Semantic Attacks on Wireless Medical Devices

Renchi Yan, Teng Xu and Miodrag Potkonjak
Computer Science Department
University of California, Los Angeles
{renchi.yan, xuteng, miodrag}@cs.ucla.edu

***Abstract*—Security of medical embedded systems is of vital importance. Wireless medical devices used in wireless health applications employ large number of sensors and are in particular susceptible to security attacks. They are often not physically secured and are usually used in hostile environments. We have developed theoretical and statistical framework for creating semantic attacks where data is altered in such a way that the consequences include incorrect medical diagnosis and treatment. Our approach maps a semantic attack to an instance of optimization problem where medical damage is maximized under constraints of the probability of detection and root cause tracing. We use a popular medical shoe to demonstrate that low energy and low cost of embedded medical devices increases the probability of successful attacks. We have proposed two types of semantic attacks, respectively calibration attack, and time synchronization attack under two scenarios, a shoe with 99 pressure sensors and a shoe with 20 pressure sensors. We test the effects of the attacks and compare them. Our results indicate that it is surprisingly easy to attack several essential medical metrics and to alter corresponding medical diagnosis.**

I. Introduction

Wireless sensor networks are widely applied and embedded in medical devices. The automatic sense data collection enables doctors to keep track of the patient's health status and prevent possible emergency. For example, by analysing the trend of a patient's daily sensor data, any abnormality can easily be detected by a remote doctor, so that facilitating remote diagnose.

However, due to the fact that wireless sensor networks are usually exposed in open and hostile environment, security has emerged to be an important issue. More importantly, for wireless medical devices, the integrity of sensor data has become especially important because it directly affects or even decides the diagnose of a doctor. Traditional cryptographic approaches employ the problem of high power consumption while power is the main constrain in wireless sensor networks, so that many lightweight security protocols are proposed to secure the sensor networks [1][2][3][4]. Meanwhile, hardware based technology has been proposed to secure the sensor network [5][6]. Moreover, techniques that enabled security compromise of popular and important devices such as pacemaker [7], implantable cardiac defibrillator[8] and insulin pumps are proposed [9][10][11][12]. The defence technology to check the data integrity in wireless sensor networks is proposed in [13].

While the previous efforts emphasized vulnerabilities of used wireless security protocols and their potential fixes, we propose the concept of semantic attack. Semantic attacks focus on actual alteration of collected sensor data in such a way that semantic conclusion of medical experts are altered. This attack can be taken by any one who has the access to the sensor reading or the store of sensor data. The attack leads to incorrect diagnose, results in the medical well being of a subject being compromised. Specifically, in this paper, we analysis the approach and the effect of semantic attacks on a medical shoe. The key issue is that in the attack, how to alter the sensor data so that the diagnose result is dramatically altered while avoiding the doctor from suspecting the data integrity. In another word, the attacker should not modify the sensor data too much or too obviously.

Our proposed semantic attacks can be applied in real scenarios. For example, if a malicious attacker is able to break into the computer of a medical expert or even simper, he/she somehow has the access to the data of the patients. His/her goal now is to modify the data which he/she has access to, so that to mislead the diagnose from the medical expert. Note that in real scenario, this malicious party can even be the manufacturer for the medical shoes so that the back doors are made to the embedded sensors, hence, he/she can easily access and tamper the sensor data. This can be very dangerous if the medical expert will draw wrong conclusion of the patient because of the modified data. However, from the perspective of attacker, he/she can not be too aggressive, otherwise too much deviation from the original data can easily lead the medical expert to suspect the data might has been tampered. Therefore, to summarize, the attacker aims at modifying the data of the patient in such a way that the diagnose can be abused to a maximum extend while keeping the medical expert from being suspicious.

In this paper, we have proposed two approaches of semantic attacks. One is calibration attack and the other is timing synchronization attack. We introduce the preliminaries and metrics in Section II and Section III. In Section IV, we discuss the algorithms of the two attacks. Finally we conclude the paper with Section V summarizing our findings and stating our conclusions.

II. Preliminaries

We evaluate our semantic attacks on Hermes medical shoe platform [14]. The medical shoe consists of 99 pressure sensors distributed about the bottom of the shoe numbering from sensor 1 to sensor 99. Based on the medical shoe, we collect the sensor pressure readings over all the 99 sensors for each shoe sampled at 50HZ. We test four persons, for each of them, we test seven different scenarios namely walk, jump, lean, run, stand, limp, slow-walk. In this paper, we focus on slow-walk, walk and run readings and calculate the impact of our attacks mechanisms.

III. Metrics and Formulation

The goal of the semantic attacks is to mislead the diagnose from the medical expert as much as possible. Maki [15] has observed that stride-to-stride variability in speed has a strong correlation with the risk of falling. Stride-to-stride variability takes into account the average of differences between two consecutive values of a specific feature. In our paper, we take two metrics into consideration. One is the variability of stride period, the other one is the variability of double support. By attacking, we could change the variability of these two metrics to the farthest extend.

In order to calculate the stride period variability, we add up the pressure of all 99 sensors in each shoe separately at each time slot. Figure 1 shows the left foot pressure waveform for scenario walk and slow-walk, *SP(i)* represents stride period at i^{th} step. The peaks represent the moment of highest pressure and hence representing the time when the foot contacts with the ground. The stride period is defined as the number of time slots between two successive pressure peaks. Then variation is calculated by taking the average of all the absolute stride period differences in every two consecutive steps.

Another metric is double support. Figure 2 shows left and right foot waveforms together for the scenario of walking and slow-walking. By definition, double support represents the number of time slots when both feet are on ground. In Figure 2, we use 1000kPa as the threshold, and if both feet has total pressure larger than 1000kPa, we regard that both feet are on ground. The contacting time for i^{th} step is *ds(i)*. Similar to stride period metric, variation is calculated by taking the average of absolute double support time differences between two consecutive steps.

$$Var_{SP} = 1/n \sum_{i=1}^{n} |SP(i+1) - SP(i)| \tag{1}$$

$$Var_{DS} = 1/n \sum_{i=1}^{n} |\frac{ds(i+1)}{min(SP(i+1))} - \frac{ds(i)}{min(SP(i))}| \tag{2}$$

Thus the variations for stride period and double support metric can be calculated with Equation 1 and Equation 2. Note that in Equation 2, $min(SP(i))$ represents the smaller stride period between left foot and right foot in the i^{th} step. The instability of a patient can be calculated with Equation 3. The co-efficients γ_{SP} and γ_{DS} indicate the significance of a particular metric. The medical specialists can adjust these values according to the individual patient.

$$Instability = \gamma_{SP} Var_{SP} + \gamma_{DS} Var_{DS} \tag{3}$$

IV. Semantic Attacks

In following section, we propose two types of semantic attacks ans test the effect of the attacks based on walk, slow-walk and run dataset. We also use stride period and double support as metrics.

A. Attack Modeling

The first type of attack is called calibration attack. In this attack, we assume that the attacker can change the pressure value of some number of sensors and the pressure at each time slot can be changed by k percent. The second type of attack is called timing synchronization attack, the attacker postpones the pressure data of some number of sensors for certain time slots. The idea behind the two attacks is that the attacker has access to some number of sensors, he/she wants to alter the variation of metrics. However, regarding each sensor, he/she can not alter too much pressure reading or postponing too much time slots, otherwise can easily be detected.

B. Scenarios

One scenario for the doctor is to use the summation of all the 99 sensors to generate the waveform of each metric. However, another scenario is that the doctor can employ much fewer number of sensors to generate the waveform of the metric. The is due to the fact that many sensors are close to each other, thus providing overlapping information. In this scenario, much fewer sensors are required. Therefore, in the second scenario, we assume that the doctor only uses twenty important sensors to fetch the data and further makes the diagnosis based on that.

C. Attack Description

Since our semantic attacks want to mislead the medical diagnosis as far as possible, as a result, the attacker wants to alter the original Var_{SP} and Var_{DS}. The largest challenge is to alter the variation to the maximum extend while not being suspicious. Therefore, we use three constraints to avoid suspicious. The first is to change only a limited number of sensors, the second is to change the pressure values in calibration attack or the postponed time slot in timing synchronization attack in a limited range. For calibration attack, K which is the changed pressure needs to be smaller than k, and for timing synchronization attack, T which is the postponed time slots needs to be smaller than t, The last is that the number of steps of individual patient cannot be changed beyond certain percentage after the attack. The first constraint is based on the assumption that the attacker only has limited access to the pressure data he/she can change. Based on the above assumption, we convert the problem into an optimization problem where the goal is to maximize the variation within the scope of constrains. The mathematics description is shown as below.

$$\begin{aligned} &\text{Minimize } |Var - Var_0| \\ &\text{Subject to} \\ &\qquad K \leq k(T \leq t) \\ &\qquad N \leq n \\ &\qquad |S - S_0|/S_0 \leq \sigma \\ &\text{where} \end{aligned} \tag{4}$$

- Var is the variation after attack.
- Var_0 is the variation before attack.
- K is the pressure to be changed.

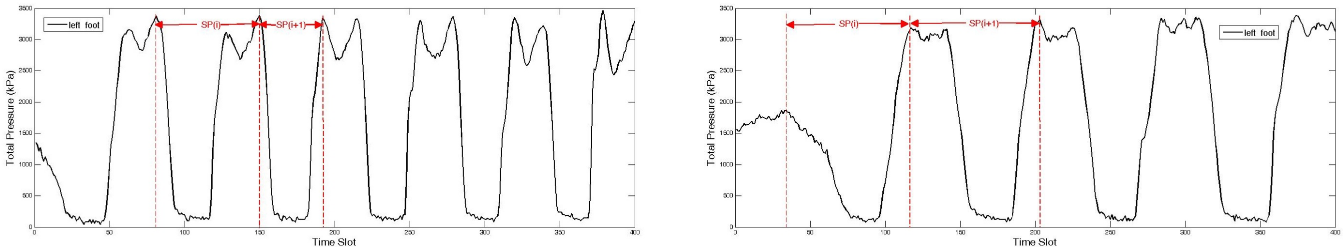


Fig. 1: Total pressure waveform of walk and slow walk for stride period metric.

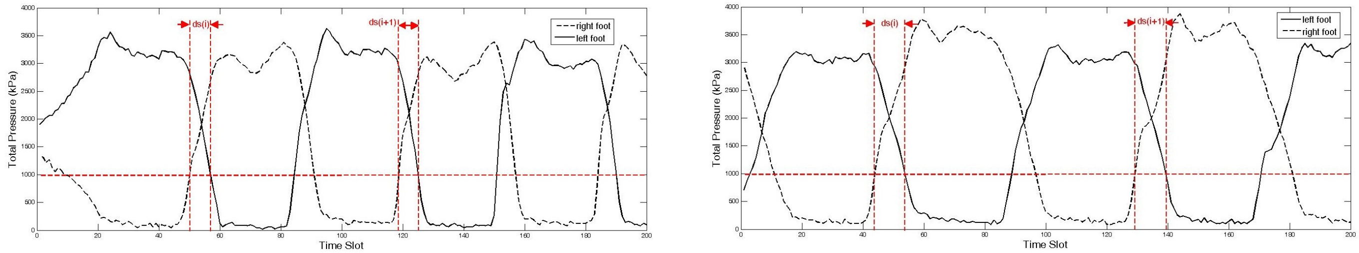


Fig. 2: Total pressure waveform of walk and slow walk for double support metric.

- T is the time slots to be postponed.
- N is the number of sensors attacked.
- S is the number of steps after attack.
- S_0 is the number of steps before attack.
- n, k, and σ are constants.

D. Algorithm for Attacks

Theoretically, to solve the above problem, it is possible to try all the combination of N sensors out of all the sensors with each sensor changing pressure within K percentage or postponing within T timeslots. However, this would be exponential search space complexity, instead, we use dynamic programming (DP.) to implement the problem. The pseudocode is shown in Algorithm 1. We do the N-sensor selection step by step. As described in Algorithm 1, the first step is to iteratively choose each sensor to attack, vary its pressure in every time slot by K percent, calculate the variation after attack. Then we take the top M best attack situations from all the possibilities. For the following steps, each step we iteratively select each sensor to attack based on M best attack situations in previous step. Keep top M best attack situations. We repeat the above procedure for another $N-1$ steps, thus to choose N sensors which cause the maximum damage. In this way, we reduce the exponential time complexity to $O(|sensors|MN)$, where $|sensors|$ is the number of sensors in the system.

E. Experimental Results

We apply the two attacks to stride period and double support metrics on walk, slow-walk and run dataset. For each situation, we try both 99 sensors and 20 sensors scenario. We use the average percentage change of variation across the four tested persons to represent the effect of the attacks. Figure 3 shows the results.

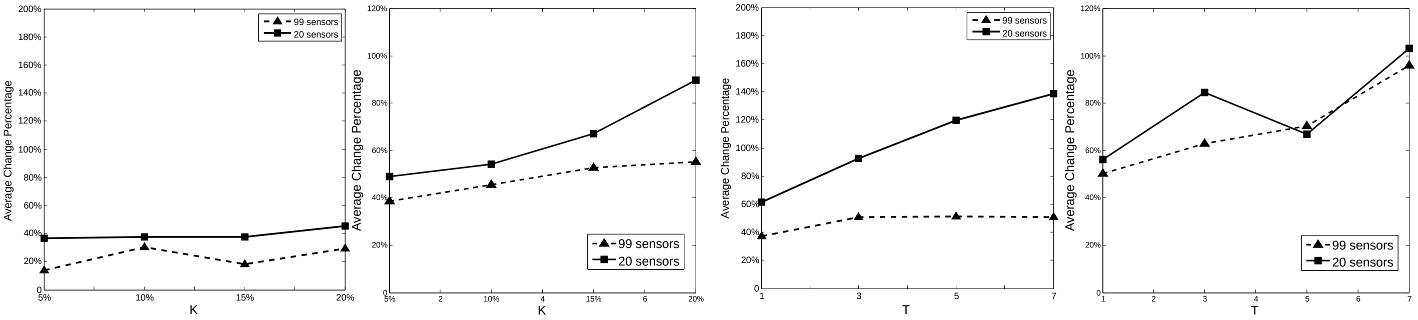
Algorithm 1 Dynamic Programming for Sensor Selection

Input: N - number of sensors to attack.
Input: M - number of optimal values to preserve in previous DP. step.

```
vec = vector that contains the attack situation.
for step from 1 to n do
  for each sensor $s_i$ do
    for each attack situation $vec_i$ do
      Attack $s_i$ under constrains on $vec_i$.
      Generate new attack situation.
    end for
  end for
  $vec$ = TopM(all new situations)
end for
Output: $vec$
```

F. Evaluation

Through these figures, we can see that basically more the change in pressure, the more effective is the attack. However, in Figure 3a and 3b, it can be observed that the average change in the percentage of variation when K is 10% is higher than both when K is 15% and 20% respectively. This abnormal phenomenon occurs because metric formulations that transform the raw pressure data to variation is not a linear function. Besides, the constrains that number of steps of individual patient cannot be changed beyond certain percentage after the attack also affect the result. Because the change of pressure may lead to the result that number of steps change beyond σ.



(a) (b) (c) (d)

Fig. 3: Average change percentage by calibration attack. (a) attack stride period metric on walk dataset. (b) attack stride period metric on run dataset. Average change percentage by timing synchronization attack. (c) attack double support metric on walk dataset. (d) attack double support metric on slow-walk dataset.

In general, a few conclusions can be drawn from the results. (i) Both attacks can dramatically change the variation for both stride period metric and double support metric. (ii) Within certain scope, when the pressure of the sensors changes by more percentage or postponed for more time slots, the attack is more effective. (iii) The scenario with 99 sensors is more resilient against attacks compared to the scenario with 20 sensors. (iv) The dataset of slow-walk is most resilient against the attacks. The dataset of walk is the second and run dataset is the worst. This is because run has higher variation than walk, its waveform is more easy to be disrupted.

V. Conclusion

We have proposed and analysed the semantic attacks on wireless medical devices. The proposed attack can not be prevented or detected by traditional cryptography because the attack is directly dealing with data after sampling. Traditional cryptography can only guarantee the data to be safe through the wireless channels. The semantic attacks can be converted to an optimization problem in which we seek for the maximum damage to the diagnose under the constrains of producing unsuspicious data. Two types of attacks under two scenarios are analysed over the dataset of slow walk, walk, and run. Our results indicate that both attacks can be threatening to the diagnose of the doctor.

VI. Acknowledgement

This work was supported by the NSF under Award CNS-0958369, Award CNS-1059435, and Award CCF-0926127.

References

[1] H. S. Ng, M. L. Sim, and C. M. Tan, "Security issues of wireless sensor networks in healthcare applications," *BT Technology Journal*, vol. 24, no. 2, pp. 138-144, 2006.

[2] M. A, Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of medical systems* vol. 36, no. 1, pp. 93-101, 2012.06.

[3] T. Xu, M. Potkonjak, "Lightweight digital hardware random number generators," *IEEE SENSORS*, pp. 1-4, 2013.

[4] T. Xu, J. B. Wendt, and M. Potkonjak, "Matched Digital PUFs for Low Power Security in Implantable Medical Devices," to appear in *IEEE International Conference on Healthcare Informatics (ICHI)*, 2014.

[5] T. Xu, J. B. Wendt, M. Potkonjak, "Digital Bimodal Function: An Ultra-Low Energy Security Primitive," *IEEE/ACM ISLPED*, pp. 292-297, 2013.

[6] T. Xu, M. Potkonjak, "Robust and Flexible FPGA-based Digital PUF," to appear in *FPL*, 2014.

[7] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W.H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," *In IEEE Symposium on Security and Privacy*, pp. 129-142, 2008.

[8] B. Haran, and D. Senouf, "Remote monitoring and follow-up of pacemakers and implantable cardioverter defibrillators," *Europace*, vol. 11, no. 6, pp. 701-709, 2009.

[9] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *Pervasive Computing, IEEE*, vol. 7, no. 1, pp. 30-39, 2008.

[10] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," *ACM SIGCOMM Computer Communication* , vol. 41, no. 4, pp. 2-13, 2011.

[11] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): authentication for implanted medical devices," *In Proceedings of the 2013 ACM SIGSAC conference on Computer and communications security*, pp. 1099-1112, 2013.

[12] C. Li , A. Raghunathan and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," *In 13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*, pp. 150-156, 2011.

[13] R. Yan, V. C. Shah, T. Xu and M. Potkonjak, "Security Defenses for Vulnerable Medical Sensor Network, to appear in *International Conference on Healthcare Informatics (ICHI)*, 2014.

[14] H. Noshadi, S. Ahmadian, H. Hagopian, J. Woodbridge, N. Amini, F. Dabiri, and M. Sarrafzadeh, "Hermes-Mobile Balance and Instability Assessment System," *BIOSIGNALS*, 2010.

[15] B. E. Maki, "Gait changes in older adults: predictors of falls or indicators of fear." *Journal of the American geriatrics society*, vol. 45, no. 3, pp. 313-320, 1997.