly people in the world's population is increasing significantly. The number of people 60 years of age and over has been projected to reach approximately 700 million by 2009 and 2 billion by 2050 [1]. This will increase the burden on the medical sector. Therefore, scientists are now trying to shift towards personalized remote healthcare solutions. This personalized remote healthcare will help in early prediction and detection of the disease by the continuous and remote monitoring of a patient's health. Such personalized remote healthcare solutions can be achieved using a Wireless Body Area Network (WBAN), which is a special kind of network formed by placing wireless physiological monitoring sensors on the human body [2]–[8]. These sensors measure a patient's vital signs, i.e., electrocardiogram (ECG), electroencephalogram (EEG), and blood pressure, and these are then transmitted to a Personal Server (PS) using wireless communication devices. The PS then transmits this information to the remote medical system to enable remote health monitoring and diagnosis.

In order to provide risk free ubiquitous healthcare facilities, immense work has been done using ECG analysis and diagnosis in recent years. Most of the work in the literature is related to the analysis and diagnosis of Cardiovascular

Diseases (CVDs) [9]–[11]. In most of the architectures presented in the literature, the analysis and diagnosis are done on medical servers. Hence, there is a need for live and continuous healthcare monitoring to analyze and diagnose chronic diseases. The focus of most of the literature is the detection of abnormalities in the ECG data caused by diseases. However, none of the existing work considered intentional attacks and modifications caused to the data during communication in the case of WBANs. This work considers two situations where the physiological values change. First, the involvement of wireless media makes WBANs very susceptible to attacks like insertions, modifications, and forgeries. Moreover, the physiological status also varies as a result of abnormal conditions of the subject (patient carrying the WBAN) e.g., in the case of CVDs. Attacks on the ECG data during wireless communication may lead to the wrong diagnosis. Similarly, the early detection of changes in the ECG readings may save the user from a massive heart attack and severe consequences. To ensure fully automated, reliable, and continuous ubiquitous health monitoring, it is crucial to detect abnormal conditions and any intrusions or changes in the physiological values. The abnormality, intrusion, or change detection will surely allow clinicians and medical personnel to accurately diagnose CVDs.

In this paper, we present a centralized change detection mechanism for continuous and ubiquitous monitoring using WBANs. Change can be in the form of an intrusion, a modification, or an abnormality. Because of the time-variant nature of the ECG data, a Markov model-based detection mechanism is proposed. ECG is a sequence of data points, measured typically at successive points in time spaced at uniform time intervals. The amplitudes of the ECG frequency components change with time. Therefore, a Markov model is an optimal choice for such time series data. The proposed detection system architecture is depicted in Fig. 1, where different physiological monitoring sensors are attached to the human body, and a centralized PS collects data from these sensors for real-time abnormal event detection. Moreover, the centralized change detection mechanism runs on the PS to protect the human personal data, and to highlight anomalies and intrusions before sending it for further diagnosis to the medical servers. The system attaches a high priority or emergency tag called an abnormal tag to the data whenever it detects anomalies or intrusions in the data. On the receiving side, when this tag reaches the medical systems, it raises an alarm, and the corresponding medical personnel check the status of the physiological data. The proposed scheme is tested and evaluated with different window sizes and different levels of attack severity. The attack severity increases as we increase the number of insertions and modifications in the data. The proposed scheme has a better True Positive Rate (TPR) and True Negative Rate (TNR), which result in high performance in terms of intrusion detection. Similarly, the scheme shows a very low False Positive Rate (FPR) and False Negative Rate (FNR), which reduce the overburdening of the system. Moreover, the scheme is computationally inexpensive and consumes a very small amount of time for evaluating 10,000 records.

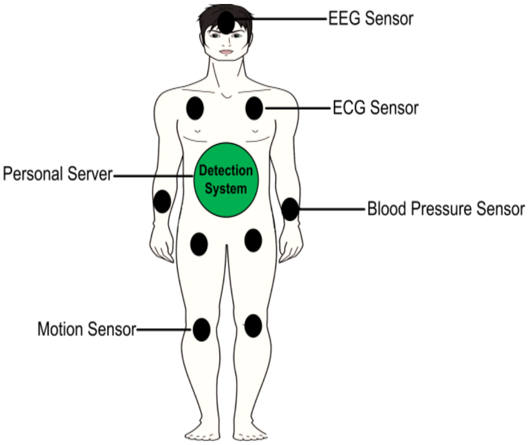

FIGURE 1. **WBAN-based change detection architecture.**

The remainder of this paper is organized as follows: In section 2, the background and related literature is discussed. Section 3 elaborates on the proposed change detection system. Section 4 presents experimental analysis and results of our proposed scheme. Finally, section 5 concludes our work.

II. RELATED WORK

Security, privacy, and attack-free communication can lead to an optimal and realistic healthcare system. To ensure attack-free communication in remote healthcare systems, there must be some countermeasures to protect the data and detect any intrusions in the human personal data during wireless communications in healthcare systems. Similarly, the physiological values also change in case of an emergency. Therefore, there should be some measures or techniques to detect these changes in the physiological values during an emergency to provide an early response to the user of the system.

There are some remote and personal healthcare systems in the literature, including CodeBlue [12], which is an ad hoc sensor network infrastructure for emergency medical care comprising low-power physiological sensors and PDAs. MobiHealth [13] provides an end-to-end healthcare platform for ambulant patient monitoring. The user of MobiHealth is equipped with different sensors that constantly monitor physiological values, e.g., blood pressure and electrocardiogram (ECG) data. A PDA-based Patient-Monitoring System [14] uses a PDA to monitor physiological data such as the heart rate, electrocardiogram, and SpO2. In [15], the authros use an IoT based data accessing scheme for ubiquitous emergency medical services. The authors in [16] propose a smarthome-based health monitoring and medicine packaging using IoT where the main services of the system are health monitoring, emergency response, and intelligent pharmaceutical packaging (iMedPack) with communication capability of passive radio-frequency identification (RFID) and actuation capability enabled by functional materials. Most of these systems focus on the architecture and services. Some consider secure communications, but none of the systems provide services for attack mitigation or change detection in the physiological data.

There are some schemes in the literature for detecting anomalies in the ECG data for arrhythmia detection [17], cardiomyopathy [18], and coronary blood flow abnormalities [19]. In this regard, [20] gives a cluster-based approach for detecting cardiovascular abnormalities in the ECG data. Characteristic frequencies are assigned to the compressed ECG data, and then the correlations between these frequencies are obtained. On the basis of these correlations, two clusters, i.e., normal and abnormal, can be formed. In [14], ECG biometrics are used for detecting cardiovascular diseases. The scheme in [21] is based on the idea that the characteristic frequencies taken from compressed ECG data at enrollment and recognition are the same. Similarly, in [11], R-wave events are detected using geometrical techniques. The R-wave detection will help to evaluate and predict abnormal cardiac rhythms. Similarly, there are schemes that consider the detection of abnormalities in ECG data using mobile devices [22], [23]. Although these schemes detect abnormalities like CVDs in ECG data, they do not consider the detection of intentional changes made by an attacker. Moreover, most of the above schemes run on hospital servers, and hence do not provide continuous and ubiquitous patient monitoring. The scheme proposed in this paper learns and detects new changes (i.e., anomalies and attacks) on the basis of the learned behavior.

There are some Markov model-based schemes for intrusion detection in wireless sensor networks (WSN). In this regard, [24] uses a classifier method for the detection of intrusions in log files using a Hidden Markov Model (HMM). The scheme uses an HMM and a k-mean for the classification of normal and abnormal traffic data. An intelligent mobile robot response system was presented in [25], which used enhanced fuzzy Adaptive Resonance Theory (ART) for learning and a Markov model for intrusion detection in a WSN. Another example is the use of a non-parametric version of HMM [26] for intrusion detection. The scheme uses scores and deviation alarms when the behavior changes.

The above healthcare systems are prone to attacks and modifications during wireless communications. If by any chance an attacker succeeds in forging and modifying human personal information during communication in remote healthcare systems, it will lead to a wrong diagnosis, which will ultimately result in serious consequences for the user of the healthcare system. Because of the harsh wireless communication environment, there is a need to incorporate a proper intrusion and modification detection system in the remote healthcare systems. Similarly, the above-mentioned Markov model-based schemes used for intrusion detection were designed by considering the specific requirements of the WSN. None of the Markov model-based schemes considered medical applications and WBANs.

In this paper, the proposed scheme uses a Markov model to detect modifications and abnormal behavior in the ECG data, as shown in Fig. 2. In Fig. 2, the red lines in the plot represent abnormal behavior, while the blue lines show the normal behavior. An ECG signal has the characteristics of time series data, where the amplitude of the signal changes as the time progresses. Keeping in mind the time series characteristics of the ECG data, Markov model-based intrusion and change detection is done for qualitative, reliable, and ubiquitous healthcare services. The proposed scheme helps to detect forgeries and modifications performed by an attacker to misguide the diagnosis process. In the same way, the proposed scheme will detect the abnormal behavior that occurs in case of a heart attack emergency. Moreover, the scheme learns the behavior of the changes and attacks. Whenever a new type of change or attack occurs, the scheme successfully detects and raises an alarm in the medical systems. For example, if there are some abrupt changes in the ECG data of a patient, the system will notify the clinicians prior to the heart attack.

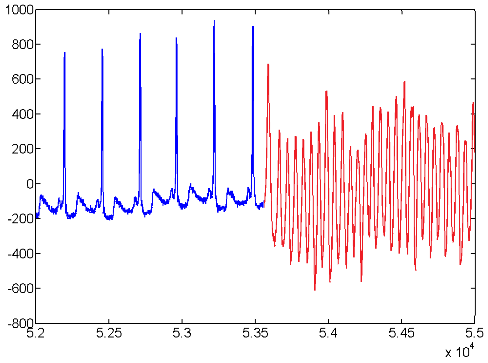

FIGURE 2. Normal and abnormal ECG behaviour.

III. PROPOSED CENTRALIZED CHANGE DETECTION SYSTEM

A WBAN-based remote healthcare system uses sensor devices for physiological monitoring, and then the sensed data are transferred to the medical servers for experts and clinicians for analysis and diagnosis. In our proposed system, all the physiological sensors are attached to a PS, which collects the physiological data from the sensors and then, after applying the intrusion and anomaly detection mechanism, sends the data along with the associated normal or abnormal tags to the medical servers. The clinicians then decide whether the condition of the patient under continuous observation is normal or needs an emergency response. If the condition is normal, the proposed system observes and evaluates the ECG data, detects attacks, and informs the patient as well as the clinicians about the attack. Our proposed architecture is depicted in Fig. 3, and is based on the following main steps:

A. FEATURE EXTRACTION

In this step, the PS extracts features from the physiological values received from the sensor nodes. All the physiological sensors sample the ECG values at a specific sampling rate and fixed duration of time. Then, by applying a Discrete Wavelet

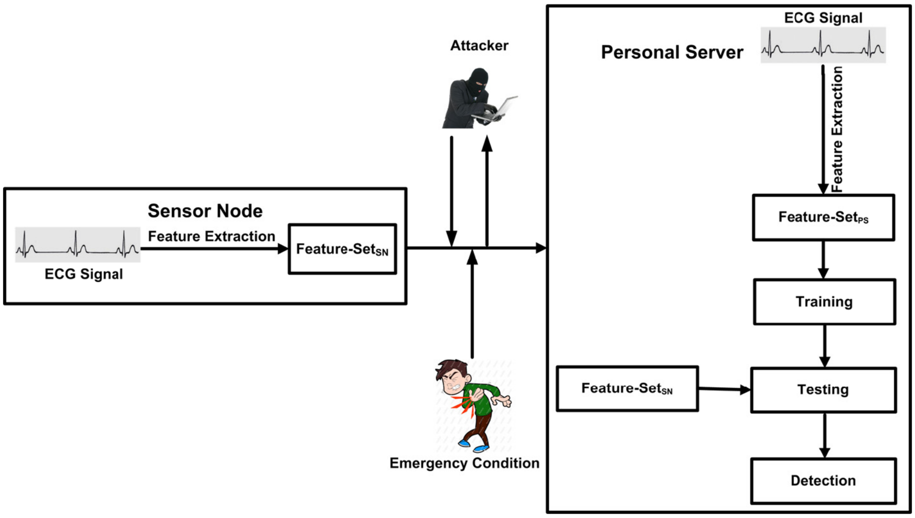

FIGURE 3. Markov Model-based change detection architecture.

Transform (DWT), the features are extracted from the ECG signal. All the sensor nodes extract the features and send them to the PS. The PS also extracts its set of features from the ECG signal. The set of features (FeatureSet$_{PS}$) from the PS are used for training, while the sensor node's features (FeatureSet$_{SN}$) are used for testing purposes.

B. Markov MODEL-BASED CHANGE DETECTION MECHANISM

Let us assume that {X_t, t ∈ T} is a sequence of random variables, where T = Z+ ={0,1,2,3…}. This sequence has a Markov property [29] if it satisfies the following conditions:

1) For any t ∈ T, the future process at ŧ, ($X_{ŧ}$, where ŧ > t and ŧ ∈ T) is independent of any past processes (X_γ, where γ < t and γ ∈ T).
2) The conditional probability distribution of such future process ($X_{ŧ}$) (where ŧ > t and ŧ ∈ T) depends only upon the present state (X_t , t ∈ T)

In other words, if X_t belongs to some countable set of states (S), then {X_t, t ∈ Z+} will satisfy the Markov property if and only if

$$P\left(X_{t+1}=j\,|\,X_0=i_0, X_1=i_1, \ldots, X_t=i_t\right)$$
$$= P(X_{t+1}=j\,|\,X_t=i_t),\ \forall t \in Z_+ \ and\ \forall i_0, i_1, \ldots, i_t,\ j \in S$$

The set of such countable states (S) is called the Markov chain. Therefore, a Markov chain can be defined as a mathematical model of random variables that evolve over time in such a manner that the future is affected only by the present and is independent of the past events.

1) Markov MODEL

A random variable X will be called a discrete random variable if it is finite or countably infinite and conforms to the following condition: $\sum_{x}$ P (X = x) = 1, where x is each possible value of random variable X. The probability mass function (pmf) of two such discrete variables, X0 and X1, is defined as

$$P\left(X_0=x_0, X_1=x_1\right) = P\left(X_1=x_1\,|\,X_0=x_0\right).P\left(X_0=x_0\right)$$

In the same way, for a total of n+1 such discrete random variables, X_0, X_1, X_2, …, X_n, the joint probabilities can be expressed as

$$\begin{aligned} &P\left(X_0=x_0, X_1=x_1, X_2=x_2, \ldots, X_n=x_n\right)\\ &= P\left(X_1{=}x_1, X_2{=}x_2, \ldots, X_n{=}x_n\,|\,X_0{=}x_0\right).P\left(X_0=x_0\right)\\ &= P\left(X_2{=}x_2, \ldots, X_n{=}x_n\,|\,X_1{=}x_1\right).P\left(X_1{=}x_1|X_0{=}x_0\right)\\ &\quad \cdot P\left(X_0=x_0\right)\\ &= P\left(X_0=x_0\right).P\left(X_1=x_1|X_0=x_0\right)\\ &\quad \cdot P\left(X_2=2|X_1=x_1\right)\ldots P\left(X_n=x_n|X_{n-1}=x_{n-1}\right) \end{aligned} \quad (1)$$

The initial probability of state x_0∈ S is defined as

$$q_{x_0} = P(X_0 = x_0) \quad (2)$$

and the other conditional probability chunks of (1) are denoted as

$$\begin{aligned} p_{x_n,x_{n+1}} &= P\left(X_{n+1}=x_{n+1}\,|\,X_n=x_n\right),\\ &\forall x_n, x_{n+1} \in S, n \geq \end{aligned} \quad (3)$$

The joint probability distribution in (1) can be simplified using (2) and (3) as follows:

$$\begin{aligned} &P\left(X_0=x_0, X_1=x_1, X_2=x_2, \ldots, X_n=x_n\right)\\ &= q_{x0}.(p_{x_0,x_1}.p_{x_1,x_2}\cdots p_{x_{n-1},x_n})\\ &= q_{x_0}\prod_{t=1}^{n} p_{x_{t-1},x_t} \end{aligned} \quad (4)$$

The function q_{x_0} in (2) is called the Initial Distribution, and $p_{x_n,x_{n+1}}$ in (3) is called the Transition Probability from state x_n at time n to state x_{n+1} at time n+1.

The transition probability is described in a more convenient manner as follows:

The transition probability matrix (P) is a matrix representation of the transition probabilities. Let p_{ij} be the transition probability of a system that is in state j at time t+1 and whose previous state was i at time t [25]–[27]. If the system has a total of "n" states, P will be defined as

$$P = \begin{bmatrix} p_{11} & p_{12} & \cdots & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & \cdots & p_{2n} \\ \vdots & \vdots & \vdots & \vdots & \\ p_{n1} & p_{n2} & \cdots & \cdots & p_{nn} \end{bmatrix} \quad (5)$$

A Markov model is a stochastic process. Hence, the sum of the probabilities of transitioning from state i to some other states will be 1, i.e., the sum of each row of transition matrix P will be equal to 1.

$$\sum\nolimits_{j=1}^{n} p_{ij} = 1 \quad (6)$$

By observing a system's behavior, the transition probability, as well as the initial probability, can be calculated.

Let N_{ij} = the total number of observations where X_t is in state i at time t and X_{t+1} is in state j at time (t+1).

If M = the total number of observations where X_t is in state i and X_{t+1} is in any one of the states 1, 2, 3, …, n,

N_i = the number of X_t in state i, and

N = the total number of observations, then

$$p_{ij} = \frac{N_{ij}}{M} \quad (7)$$

and

$$q_i = \frac{N_i}{N} \quad (8)$$

2) Markov MODEL-BASED ECG ANALYSIS SCHEME

This section elaborates on the application of the Markov model to intrusion and abnormality detection in the time series ECG data. The Markov model is used to represent the temporal profile of the normal behavior of the continuously collected ECG data set. Our target is to detect any abnormalities or intrusions in a human ECG pattern in real-time and continuous health monitoring systems. For the detection of intrusions and anomalies in the ECG data, normal ECG values, i.e., measured by the PS itself ($\text{FeatureSet}_{\text{PS}}$), are used to compare with the testing dataset, i.e., measured by the physiological sensors ($\text{FeatureSet}_{\text{SN}}$).

The ECG dataset collected from [28] contains a total of 310 ECG recordings of 90 different persons. There were 44 male and 46 female volunteers ranging in age from 13 to 75. Some records were collected periodically over 6 months. For experimental purposes, the first ECG records for persons 1 to 25 are used. The header (*.hea)* file of these records contains information about the person's age, gender, recording date, etc. Each record contains raw as well as filtered data signals. The filtered signals are used here for analysis and experimentation. Each ECG record contains a total of 10,000 signal values at 0.002-s intervals. An ECG signal value is denoted in millivolts, which varies in the ±10 mV range. In order to reduce the dimensions of the ECG data for better classification and improved detection, a Haar-based discrete wavelet transformation (DWT) is applied to the signal. With the goal of reducing the number of random variables from the ECG dataset, the dimensions were reduced by 50% in each record using DWT. The reduced set of data is further used for abnormality and intrusion detection.

Moreover, to validate our scheme, some user-defined intrusive data are imposed on the normal dataset in random locations of the collected ECG patterns, which is then used as testing data. Both 5% and 10% insertions and modifications are randomly injected into the dataset to prepare it for testing purposes. Thus, these testing datasets contain 95% and 90% normal patterned data, respectively.

3) TRAINING

In order to train the system, PS uses its own measured ECG feature set, i.e., $\text{FeatureSet}_{\text{PS}}$. This is done because the sensor nodes and PS reside on the same body, and hence measure similar ECG values. It is worth mentioning here that the ECG values measured at two different locations on the same body may have slight differences, but these differences can be eliminated or rectified by using some correction or reconciliation schemes [8], [30]. Moreover, as the scheme runs on the PS, the PS uses its own feature set of normal ECG data to train the system. The system builds a simplified Markov model by learning a transition probability matrix, as well as the initial probability distribution from normal ECG data. An observation window size *N* (20, 40, and 60) is used to divide the whole ECG signal into different set of states. For a total of *M* states ($M - N + 1$), different sets of states of size *N* will be available. The sequence of states for each chunk will remain the same. The steps of the proposed scheme are shown in Algorithm 1.

4) TESTING

After performing training, the system was able to detect any abnormality and change in the ECG data. For testing purposes, the feature set ($\text{FeatureSet}_{\text{SN}}$) received from sensor nodes is passed through the system.

Hence,

$$\begin{aligned} S_0 &= X_0, X_1, X_2, X_3, \ldots, X_{N-1} \\ S_1 &= X_1, X_2, X_3, X_4, \ldots, X_N \\ S_2 &= X_2, X_3, X_4, X_5, \ldots, X_{N+1} \\ &\cdot \\ &\cdot \\ &\cdot \\ S_{M-N} &= X_{M-N}, X_{M-N+1}, X_{M-N+2}, X_{M-N+3}, \ldots, X_{M-1} \end{aligned}$$

In general, $S_i = X_i, X_{i+1}, X_{i+2}, X_{i+3}, \ldots.., X_{i+N-1}$, where $0 \le i \le$ M-N. We can now compute the probability of each

Algorithm 1 Implementation of Markov Chain in ECG data

```
1. Initialization:
   Observation Window Size = w;
2. Step 1:
   Calculate total number of ECG data instance (M).
   Calculate total number of unique ECG data instance (U).
   Total_Number_of_Unique_Data (u) ≤
   Total_Number_of_Data (m)
3. Step 2:
   Assign unique index number to Unique ECG data
   instances, start from 0 to (u-1).
   Set of available states, $X = \{X_u, 0 \leq u < U\}$
4. Step 3:
   Extract ECG States based on original ECG data. Label
   as training dataset.
5. Step 4:
   Rename the time-based sequence of states available in
   training data with respect to state number available in X.
   Training Data Set, $TD = (X_v)_t, 0 \leq v < u, t = 0,1,2,\ldots$
6. Step 5:
   Calculate initial distribution of set of states, X.
   Calculate transition probability, $P_{ij}$ $(0 \leq i,j \leq u)$ of state
   transition from one state to another. Transition
   probability is based on Training Data Set, TD.
7. Step 6:
   Label Testing Data Set (TS) as in Step 4 and split the
   Testing Data Set into different chunk of entries (Si),
   termed as chunk of sequence
   $Si = (X_i, X_{i+1}, X_{i+2}, X_{i+3}, \ldots, X_{i+w-1})$ where, $0 \leq i \leq$
   m-w+1 and m = |TS|
8. Step 7:
   Calculate probability of occurrence of each sequence
   (Si), $\mathbf{P}(\mathbf{S_i}) = \mathbf{P}(\mathbf{X_i}, \mathbf{X_{i+1}}, \ldots, \mathbf{X_{i+w-1}})$
       $= \mathbf{q_{X_i}} \prod_{t=i+1}^{w} \mathbf{P_{X_{t-1}X_t}}, \mathbf{where 0} \leq \mathbf{i} < \mathbf{m} - \mathbf{w} + \mathbf{1}$
9. Step 8:
   Assign a Threshold value ($\tau$) for detecting the effected
   sequences. The probability of sequence (P(Si)) lesser
   than Threshold value ($\tau$), will confirm chance of
   abnormal changes. i.e., P(Si) <= $\tau$, detect
   abnormalities
```

sequence using (4).

$$
\begin{aligned}
P(S_i) &= P(X_i, X_{i+1}, \ldots, X_{i+N-1}) \\
&= q_{X_i} \prod_{t=i+1}^{N-1} P_{X_{t-1}X_t}, \textit{ where } (0 \leq i \leq M - N)
\end{aligned}
$$

The feature set contains 5% and 10% attack data, placed at random locations. If a total of M states are divided into $(M - N + 1)$ sliding windows of size N, each chunk (S_i) will contain N entries. If the probability is higher than a predefined threshold, the tendency of the sequence increases toward normal. On the other hand, if some sequence of states receives lower (tending to 0) probability scores, then there is a chance of an abnormality or intrusion activity in that sequence. This can be seen in Fig. 5, where a red line represents a threshold value. Touching the threshold raises an alarm.

5) NUMERICAL REPRESENTATION OF PROPOSED SYSTEM

In this section, we represent the process of detecting changes in a sample data set. For training purposes, time series data with 27 (i.e., (x_t, t), 0<t<27) states are given below. Let our exemplar data set contains a total of five unique states ($\{x_u, 0 \leq u < 5\}$). These states are discrete random variables, which are countably infinite.

Thus, unique states = $\{x_u, 0 \leq u < 5\} = (x_0, x_1, x_2, x_3, x_4)$

State occurrence = $\{(x_u, t)$, where $0 \leq u < 5$ and $0 < t < 27\}$. Here, "t" is the time index, which is incremented by 1 when a state changes to the same or a different state. The states are independent of the time t. For example, if at time t=0, the present state is x_0, the next state at t=1 will be any one of $(x_0, x_1, x_2, x_3, x_4)$, i.e., the next state = $\{x_u\}$, $0 \leq u < 5$.

The state occurrence of sample data is given as S = $(x_0, x_2, x_1, x_3, x_4, x_3, x_3, x_2, x_0, x_4, x_2, x_2, x_0, x_2, x_3, x_0, x_4, x_3, x_1, x_1, x_2, x_2, x_0, x_1, x_4, x_3, x_1)$. The initial distribution for five unique states can be calculated using (8).

Thus, the initial distribution q = [0.185, 0.185, 0.259, 0.222, 0.148].

The transition probability matrix can be calculated using (7). The last state in the sample data is given as x_1. As the sample data set is continuous, we expect another state as x_4 even after the last state of S. Here, the transition probability matrix is represented, where the transition probability from one state to another is rounded off to two decimal places.

$$
P = \begin{bmatrix}
0 & 0.20 & 0.40 & 0 & 0.40 \\
0 & 0.20 & 0.20 & 0.20 & 0.40 \\
0.43 & 0.14 & 0.29 & 0.14 & 0 \\
0.17 & 0.33 & 0.17 & 0.17 & 0.17 \\
0 & 0 & 0.25 & 0.75 & 0
\end{bmatrix} \tag{9}
$$

The sum of each row of P is equal to 1, i.e., $\sum_{j=1}^{n} p_{ij} = 1$ is satisfied.

Based on the transition probability and initial distribution, any new sequence behavior can be measured. Let another set of states be $S_{New} = (x_0, x_2, x_1, x_3, x_4, \mathbf{x_1}, x_3, x_2, x_0, \mathbf{x_3}, x_2, x_2, x_0, x_2, x_3, x_0, x_4, x_3, x_1, x_1, x_2, x_2, x_0, x_1, x_4, x_3, x_1)$. However, the transition matrix is already created using the training data set S. This matrix information is essential for identifying any abnormalities in the future set of transition states. The initial distribution of unique states along with the transition from one state to another are the bases for the abnormality assessments. Let us assume that there are some changes in the set of states S_{New}. Some intrusion or abnormality has occurred in the sixth and tenth position of the data set S_{New} of the same profile. Our target is to detect any changes in such a time series data. For experimental purposes, let us take an observation window size of N = 4 with a hop size of 1. Thus, the sequence of states will be divided into ($|S_{New}|$-N+1) = 24 chunks, where the chunks are represented as C_k,

$1 \leq k \leq (|S_{New}|\text{-}N\text{+}1)$. The elements in each chunk are given below:

$C_1 = (x_0, x_2, x_1, x_3)$, $C_2 = (x_2, x_1, x_3, x_4)$, $C_3 = (x_1, x_3, x_4, \mathbf{x_1})$, $C_4 = (x_3, x_4, \mathbf{x_1}, x_3)$, $C_5 = (x_4, \mathbf{x_1}, x_3, x_2)$, …, $C_{24} = (x_1, x_4, x_3, x_1)$. The occurrence probability of each chunk in our system will be calculated using (4).

$$\begin{aligned}
P(C_1) &= P(x_0, x_2, x_1, x_3) = q_{x_0} \cdot p_{x_0x_2} \cdot p_{x_2x_1} \cdot p_{x_1x_3} \\
&= (0.185) . (0.4) . (0.14) . (0.20) = 0.002072 \\
P(C_2) &= P(x_2, x_1, x_3, x_4) = q_{x_2} \cdot p_{x_2x_1} \cdot p_{x_1x_3} \cdot p_{x_3x_4} \\
&= (0.259) . (0.14) . (0.20) .(0.17) = 0.001233 \\
P(C_3) &= P(x_1, x_3, x_4, x_1) = q_{x_1} \cdot p_{x_1x_3} \cdot p_{x_3x_4} \cdot p_{x_4x_1} \\
&= (0.185) . (0.20) . (0.17) .(0) = 0 \\
P(C_4) &= P(x_3, x_4, x_1, x_3) = q_{x_3} \cdot p_{x_3x_4} \cdot p_{x_4x_1} \cdot p_{x_1x_3} \\
&= (0.222) . (0.17) . (0) .(0.20) = 0 \\
P(C_5) &= P(x_4, x_1, x_3, x_2) = q_{x_4} \cdot p_{x_4x_1} \cdot p_{x_1x_3} \cdot p_{x_3x_2} \\
&= (0.148) . (0) . (0.20) .(0.17) = 0
\end{aligned}$$

and so on.

$$\begin{aligned}
P(C_{24}) &= P(x_1, x_4, x_3, x_1) = q_{x_1} \cdot p_{x_1x_4} \cdot p_{x_4x_3} \cdot p_{x_3x_1} \\
&= (0.185) . (0.40) . (0.75) .(0.33) = 0.018315
\end{aligned}$$

After calculating the joint probability of each chunk, a threshold probability is defined. A higher probability indicates a greater likelihood that a chunk in the sequence state deviates from the normal behavior [31]. Abnormal or forged activities are expected in those sequences of states where the probabilities of the chunks are very low (below the threshold). The probabilities of the chunks of the sequence, with their states, are listed in Table 1.

The threshold value is calculated based on the normal profile behavior. The occurrence probability of each chunk in the normal profile dataset S is calculated to find out the sequence of states, which has the lowest probability value. Nevertheless, we have followed the same steps to calculate the occurrence probability of the normal profile as stated earlier in this section. The particular state sequence number, for which the sequence probability is minimum, is identified using equation (10).

$$m = \arg\min_{k;1\leq k\leq(|s|-N+1)} P(C_k) \tag{10}$$

It is found that for the value m = 2, the chunk C_2 (which contains the (x_2, x_1, x_3, x_4) sequence of states) produces the lowest value out of any other sequence combinations in the normal circumstances. The probability corresponding to the chunk C_2 is calculated as 0.001, which is identified as the lowest probability among the other chunks in the normal profile conditions. The threshold is assigned a value, which is lesser than the lowest occurrence probability among the chunks (i.e., $P(C_2)$) in a normal profile. We assigned the threshold as a fraction lower (i.e., 0.0001) than the lowest occurrence probability among the chunks (i.e., 0.001) available in the training data. Using equation (11), the threshold value is calculated as 0.0009 for the particular profile.

$$Threshold\ (\tau) = P(C_m) - 0.0001 \tag{11}$$

TABLE 1. Probabilities of chunks of sequence of states of test data set (SNew) in respect to Markov Model of normal profile data set.

Chunk Number	Sequence of States	Probability
C_1	(x_0, x_2, x_1, x_3)	0.002072
C_2	(x_2, x_1, x_3, x_4)	0.001233
C_3	$(x_1, x_3, x_4, \mathbf{x_1})$	0
C_4	$(x_3, x_4, \mathbf{x_1}, x_3)$	0
C_5	$(x_4, \mathbf{x_1}, x_3, x_2)$	0
C_6	$(\mathbf{x_1}, x_3, x_2, x_0)$	0.002705
C_7	$(x_3, x_2, x_0, \mathbf{x_3})$	0
C_8	$(x_2, x_0, \mathbf{x_3}, x_2)$	0
C_9	$(x_0, \mathbf{x_3}, x_2, x_2)$	0
C_{10}	$(\mathbf{x_3}, x_2, x_2, x_0)$	0.004706
C_{11}	(x_2, x_2, x_0, x_2)	0.012919
C_{12}	(x_2, x_0, x_2, x_3)	0.006237
C_{13}	(x_0, x_2, x_3, x_0)	0.001761
C_{14}	(x_2, x_3, x_0, x_4)	0.002466
C_{15}	(x_3, x_0, x_4, x_3)	0.011322
C_{16}	(x_0, x_4, x_3, x_1)	0.018315
C_{17}	(x_4, x_3, x_1, x_1)	0.007326
C_{18}	(x_3, x_1, x_1, x_2)	0.002930
C_{19}	(x_1, x_1, x_2, x_2)	0.002146
C_{20}	(x_1, x_2, x_2, x_0)	0.004614
C_{21}	(x_2, x_2, x_0, x_1)	0.006459
C_{22}	(x_2, x_0, x_1, x_4)	0.008910
C_{23}	(x_0, x_1, x_4, x_3)	0.011100
C_{24}	$(x_1, x_4, x_3, x_{1)}$	0.018315

TABLE 2. Transition from initial state to final state with corresponding transition probability.

Transition (N_i, t11, s0, w) → (N_j, t11, s1, w)

Initial State	Final State	Transition Probability
(N_i,t11,s0,w)	(N_j,t11,s1,w)	$\int_0^t \int_0^\infty \int_{t-x}^\infty f_{nn}(x). f_n(s) . f_{t_{11}}(t) dxdsdt$

Transition (N_i, t12, s0, w) → (A_j, t12, s1, w)

Initial State	Final State	Transition Probability
(N_i,t12,s0,w)	(A_j,t12,s1,w)	$\int_0^t \int_0^\infty \int_{t-x}^\infty f_{na}(x). f_a(s) . f_{t_{12}}(t) dxdsdt$

Transition (A_i, t22, s0, w) → (A_j, t22, s1, w)

Initial State	Final State	Transition Probability
(A_i,t22,s0,w)	(A_j,t22,s1,w)	$\int_0^t \int_0^\infty \int_{t-x}^\infty f_{aa}(x). f_a(s) . f_{t_{22}}(t) dxdsdt$

Transition (A_i, t21, s0, w) → (N_j, t21, s1 w)

Initial State	Final State	Transition Probability
(A_i,t21,s0,w)	(N_j,t21,s1,w)	$\int_0^t \int_0^\infty \int_{t-x}^\infty f_{an}(x). f_n(s) . f_{t_{21}}(t) dxdsdt$

The chunks whose probabilities are lower than the threshold τ, are supposed to contain some abnormal states in the corresponding chunks. It can be noticed from Table 1 that the probabilities of chunk numbers C_3, C_4, C_5, C_7, C_8, and C_9 are lower than the predefined threshold.

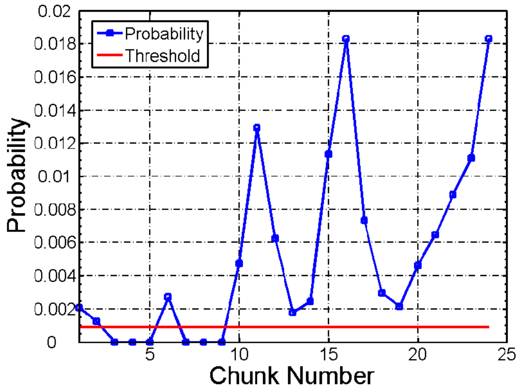

FIGURE 4. Normal and Abnormal behavior detection using threshold.

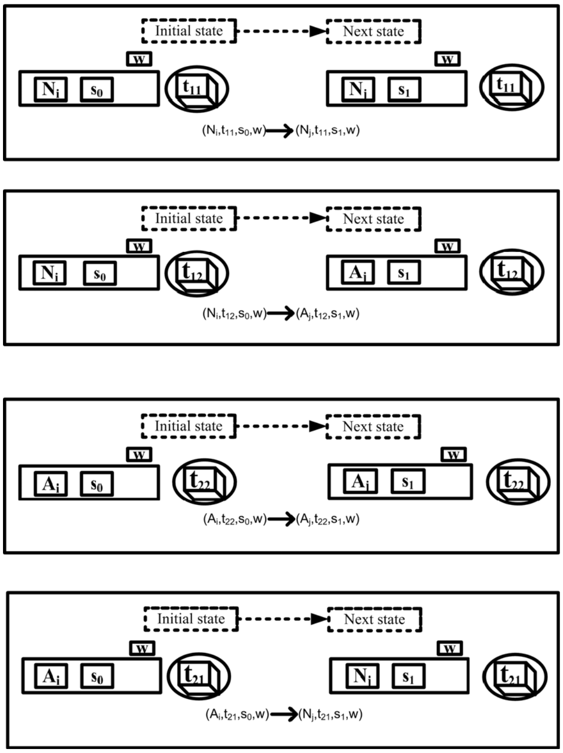

FIGURE 5. Markov Chain Transitions from one state to another state.

The proposed model identifies that there may exist some abnormalities in these six chunks. It is clear from Fig. 4 that these particular six chunks of sequences satisfy the abnormality condition as the probabilities of the occurrence of these sequences are below the threshold value. In the figure, the red line is marked as the threshold value. However, the threshold value is not fixed for different profiles. The threshold value is highly dependent on the training data of a normal profile. For each profile (i.e., patient), it is necessary to calculate the threshold value using the sufficient set of normal data. The more the satisfactory normal dataset is used as the training; the chances of generating the suitable threshold for the particular profile become high.

TABLE 3. Threat model.

Threat	Consequences
Node capture	Nodes physically compromised. This will yield all the ECG data and the attacker will be able to modify the data.
Impersonation attack	Intercepted legitimate ID or fake legitimate identity that lead to information disclosure or tampering
Spoofing attack	Disguise as a legitimate component to obtain data or tamper information

6) Markov CHAIN TRANSITIONS

A state transition system consists of a set of transition states, transition relations, and a set of initial states. A transition is basically a set of rules that is responsible for changing states from the source to the target. Different possible transitions that can occur in the proposed model are described in the subsections below. A total of four different types of transitions are available in our system.

a: TRANSITION FROM $(N_i, t_{11}, s_0, w) \rightarrow (N_j, t_{11}, s_1, w)$

Consider the case where $_{Ni}$ represents a normal chunk. $_{Ni}$ contains a total of w states. The initial state is represented as $s_0 \in S$. t_{11} is the condition for checking the normality of any chunk. After applying the Markov model on chunk Ni, if the joint probability of chunk $_{Ni}$ is lower than some threshold value (which is to be set by observing the normal system behavior), the next stage will be treated as normal (Nj) with initial state s_1. Here, the initial state will be changed to the state that is next to the initial state of chunk Ni. For example, assume window size w = 5 and let us assume that there are a total of six states available in the system, S = (S_0, S_1, S_2, S_3, S_4, S_5). As w = 5, so N_i and N_j will be treated as a chunk with a total of five elements, i.e., $|N_i| = |N_j| = 5$.

A sequence of states is available as follows: S_2, S_3, S_1, S_3, S_4, S_2, S_5, S_1, S_3, S_4, S_0, S_1, S_1, S_0, S_4. We take the chunk, N_i, which occurs in the following sequence: S_2, S_3, S_1, S_3, S_4. The initial state here is $s_0 = S_2$. After applying the Markov Model on N_i, if it satisfies the normal condition (a_1), the process will reach the next stage. In this case, N_j will be the next chunk whose states of occurrence will be S_3, S_1, S_3, S_4, S_2. Here, the initial state $s_1 = S_3$. This clearly shows a normal-to-normal transition.

b: TRANSITION FROM $(N_i, t_{12}, s_0, w) \rightarrow (A_j, t_{12}, s_1, w)$

In this case, if the joint probability after applying the Markov Model on chunk N_i satisfies the abnormality condition (t_{12}),

TABLE 4. **Total running time of ecg dataset execution.**

Person	Window Size in 5% Intrusion			Window Size in 10% Intrusion		
	20	40	60	20	40	60
	Time (ms)			Time (ms)		
1	2689	2681	2697	2776	2208	2663
2	2671	2639	2729	2598	2618	2602
3	2678	2643	2681	2671	2574	2750
4	2647	2643	2677	2641	2586	2644
5	2653	2654	2674	2645	2569	2604
6	2664	2652	2676	2614	2597	2615
7	2644	2655	2670	2226	2567	2596
8	2754	2642	2701	2595	2557	2596
9	2795	2635	2661	2622	2597	2601
10	2738	2641	2649	2580	2587	2594
11	2767	2620	2639	2621	2582	2626
12	2652	2650	2658	2558	2578	2636
13	2666	2639	2671	2583	2586	2277
14	2651	2662	2665	2580	2567	2246
15	2614	2659	2698	2596	2586	2576
16	2716	2846	2711	2600	2575	2641
17	2728	2662	2709	2655	2632	2632
18	2690	2677	2671	2637	2613	2598
19	2735	2636	2792	2663	2615	2590
20	2748	2720	2668	2603	2574	2623
21	2722	2587	2690	2756	2658	2615
22	2630	2593	2634	2650	2621	2648
23	2627	2627	2644	2760	2635	2644
24	2637	2622	2679	2628	2584	2653
25	2615	2610	2669	2603	2590	2635
Average	**2685.24**	**2651.8**	**2680.52**	**2618.44**	**2578.24**	**2596.2**

the next sequence of states (A_j) will be abnormal. Here, the initial state will be changed from s_0 to s_1 in the next transition. This type of scenario shows a normal to abnormal transition.

c: TRANSITION FROM $(A_i, t_{21}, s_0, w) \rightarrow (N_j, t_{21}, s_1, w)$

Let us suppose that a system is in an abnormal state and the initial state is s_0. If the probability of the sequence in A_i with respect to the initial state satisfies the normal condition (t_{21}), the next chunk of the sequence (N_j) will be in the normal state. This scenario shows the transition from an abnormal to a normal state.

d: TRANSITION FROM $(A_i, t_{22}, s_0, w) \rightarrow (A_j, t_{22}, s_1, w)$

In this case, an abnormal state (A_i) will be unchanged (A_j) if the probability of chunk A_i, which contains some sequence of states of size w, still satisfies the abnormality condition (t_{22}). If $A_i = (S_1, S_3, S_4, S_0)$, when $s_0 = S_1$, A_j will be the sequence (S_3, S_4, S_0, S_1) with $s_1 = S_3$. In this case, both A_i and A_j will be in the abnormal condition.

These transitions are depicted in Fig. 5, and a similar transition from the initial state to the final state with the corresponding transition probability is shown in Table 2. Moving from the initial state i_1 to the final state j_1 at time t will require the value of the integral multiplications of the probability mass functions.

IV. EXPERIMENTS AND RESULTS

This section provides a detailed description of the experiments and a discussion on the generated results.

A. EXPERIMENTAL SETUP

In order to perform different experiments and analyses, we use Java and MATLAB-based simulations. The dataset is taken from MIT-PHYSIOBANK [28], and we use different records taken from the ECG recordings of 25 persons.

TABLE 5. Results for 5% abnormal or attack data.

Person	Window Size														
	20					40					60				
	T.P.R	T.N.R	F.P.R	F.N.R	Prec.	T.P.R	T.N.R	F.P.R	F.N.R	Prec.	T.P.R	T.N.R	F.P.R	F.N.R	Prec.
1	91.6	99.7	4.4	8.4	95.4	92	99.6	6.8	8	93.1	91.2	99.7	5.2	8.8	94.6
2	91.2	99.8	3.2	8.8	96.6	91.2	99.8	3.2	8.8	96.6	90.4	99.8	4.8	9.6	95.0
3	92.4	99.8	3.2	7.6	96.7	92.4	99.7	4.8	7.6	95.1	92	99.8	4	8	95.8
4	90.8	99.9	2	9.2	97.8	90.4	99.8	4	9.6	95.8	90.4	99.7	5.2	9.6	94.6
5	93.2	99.9	1.6	6.8	98.3	91.6	99.8	3.2	8.4	96.6	91.2	99.9	2.8	8.8	97.0
6	93.6	99.9	1.6	6.4	98.3	93.2	99.6	6	6.8	94.0	93.2	99.6	0.8	6.8	99.1
7	94.8	99.8	0.4	5.2	99.6	94.4	99.8	2	5.6	97.9	94	99.7	1.2	6	98.7
8	94.0	99.6	8.8	6	91.4	92.8	99.7	0.8	7.2	99.1	92	99.6	4	8	95.8
9	96.8	99.9	0.4	3.2	99.6	96	99.8	3.6	4	96.4	96	99.8	3.6	4	96.4
10	94.4	99.8	4.4	5.6	95.5	94	99.7	1.6	6	98.3	93.2	99.7	1.2	6.8	98.7
11	94.8	99.8	4	5.2	96.0	94.8	99.8	2.4	5.2	97.5	94.4	99.8	0.8	5.6	99.2
12	92.8	99.7	2.8	7.2	97.1	92.4	99.7	4.8	7.6	95.1	92	99.6	0.8	8	99.1
13	96.8	99.9	2.4	3.2	97.6	96	99.8	3.2	4	96.8	96	99.8	1.2	4	98.8
14	94.0	99.7	0	6	100	93.6	99.7	2	6.4	97.9	92.8	99.7	2	7.2	97.9
15	89.6	99.5	1.6	10.4	98.2	89.2	99.5	3.6	10.8	96.1	88.8	99.5	0.8	11.2	99.1
16	91.2	99.6	3.2	8.8	96.6	90.8	99.6	2	9.2	97.8	90.8	99.6	1.6	9.2	98.3
17	91.2	99.6	2.8	8.8	97.0	91.2	99.6	0.4	8.8	99.6	90.8	99.6	1.2	9.2	98.7
18	92.0	99.6	3.6	8	96.2	92	99.6	0.4	8	99.6	90.8	99.6	2.4	9.2	97.4
19	95.2	99.8	0.4	4.8	99.6	95.2	99.8	1.6	4.8	98.3	95.2	99.8	0.4	4.8	99.6
20	95.6	99.8	0.8	4.4	99.2	95.6	99.8	2.8	4.4	97.2	95.6	99.8	1.2	4.4	98.8
21	95.2	99.8	1.6	4.8	98.3	94.8	99.8	5.2	5.2	94.8	94.8	99.8	4.8	5.2	95.2
22	96.8	99.9	0.8	3.2	99.2	96.8	99.9	0	3.2	100	96.4	99.9	0.4	3.6	99.6
23	95.6	99.8	2	4.4	98.0	95.6	99.8	2.4	4.4	97.6	94.8	99.8	3.6	5.2	96.3
24	88.8	99.5	9.2	11.2	90.6	88.4	99.4	2.8	11.6	96.9	88.4	99.4	3.2	11.6	96.5
25	98.4	100	0.4	1.6	99.6	97.6	99.9	1.2	2.4	98.8	97.6	99.9	2.4	2.4	97.6
Avg.	**93.6**	**99.8**	**2.6**	**6.4**	**97.3**	**93.3**	**99.7**	**2.8**	**6.7**	**97.1**	**92.9**	**99.7**	**2.4**	**7.1**	**97.5**

For an in-depth analysis, we examine the effect of increasing the window size on the detection rate and running time performance of the proposed scheme. The experiments are performed for different window sizes of 20, 40, and 60. Similarly, the experiments are done using 5% and 10% attack data.

B. RUNNING TIME

The experiments are performed using the data from 25 subjects, where each data set contains 10,000 values. The experiments are performed for different window sizes of 20, 40, and 60, with 5% and 10% intrusive data. On average, the schemes take almost 2.6 s to detect and evaluate the 5% and 10% intrusive data. Hence, it is evident from Table 4 that the total running time for a particular experiment is 2.6s. The running time analysis shows that the proposed scheme is usable in limited resource networks like WBANs for continuous monitoring and security provisioning.

C. SECURITY ANALYSIS

Since WBANs use wireless technologies for communication, most of the threats inherent in WSNs can also be launched against WBANs [32]. In Table 3, some of the attacks that can be launched against the proposed scheme and are able to modify the ECG values in order to disturb the diagnosis process are described.

For the security analysis, the proposed scheme is analyzed and evaluated in terms of the True Positive Rate (*TPR*), True Negative Rate (*TNR*), False Positive Rate (*FPR*), and False Negative Rate (*FNR*). The experiments are performed for various window sizes, and as we increase the window size, a slight variation is observed in the TPR or detection rate, as can be seen in Tables 4 and 5. Thus, we conclude that

TABLE 6. Results for 10% attack or abnormal data.

Person	Window Size														
	20					40					60				
	T.P.R	T.N.R	F.P.R	F.N.R	Prec.	T.P.R	T.N.R	F.P.R	F.N.R	Prec.	T.P.R	T.N.R	F.P.R	F.N.R	Prec.
1	84.8	98.4	7.4	15.2	92.0	85	98.4	3.4	15	96.2	84.8	98.4	4.6	15.2	94.9
2	87.6	98.7	3	12.4	96.7	87.4	98.7	2.4	12.6	97.3	87.2	98.6	1.6	12.8	98.2
3	85.2	98.4	2.4	14.8	97.3	84.6	98.4	2.8	15.4	96.8	84.6	98.4	4	15.4	95.5
4	85	98.4	2	15	97.7	84.6	98.4	0.4	15.4	99.5	84.2	98.3	0.6	15.8	99.3
5	83.8	98.3	2.2	16.2	97.4	83.8	98.3	3.8	16.2	95.7	83	98.2	2.2	17	97.4
6	85.2	98.4	3.4	14.8	96.2	84.6	98.4	3	15.4	96.6	84.6	98.4	1.6	15.4	98.1
7	90.6	99	4	9.4	95.8	90.4	99	2	9.6	97.8	90	98.9	1.4	10	98.5
8	91.2	99.1	3	8.8	96.8	90.8	99	0.8	9.2	99.1	90.8	99	0	9.2	100.0
9	88.8	98.8	2.4	11.2	97.4	88.6	98.8	1.2	11.4	98.7	88.4	98.8	2.8	11.6	96.9
10	89.8	98.9	1.4	10.2	98.5	89.4	98.9	1.6	10.6	98.2	89	98.8	1.8	11	98.0
11	89.8	98.9	1.8	10.2	98.0	89.6	98.9	2.2	10.4	97.6	89.4	98.9	0.4	10.6	99.6
12	85.4	98.5	1.6	14.6	98.2	85	98.4	2.8	15	96.8	84.6	98.4	2	15.4	97.7
13	85.6	98.5	1	14.4	98.8	85.4	98.5	1.8	14.6	97.9	84.8	98.4	1	15.2	98.8
14	88.2	98.8	2.4	11.8	97.4	87.8	98.7	0.2	12.2	99.8	87.4	98.7	2	12.6	97.8
15	84.6	98.4	4.4	15.4	95.1	83.8	98.3	1.2	16.2	98.6	83.8	98.3	1.2	16.2	98.6
16	84	98.3	5.6	16	93.8	83	98.2	0.6	17	99.3	82.6	98.2	1.2	17.4	98.6
17	91	99.1	1.2	9	98.7	91	99.1	0.2	9	99.8	90.8	99	0.6	9.2	99.3
18	85.6	98.5	1.2	14.4	98.6	85.4	98.5	0.8	14.6	99.1	84.8	98.4	0	15.2	100.0
19	88.2	98.8	0.8	11.8	99.1	87.8	98.7	1.2	12.2	98.7	87	98.6	1.6	13	98.2
20	84.4	98.3	2.4	15.6	97.2	84	98.3	1.2	16	98.6	83.2	98.2	0.4	16.8	99.5
21	93.2	99.3	1.4	6.8	98.5	93.2	99.3	0.8	6.8	99.1	93.2	99.3	1.8	6.8	98.1
22	89.2	98.9	1.2	10.8	98.7	89.2	98.9	3.6	10.8	96.1	89.2	98.9	2.8	10.8	97.0
23	90.8	99	1.6	9.2	98.3	90.6	99	0.2	9.4	99.8	90.6	99	1.2	9.4	98.7
24	89.6	98.9	1.8	10.4	98.0	89.6	98.9	1	10.4	98.9	89.6	98.9	1.2	10.4	98.7
25	92.8	99.3	0.8	7.2	99.1	92.8	99.3	1.6	7.2	98.3	92.8	99.3	0.8	7.2	99.1
Avg.	**87.8**	**98.7**	**2.4**	**12.2**	**97.3**	**87.5**	**98.7**	**1.6**	**12.5**	**98.2**	**87.2**	**98.7**	**1.6**	**12.8**	**98.3**

the increase in window size affects the performance of the proposed scheme in terms of the intrusion and anomaly detection. Similarly, it is also observed that, when we increase the insertion and modification percentage from 5% to 10% intrusive data, the detection rate decreases. Moreover, the *TNR* has maximum value of 99.8% for the 5% attack or abnormal data, and 98.7% for the 10% attack or abnormal data, which clearly draws a line between the normal and intrusive or abnormal data.

Similarly, the *FPR* interprets the false alarms raised by the system when it calls a normal sequence or record of data intrusive or abnormal. The proposed scheme limits the *FPR* to 2.8% at the maximum for the 5% attack or abnormal data, and 2.4% for the 10% attack or abnormal data. Moreover, the *FNR* presents a scenario where there is an attack or abnormality in the data but the scheme did not raise an alarm. In this scenario, the scheme fails to detect the abnormality or intrusion in the data. In our experiments, the proposed scheme restricted *FNR* to 7.1% at a maximum for the 5% attack or abnormal data, and 12.8% for the 10% attack or abnormal data.

Similarly, the maximum precision (Prec.) of the proposed scheme is 97.5% in the case of the 5% attack or abnormal data, and 98.3% on for the 10% attack or abnormal data. This shows the accuracy and usefulness of the proposed scheme in the presence of some abnormality or attack. A Receiver Operating Characteristic (ROC) curve is a two dimensional depiction used to evaluate and analyze the performance of any detection system. The ROC curve depicts the dependence of the FPR (i.e., accepted imposter attempts) on the TPR (i.e., accepted legitimate attempts).

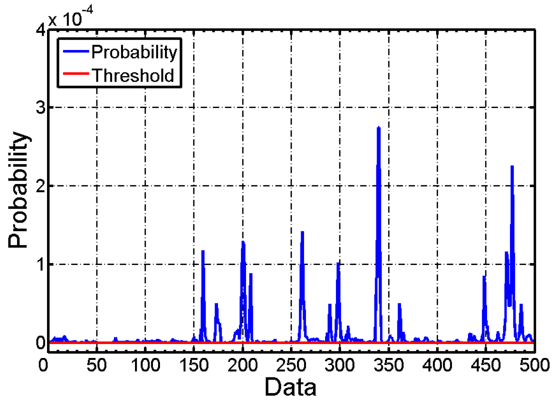

FIGURE 6. Threshold based detection of change.

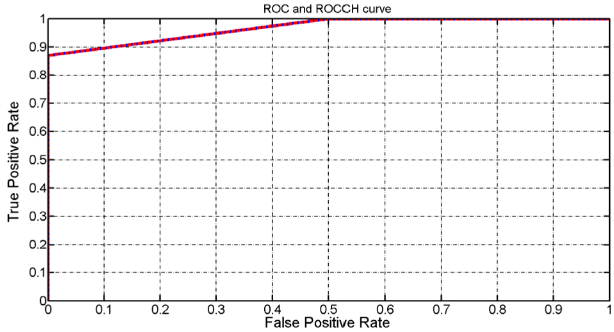

FIGURE 7. ROC and ROCCH curves for 5% anomaly data, 20 window size, and 90% threshold.

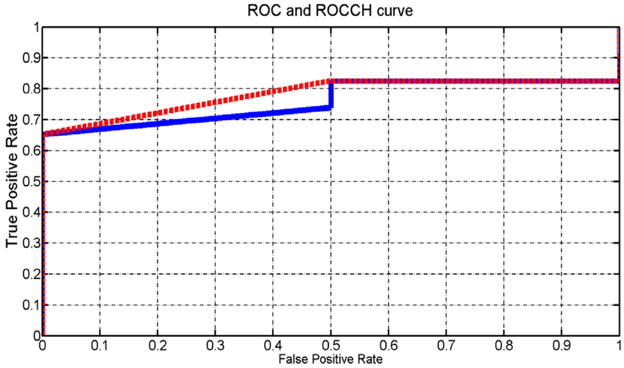

FIGURE 8. ROC and ROCCH curves for 5% anomaly data, 40 window size, and 90% threshold.

Similarly, the Area Under Receiver Operating Characteristic (AUROC) summarizes the total accuracy of the intrusion detection system. The AUROC number always ranges from 0.5 to 1.0, and the worst ROC curve lies along the positive diagonal y = x and has the corresponding area of 0.5. The best ROC curve lies on the y-axis, reaches the top corner (0, 1), and has an area of one.

When the corresponding area approaches 0.5, this means that the probability of the anomaly or intrusion detection is 50%. On the other hand, when it reaches one, this means that the probability of an anomaly or intrusion is 100%.

It is evident from Fig. 7 that for the 5% attack or abnormal data with a window size of 20 and a 90% threshold, the AUROC is 0.967391 and AUROCCH is 0.967391. Similarly, in Fig. 8, when we increase the window size to 40, the AUROC and AUROCCH decrease to 0.760870 and 0.782609, respectively.

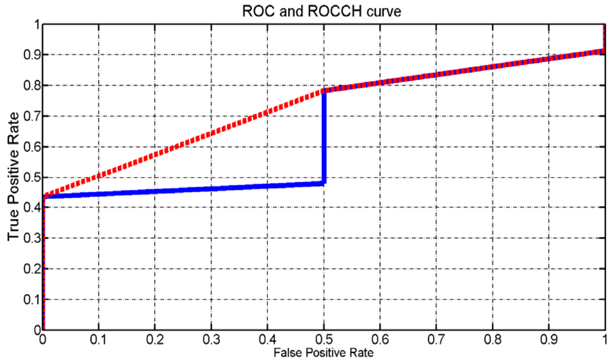

FIGURE 9. ROC and ROCCH curves for 5% anomaly data, 60 window size, and 90% threshold.

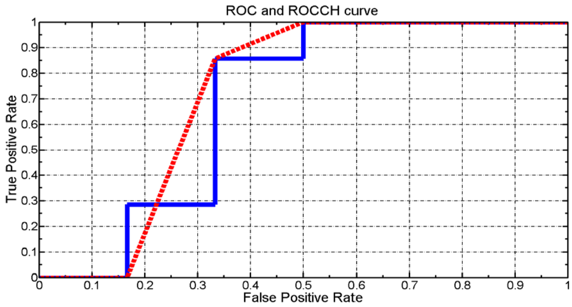

FIGURE 10. ROC and ROCCH curves for 10% anomaly data, 20-window size, and 90% threshold.

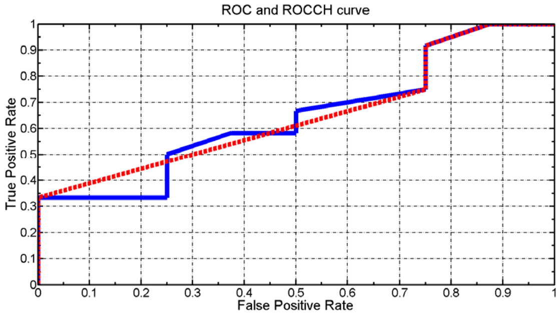

FIGURE 11. ROC and ROCCH curves for 10% anomaly data, 40-window size, and 90% threshold.

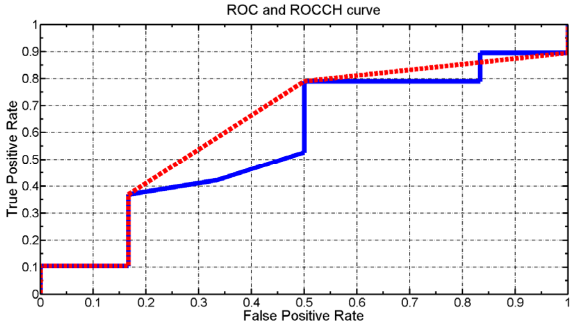

FIGURE 12. ROC and ROCCH curves for 10% anomaly data, 60-window size, and 90% threshold.

In Fig. 9, the AUROC and AUROCCH decrease to 0.652174 and 0.728261, respectively, for the window size of 60.

Fig. 10 shows that for the 10% attack or abnormal data with the window size of 20 and the 90% threshold, the AUROC is 0.690476 and ROCCH is 0.726190.

Similarly, in Fig. 11, when the window size increases to 40, AUROC becomes 0.645833 and AUROCCH becomes 0.651042. In Fig. 12, when the window size increases to 60, AUROC decreases to 0.574561 and AUROCCH decreases to 0.631579.

V. CONCLUSION

Detecting the changes that occur in ECG readings in continuous health monitoring systems is very hard. This abnormality detection task becomes more difficult when there is a chance of erroneous communication or some attacker intentionally introduces errors or makes changes in the patient's personal data during wireless communication. Our proposed work detects changes or abrupt variations in the ECG data. Similarly, it learns the behavior and detects new changes on the basis of this learned behavior to inform medical personnel by raising an alarm in the hospital systems. Moreover, the proposed scheme mitigates forgery, unauthorized insertions, and modifications in the ECG data, hence preventing misleading data in the diagnosis process. The proposed scheme shows good results in terms of its detection rate, true negatives, and running time complexity, which make it a better choice for resource-constrained WBANs.

In the future, the proposed system will be enhanced by automatically labeling the illegal attack and emergency heart attack. In this case, a semi-supervised system will be integrated with our proposed system, which will notify the corresponding abnormality indexes with timestamps and patient IDs to the medical representative. It is the responsibility of the clinicians to promptly contact patients to check their physical conditions. In case the patients suffer from symptoms related to an emergency heart attack, the clinician will inform the system about the emergency. On the other hand, if the system has already alerted about some abnormality and the clinicians have confirmed it as a normal heart condition, then the system will treat it as an intrusive activity happened around the time frame. Based on the clinicians' input, a semi-supervised model will be presented to label the illegal and emergency heart attacks.

ACKNOWLEDGMENT

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for its funding of this research through the Research Group Project no. RGP-214.

REFERENCES

[1] "World population prospects the 2008 revision: Volume I: Comprehensive tables," United Nations, Dept. Econ. Soc. Affairs, Population Division, New York, NY, USA, Tech. Rep. ST/ESA/SER.A/287, 2009.

[2] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60–68, Jan. 2010.

[3] A. Ali, S. Irum, F. Kausar, and F. A. Khan, "A cluster-based key agreement scheme using keyed hashing for body area net-works," *Multimedia Tools Appl.*, vol. 66, no. 2, pp. 201–214, 2013.

[4] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proc. IEEE INFOCOM Workshops*, Phoenix, AZ, USA, Jul. 2008, pp. 1–6.

[5] A. Ali and F. A. Khan, "An improved EKG-based key agreement scheme for body area networks," in *Proc. 4th Int. Conf., (ISA)*, 2010, pp. 298–308.

[6] A. Ali and F. A. Khan, "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, p. 216, 2013.

[7] A. Wood *et al.*, "ALARM-NET: Wireless sensor networks for assisted-living residential monitoring," Dept. Comput. Sci., Univ. Virginia, Charlottesville, VA, USA, Tech. Rep., 2006.

[8] A. Ali and F. A. Khan, "A broadcast-based key agreement scheme using set reconciliation for wireless body area networks," *J. Med. Syst.*, vol. 38, no. 5, pp. 1–12, 2014, doi: 10.1007/s10916-014-0033-1.

[9] G. M. Friesen, T. C. Jannett, M. A. Jadallah, S. L. Yates, S. R. Quint, and H. T. Nagle, "A comparison of the noise sensitivity of nine QRS detection algorithms," *IEEE Trans. Biomed. Eng.*, vol. 37, no. 1, pp. 85–98, Jan. 1990.

[10] P. S. Hamilton and W. J. Tompkins, "Quantitative investigation of QRS detection rules using the mit/bih arrhythmia database," *IEEE Trans. Biomed. Eng. (BME)*, vol. 33, no. 12, pp. 1157–1165, Dec. 1986.

[11] K. V. Suarez, J. C. Silva, Y. Berthoumieu, P. Gomis, and M. Najim, "ECG beat detection using a geometrical matching approach," *IEEE Trans. Biomed. Eng.*, vol. 54, no. 4, pp. 641–650, Apr. 2007.

[12] D. Malan *et al.*, "CodeBlue: An Ad Hoc sensor network infrastructure for emergency medical care," *Int. Workshop Wearable Implant. Body Sensor Netw.*, Apr. 2004, pp. 12–14.

[13] A. V. Halteren *et al.*, "Mobile patient monitoring: The mobi-health system," *J. Inf. Technol. Healthcare*, vol. 2, no. 5, p. 365373, 2004.

[14] Y.-H. Lin, I.-C. Jan, P. C. I. Ko, Y.-Y. Chen, J.-M. Wong, and G.-J. Jan, "A wireless PDA-based physiological monitoring system for patient transport," *IEEE Trans. Inf. Technol. Biomed.*, vol. 8, no. 4, pp. 439–447, Dec. 2004.

[15] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans Ind. Informat.*, vol. 10, no. 2, pp. 1578–1586, May 2014.

[16] G. Yang *et al.*, "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," *IEEE Trans Ind. Informat.*, vol. 10, no. 4, pp. 2180–2191, Nov. 2014.

[17] V. Eveloy, Y. Liu, and M. Pecht, "Developments in ambulatory electrocardiography," *Biomed. Instrum. Technol.*, vol. 40, no. 3, pp. 238–245, May/Jun. 2006.

[18] J. G. Webster, *Medical Instrumentation: Application and Design*. 3rd ed. Hoboken, NJ, USA: Wiley, 1998.

[19] A. C. Guyton and J. E. Hall, *Textbook of Medical Physiology*, 10th ed. Philadelphia, PA, USA: W. B. Saunders, 2000.

[20] F. Sufi, I. Khalil, and A. N. Mahmood, "A clustering based system for instant detection of cardiac abnormalities from compressed ECG," *Expert Syst. Appl.*, vol. 38, no. 5, pp. 4705–4713, May 2011.

[21] F. Sufi, I. Khalil, and A. N. Mahmood, "Compressed ECG bio-metric: A fast, secured and efficient method for identification of CVD patient," *J. Med. Syst.*, vol. 35, no. 6, pp. 1349–1358, Dec. 2011.

[22] M. Blount *et al.*, "Remote health-care monitoring using personal care connect," *IBM Syst. J.*, vol. 46, no. 1, pp. 11–95, 2007.

[23] K. Hung and Y.-T. Zhang, "Implementation of a Web-based telemedicine system for patient monitoring," *IEEE Trans. Inf. Technol. Biomed.*, vol. 7, no. 2, pp. 101–107, Feb. 2003.

[24] K. A. Garcia, R. Monroy, L. A. Trejo, C. Mex-Perera, and E. Aguirre, "Analyzing log files for postmortem intrusion detection," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 42, no. 6, pp. 1690–1704, Nov. 2012.

[25] Y. Y. Li and L. E. Parker, "Intruder detection using a wireless sensor network with an intelligent mobile robot response," in *Proc. IEEE Southeast Conf.*, Apr. 2008, pp. 37–42.

[26] X. Song, G. Chen, and X. Li, "A weak hidden Markov model based intrusion detection method for wireless sensor net-works," in *Proc. Int. Conf. Intell. Comput. Integr. Syst. (ICISS)*, Oct. 2010, pp. 887–889.

[27] W. L. Winston, *Operations Research: Applications and Algorithms*. Belmont, CA, USA: Duxbury Press, 1994.

[28] *MIT PhysioBank*, accessed on Aug. 24, 2014. [Online]. Available: http://www.physionet.org/physiobank/database/ecgiddb/

[29] T. Konstantopoulos. *Introductory Lecture Notes on Markov Chains and Random Walks*, accessed on Aug. 24, 2014. [Online]. Available: http://www2.math.uu.se/ takis/L/McRw/mcrw.pdf

[30] K. S. S. Gupta, T. Mukherjee, and K. K. Venkatasubramanian, *Body Area Networks Safety, Security, and Sustainability*. Cambridge, U.K.: Cambridge Univ. Press, May 2013.

[31] N. Ye, "A Markov chain model of temporal behaviour for anomaly detection," in *Proc. Workshop Inf. Assurance Security*, Jun. 2000, pp. 171–174.

[32] A. Ali and F. A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *J. Med. Syst.*, vol. 39, no. 10, pp. 1–12, 2015.

FARRUKH ASLAM KHAN (SM'15) received the M.S. degree in computer system engineering from the GIK Institute of Engineering Sciences and Technology, Pakistan, in 2003, and the Ph.D. degree in computer engineering from Jeju National University, South Korea, in 2007. He is currently an Associate Professor with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He is also the Founding Director of the Wireless Networking and Security Research Group, National University of Computer and Emerging Sciences, Islamabad, Pakistan. He has successfully supervised two Ph.D. students and 16 M.S. theses students. Several Ph.D. students are currently working under his supervision. He has over 70 publications in refereed international journals and conferences. His research interests include cyber security, body sensor networks, e-health, bio-inspired and evolutionary computing, and Internet of Things. He has served as a Co-Organizer and a TPC member of numerous international conferences and workshops. He has also served as an Associate Editor, a Guest Editor, and a Reviewer for various reputed international journals.

NUR AL HASAN HALDAR received the master's degree from Jamia Millia Islamia, New Delhi, India, in 2009. He was a Researcher with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He is currently a Doctoral Fellow with the School of Computer Science and Software Engineering, The University of Western Australia, Perth, WA. He is keenly interested in developing analytical frameworks using data mining techniques for varied applications, including social network analysis, cyber forensics, web surveillance, and biomedical informatics. His research interests are in the areas of data analytics, machine learning, graph modeling, digital forensics, social computing, and eHealth.

AFTAB ALI received the M.S. and Ph.D. degrees in computer science from the National University of Computer and Emerging Sciences, Islamabad, Pakistan, in 2009 and 2015, respectively. He is currently a Researcher with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. His research interests include wireless body area networks, key management, e-health, and cloud computing. He has served as a Reviewer of various international journals and conferences.

MOHSIN IFTIKHAR received the B.Sc. degree in electrical engineering from the University of Engineering and Technology at Lahore, Pakistan, in 1999, the M.Eng.Sc. degree in telecommunications from the University of New South Wales, Australia, in 2001, and the Ph.D. degree from The University of Sydney, Australia, in 2008. He was a Consultant for National Information, Communication and Technology Australia and Soul Communications, Australia, from 2007 to 2009. He was an Associate Professor with the Computer Science Department, King Saud University, Riyadh, Saudi Arabia. He is currently a Senior Lecturer with Charles Sturt University, Australia. His research interests include quality of service, traffic modeling, polling models, 3G/4G networks, markov chains, stochastic processes, network calculus, sensor networks, and wireless body area networks. He is a member of the ACM, IET, and PMI. He has received many competitive research grants of worth U.S. $1.5 million in recent years.

TANVEER A. ZIA received the Ph.D. degree from The University of Sydney, the Master of Interactive Multimedia degree from the University of Technology Sydney, the M.B.A degree from Preston University, USA, and the B.Sc. degree in computer sciences from Southwestern University, Philippines. He is currently an Associate Professor in computing with the School of Computing and Mathematics, Charles Sturt University, NSW, Australia. His broader research interests are in ICT security, specifically interested in security of low-powered mobile devices and also in biometric security, cyber security, IoT security, cloud computing security, information assurance, trust management, and forensic computing.

ALBERT Y. ZOMAYA (M'90–SM'97–F'04) is currently the Chair Professor of High Performance Computing and Networking with the School of Information Technologies, The University of Sydney. He is also the Director of the Centre for Distributed and High Performance Computing, which was established in 2009. He has authored/co-authored seven books and over 500 publications in technical journals and conferences. His research interests are in the areas of parallel and distributed computing and complex systems. He is a fellow of the AAAS and IET, a Distinguished Engineer of the ACM, and a Chartered Engineer. He received the 1997 Edgeworth David Medal from the Royal Society of New South Wales for outstanding contributions to Australian Science. He was a recipient of the IEEE Computer Society's Meritorious Service Award and the Golden Core Recognition in 2000 and 2006, respectively. He was a recipient of the IEEE Technical Committee on Parallel Processing Outstanding Service Award (2011), the IEEE Technical Committee on Scalable Computing Medal for Excellence in Scalable Computing (2011), and the IEEE Computer Society Technical Achievement Award (2014). He was the Chair of the IEEE Technical Committee on Parallel Processing from 1999 to 2003 and serves on its executive committee. He served as the General and Program Chair for over 100 events and served on the committees of over 700 ACM and IEEE conferences. He delivered more than 170 keynote addresses, invited seminars, and media briefings. He was the Editor-in-Chief of the IEEE Transactions on Computers (2010–2014) and serves as an Associate Editor for 20 journals including some of the leading journals in the field. He is the Editor of 20 books and 29 conference proceedings.