PIPAC: Patient Infusion Pattern based Access Control Scheme for Wireless Insulin Pump System v2

Xiali Hei, Xiaojiang Du, Shan Lin
Department of Computer and Information Sciences
Temple University
Philadelphia, PA 19122, USA
Email: {xiali.hei, dux, shan.lin}@temple.edu

Insup Lee
Department of Computer and Information Science
University of Pennsylvania
Philadelphia, 19104, USA
Email: lee@cis.upenn.edu

***Abstract*—Wireless insulin pumps have been widely deployed in hospitals and home healthcare systems. Most of these insulin pump systems have limited security mechanisms embedded to protect them from malicious attacks. In this paper, two attacks against insulin pump systems via wireless links are investigated: a single acute overdose with a significant amount of medication, and chronic overdose with an insignificant amount of extra medication over a long time period, e.g., several months. These attacks can be launched unobtrusively and may jeopardize patients' lives. It is very important and urgent to protect patients from these attacks. To address this issue, we propose a novel patient infusion pattern based access control scheme (PIPAC) for wireless insulin pumps. This scheme employs a supervised learning approach to learn normal patient infusions pattern with the dosage amount, rate, and time of infusion, which are automatically recorded in insulin pump logs. The generated regression models are used to dynamically configure a safety infusion range for abnormal infusion identification. The proposed algorithm is evaluated with real insulin pump logs used by several patients for up to 6 months. The evaluation results demonstrate that our scheme can reliably detect the single overdose attack with a success rate up to 98% and defend against the chronic overdose attack with a very high success rate.**

***Index Terms*—wireless insulin pump; implantable medical devices; access control; infusion pattern; patient safety**

I. Introduction

The US Centers for Disease Prevention and Control estimate that 25.8 million Americans (8.3% of the population) [1] live with diabetes. To treat chronic diabetes, implantable medical devices (IMDs) have been widely used. A rapidly growing number of wireless insulin pumps have been used by diabetic patients to deliver insulin into their circulatory systems. In 2005, there were approximately 245,000 pump users, with this market expected to grow 9% annually between 2009 and 2016 [2, 3]. It is very important that these wireless insulin pumps are reliable, secure, and safe.

Unfortunately, most of the existing wireless insulin pumps lack sufficient security mechanisms to protect patients from malicious attacks and overdose incidents. For example, a pump malfunction has caused at least one death [4], where the pump went into the PRIME function when the patient was asleep and delivered the entire cartridge of insulin. Insulin pumps have preset minimum and maximum dosage levels as well as infusion rates, as is required by the FDA [5]. However, researchers have shown that these levels could be remotely disabled by attackers [6]. Without this basic protection mechanism, the insulin pump is vulnerable to various attacks. In this paper, we investigate two new fatal attacks that are specially targeted to wireless insulin pumps. The first type of attack is a single acute overdose attack: the attacker can issue a one-time overdose (underdose) containing a significant amount of medication to a patient. For diabetic patients, the effects of the insulin overdose can include dizziness, drowsiness, and nausea, ultimately leading to seizures, coma, and in the worst case death [7]. The second type of attack is chronic overdose (underdose) with an insignificant amount of medication being delivered over a long time period, e.g. months. The chronic overdose of insulin can directly cause low blood glucose (BG), which leads to various complications and is extremely difficult to detect. Given that this attack can be performed even without modifying the insulin pump settings, it can be even more challenging to defend against.

To protect patients' safety, it is essential to defend against these two types of attacks on insulin pumps. In this paper, we propose a novel access control mechanism using a supervised learning approach. Many wireless insulin pumps, e. g. Metronic MiniMed 512, automatically records detailed information about each infusion in its log file. The detailed information includes the infusion rate, dosage, BG level, patient id, and time of day for each infusion. Given this information, we observe normal infusion patterns for home care diabetic patients. To learn these normal patterns, regressions are designed to analyze infusion dosage history and predict future infusion dosages. Once collected and analyzed, our scheme can generate a safety range for a specified time interval. Our access control algorithm design has three unique features: 1) this algorithm utilizes the temporal correlation of infusions for any specific patient. Patient specific infusion patterns are captured over time, and the long term changes of infusion patterns can also be detected; 2) a safety range is dynamically updated at different times of the day based on the online model, (the safety range counts for the in-situ variations of the insulin injection) and 3) this algorithm doesn't require any extra information, all the data required is automatically recorded in the insulin pump logs. Also, the linear regression

design requires little memory and computing capacity, which can be done in real-time even on resource limited computing platforms. Our algorithm can also identify infusion mistakes made by doctors or patients, such as erroneous dosage input. In emergency situations, insulin pump users should be allowed to infuse a larger than normal dosage. Many bio-metric based solutions have been proposed to address this problem; however, this is not the focus of this paper.

There are a number of prior works on implantable medical devices. These works provide valuable research results for our study. For example, with a pump serial number (SN) and USB device easily purchased from eBay, Radcliffe was able to track data transmitted from the computer and control the insulin pump's operations [9]. Radcliffe was also able to cause BG management devices to display inaccurate readings by intercepting wireless signals sent between the sensor device and the management device. Kevin Fu et al. detailed how to remotely reprogram an implantable defibrillator, causing the victim to receive a malicious shock [10]. Additionally, harvesting patient data in a region is an easily executed eavesdropping attack. Previous literature [8] has analyzed the possible attacks and has proposed to use a traditional cryptographic approach (rolling code) and body-coupled communication to protect the wireless link and insulin pump system. However, these proposed solutions do not address the overdose attacks that are studied in this paper. In this paper, we present a novel supervised learning based approach for insulin pump access control.

Our solution is evaluated with real insulin pump logs collected from Medtronic MiniMed 512 pumps in a home care system for diabetic patients. Several log files are tested. Each log file contains the infusion records of a specific patient for up to 6 months. We use a cross-validation approach to tune our model. The first 80% of logs are selected as training data set, and the remaining 20% are used for testing. Malicious attacks are simulated in combination with the normal infusions. Evaluation results show that our algorithm can effectively detect the single overdose attack with a success probability up to 98% and detect the chronic overdose attack with a very high success rate.

Our contributions are summarized as follows:

- A novel patient infusion pattern based access control scheme for wireless insulin pump is proposed. To the best of our knowledge, we are the first group to utilize patient specific infusion patterns to identify malicious overdose attacks on insulin pumps.
- Our solution dynamically calculates a safety dosage range at different times based on the online learning model.
- Experimental results with real insulin pump data sets demonstrate that our solution can defend against the overdose attacks effectively with a success rate above 98%.

The remainder of this paper is organized as follows: In Section II we describe the background and attack models. We analyze patient infusion patterns in Section III. In Section IV we present the detail patient infusion pattern based access control scheme. We describe our real experimental results in Section V. We present related discussions in Section VI. In Section VII, we discuss the related work, and we conclude the paper in Section VIII.

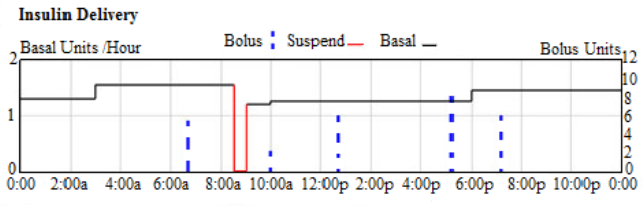

Fig. 1. Daily insulin dosage example of patient A

II. System and Attack Models

A. Background and System Model

An infusion pump infuses fluids or medication into a patient's circulatory system. To treat diabetes, wireless insulin pumps are widely used to deliver insulin into a diabetic patient's body. An insulin pump usually delivers a single type of rapid-acting insulin in two ways:

- A bolus dose that is pumped to cover food eaten or to correct a high BG level.
- A basal dose that is pumped continuously at an adjustable basal rate to deliver insulin needed between meals and at night.

It is the responsibility of the pump user to manually start a bolus or change the basal rate. Fig. 1 shows the insulin infusion record for a diabetic patient over 24 hours. As illustrated in the figure, the insulin basal rates are slightly different during different time periods within one day. The basal rate is a continuous infusion that lasts for 24 hours. The infusions with the bolus dosages are discrete, and occur around 7am, 10am, 12pm, 5pm, and 7pm each day. The bolus dosages have three categories: normal, square, and dual. Patients choose any type of them with specified amounts of dosages. The diabetic individuals usually deliver a square bolus or a normal bolus at a fixed time interval that accounts for breakfast, lunch, dinner, and other cyclical events every day. Factors such as carbohydrate (carb) ratio, insulin sensitivity, and target high BG are typically unique to each patient.

Fig. 2 shows the components of a Medtronic Paradigm real time insulin pump system. The OneTouch meter obtains BG readings from an implanted sensor via the wireless link 3. The BG information is transmitted from OneTouch meter to the insulin pump via the wireless link 2. The insulin pump delivers insulin to the patient. The remote control unit is operated by the user to send instructions (such as suspend and resume basal rate) to the insulin pump via wireless link 1. Wireless link 4 transmits historical BG readings to a USB device that uploads the information to a web service. Wireless link 5 allows the Carelink USB device to gather reports on BG trends and patterns. Wireless link 6 sends current BG levels to the pump. A laptop or PC is utilized by the Carelink USB device to upload data to a web-based management system.

B. Overdose Attack over Wireless

Given the wireless insulin pump system, we discuss potential attacks. To connect two components, such as the Carelink USB device and the insulin pump, a user must manually enter the SN of that component being wirelessly connected. Once all of the wireless connections among components are established, the insulin pump can display BG readings from sensors and adjust bolus and basal rate according to control unit commands.

The wireless communication in the system is not encrypted. As a result, attackers can easily compromise the wireless links in this system. Various malicious actions can be conducted after the wireless links are compromised. For example, attackers can display incorrect BG readings on the insulin pump via link 2. We refer to this attack as the Radcliffe's attack. Another attack is that an attacker suspends the basal rate delivery using link 1. We do not discuss this attack in our paper because it can be easily noticed by patients.

Insulin pump users can modify the pump settings using the Carelink Pro software on a computing device, such as a laptop. The new settings are uploaded to the pump using the attached Carelink USB device via wireless link 5. In this case, attackers may use customized software and a wireless sniffer to obtain the SN of all pumps within 300 feet, and can therefore compromise wireless link 5 to change the settings of the pump without being noticed. Using this security flaw, an attacker can 1) disable the alarms of the pump, 2) change the maximum allowable dosage of the pump, and 3) deliver a fatal dose to the insulin pump user. The delivery of a lethal dose is life-threatening and must be defended against.

In this paper, we focus on the attacks that are based on the compromised wireless link 5. Specifically, we focus on two types of attacks related as follows,

- *Single acute overdose*. This attack issues a one-time overdose (underdose) to the patient. A significant amount of medication that is beyond the normal dosage will be delivered to the patient using the insulin pump in a short time period. Given the fatal damage to the patient in a short time period, it is critical to prevent from this attack.
- *Chronic overdose*. This attack issues extra portions of medication to the patient over a long time period, e. g. weeks or months. One or two instances of the small overdose are not critical; however, such overdose for a long time period can put the patient's life in dangers. The clinicians and patients may not notice the small amount of overdose, since it does not cause obvious symptoms until the dosages have accumulated to a serious level. This can also cause various complications to the patient.

The authentication scheme is critical. However, the existing authentication with a code is not secure if an attacker can get close enough. Right now, there is no any authentication scheme over wireless link 5. In this paper, we can assume the wireless link 5 has a standard authentication scheme and the patient's parameters can only be changed manually.

Fig. 2. A real time insulin pump system

III. Data analysis

Our study is based on real insulin pump records provided by anonymous diabetic patients. Over the last year, several patients used Medtronic wireless insulin pumps at their homes for at least three months. All those patients were able to upload their infusion log data to the Carelink online management system.

A. Infusion Record Analysis

Since the dataset was real patient data in a format proprietary to Medtronic Inc., a substantial effort was required to clean the data. First of all, many of the recorded events are not directly related to the delivered patients' dosages. Secondly, there is a time difference between the time of recording features that we used in subsection C and the programming of doses. We must preprocess this data to make it suitable for analysis. If a record is unrelated to the basal rate and bolus, it was filtered out. Otherwise, we extracted the record, labeled it, and classified it into basal rate logs and bolus logs. We also calculated the total dosage of bolus during each time period Δ, which starts when the patient requires a bolus. The mean E and standard deviation σ of daily total insulin were calculated as well.

From the preprocessed data set, we found that the estimated bolus dose and other nine variables (BG level, active insulin and insulin sensitivity et al.) were correlated. There are a few other variables (e.g. the amount of exercise) that are known to affect the estimated bolus level. Unfortunately, we do not have access to them.

We explored the infusion records of patient A over the course of several days. We observed that during breakfast time, there were 1-2 bolus doses; during lunch time, there were 1-3 bolus doses; during dinner time, there were also only 1-2 bolus doses. Fig. 3 is the histogram of patient A's daily bolus dosage in 3 months. It shows that the bolus delivery was highly aligned with the time of the day. We also performed the Shapiro-Wilk test for all the patients' total daily insulin. The test result shows that they all obey normal distribution because all the p of them is greater than 0.05. These results

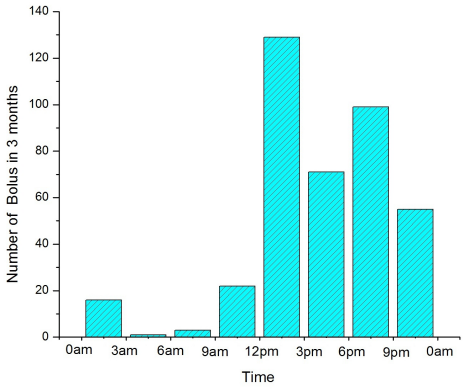

Fig. 3. The histogram of patient A's daily bolus dosage in 3 months

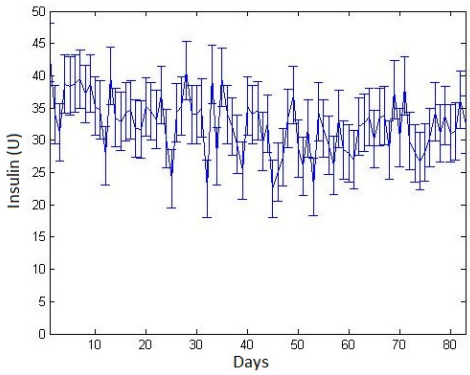

Fig. 4. The 2σ-errorbar of patient A's daily total insulin dosage

suggest that the mean of daily total insulin dosage of a patient is stable over the treatment period. For example, Fig. 4 shows the mean E and 2-standard deviation 2σ of patient A's total daily insulin in 3 months. We can see that they are bounded within $[E-2\sigma,\ E+2\sigma]$. Fig. 5 is the histogram of patient A's total daily insulin for 3 months, which indicated to us it may follow the normal distribution.

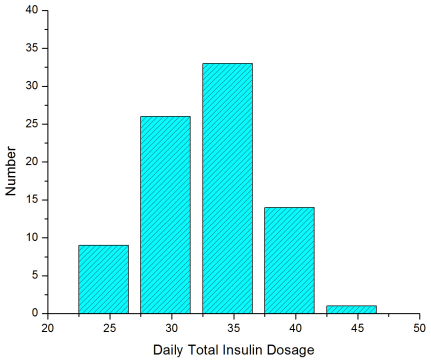

Fig. 5. The histogram of patient A's daily total insulin dosage in 3 months

B. Patient Insulin Dosage Pattern

From the analysis results, we observed that there generally exist patterns of bolus and basal rate infusions, even though each patient may have his/her own circadian rhythm. A patient's eating habits can be manifested from various factors, including their profession, diet, exercise routine, degree of insulin sensitivity, or a host of other factors. However, there are five main periods related to the infusion. These are breakfast, lunch, dinner, evening, and the time when the patient is asleep. A patient can choose a preferred time for infusion during one of these time periods. Typically, a patient requires a high insulin doses in the morning, and less around 4-6pm, then more after 12am to counter regulatory hormones during the night. Different patients also exhibit different peak times of BG levels. Although there are exceptions preventing adherence to a rigorous schedule, a patient still has his/her own schedule pattern based on the functions that the insulin pump can provide. We reasonably believe that each patient exhibits a pattern that is distinguished enough that it may be used to identify abnormal events.

C. Data Features

Our assumption is that history records are helpful in the prediction of the insulin dosage of the same patient. This is true for most patients. Having this in mind, related features were extracted. The features we considered to be relevant to our regression model are: Time, Estimate Bolus, Target High BG, Target Low BG, Carb Ratio, Insulin Sensitivity, Carb Input, BG Input, Correction Estimate, Food Estimate, Active Insulin, Daily Total Insulin, Basal Pattern Name, Index, Basal Rate, and Start Time. All of these features are expected to have a strong correlation with the timestamps of the records. We will use some of them in our detection models.

IV. Details of Our PIPAC Scheme

In this Section, we present our access control scheme in detail. If our model returns "Fail", the dosage will not be accepted by the insulin pump, and an alarm will be issued to the patient as well. Our scheme can defend against the two kinds of attacks that we have outlined.

A. Intuitive Solution

A simple public key pair can address this issue because each device is certificated by the vendor. Both pump and read/controller can be installed with a certificate to solve the authentication issue. The whole point of certification is no trusted third party online all the time. A simple public-key authentication is needed only once to authenticate the pump and the reader/control. All remaining operations can be done with a shared secret in symmetric encryption. The user code can be used as another parameter to set up the shared secret. In the meantime, we can encrypt the wireless control link easily. Another concern is that if every device needs to maintain a public key pair, it is a burden for patients having several devices due to the maintaining fee. Also, the patients do not want the vendor (knowing all the SN) to have super power and control their devices and data.

TABLE I
NOTATIONS DESCRIPTION IN PIPAC SCHEME

Notation	Description
$Bolus_p$, $Basal_p$	Predicted Bolus and Basal rate
CB, Bo	Cumulative bolus dosage from Δ_{st}, Bolus dosage to be checked
Δ, Δ_{st}	Time window, Start Time of each Δ
SR_l, SR_u	Lower bound and upper bound of safety range
TL, EB, Ba	Time label, Estimate bolus, Basal rate to be checked
BG_h, BG_l,	Target high BG, Target low BG,
CR, IS	Carb ratio, Insulin sensitivity
T, CI, BG_i,	Time, Carb input, BG input
CE, FE	Correction estimate, Food estimate
AI, OT	Active insulin, Operation type
PN, Index	Pattern name, Index in pattern
R, ST	Basal rate, Start time of one rate
D, TDI	Dosage, Total daily insulin

B. Overall Detection Model

The goal of our scheme is to identify abnormal infusions of bolus dosage, basal rate, and total daily insulin. Table I summarizes the notations used in the rest of the paper.

We use the Mean Squared Error (MSE) to measure the performance, which is given in equation (1). The error is the difference between the estimated value and the real value, where $\bar{m}$ is the test sample size.

$$MSE = \frac{1}{\bar{m}} \sum_{i=1}^{\bar{m}} (f(u_i - v_i))^2. \quad (1)$$

The squared correlation coefficient (SCC) is the predictive percent of behavior in the output that can be explained by the input. If the SCC value is between 70% to 100%, it is considered to have a strong relationship. By any regression method, we only can predict a value. Instead, we want to obtain a safety range. According to the definition of MSE, we define the safety range SR for bolus dosage and basal rate as follows.

Definition 1 :

$SR = [SR_l, SR_u]$, where $SR_l = Y - 2\sqrt{MSE}$, the $SR_u = Y + 2\sqrt{MSE}$, and Y is the regression output for an input vector.

Regardless of the values of bolus dosage and basal rate, we will use the above safety range SR instead.

C. The Detection Model for Abnormal Bolus Dosage

As illustrated in Fig. 1, the bolus doses (blue dotted lines) are discrete. A patient's records can be denoted as a vector: $x =< TL(x),\ EB(x),\ BG_h(x),\ BG_l(x),\ CR(x),\ IS(x),\ CI(x),\ BG_i(x),\ CE(x),\ FE(x),\ AI(x),\ T(x) >$, representing Time label, Estimate Bolus, Target High BG, Target Low BG, Carb Ratio, Insulin Sensitivity, Carb Input, BG Input, Correction Estimate, Food Estimate, Active Insulin and Time, respectively. For $TL(x)$, we may represent one day as [1-24], [1-12], or [1-8]. For other features, we use the original values from the patient's records. Many patients calculate their estimated bolus using bolus wizard function, which determines the estimated bolus according to the following rule:

- If $BG_i(x) > BG_h(x)$, $EB(x) = \frac{BG_i(x) - BG_h(x)}{IS} + \frac{CI}{CR} - AI(x)$;
- If $BG_i(x) < BG_l(x)$, $EB(x) = \frac{BG_i(x) - BG_l(x)}{IS} + \frac{CI}{CR} - AI(x)$;
- Otherwise, $EB(x) = \frac{CI}{CR} - AI(x)$.

To deliver one bolus, a patient has to enter "BG Input" and "Food Estimate" values. Considering "BG Input" as a feature, our scheme has the close-loop property. Based on the patient pattern, we choose the support vector machine (SVM) [24] regression model to predict bolus dosages.

In our SVM based design, we select the best hyperplane representing the largest separation, or margin, between the two classes. Hence, we choose the hyperplane such that the distance from it to the nearest data point on each class is maximized. The optimization problem to maximize the margin with kernel trick is formulated as follows:

$$\begin{aligned} &min\{\tfrac{1}{2} w^T w + C \textstyle\sum_{i=1}^{l} \xi_i\} \\ &subject\ to : q_i(w^T \varphi(p_i) + b) \geq 1 - \xi_i,\ \xi_i \geq 0. \end{aligned} \quad (2)$$

where q_i is either 1 or -1, indicating the class to which the point p_i belongs. Each p_i is a n-dimensional real vector. $C(>0)$ is the penalty parameter of the error term. In equation (3), w is also in the transformed space, and $w = \sum_i a_i q_i \varphi(p_i)$. Dot products with w for classification can again be computed by the kernel trick, i.e., $w \bullet \varphi(p) = \sum_i a_i q_i k(p_i, p_j)$. Hence, once we obtain C and γ that maximize the margin, we obtain the SVM of normal behavior. The kernel function $k(p_i, p_j) = \varphi(p_i)^T \varphi(p_j)$. In our work, we use a radial basis function as the kernel function: $k(p_i, p_j) = exp(-\gamma \|p_i - p_j\|^2),\ \gamma > 0$.

The use of SVM requires user-defined penalty parameter C for error and kernel specific parameters γ. We use a genetic algorithm (GA) [25] to get the optimal C and γ. After we obtain the optimal parameters (i.e., the best model), we test it using additional data and get MSE. After having the MSE and the $Y = Bolus_r$ for an input vector x, we can calculate the safety range SR of bolus dosage within time window Δ. Then, we check whether $EB(x)$ is 0 or not. If 'No', we record the $T(x)$ as Δ_{st} and initiate $CB = Bo$. If CB falls out of SR, it is an abnormal bolus dosage and an alarm will be sent to the patient. Otherwise, we check whether $T(x)$ is earlier than $\Delta_{st} + \Delta$. If 'YES', we update the cumulative bolus dosage CB from the start time of Δ_{st} by adding the bolus dosage Bo. If the updated CB falls out of SR, it is an abnormal bolus dosage and an alarm will be sent to the patient. Otherwise, it is considered as a normal bolus dosage. The detection model is presented in Algorithm 1.

D. The Detection Model for Abnormal Basal Rate

As we can see in Fig. 1, the basal rates (black solid line) are slightly different during different time periods of a day. In addition, the basal rate follows certain rules. Because the basal rate within one day is a piecewise function, we choose the SVM to predict the basal rate. For basal rate prediction, we only need some records from the patient dataset. The data can be denoted as a vector: $w =< TL(w),\ PN(w),\ Index(w),\ R(w),\ ST(w) >$, representing Time label, Pattern Name, Index, Rate, and Start Time, respectively. Regarding $TL(u)$, we label the real Time according to time interval of the Pattern. For example, if the time is 1:00pm and

Algorithm 1 Abnormal Bolus Dosage Detection

Input: Vector x to predict, Bo to be checked, Δ_{st}, CB;
Output: Pass or Fail;
Get best C and γ through GA method off-line;
Get SVM model using best C and γ;
Predict $Bolus_p$ for Vector x using SVM regression and get MSE;
Calculate the SR for Δ;
if $EB(x)$ is not 0 **then**
  $\Delta_{st} = T(x)$, $CB = Bo$;
  if CB falls in SR **then**
    RETURN PASS;
  else
    RETURN FAIL;
else
  if $T(x) < \Delta_{st} + \Delta$ **then**
    $CB = CB + Bo$;
    if CB falls in SR **then**
      RETURN PASS;
    else
      RETURN FAIL;
  else
    RETURN FAIL;

Algorithm 2 Abnormal Basal Rate Detection

Input: Vector w to predict, Basal rate Ba to check;
Output: Pass or Fail;
Get best C and γ through GA method off-line;
Get SVM model using best C and γ;
Predict $Basal_p$ for Vector w using SVM regression and get MSE;
Calculate the SR;
if Ba falls in SR **then**
  RETURN PASS;
else
  RETURN FAIL;

it falls in the fifth interval of the pattern, we label the time as 5. $ST(w)$ should be divided by 3600000, which changes its unit from millisecond to hour. We use the similar method to get optimal parameters and MSE. After we obtain the MSE at the testing phase and the $Y = Basal_r$ at the detection phase, we can calculate the safety range SR of basal rate at this time. If the basal rate Ba to be checked falls out of the SR, it is an abnormal basal rate and we will send an alarm to the patient. Otherwise, it is considered as a normal basal rate. We present our model in Algorithm 2.

E. The Daily Total Insulin Dosage Monitoring Model

Before we design the detection scheme, we have verified that the total insulin dose follows the normal (Gaussian) distribution by Shapiro-wilk test. Thus, we can determine the normal total daily insulin dose region according to the properties of Gaussian distribution. For example, for a confidence of 99.7%, the safety range of total daily insulin dose is $[E - 3\sigma,\ E + 3\sigma]$. Here, E is the mean of the total daily insulin dose in 3 months and σ is the standard deviation of the total daily insulin dose in 3 months.

Algorithm 3 Abnormal Dosage Detection Process

Input: Vector s;
Output: Pass or Fail or Deactivation;
if $BG_i \geq 250$ **then**
  RETURN Deactivation;
else
  if $BG_i \leq 40$ **then**
    deliver an alarm to the patient;
  else
    if PASS Algorithm 1 or 2 by $OT(s)$ and Time is not 12:05am **then**
      RETURN PASS;
    else
      if Time is 12:05am **then**
        if TDI is in safety range **then**
          RETURN PASS;
        else
          RETURN FAIL;

(a) Communications with our insulin pump without Medtronic's software

(b) Our pump

Fig. 6. Our real insulin pump test-bed

F. Combining The Three Models Together

To combine the three models together, we use a vector $s =< OT(s),\ T(s),\ \Delta(s),\ D(s),\ TDI(s) >. < OT(s),\ T(s),\ \Delta(s),\ D(s),\ TDI(s) >$, representing Operation Type, Time, Time interval, Dosage, and Total Daily Insulin, respectively. Operation Type includes bolus or basal, and Time is the event time. Δ is a fixed time window. Dosage is the actual dosage. Total Daily Insulin is the actual value. If the BG_i is higher than 250(mg/dl), it is an emergency: deactivate PIPAC scheme. If the BG_i is lower than 40(mg/dl), deliver an alarm to the patient. Otherwise, choose the Algorithm 1 or 2 by the Operation Type $OT(s)$. After this, we check the TDI every 24 hours (at 12:05am). Algorithm 3 implements this scheme.

V. Performance Evaluation

We conduct experiments using real patient data to evaluate the performance of our scheme. Fig. 6 shows our insulin pump system.

A. Experimental Setup for Support Vector Machines

SVM is a form of supervised learning, which provides an effective way to predict bolus dosage and basal rate. In

TABLE II
BOLUS DOSAGE TEST RESULTS USING NON-LINEAR SVM REGRESSION

Add missing data?	Time label	best$C$	bestγ	MSE	SCC
Yes	48	5.4062	0.0009	0.0006	0.9990
Yes	12	6.9513	0.0134	0.0022	0.9988
Yes	8	44.05	0.0029	0.0011	0.9995
No	48	3.5472	0.0334	0.0079	0.9953
No	12	9.43	0.1345	0.0407	0.9758
No	8	7.65	0.014	0.0033	0.9980

this work, we design an efficient dosage prediction scheme using multiple SVMs. The use of SVMs requires setting user-defined parameters such as C, type of kernel, and γ. The SCC and MSE values were compared to choose a suitable time label methods. In our experiment, we choose the radial basis function as the kernel function. In addition, we use a GA in combination with k-fold (k=5) cross validation scheme [26] to get the optimal parameters C and γ for a non-linear SVM regression using kernel function. After obtaining the best model using the optimal parameters, we test it using additional data.

B. Experiments for Abnormal Bolus Dosage Detection

1) Experimental Results: In our experiments, we first pre-process the patient's records. The total sample size is about 500 for each patient. We use 80% of the samples to train the SVM model, and the remaining 20% to test it. After we use a GA to get the optimal parameters C and γ, we use them to obtain the optimal SVM model for each patient. Then we test it. Table II shows the best parameters and the test results including the MSE and SCC for patient A. We then use a linear SVM model to repeat our experiments.

Table III lists the MSE and SCC of patient A using the linear SVM regression scheme. Comparing Table II and III, we can see that a non-linear SVM is more suitable for Bolus dosage prediction. In addition, the real time labeled as [1-48] within a day gives a better result for patient A. We choose the non-linear SVM to predict the Bolus dosage for patient A, and the best MSE that we get by using the near optimal linear SVM regression is 0.0006. We find that $[Bolus_p - 2\sqrt{0.0006}, Bolus_p + 2\sqrt{0.0006}]$ is the safety range for that time window Δ. Recall that SCC = 70% to 100% is considered as a strong relationship. In our scheme, the best SCC is greater than 99%. This means that we can use the SVM regression to predict a patient's bolus dosage in real time, according to their previous bolus dosage pattern. We also repeat these experiments for other patients. Table IV shows the results.

2) Parameters Update Policy: Our scheme can monitor the "Raw-Type" data in logs and capture changed settings. If there is no configuration change to insulin sensitivity, carb ratio, target low BG and target high BG, the SVM regression model is adjusted every 90 days to handle patient dynamics. A subset of the previous 90-day history is used for training, and the new regression is used for the next 90-day interval. After the adjustment, the corresponding parameters C and γ are also changed. When the patient is sick, the parameters adjustment cycle can be changed from 90 days to one week.

TABLE III
BOLUS DOSAGE TEST RESULTS USING LINEAR SVM REGRESSION

Add missing data?	Time label	MSE	SCC
Yes	48	0.0022	0.9988
Yes	12	0.0198	0.9894
Yes	8	0.0280	0.9866
No	48	0.0383	0.9767
No	12	0.0394	0.9761
No	8	0.0409	0.9751

TABLE IV
BOLUS DOSAGE TEST RESULTS USING NON-LINEAR SVM REGRESSION

Patient label	best MSE	best SCC
A	0.0011	0.9874
B	0.0011	0.9895
C	0.0013	0.9848
D	0.0009	0.9973

TABLE V
BASAL RATE TEST RESULTS USING NON-LINEAR SVM REGRESSION

Patient label	best$C$	bestγ	MSE	SCC
Patient A	83.73	26.8	0.000355	0.968229
Patient B	2.20	2.80	0.000445	0.958320
Patient C	2.00	3.00	0.000438	0.958636
Patient D	34.4	5.5	0.000356	0.968123

TABLE VI
BASAL RATE TEST RESULTS USING LINEAR SVM REGRESSION

Patient label	MSE	SCC
Patient A	3.03487	0.010829
Patient B	0.00667	0.555384
Patient C	3.01424	0.013546
Patient D	2.54386	0.018783

C. Experiments for Abnormal Basal Rate Detection

1) Experimental Results: In our experiments, we first pre-processed the patients' records. The total sample size is about 600 for each patient. We use 80% of the samples to train the SVM model, and the remaining 20% to test it. We use a similar approach as the previous subsection. For patient A, the best C=83.73 and the best γ =26.8. After we obtain the best model using the optimal parameters, we run tests. Table VI shows the best parameters and test results including the MSE and SCC for four patients. We then use a linear SVM model to repeat the experiments.

Table VII lists the MSE and SCC of 4 patients using the linear SVM regression scheme. Comparing Table VI and VII, we can see that non-linear SVM regression is more suitable for Basal rate prediction. When we use the non-linear SVM to predict the Basal rate, for patient A, the MSE is close to 0.0004. We determine that $[Basal_p - 2\sqrt{0.0004}, \quad Basal_p + 2\sqrt{0.0004}]$ is safety range for the Basal rate. In our scheme,

TABLE VII
ACCURACY OF THE SYSTEM OF FOUR PATIENTS

Patient label	Accuracy
Patient A	99.43%
Patient B	99.12%
Patient C	98.65%
Patient D	98.79%

the SCC is greater than 95%, indicating that we can use this SVM-based scheme to predict patient basal rate in real time, according to their previous basal rate pattern.

2) Parameters Update Policy: Our scheme can monitor the "Raw-Type" and capture changed settings that have. If the "ChangeBasalProfile" is not actively used, the linear SVM regression is adjusted every 90 days if the patient is not sick. When the patient is sick, the parameters adjustment cycle can be set to one week.

The parameters update policy of the Total Daily Insulin Prediction Model is similar to the one in the previous subsection.

D. Experiments using All Data

According to all patients' dataset, we obtain a number of abnormal vectors (including time, bolus dosage, basal rate, etc.) and use them to test our PIPAC scheme. Here, we choose the time window $\Delta = 15mins$. Table VII shows the accuracy of detecting abnormal dosages. Note that the time window is changeable. We recommend the range of the time window is 5mins - 15mins.

VI. DISCUSSIONS

A. Safety Analysis

Under our scheme, for one patient, the maximum error of Bolus dosage is $2\sqrt{MSE}$. For patient A, $2\sqrt{MSE} = 0.048$, suppose the total number of safety ranges we counted is 10, then the total error of insulin is $10 \times 0.048 = 0.48(u)$. This is less than 1u and therefore is negligible. For basal rate, the maximum error is $2\sqrt{MSE}$, and the maximum number dose hours that may be administered in one day is 24. Hence, the total insulin error is $2\sqrt{MSE} \times 24$. For patient A, $2\sqrt{MSE} = 0.04$, hence the total insulin error is $24 \times 0.04 = 0.96(u)$. It is less than 1u and is also negligible. In summary, it is safe to use our scheme.

B. Overhead Analysis

A Medtronic insulin pump operates at 916.5 MHZ. It requires approximately 0.5ms to finish the non-linear SVM regression. The energy consumed is negligible compared with ordinary therapy or communication. However, if we use non-linear SVM regression, it may require several minutes to obtain the optimal C and γ via the GA method when we update the model every 3 months. From this point of view, the linear SVM regression for bolus prediction still has its advantage. Furthermore, the verification time of our scheme is short, which is very important in regards to the patient's convenience. Our scheme needs to store two small records for Basal rate and Bolus dosage detection. In addition, we need to store PIPAC program in the insulin pump. All the storage requirements are acceptable to today's insulin pumps.

C. Security Analysis

1) Defending Against the First Attack: The first attack is to deliver one large overdose in one shot. Since the upper bound of SR is $Y+2\sqrt{MSE}$, and the $2\sqrt{MSE} = 0.048$ is far less than 1u, it is impossible to deliver (in one shot) a dose 1u larger than the estimated dosage. Hence, we can defend against this attack. Since the error of BG testing is far less than insulin sensitivity, we ignore it.

2) Defending Against the Second Attack: If the attacker gradually increases the dose over a period of several days, our system can still defend against this attack. First, BG_i is one of the features being monitored. If the attack happens, BG_i will be lowered. Correspondingly, the predicted bolus SR will be decreased. Hence, the attack will be detected due to a detection of bolus (or basal rate) out-of-range. Second, we monitor the cumulative bolus dosage CB within a time window. It is impossible for the attacker to deliver total bolus greater than SR_u unless BG_i is greater than 250 mg/dl. For basal rate, this kind of attack does not affect the total insulin a lot. Third, our scheme verifies the TDI daily. A suspicious dose can be identified if the TDI falls out of the corresponding safety range. The patient can then check the history log and discover the attack.

3) Defending Against the Radcliffe's Attack: We can monitor: (1) the BG reading from the sensor; and (2) patient's BG_i input. As the BG testing technology may have some errors, we use the following approach: if the difference between (1) and (2) is more than 20%, then we consider there is an intercepting attack between the sensor and the pump. The above approach can not defend against the Radcliffe's attack 100% but can mitigate it.

D. Emergency Situations

It is an orthogonal problem to allow easy access to medical devices under emergencies. Many researchers suggested to use open access operated by clinical staff during emergencies, e.g., in [12], [13], and [15]. To handle the emergency situation, we also can deactivate PIPAC scheme. Some literatures (e.g. in [17] and [19]) focused on the emergency case. Also since a large dosage has a high probability of causing hypoglycemia, doctors or patients try to avoid this from happening. For a patient with larger weight, the maximum dose may be set to a larger dose. Their safety ranges are also set to a larger value. If the patient becomes hypoglycemic, our scheme issues an alarm to the patient, and the patient can ingest some food that is high in sugar to relieve this situation. What's more, in emergency situations, i.e. the BG is over 250(mg/dl) or lower than 50(mg/dl), the safety range will vary accordingly because our scheme is an online prediction scheme rather than a classification scheme. Thus, our PIPAC scheme can cover this case. When the expected dose is larger than the maximal dose limit, the doctor can change the settings. Also, the patients can split a large dose into several smaller doses. We observed this method in the patients' medical records. Even though, in

this paper we still deactivate the PIPAC scheme to allow open access to wireless insulin pumps.

VII. Related Work

Using an easily obtained USB device, Radcliffe [9] was able to capture data transmitted from the computer and control the insulin pump's operations by intercepting wireless signals sent over link 3. He could even cause the monitors to display inaccurate readings with SN of the target device. Barnaby Jack was able to hypothetically deliver fatal doses to diabetic patients [6]. Literature [8] proposes a traditional cryptographic solution (rolling code) and body-coupled communication to protect the wireless link. However, Jack's attack exploits a vulnerability between the Carelink USB and the pump, neither of which can utilize body-coupled communication. Paper [11] establishes a safety-assured implementation of Patient-Controlled Analgesic insulin pump software based on the generic PCA reference model provided by the U.S. FDA. There are also many solutions proposed to address the security issues of IMDs during non-emergency situations. Authors of [12], [13] and [18] proposed to use an additional external device. However, these external devices may become stolen, lost, or forgotten by the patient. The device also discloses the patient's status. Most importantly, this kind of solution adds another device that must be managed by the patient, making it an inconvenient solution for patients especially when diabetic patients already have to wear many devices. Certificate-based approaches have been proposed in [14], but it requires the device to access the Internet and verify certificates. Rasmussen et al. proposed allowing IMDs to emit an audible alert when engaging in a transaction [15]. However, this approach may consume scarce power resources. Our previous work [16] proposed utilizing the patient's IMD access pattern and designs a novel SVM-based scheme to address the resource depletion attack. It uses a classification scheme rather than the regression scheme used here. It is very effective in non-emergency situations. In another previous work [17], we proposed a novel Biometric-Based two-level Secure Access Control scheme for IMDs when the patient is in emergency situations (such as a coma). [20] proposed using friendly jamming to prevent adversarial access to IMDs. In addition, literature [21] deals with jamming attack, which can be used to handle the Radcliffe's attack in our paper. Literatures [22-23] focus on security of health care systems.

VIII. Conclusion

For wireless insulin pump systems, there are two kinds of harmful attacks that are related to dosages, and the vulnerability comes from no authentication on wireless link 5. In this paper, we proposed a PIP based access control scheme that can defend against these attacks. Our scheme leverages the patient dosage history to generate two SVMs models, and then we determined the safety ranges for each input vector. We employed real patient data to test our scheme, and the results show that our scheme works well and exhibits good performance. Our scheme can be generalized to other infusion systems as well.

Acknowledgment

We would like to thank Benjamin West for discussion with us about the patient's behavior and normal clinical actions. Also our thanks are given to Min Xiao and Oleg Sokolsky for comments. This work was supported in part by the US NSF under grants CNS-0963578, CNS-1022552, CNS-1065444, IIS-1231680, CNS-1239108, and CNS-1035715.

References

[1] "2007 national diabetes fact sheet," http://www.cdc.gov/diabetes/pubs/pdf/ndfs 2011.pdf.
[2] "US healthcare equipment and supplies - diabetes." http://www.research.hsbc.com.
[3] "Insulin pumps - global pipeline analysis, opportunity assessment and market forecasts to 2016, GlobalData," http://www.globaldata.com.
[4] http://www.tudiabetes.org/forum/topics/more-interesting-facts-on.
[5] FDA, "Medical Devices: Infusion Pumps," 2010, http://www.fda.gov/infusionpumps.
[6] http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack.
[7] National Diabetes Information Clearinghouse, http://www.diabetes.niddk.nih.gov/dm/pubs/hypoglycemia/index.aspx.
[8] C. Li, A. Raghunathan and N. K. Jha, "Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System", in *Proc. of the 13th IEEE Intl. Conf. on e-Health Networking, Applications and Services*, pp. 150-156, 2011.
[9] J, Radcliffe. https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11 _Radcliff_Hacking_Medical_Devices_WP.pdf
[10] D. Halperin et al., "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses," In *Proc. of the 2008 IEEE Symp. on SP'08*, pp. 129-142, 2008.
[11] B. Kim et al., "Safety-Assured Development of the GPCA Infusion Pump Software," In *Proc. of the Intl. Conf. on EMSOFT'11*, Taipei, 2011.
[12] P. Inchingolo, S. Bergamasco, and M. Bon, "Medical data protection with a new generation of hardware authentication tokens," in *Proc. of Mediterranean Conf. on Medical and Biological Engineering and Computing*, 2001.
[13] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: new directions for implantable medical device security," in *Proc. of the 3rd Conf. on Hot topics on security*, pp. 1-7, 2008.
[14] E. Freudenthal, R. Spring, and L. Estevez, "Practical techniques for limiting disclosure of RF-equipped medical devices," in *Proc. of Engineering in Medicine and Biology Workshop*, pp. 82-85, 2007.
[15] K. B. Rasmussen et al., "Proximity-based access control for implantable medical devices," in *Proc. of ACM CCS '09*, pp. 410-419, 2009.
[16] X. Hei et al., "Defending Resource Depletion Attacks on Implantable Medical Devices," in *Proc. of IEEE Globecom'10*, pp. 1-5, 2010.
[17] X. Hei and X. Du, "Biometric-based Two-level Secure Access Control for Implantable Medical Devices during Emergencies," in *Proc. of IEEE INFOCOM'11*, pp. 346-350, 2011.
[18] S. Gollakota et al., "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proc. ACM Conf. SIGCOMM'11*, pp. 2-13, 2011.
[19] J. Sun et al., "HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare," in *Proc. of ICDCS'11*, pp. 373-382, 2011.
[20] F. Xu et al., "IMDGuard: Securing implantable medical devices with the external wearable guardian," In *Proc. of IEEE INFOCOM'11*, Shanghai, China, Apr. 2011.
[21] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," In *Proc. of USENIX Security Symp.'09*, 2009.
[22] G. Hackmann et al., "Reliable Clinical Monitoring using Wireless Sensor Networks: Experience in a Step-down Hospital Unit," in *Proc. of ACM Conf. on SenSys'10*, Zurich, Switzerland, 2010.
[23] X. Liang et al., "Enabling Pervasive Healthcare with Privacy Preservation in Smart Community", in *Proc. of IEEE ICC'12*, Ottawa, Canada, 2012.
[24] C. Cortes and V. Vapnik, "Support-vector networks", in *Journal of Machine Learning*, vol. 20, no. 3, pp. 273-297, 1995.
[25] http://en.wikipedia.org/wiki/Genetic_algorithm.
[26] http://en.wikipedia.org/wiki/Cross-validation_(statistics).