Using Bowel Sounds to Create a Forensically-aware Insulin Pump System

Nathan L. Henry Jr.[†], Nathanael R. Paul[†‡], Nicole McFarlane[†]
[†]University of Tennessee, Department of Electrical Engineering and Computer Science
[‡]Oak Ridge National Laboratory
[nlh, pauln, mcfarlane]@utk.edu

***Abstract*—Patients are increasingly reliant on implantable medical device systems today. For patients with diabetes, an implantable insulin pump system can greatly improve their quality of life. As with any device, these devices can and do suffer from software and hardware issues, often reported as a safety event. For a forensic investigator, a safety event is indistinguishable from a potential security event. In this paper, we propose a new sensor system that can be transparently integrated into existing and future electronic diabetes therapy systems while providing additional forensic data to help distinguish between safety and security events.**[1]

I. Introduction

Diabetes affects over 25.8 million people in the United States or approximately 8.3% of the U.S. population [CDC11]. In 2007, the estimated cost of diabetes care in the United States was $174 billion dollars including direct medical costs and indirect medical costs (e.g., disability, work loss, premature mortality). Various therapy methods exist to treat diabetes. For patients with type 2 diabetes, diet and exercise can typically help control blood glucose levels. For type 1 diabetes, patients require insulin therapy. This insulin can be administered via syringes, insulin pens, or electronic insulin pumps. Patients are increasingly using electronic insulin pump systems as a form of treatment.

These electronic insulin pump systems provide great benefits to patients. For example, they allow patients to take fast acting insulin continually throughout the day. This allows insulin delivery to better mimic pancreatic insulin delivery. These pumps now use wireless communication to interact with PCs, remote controls, blood glucose meters, and continuous blood glucose monitoring systems (in the future, they will interact with cars and other mobile systems [Ford11]).

Recently, there have been several reports and demonstrations of unauthorized remote access to insulin pump systems [Benedict04], [Klonoff08], [Radcliffe11], [Jack11], [Li11]. Newer insulin pump system architectures are completely dependent on wireless communication. For example, some patch pump systems have no physical interface on the pump component. A user must use a remote control to issue any commands or to interact with the pump.

Several solutions have been suggested to prevent and detect implantable medical device security breaches. While our proposed bowel sound system does not actively prevent security breaches, active prevention is an eventual goal. Some have used past glucose trends to detect anomalous insulin pump system behavior [Hei13]. Anomalous detection is promising in that the false positive rate (the rate at which a system identifies malicious abnormal usage when the pump usage is benign) is less than one percent. In practical use, a false positive would happen approximately once every 20-25 days (assuming a patient eats three meals a day and eats periodic snacks). This approach could potentially result in incorrect patient operational use.

As implantable medical devices make use of encrypted communication, key management is an emerging topic [Chang12], [Schechter10]. Dealing with key management in an emergency situation is especially difficult with respect to safety. Li takes a simpler approach by suggesting rolling codes just as they are used in garage doors to protect against unauthorized entry [Li11]. This is a simple effective approach to protect against unauthorized access, but emergency access remains an issue.

In 2011, Gollakota introduced an independent device that acts as a shield and transmitter [Gollakota11]. An independently worn secure communication device has been successfully prototyped for a cardiac device. Experimentation is needed to verify if the same approach would work for externally worn but subcutaneously implanted devices (e.g., insulin pump systems). For battery-powered systems, jamming would drain the battery resulting in more frequent battery changes. For insulin pump systems, requiring the patient to replace an expired battery more often may not be an acceptable burden.

Others have proposed using a wrist-worn watch [Sorber12a] or a smart card [Sorber12b] to protect against unauthorized communication. Some patients with diabetes have previously used a wrist watch for blood glucose control (the Glucowatch helped in non-invasive blood glucose control [Glu01]). Similarly, a smart card could provide widely available access to stronger secu-

[1] This publication was made possible by Grant Number HHS 90TR0003/01. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the HHS.

rity primitives than what is currently available in current insulin pump systems. This is similar to the approach that some blood glucose monitoring devices use when pairing a blood glucose monitor to coded test strips. One challenge to the adoption of these approaches is that portions of the patient population will not be able to use the device. Some patients will not own or use a watch, and others will not own a device capable of using a smart card (e.g., a phone).

All of these systems are promising. However, many systems that prevent security issues also require that patients make a significant operational change in how they use their medical device. When a significant operational change happens, this may cause a safety issue. Our goal is to provide security without weakening safety. For our initial work, we provide improved forensic information about an implantable insulin pump system. This improved forensic information could serve as a deterrent to potential device misuse. A patient using this device would not need to operationally change how she uses the pump.

In the future, we will seek to support a sensor system to help prevent device misuse in real-time, but our prioritization on safety would preclude a significant operational change. We suggest prior usability and device effectiveness studies before this type of system design change in order to ensure patient safety.

The most relevant forensic incident about intentional insulin pump misuse was in 2004 [Benedict04]. A nurse used an insulin pump to deliver fatal doses of the drug laudanosine. The patient had type II diabetes but relied on an insulin pump for blood glucose control. In this case report [Benedict04], the authors cite the potential for misuse of an insulin pump remote control. Given the increase of patients with diabetes and the growing use of insulin pump systems, the authors theorize that their misuse in homicides and/or suicides may become more prevalent.

While this earlier case provides specific evidence of malfeasance against a patient with an insulin pump system, we favor safety in the design of a system that attempts to mitigate this malfeasance. The risk of negative safety events is well known [Meier10]. A potential safety issue that may arise from implementing a security mitigation is a design tension.

Today, an insulin pump security incident could occur where an insulin bolus is used to cause *hypoglycemia* (i.e., a low blood glucose state that could lead to a diabetic coma). This security event is virtually indistinguishable from a safety event (e.g., where a patient accidentally overdoses). In the rest of this paper, we introduce a new type of insulin pump sensor system that provides data about patient eating behavior. Our eventual goal is to create a system that uses eating instances in real time to prevent negative security events. This paper describes our initial step in this process: using eating data to demonstrate a new design for a forensically-aware insulin pump system that can detect potentially malicious events.

Our contributions include (1) a forensically-aware insulin pump system that can help a forensic investigator focus on the events that could potentially indicate malfeasance; (2) as a side effect, we provide data from detected bowel sounds that can improve patient health; (3) we introduce a seamless method to integrate the bowel sound detection sensor into an insulin pump system; and (4) we introduce forensic rules that could be used to detect anomalous system use (i.e.,when the patient′s own device is used against them).

Security Model. A security event from the misuse of an insulin pump system could cause euglycemia (a normal blood glucose value), hypoglycemia (a low blood glucose value), or hyperglycemia (a high blood glucose value). Euglycemia is normal, and the desired state of the patient. Our ultimate goal is to protect against hypoglycemia and hyperglycemia.

While hyperglycemia is harmful, the greater danger is hypoglycemia. A patient can become desensitized to hypoglycemia, and it can quickly negatively affect the patient. As we prioritize hypoglycemia, we make the following assumptions:

1) We focus on those that can remotely interact with devices of the system (anyone with physical access to a patient is not of primary interest). Those that use a patient′s own device to remotely interact with other parts of the system are of interest.
2) Detection of conditions that can lead to hyperglycemia is less important than hypoglycemia, but any approach that can also detect hyperglycemia will be a potential solution candidate.
3) There are operational changes that could accomplish hypoglycemia and avoid detection policies. For example, a policy that identified a large insulin bolus given in the absence of food intake would not detect several smaller insulin boluses which could achieve the same amount of insulin delivery. To counter this issue, improved forensic policies could be implemented. For example, events could be marked where the intake of insulin over a period of time crosses a threshold where the patient has not eaten (i.e., keep the insulin in the body, insulin on board, at a safe level). This would stop the delivery of several smaller insulin boluses that sum to an amount that would be greater than a single safe insulin bolus.

II. Insulin Pump Forensic Activity

Because blood glucose control is critical to addressing health complications related to diabetes, current insulin pumps record blood glucose data and information related to blood glucose data. Patients and physicians use this data to improve patient blood glucose control through reprogramming the pump′s insulin delivery. This data can be broken into two categories. First, the insulin pump, as the main system actuator device, records user information including user-adjusted settings, insulin basal rates, amount of delivered insulin, errors, and alarms. Second, many other system components generate data including: a continuous glucose monitor (CGM), a glucose meter, or the patient (e.g., by marking the type of food or amount of carbohydrates consumed).

We can use insulin pump system data to better address the factors that contribute to a high or low blood glucose value. In modern insulin pump systems, a patient will issue a bolus to correct a high blood glucose value, or she will give a bolus in response to, or in anticipation of, the consumption of food. If an insulin bolus causes hypoglycemia, it is not a straightforward process to determine whether the bolus was issued to prevent a case of *hyperglycemia* (high blood glucose) or in conjunction with food consumption. In fact, a patient could issue a bolus mistakenly. Improved logging of bolus events is needed. Thus, we explicitly define three forensic goals for a forensic investigator:

1) To determine what steps led to a negative patient event (e.g., miscounting of carbohydrates causes patient to issue high amount of insulin).
2) To determine what specifically caused a negative patient event (e.g., overdose of insulin caused hypoglycemia).
3) To take the steps that led to a negative patient event and the specific causes for that event and to determine the type of negative patient event. The event will either be a safety event or a security event.

In this paper, we propose a system to forensically detect and identify the presence or absence of a common patient activity - eating, and we use this data to determine if the patient is likely to experience an unsafe blood glucose level (hypoglycemia or hyperglycemia). Factors that could have an effect on glucose levels include food consumption, body temperature, odors, heart rate, body acoustics, exercise, and skin moisture.

Food consumption is one of the primary methods by which a patient alters her blood glucose level. Our system uses bowel sounds to allow a forensic investigator to determine if a patient is eating. From the knowledge of food ingestion, an investigator could label an increased insulin delivery as anomalous and decide to investigate how the anomalous insulin delivery is related to a safety event. For example, a patient could measure her blood glucose and note a low (hypoglycemic) value of 48 mg/dL. If the system had also detected that this patient had not eaten for 8 hours and that she had just issued 25 units of insulin, then the system could mark the 25-unit insulin bolus for further investigation.

Fig. 1 shows an example graph of a patient′s blood glucose (the data has been populated with realistic but artificial values). This graph shows eating assumptions made by the software of a leading insulin pump manufacturer. The day is broken into periods corresponding to different meals. Patient behavior will not always comply. Even if the system used associated bolus data to infer food consumption, the person giving the bolus is responsible for marking the bolus as one for food consumption. A forensic investigator does not have a reliable way to know why a large bolus is warranted. If the investigator could know when food consumption had taken place, this would help explain an instance of a potentially larger bolus.

In Fig. 2, a patient receives a bolus at 1:00 am. The patient is asleep during this time. A forensically-aware pump that could detect and record patient eating instances would allow forensic investigators to note a possible case of hypoglycemia. The possibility of hypoglycemia coupled with the fact that the bolus was given early in the morning when a patient is assumed to be asleep could indicate an unauthorized bolus. At 6:30 am the patient′s glucose level rises. This could be indicative of a meal or of the dawn phenomenon [ADA13]. With a forensically-aware pump, a forensic investigator may infer the absence of a meal and a possible case of hyperglycemia. At 6:30 pm, a bolus is given without a corresponding meal. Abnormal bolus patterns that do not correspond with a meal could be indicative of a forgotten bolus, radio interference, or unauthorized third party interaction with the insulin pump.

As a secondary benefit, medical professionals could use this eating data to identify patient trends and identify vectors of treatment that could increase insulin pump system effectiveness. For example, a nurse may notice that a patient experiences hyperglycemia from continually failing to issue an insulin bolus for food that would require insulin.

We demonstrate the feasibility of our approach through experimentation. Eating is a critical factor in a patient′s blood glucose level. This information correlated with bolus and blood glucose records can yield much forensic information. Through these experiments, we show that we are able to determine when a person is eating when they transition from a fasting (has not eaten food for at least two hours) to a fed state. The transition from a fasting to fed state should be the simplest to

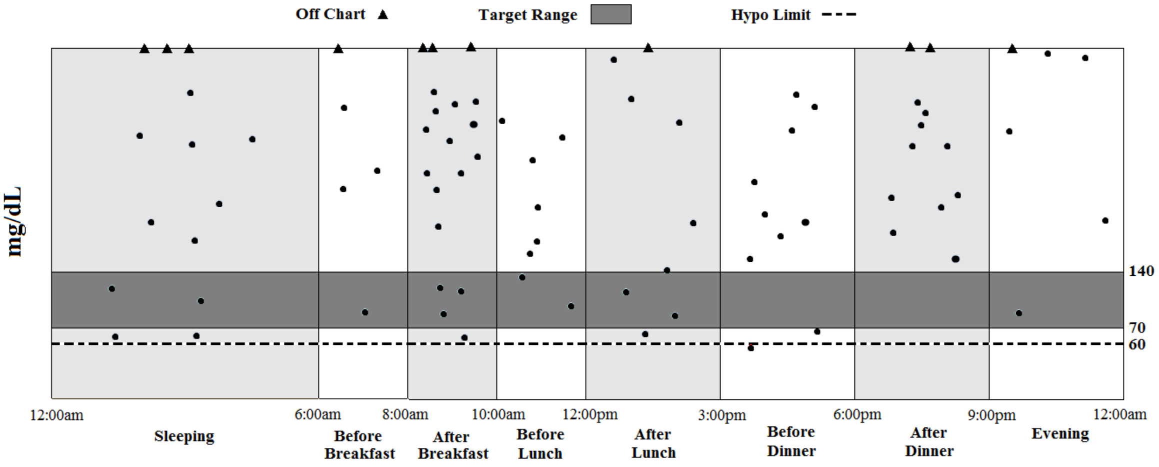

Fig. 1. **Example Blood Glucose Report.** An example report that is based on a leading manufacturer′s insulin pump system software. Dots represent finger sticks (blood glucose checks) taken over the period of a month. Specific periods of the day are assumed to correspond to a meal.

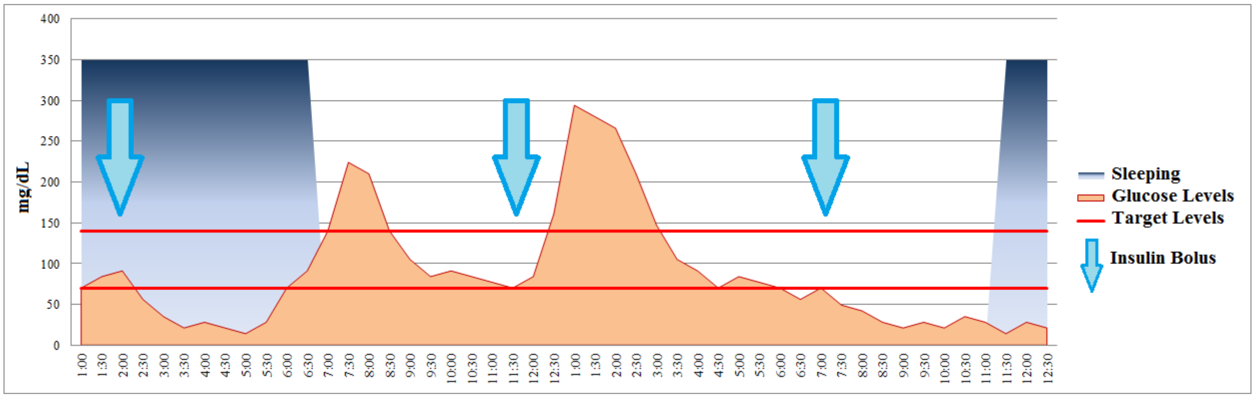

Fig. 2. **A Day in the Life of a Patient.** This figure shows an example patient′s blood glucose through a day. An increase in forensic information can improve the ability to determine what contributed to a high or low blood glucose value.

detect. Later experiments should be run on test subjects that are not in a fasting state.

III. Experimental Setup

Today, physicians and nurses use stethoscopes to determine the presence of bowel sounds following surgery and during routine physicals. Fig. 3 is an example of a single bowel sound.

Our intuition is that we can use bowel sounds to detect when a patient is eating and use that information to infer system activity that could help in a forensic investigation. In an effort to detect eating instances, we recruited test subjects to eat a meal while we monitored their intestinal activity. We obtained IRB approval for our tests and all volunteers gave their signed consent. For the experimental equipment, we used a Thinklabs ds32a+ stethoscope to record bowel sounds (see Fig. 4). The stethoscope head was set to diaphragm mode (a mode used to detect heart and bowel sounds) and placed in the right lower quadrant of the stomach. The stethoscope head was secured to the abdomen by medical tape and pressure was applied to the stethoscope head via a medical bandage wrapped around the abdomen (see Fig. 4).

In order to encourage the subject to decrease the amount of activity that may cause extra noise, we had subjects sit at a table (they could read or perform other activities that did not include standing or a large amount of movement). Five subjects participated in the experiment. Sounds were recorded from a 2.5 mm output jack on the stethoscope to a 3.5 mm input jack on a PC. Using the PC, we converted the analog signals to a digital signal and recorded the data at 22050 Samples/second in a 16-bit PCM encoding using Audacity (http://audacity.sourceforge.net/). We processed

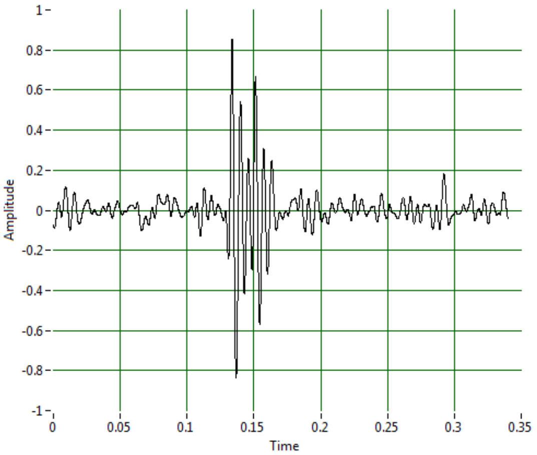

Fig. 3. **A Single Bowel Sound from a Fasting Test Subject.** We consider a patient to have fasted if no food had been consumed within two hours of our experiment.

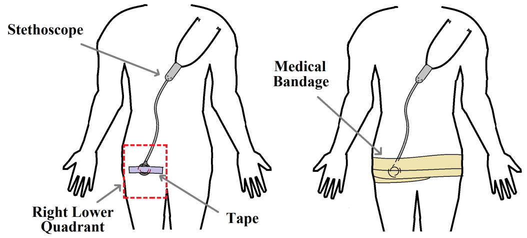

Fig. 4. **Experimental Sensor Attachment**. We positioned the stethoscope head over the subject′s abdomen and used tape to secure the stethoscope head to the body. The medical band supports the stethoscope head and applies pressure to the head to create a better contact point with the body.

the recorded audio signals using National Instruments LabView.

IV. Experimental Approach

To experimentally verify that we can detect eating through bowel sounds, we performed experiments where we recorded patient abdominal acoustic activity before, during, and after food consumption (three stages).

Pre-eating. We use the pre-eating stage to set a fasting baseline - the number of bowel sounds detected in a time interval before eating. We use a simple bowel sound detection scheme to calculate the number of bowel sounds that occur in a five-minute period. For each subject, we first compute a threshold value derived from the recorded fasting data (We detail the threshold computation in the eating phase). Any acoustic signal crossing the computed threshold within a calculated duration is considered a bowel sound.

Different issues can interfere with the recorded fasting data. To avoid any lingering bowel sound activity from previously consumed food, each test subject refrained from eating food for at least two hours before we established the subject′s fasting baseline. Ambient environmental noise can also affect detection of bowel sound activity. Each subject was encouraged to decrease motion (e.g., no talking or walking).

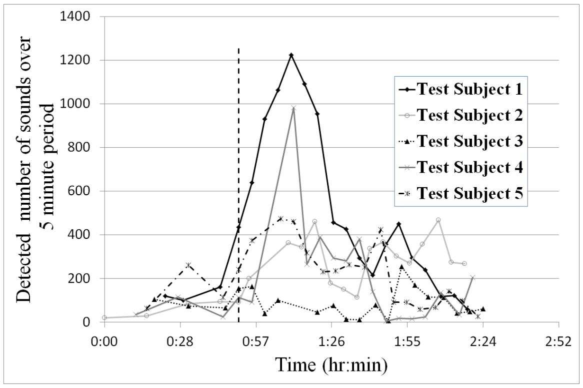

Fig. 5. **Patient Bowl Sounds over 5-minute Period.** Data has been shifted so that the start of every meal will be the same. Each value represents the number of detected bowel sounds over a five-minute period.

After reducing potential interfering noise as we collect data to compute the baseline, we record all of the fasting acoustic activity for three five-minute intervals approximately 10 minutes apart. With this data, we compute the average number of the recorded bowel sounds and record this as the subject′s baseline.

Eating. During the eating stage, we record acoustic activity as a test subject consumes her meal. Similar to the pre-eating phase, we detect bowel sounds over a five-minute period. For successful detection, our algorithm will confirm that a subject is eating when a certain number of bowel sounds is reached within a certain time interval.

After the detection algorithm detects a number of bowel sounds that exceed the computed baseline value, the algorithm will determine that a subject is eating. In our current work, we detect eating when the number of bowel sounds for a 5-minute time interval is 1.5 times the baseline number (determined in the pre-meal stage). An increase in bowel sounds is consistent with what has been observed in previous gastrointestinal research [Craine99] that showed an increase in the number of bowel sounds from the fasting to fed state.

Our initial testing shows the feasibility of the detection approach, and we are currently refining methods to address false positives (Section VI details our strategy for working with detected false positive activities).

Post-eating. After the initial eating period of up to 20 minutes, we continued to record bowel sounds for one hour and thirty minutes after the start of eating. We will use this data in future work to detect when a subject begins to eat from a non-fasting state.

V. Bowel Sound Detection

In our initial work of bowel sound detection, we first attempted to use a single threshold for all five subjects. If any sound recorded from a subject went beyond the threshold value, that sound was deemed to be a bowel sound. We processed the recorded raw data using a 25 Hz low-pass filter. The threshold detection algorithm detects a bowel sound if the filtered signal crosses our determined threshold.

Fig. 3 shows a detected bowel sound. This bowel sound is similar to the sounds from previous research [Craine99]. We found that recorded bowel sound amplitudes varied between each test subject and between individual bowel sounds within each test subject′s dataset. This difference was due to different body types, attachment of the sensor, body position as well as type, amount, and time since last meal or increased physical activity. The variance between each test subject′s bowel sounds indicates that a single global detection threshold may not be suitable. Thus, we use a newly computed threshold for each patient in order to determine if a sound is a bowel sound.

To compute this bowel sound detection threshold, we compute the mean of the filtered fasting data. We then set the threshold to be three standard deviations above the mean value. This computation is performed for each subject.

When the detection algorithm detects a bowel sound, there is a potential for a false positive. In our data (and in previous research [Craine99]), bowel sounds can be characterized according to a time duration. We characterize a bowel sound based on the amount of time a filtered bowel sound remains above the detection threshold value, and we use this value to distinguish between sounds that remain above the threshold for a longer period of time (e.g., talking). We discard any sound that is three standard deviations above the mean bowel sound time duration determined during fasting.

Bowl Sound Detection Results. In each subject′s dataset, the number of recorded bowel sounds increases in the first five-minute interval after the start of the meal. The detected number of bowel sounds rises to approximately 1.5 times the baseline number. When the number of bowel sounds reaches 1.5 times the average of the fasting signal, the subject is eating. The time that this increased number of bowel sounds lasts varies from subject to subject. The number of bowel sounds of four of the subjects began to decline after approximately 45 minutes. This is consistent with what has been observed in past research [Campbell89].

Subject two sustained an increased in the number of bowel sounds after the meal for the remainder of the experiment. While we expect the duration of increased bowel sound activity to be different for each patient, this is a topic for further tests.

The increases in the number of sounds observed in test subject five′s activity at 1:45 and the increase in test subject three at 1:53 can be attributed to a change in position of the subject. Further testing should be used to determine the accuracy of the method on other subjects. Adequately addressing different body positions will require more experimentation, but developing methods for common body positions can have a large impact (e.g., eating detection when the patient is sitting and eating with little movement).

VI. Bowel Sound False Positives and False Negatives

In our testing, we limited patient motion to decrease environmental noise. To be deployed as a sensor in an electronic insulin system, we need to address potential false positives that are caused by patient activity. We evaluated several potential false positive activities including talking, walking, coughing, and a vibrating cellphone.

We found that all four activities have the potential to cause false positives in our simple bowel sound detection scheme. Fortunately, there was a distinct difference in the active frequency ranges of the four activities in comparison to eating. Walking produced a periodic signal dependent on the test subject′s gait. Coughing produced signals with dominant frequencies ranging from 0-50 Hz. Vibrating cell phones had strong frequencies of approximately 200 Hz.

Talking. Of the four false positive activities tested, talking presents the most difficulty. Talking is aperiodic and in a similar frequency range as that of bowel sounds. Fig. 8 shows the average power spectral density (PSD) of talking (i.e., reading aloud) for all five subjects over a five-minute period.

We found that talking centered around two approximate frequencies of 100 Hz and 190 Hz (See Fig. 8). If we can determine that a patient is talking, then a detected talking event could be eliminated as a false positive and labeled as a non-bowel sound. Fig. 9 is the average five-minute PSD of all five subjects 20 minutes after the start of eating. During this time interval, subjects were asked to be silent, subjects were finished eating and the detected number of bowel sounds should have reached its peak. This information should allow us to determine when a patient is talking.

When eliminating talking from the data, we inevitably eliminate bowel sounds that simultaneously occur when the subject is talking. To detect that someone is eating,

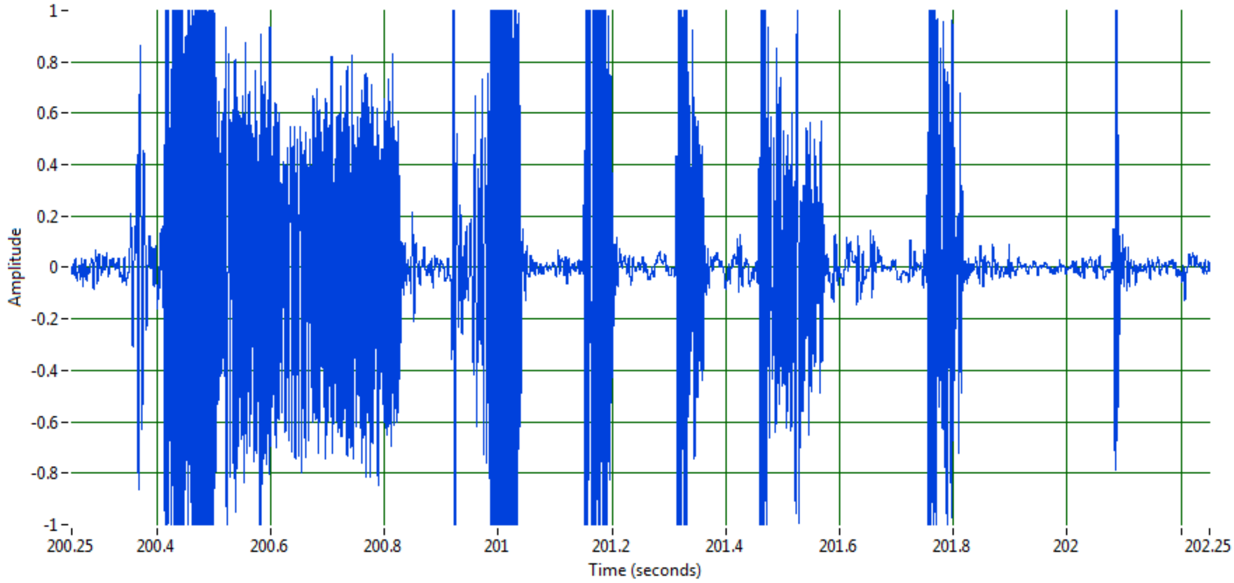

Fig. 6. **Bowel Sound Detection Method:** Raw signal before processing.

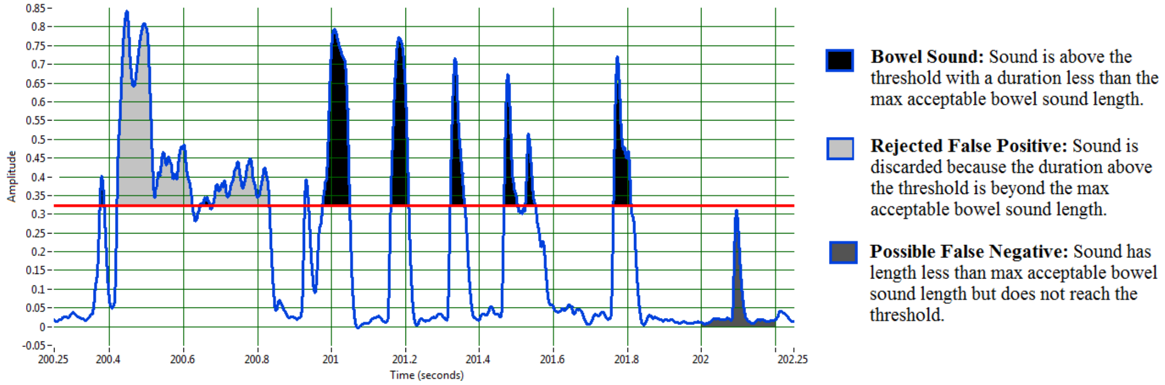

Fig. 7. **Bowel Sound Detection Method:** Processing scheme.

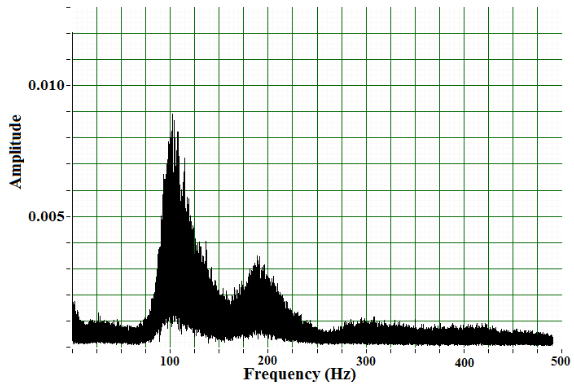

Fig. 8. **Average PSD of talking for all five subjects.** Subjects were asked to read continuously for the five minute period.

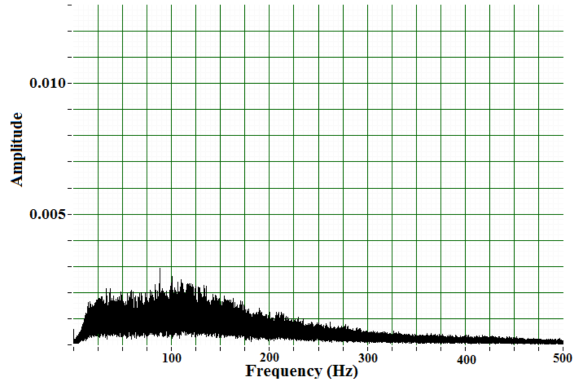

Fig. 9. **Average PSD 20 minutes after start of eating for all five subjects.** Subjects were asked to limit movement and remain silent during this time to better detect bowel activity.

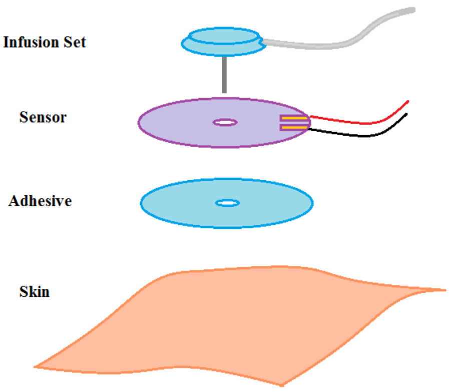

Fig. 10. **Sensor Integration.** Our goal is to integrate a sensor with components already used in insulin pump systems such as the infusion set, continuous glucose monitor, or the insulin pump device itself.

we do not have to detect all bowel sounds. We simply have to record enough bowel sounds over a specific time period that shows someone is eating when compared to their baseline bowel sound activity.

We make several observations to deal with the introduced false negatives. When eating, we assume that there are times when a patient will not be talking (i.e., the patient must breathe). A person that is in a conversation will need to pause to listen, breathe, or she will eventually need to take a bite or swallow (from eating or drinking). We have the opportunity to detect bowel sounds during these breaks from talking.

VII. Sensor Integration

Current insulin pump patients have an insertion site (where insulin is delivered subcutaneously into the body) and a continuous blood glucose monitor. With a continuous glucose monitor, the patient has the additional burden of wearing another device, but patients derive great benefit from continuous real-time data on blood glucose levels. Because patients are already burdened with a high number of devices, we have an additional design constraint to not increase this device burden.

Any additional sensor should be seamlessly integrated (as much as possible). Our plan is to integrate our sensors onto already existing electronic insulin pump components (e.g., the continuous blood glucose monitor or insulin insertion site). To increase patient acceptance and to decrease patient discomfort, the sensor is noninvasive. The envisioned system design is shown in Fig. 10.

A patient that would use this system would not change any way that they currently use the pump infusion sets. Usability will be at least equal to the usability of current systems, because a patient could use a forensically-aware system without knowledge of the forensic data capability. Patient compliance in using a forensic system will be the same as that of using a normal insulin pump system, because the patient would not be required to adopt new usage procedures.

VIII. Discussion

We use the patient eating data to develop three forensic rules for a modified insulin pump system. These rules are potential policies that could help a forensic investigator better understand how to evaluate a potential security (or safety) event. Each rule is based on the expected behavior of a patient. This behavior is shown in Fig. 11.

> **No Pre-eating Bolus Forensic Event:** If food consumption is detected and no bolus is detected within an appropriate time of the food consumption, then there is an increased probability of hyperglycemia.

There are several possibilities for a patient not to issue a bolus before eating (the pre-eating bolus in Fig. 11). A patient could have forgotten to have given a pre-meal (or pre-snack) insulin bolus, or she could have developed a poor habit where she may issue an insulin bolus after a meal. For a carb-free food (e.g., nuts), a patient may eat without needing to bolus.

All of these situations can be dealt with similarly. Because there is a period of time before insulin affects a patient′s blood glucose, patients are encouraged to issue a bolus before a meal. To encourage patient compliance, the system should mark this event when food consumption is detected without the detection of a corresponding pre-eating bolus. The bolus should occur within the previous N minutes of the start of eating. A reasonable expected time between the pre-eating bolus and the beginning of eating could be 20 minutes. The long-term effect will be a lower patient HbA1c value (a patient′s average blood glucose value over the past three months). Blood glucose should be better controlled with this pre-meal bolus rather than a post-meal bolus. This policy could potentially radically improve patient health. Even a one percentage drop will reduce microvascular complications by 40% [CDC11].

Recording this event as a forgotten bolus will increase the number of false positives for those that eat a lot of food that does not require an insulin bolus. We do not expect this case to be common across all patients. If eating foods that do not require a bolus is common in a patient, the pump can ask the patient when this situation is detected (e.g., a button press). We intend to address this issue in the future.

Some patients may desire to give an insulin bolus while eating. For instance, a patient may wait to issue a bolus at a restaurant, because the food arrival time and portion size may not be known apriori. One way to

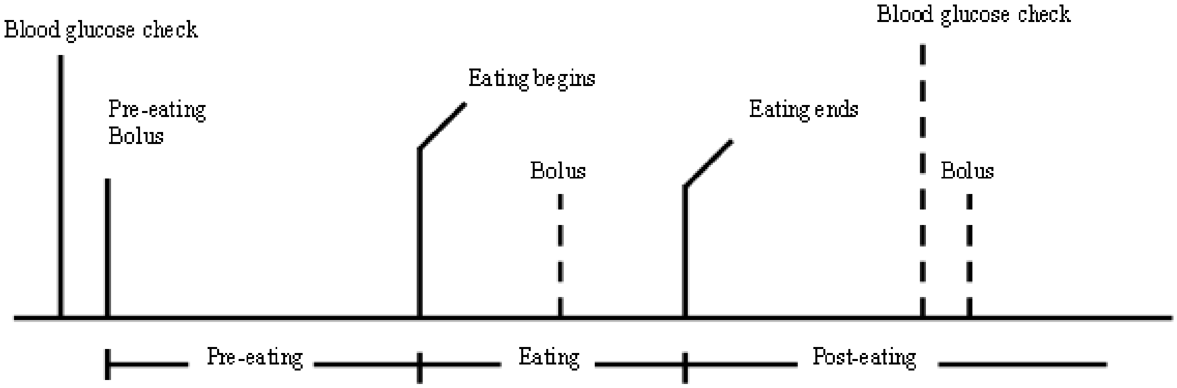

Fig. 11. **Ideal Model of Insulin Pump Patient Eating.** This model shows the actions that occur around food consumption for an insulin pump patient that is compliant. The pre-eating phase begins when the patient issues a pre-meal bolus. Eating begins when the patient swallows the first bite of food. Eating ends after the last bite of food is consumed.

address this issue is to use the patient′s location (e.g., a GPS sensor). This could provide additional context about a patient′s activity. If the GPS sensor indicates that a patient is at a location where they typically consume food, then this increases the probability that a patient is consuming food.

Wireless interference could also cause a deviation from the expected behavior. If one unintentionally or intentionally jammed a wireless bolus command, then it could block a patient from successfully issuing an insulin bolus. The result would be hyperglycemia, and the event should be recorded accordingly. If this happened on a regular occurrence, the patient could examine the recorded data, take appropriate action, or seek help.

No Food with Bolus Forensic Event: If an amount of insulin is given and there is no meal within an appropriate amount of time then there is an increased risk of hypoglycemia and a potential security breach. The amount of insulin may be different for each patient.

If a pre-eating bolus is given without the detection of food consumption, the probability of hypoglycemia is increased. There is a potential false negative in that the system could detect a correction bolus - a bolus given to decrease the current blood glucose level (typically after a blood glucose check). Food consumption is not always expected with a correction bolus. To distinguish between a correction bolus and a pre-eating bolus, the patient can record the type of bolus (assuming that the patient is compliant), or the detection algorithm can wait for potential food consumption.

The false negative is from the time between the patient issuing the pre-eating bolus and beginning to eat (in Fig. 11, this is the pre-eating time stage). We can avoid recording a policy violation by having a timeout period. Once a predetermined timeout period has passed, the event should be recorded that could warn of possible hypoglycemia. This is a possible security event, but it does not automatically indicate that a security breach has occurred.

Other system data could help distinguish between these events. If a patient continually gives insulin without checking her blood glucose, this activity could be suspect, especially when one considers historical insulin pump system data. For example, if a patient were to regularly exercise and take an abnormally large amount of insulin without food consumption, then this event would be of concern and could warrant additional investigation.

Normal Food Bolus Event: The system detects intestinal activity while the patient eats, and the pre or post meal bolus indicates normal behavior.

Knowing that a patient issued a bolus and ate a corresponding meal is important information in that a forensics investigator could ignore this normal event when looking for negative security events. This coupled with a patients historical data, could allow the forensic investigator to construct expected normal behaviors of the patient.

In the future we hope to integrate this data into a real-time detection algorithm. At this time, using these rules in real-time is not suggested without additional testing. We suggest that these rules can be used to enforce different operational policies.

For instance, we can stipulate that whenever a possible security breach or potentially damaging glycemic levels are detected, the device could record this information. If multiple events were recorded, then the system could raise an alert to a patient or physician.

Patient operational use could also be changed. For example, when a bolus command is given at a potentially dangerous time, the pump could require the user to physically interact (not issue a wireless bolus command) with the system to confirm the bolus. At the very least, the system could log the potential security breaches where they could later be examined by forensics or medical experts.

Conclusion. Under ideal conditions, we have shown intermediate results that show it is feasible to detect when a patient is eating, and we have proposed ways to deal with potential false positives. We are continuing experiments to more fully validate our current findings. We anticipate that our present and future forensic events can potentially enable forensic analysis that is not possible with today′s insulin pump systems.

References

[ADA13] American Diabetes Association. Dawn Phenomenon. Available at http://www.diabetes.org/living-with-diabetes/treatment-and-care/blood-glucose-control/dawn-phenomenon.html. Last accessed May 5, 2013.

[Benedict04] Butch Benedict, Rusty Keyes, and F. Clark Sauls, MD, FACS. The Insulin Pump as Murder Weapon: A Case Report. In *Proceedings of the American Journal of Forensic Medicine and Pathology*. 24(2):159-160. June 2004.

[CDC11] Centers for Disease Control. National Diabetes Fact Sheet, 2011. *Diabetes Public Health Resource*. Available at http://www.cdc.gov/diabetes/pubs/pdf/ndfs_2011.pdf. Last accessed May 6, 2013.

[Craine99] Craine, Brian L., Michael Silpa, and Cynthia J. O'Toole. "Computerized auscultation applied to irritable bowel syndrome." *Digestive diseases and sciences* 44.9 (1999): 1887-1892.

[Campbell89] Campbell, F. C., et al. "Surface vibration analysis (SVA): a new non-invasive monitor of gastrointestinal activity." *Gut* 30.1 (1989): 39-45.

[Chang12] Sang-Yoon Chang, Yih-Chun Hu, Hans Anderson, Ting Fu, and Evelyn Y. L. Huang. Body Area Network Security: Robust Key Establishment Using Human Body Channel. In *3rd USENIX Workshop on Health Security and Privacy*. Aug. 2012.

[Ford11] Ford Motor Company. Ford In-Car Health and Wellness Solutions. Available at http://media.ford.com/images/10031/health_wellness.pdf. Last accessed February 7, 2013.

[Glu01] Glucowatch Automatic Glucose Biographer. FDA Device Approval and Clearances. P990026.

[Gollakota11] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They Can Hear your Heartbeats: Non-invasive Security for Implantable Medical Devices. In *Proceedings of ACM SIGCOMM*. Aug. 2011.

[Hei13] Xiali Hei, Xiaojiang Du, Shan Lin, and Insup Lee. PIPAC: Patient Infusion Pattern-based Access Control Scheme for Wireless Insulin Pump System. In *IEEE INFOCOM 2013*. Apr. 2013.

[Jack11] Barnaby Jack. Life Threatening Vulnerabilities (presentation). Hacker Halted. Oct. 2011.

[Klonoff08] David C. Klonoff, MD, FACP. Designing an Artificial Pancreas System to be Compatible with Other Medical Devices. In *Proceedings of the Journal of Diabetes Science and Technology*. 2(5):741-745. Sept. 2008.

[Li11] Chunxiao Li, Anand Raghunathan, and Niraj K. Jha. Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System. In *IEEE International Conference on e-Health Networking Application and Services (Healthcom)*. June 2011.

[Meier10] Barry Meier. F.D.A. Steps Up Oversight of Infusion Pumps. *The New York Times*. Apr. 23, 2010.

[Radcliffe11] Jerome Radcliffe. Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System. In Blackhat USA 2011. Available at http://web.archive.org/web/20130310080156/https://media.blackhat.com/bhus-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf. Last accessed May 6, 2013.

[Schechter10] Stuart Schechter. Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices. In *1st USENIX Workshop on Health Security and Privacy*. Aug. 2010.

[Sorber12a] Jacob Sorber, et al. An Amulet for Trustworthy Wearable mHealth. In the *Workshop on Mobile Computing Systems and Applications (HotMobile)*. Feb. 2012.

[Sorber12b] J. Sorber, M. Shin, R. Peterson, D. Kotz. Plug-n-Trust: Practical Trusted Sensing for mHealth. In *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services (Mobisys)*. June 2012.