Defending Resource Depletion Attacks on Implantable Medical Devices

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

Fei Hu
Department of Electrical and Computer Engineering
The University of Alabama
Tuscaloosa, AL 35487, USA
Email: fei@eng.ua.edu

***Abstract*—Implantable Medical Devices (IMDs) have been widely used to treat chronic diseases such as cardiac arrhythmia and diabetes. Many IMDs are enabled with wireless communication capabilities and can communicate with an outside programmer/reader wirelessly. With the rapid growth of IMDs, IMD security becomes a critical issue since attacks on IMDs may directly harm the patient. Typical IMDs have very limited resource in terms of energy, computation and storage. In this research, we identify a new kind of attacks on IMDs - Resource Depletion (RD) attacks that could deplete IMD resources (e.g., battery power) quickly. The RD attacks could reduce the lifetime of an IMD from several years to a few weeks. The attacks can be easily launched but can not be defended by traditional cryptographic approaches. In this paper, we propose to utilize the patient's IMD access pattern and we design a novel Support Vector Machine (SVM) based scheme to address the RD attacks. Our SVM-based scheme is very effective in defending the RD attacks. Our experimental results show that the average detection rate of the SVM-based scheme is above 90%.**

***Index Terms*—Implantable medical devices; security; access pattern; support vector machines**

I. Introduction

In the recent years, Implantable Medical Devices (IMDs) have been widely used to treat chronic ailments such as cardiac arrhythmia [1], diabetes, and Parkinson's disease. Many IMDs are enabled with wireless communication capabilities and can communicate with an outside programmer through wireless. Examples of IMDs include oximeters [2], defibrillators, pacemakers [3], and patient monitors [4]. With the growth of IMDs, IMD security becomes a critical issue since attacks on IMDs may directly harm the patient [5]. There are a number of attacks that an adversary may launch on IMDs. For example, pacemakers and implantable cardioverter defibrillator (ICDs) contain a magnetic switch (or sensor) that is activated by sufficiently powerful magnetic fields [6]. The current magnetic-switch-based access does not require any authentication and thus is insecure. Vulnerabilities in the communication interface of wireless programmable IMDs may allow attackers to monitor and alter the function of medical devices without even being in close proximity to the patient [7]. The consequences of an unprotected IMD could be fatal [8]. IMDs contain sensitive patient data and information. At present, a number of mobile phones have IMD reader function. An attacker can easily launch eavesdropping attacks and harvest patient's privacy information. IMD attacks may also be launched by insurance companies. IMD readers may be installed near the gate of a building, and the readers can harvest privacy information from patients' IMDs when they walk through the gate. Hence, it is critical to provide security and privacy to IMDs. However, this is a very challenging task due to the severe resource constraints of IMDs, in terms of energy supply, processor, and storage. An IMD is implanted in patient's body and expected to run for several years. Typical IMDs are powered by a non-rechargeable battery and replacing the battery requires surgery. Re-charging an IMD from an external RF electromagnetic source causes thermal effects in the organs and thus is not recommended. Unlike general medical sensors that may use AA-type or renewable (e.g., solar) batteries, an IMD typically uses silver vanadium oxide batteries and is very vulnerable to Resource Depletion (RD) attacks. RD attacks include a number of attacks that try to consume as much IMD resource as possible, such as Denial of Service (DoS) attack and the forced authentication attack (discussed later). The kind of attacks can be easily launched but it is difficult to defend them.

A number of literatures [9-13] have studied DoS attacks on wireless sensor networks, e.g., Raymond and Midkiff [11] provide a survey of DoS attacksin sensor networks. However, the security schemes designed for sensor networks cannot be directly applied to IMDs, because IMDs have much less resources than typical sensor nodes. For example, a Mica2 mote sensor has 128KB program memory and 512K data memory [14], while an IMD may have less than 10KB memory. Furthermore, it is much easier to replace the battery for a sensor node than for an IMD. Hence, special light-weight security schemes need to be designed for IMDs. Another difference between sensor nodes and IMDs is that an IMD is implanted in a patient's body and directly involves human (the patient). Hence, effective security schemes for IMDs may utilize the human factor.

In reality, an IMD should only communicate with a small number of readers (such as those in the patient's home or the Doctor's office), and not at anytime (unless it is an emergency). Actually, for most patients, the IMD access should have a pattern. Based on this observation, we propose to first build a model of normal patient IMD access, then we can detect

malicious access attempts by using the model and an efficient classification algorithm. If an IMD detects a malicious access attempt, it will go to sleep mode and save its energy. The above scheme avoids the computation and energy expensive authentication process, which means it saves energy for the IMD and hence effectively defend the RD attacks. Specifically, in this paper we present a novel security scheme that is based on patient IMD access pattern and utilizes the Support Vector Machines (SVMs). In this scheme, we utilize the patient's cell phone to perform most of the computations (such as SVMs). The proposed security scheme is the first line of defense, i.e., the scheme will run before any authentication procedure. If an access attempt does not pass our scheme, no authentication will be performed, which saves significant amount of energy for the IMD. If a reader passes our scheme, it still needs to pass the authentication, which provides additional security to IMD access. We present the details of our SVM-based security scheme in Section IV.

The contributions of this paper include: (1) We identify a new kind of attacks (the RD attacks) on IMDs. (2) We propose to utilize patient's IMD access pattern to defend the RD attacks. (3) We choose an efficient classification algorithm (SVM) for the detection of RD attacks, and obtain very good experimental results (higher than 90% accuracy). The rest of the paper is organized as follows. In Section II, we discuss the related work on IMD security. In Section III, we give the attack model. In Section IV, we present the SVM-based security scheme. In Section V we provide our experimental results. We conclude the paper in Section VI.

II. Related work

In this Section, we discuss the related work on IMD security. There have been some recent works on defending against security threats on IMDs. Some literatures proposed to use an (additional) external device such as an access token [15] or a communication cloaker [16]. However, the external devices may be stolen, lost, or simply forgotten by the patient; also it discloses the patient's status. Certificate-based approaches [17] require the IMD reader has online access and a global certification authority needs to be maintained. The certificate-based approaches have two drawbacks. A reader may not always have online access. Second, it is costly to maintain a global certification authority.

In [18], the authors propose to let IMD emit an alert signal (sound, vibrations, etc.) when it is engaging an interaction. However, this approach may not work in noisy environments and it consumes additional battery power of IMDs. Some papers (e.g., [19][20][21]) propose schemes that deny long distance wireless interactions with an IMD unless the proximity of the IMD is verified. For example, the secure telemetric link solution in [19] proposes to use a physical backdoor to verify if the reader is close to the IMD. Access control based on close-range communication is very intuitive, however, it is not secure against an attacker that uses special equipment (e.g., high-gain antennas), and it can not prevent the resource depletion attacks. The authors in [21] propose a new IMD access control scheme based on ultrasonic-distance-bounding. The paper [22] focuses on sleep deprivation concerns; and it proposes using zero power (harvested RF energy) authentication and key exchange to protect the IMDs.

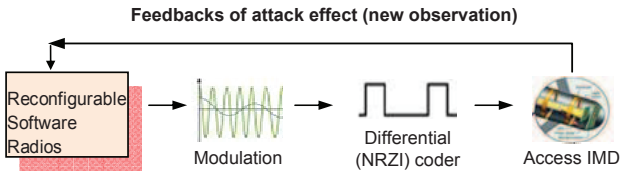

Fig. 1. Launching RD attacks using software radios

However, none of the schemes above can not defend the resource depletion attacks. That is, any scheme will allow a malicious reader to perform authentication with the IMD, which consumes considerable amount of energy of the IMD.

III. Attack model

In this paper, we consider an RD attack that can be easily launched by an attacker. The RD attack is referred to as the forced authentication attack, and it is described below. IMDs communicate wirelessly with external readers. When an external reader attempts to connect with an IMD, the first step is to perform authentication between the IMD and the reader. If the authentication does not pass, then the IMD stops the communication with the reader. However, the authentication process itself requires the IMD to perform quite a few communications and computations, which consume considerable amount of energy. If an unauthorized reader repeatedly tries to connect with an IMD, it would cause the IMD perform multiple authentications and hence waste a lot of battery power. In addition, this kind of attack generates a mass of security logs, which is a RD attack on the IMD storage.

The forced authentication attack can be easily launched by an attacker through a mature RF technology called software radios, as illustrated in Fig.1. Through the RD attacks, an attacker could cause direct harm to a patient by exhausting the IMD battery. The RD attack can reduce the effective lifetime of an IMD from several years to several weeks, rendering the IMD useless and may even cause harm to the patient. Hence, it is critical to design light-weight effective security schemes for IMDs to defend the RD attacks.

IV. The IMD Access-Pattern based Security Scheme

To defend against the RD attacks, we propose a light-weight security scheme that utilizes patient IMD access-pattern and Support Vector Machines (SVMs). Note that our scheme is the first line of defense, i.e., the scheme runs before any authentication procedure. Even if our scheme fails, an unauthorized reader still does not have access to the IMD if it can not pass the authentication. We discuss the modeling of patient IMD access pattern in subsection A, and present our SVM-based defense scheme in subsection B. Note that the focus of this paper is on IMD access when the patient is

in normal (non-emergency) conditions. In subsection C, we discuss the solutions for IMD access during emergency.

A. Modeling Patient IMD Access Pattern

An IMD is different from other wireless devices such as cell phones. A cell phone may have communications at anytime and in many different locations. However, an IMD should only communicate with a small number of readers (such as those in the patient's home and the Doctor's office), and not at anytime (unless it is an emergency). Actually, for most patients, the IMD access should have a certain pattern. For example, the patient reads the IMD every morning and/or every evening at home. The patient's IMD communicates with a Doctor's reader between 9am and 5pm in the Doctor's office. Furthermore, a particular IMD reading may have a fixed frequency, only happens in certain locations or when certain patient conditions are satisfied. Based on the above observations, we propose a patient IMD access-pattern based scheme to defend the RD attacks. The scheme is presented below.

First, the patient's normal access pattern is obtained and serve as training data. Second, an efficient classification algorithm is used to build a model of the patient normal behavior. Third, the model is implemented in patient's IMD and used to detect RD attacks in real-time.

We consider five kinds of IMD-access data: reader action type, time interval of the same reader action, location, time, and day. The data is represented as a vector: $x =< a_1(x), a_2(x), a_3(x), a_4(x), a_5(x) >$, where $a_1(x)$ is the type of action that the reader wants to perform on the IMD; $a_2(x)$ is the time interval of the same action. The types of action depend on the type of IMD. For an implantable cardioverter defibrillator (ICD), the action could be one of the followings: ICD identification; obtaining patient data; obtaining cardiac data; changing patient name; setting ICD's clock; changing therapies; and inducing fibrillation. $a_3(x)$ is the location of the IMD, which has a few authorized values: e.g., home, hospital, pharmacy; $a_4(x)$ is the time of IMD reading, e.g., 24 different values for the hour; $a_5(x)$ represents the type of the day, which has two values weekday, weekend. In our experimental implementations, all the data are normalized to get better results.

Combining the IMD reader action type with the time interval, location and timing information can be very effective in detecting possible attacks (not just RD attacks). For example, some actions (such as ICD identification and changing patient name) should only be performed in the Doctor's office. If these actions happen in other locations, it is probably an attack. During the non-emergence condition, most actions should have a pre-determined frequency. For example, reading the cardiac data is done once a day. If the time interval of this action is only 3 hours, it may be an attempt from an adversary reader. The patient's cell phone may store his/her IMD access pattern, such as reading frequency and the previous time of each action.

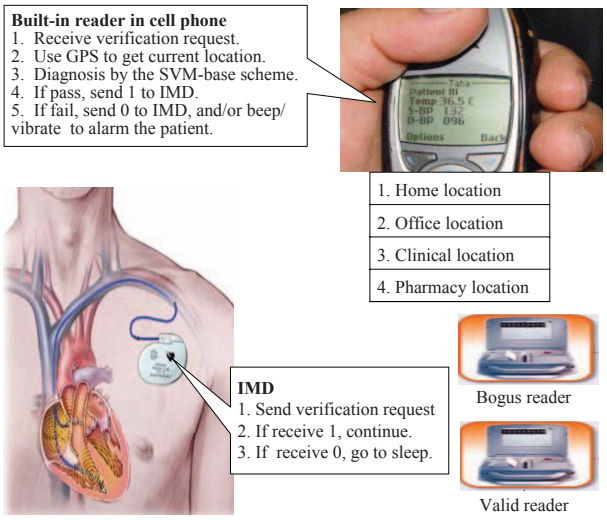

Fig. 2. Utilizing patient's IMD access-pattern to defend RD attacks

B. The SVM-based Security Scheme

Nowadays many cell phones have build-in RF reader and GPS function (such as e-GPS). Note that a cell phone has much better energy, computation and storage capability than IMDs, we propose to shift most computations and storage to the patient's cell phone. The patient's cell phone stores related data and runs the classification algorithm. We use Fig. 2 to present the scheme.

When contacted by a reader, first the IMD sends a short *Verification* message to the patient's cell phone. Then the cell phone runs the classification algorithm, based on the reader action type, current location and time, and the stored history data. With an output from the classification algorithm, the cell phone makes the following decisions: (1) if the output indicates that this is a normal access, it sends a *Continue* command to the IMD and tells the IMD to continue communication with the reader (i.e., perform the standard authentication); (2) if the output indicates that this is an attack, it sends a *Block* command to the IMD, and the IMD will go to sleep mode to avoid the RD attack and save its energy; (3) if the output does not have high confidence, then the cell phone may send an alarm (such as a few beeps) to the patient, and the patient can get involved in deciding if the IMD access is legitimate. With the patient involvement, the decision should be very accurate. In (3) we utilize the human factor in IMDs. Note that even if our scheme fails to detect an actual attack, the attacker still has no access to the IMD as long as it can't pass the authentication.

In this research, we designed an efficient classification scheme based on SVMs. Next, we discuss the details of using SVMs to detect the RD attacks on IMDs. SVMs are efficient tools for the following task: Given some data points and each point belongs to one of two classes, the goal is to decide which class a new data point will be in. Furthermore, SVM works for small sample space. Hence, it is a good candidate for our purpose. For each SVM, there are many hyperplanes that might classify the data. One reasonable choice as the best

hyperplane is the one that represents 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. A SVM can be formally represented as:

$$D = \{(x_i, y_i)|x_i \in R^p, y_i \in \{-1, 1\}\}_{i=1}^{l}), \quad (1)$$

where y_i is either 1 or -1, indicating the class to which the point x_i belongs. Each x_i is a p-dimensional real vector. We want to find the maximum-margin hyperplane that divides the points having $y_i = 1$ from those having $y_i = -1$. Any hyperplane can be written as the set of points x satisfying $w \bullet x - b = a, a \in [1, -1]$, where $\bullet$ denotes the dot product of two vectors. We want to choose the vectors w and b that maximize the margin. The optimization problem in primal form is formulated as follows:

$$\begin{array}{l} min\{\frac{\|w\|^2}{2}\} \\ subject\ to: y_i(w \bullet x_i - b) \geq 1, for\ any\ i = 1, ..., l. \end{array} \quad (2)$$

The original optimal hyperplane algorithm proposed by Vapnik in 1963 was a linear classifier. In 1992, Boser et al. proposed a way to create non-linear classifiers by applying the kernel trick [24] to maximum-margin hyperplanes [25]. The resulting algorithm is similar, except that every dot product is replaced by a non-linear kernel function, which was expressed by Boser et al. and Cortes et al. as the following optimization problem:

$$\begin{array}{l} min\{\frac{1}{2}w^T w + C\sum_{i=1}^{l}\xi_i\} \\ subject\ to: y_i(w^T\varphi(x_i) + b) \geq 1 - \xi_i,\ \xi_i \geq 0. \end{array} \quad (3)$$

Here training vector x_i are mapped into a higher dimensional space by the function φ. Then the SVM finds a linear separating hyperplane with the maximal margin in this higher dimensional space. $C(>0)$ is the penalty parameter of the error term. In equation (3), w is also in the transformed space, and $w = \sum_i a_i y_i \varphi(x_i)$. Dot products with w for classification can again be computed by the kernel trick, i.e., $w \bullet \varphi(x) = \sum_i a_i y_i k(x_i, x_j)$. Hence, once we get C and γ that maximize the margin, we obtain the SVM for the normal behavior. The SVM model is implemented in the patient's cell phone and used for real-time diagnosis for each IMD reading attempt. The kernel function $k(x_i, x_j) = \varphi(x_i)^T\varphi(x_j)$. Some common kernels include polynomial functions, radial basis functions, Gaussian radial basis functions, and hyperbolic tangent functions. In our work, we use a radial basis function as the kernel function: $k(x_i, x_j) = exp(-\gamma\|x_i - x_j\|^2),\ \gamma > 0$.

C. IMD Access During Emergency

Note that our SVM-based scheme is designed for IMD access under non-emergency conditions. When a patient has an emergency (e.g. having a heart attack), the patient may be in any location and the emergency may happen at any time, that is, the location and/or time may be different from the normal access pattern. However, the emergency personnel may still need to access the patient's IMD. To resolve the conflict, we propose the following approach. When the IMD detects an emergency of the patient (e.g., the heartbeat is above 140 per second), it will deactivate the SVM-based security scheme. Then the emergency personnel can still access the IMD without being blocked. Another approach for providing access to IMDs in emergency situations is to use back doors for IMD access. For example, a common master key may be used to access a group of IMDs. The key is secured in the hospitals. Only authorized Doctors or emergency personnel have access to the master key. When an ambulance is called, the master key is obtained and carried with the IMD reader, and then the IMD reader will be able to read patient's IMD.

V. Experimental Results

We conducted experiments to evaluate the performance of the proposed SVM-based security scheme. We consider the case of an ICD. In the experiments, first we pre-processed the patient's access data. Recall that the patient's access data are denoted as a vector: $x =< a_1(x), a_2(x), a_3(x), a_4(x), a_5(x) >$, representing reader action type, the time interval of the same action, location, time, and day, respectively. For $a_1(x)$, we label ICD identification as 1; obtaining patient data as 2; obtaining cardiac data as 3; changing patient name as 4; setting ICD's clock as 5; changing therapies as 6; and inducing fibrillation as 7. For $a_2(x)$, we classify them to three categories. If the time interval is longer than one week, we label it as 1; if the time interval is shorter than one week but longer than one day, we label it as 2; if the time interval is shorter than one day, we label it as 3. As for $a_3(x)$, we label hospital as 1; home as 2; and pharmacy as 3. For $a_4(x)$, we label 24 different values of the hours as 1 - 24. For $a_5(x)$, we label weekday as 0; and weekend as 1. For example, a vector 4, 1, 1, 9, 0 means that a reader attempted to change the patient's name in the hospital at 9am during a weekday, and the last time that the patient's name was changed was more than a week ago.

In our experiments, the total sample size is 3,000. We use 2,500 samples to train the SVM model, and use the remaining 500 samples to test it. In order to get better SVM model, we randomly choose the training data (2,500 samples) from the 3,000 samples and train the model several times. First, we use linear classifiers for the SVM model. We run a total of 50 tests. Table I lists the SVM parameters and the test accuracy of 5 (out of the 50) tests using linear classifiers. We got best w=(0.0938,0.1934,-0.1340,-1.1284,0.0460), b=-3.4654. Then, we use non-linear classifiers for the SVM model. Table II lists the SVM parameters and the test accuracy of 5 (out of the 50) tests using the non-linear classifier. The highest accuracy that we got by using the optimal non-linear SVM classifier is 99.9%, that is, only one out of 500 diagnostics was not correct. We obtain the optimal parameters ($C = 2,048$, $\gamma = 2$) for the non-linear classifier based on the training and testings. The optimal parameters are used to build the optimal non-linear SVM classifier, which achieves better accuracy on most of the tests.

Table III summarizes our experimental results of using linear and non-linear classifiers with optimal parameters over the 50 tests. Table III shows on average non-linear classifiers

TABLE I
PARAMETERS AND ACCURACY USING LINEAR CLASSIFIER

Test	w	b	accuracy
1	0.0940,0.1935,-0.1339,-1.1284,0.0460	-3.4646	88.6%
2	-0.0938,-0.1933,0.1340,1.1284,-0.0459	3.4656	90.0%
3	-0.0938,-0.1933,0.1339,1.1283,-0.0459	3.4653	88.2%
4	0.0944,0.1936,-0.1340,-1.1285,0.0463	-3.4637	89.2%
5	0.0938,0.1934,-0.1340,-1.1284,0.0460	-3.4654	91.2%

TABLE II
PARAMENTS AND ACCURACY USING NON-LINEAR CLASSIFIER

Test	C	γ	accuracy
1	2,048	2	99.9%
2	512	0.5	99.4%
3	8	2^{-15}	82.4%
4	0.5	2	98.4%
5	32	2^{-13}	84.7%

TABLE III
SUMMARY OF TEST ACCURACY OF LINEAR AND NON-LINEAR CLASSIFIERS USING OPTIMAL PARAMETERS OVER 50 TESTS

Type	Non-linear classifier	Linear classifier
Lowest	93.4%	88.4%
Highest	99.9%	91.2%
Average	97.0%	90.2%

perform better than linear classifiers. Non-linear classifiers achieve an average accuracy of 97.0%, while linear classifiers have 90.2%.

As we can see, both linear and non-linear SVM classifier achieve high attack detection accuracy. The above experimental results show that our SVM-based security scheme is very effective in defending the RD attacks on IMDs.

In the SVM-based scheme, we use the patient's cell phone to perform most of the computations. Hence, our scheme is light-weight for IMDs. Since most people have a cell phone, our scheme does not have the drawback of requiring additional external devices. Further more, we utilize the human factor in our scheme. That is, when our scheme detect a possible attack, the cell phone will generate beeps or vibrate, which alarm the patient and ask the patient to verify if this is a legitimate IMD access. With the involvement of the patient, the detection rate can be further improved.

VI. CONCLUSION

Implantable Medical Devices (IMDs) are very vulnerable to the Resource Depletion (RD) attacks because typical IMDs have very limited energy, computation and storage resources. In this paper, we proposed a novel security scheme that can effectively defend the RD attacks. Our scheme utilizes the patient IMD access-pattern and uses the SVMs for real-time diagnosis. We designed both linear and non-linear SVM classifiers and tested the performance of them. Our experimental results showed that the SVM-based scheme can detect RD attacks with very high accuracy, with an average accuracy of 90% for linear SVMs and 97% for non-linear SVMs.

ACKNOWLEDGEMENT

This research was supported in part by NSF grants CNS 0626240, CCF 0830289, CNS-0963578, CNS 0948184, CNS-1002974, CNS-1022552, as well as the US Army Research Office under grant W911NF-08-1-0334.

REFERENCES

[1] J. G. Webster (ed.), "Design of cardiac pacemakers," IEEE Press, 1995.
[2] Nonin Medical, Inc., "Avant 4000 Bluetooth Wireless Oximetry: increased safety and accuracy when administering the six-minute walk test".
[3] Medtronics, Inc. www.medtronic.com/your-health/bradycardia/device/.
[4] BodyMedia. http://www.bodymedia.com/.
[5] W. H. Maisel, "Safety issues involving medical devices," *Journal of the American Medical Association*, vol. 294, pp: 955-958, Aug. 2005.
[6] Medtronic, Inc., "Implantable pacemaker and defibrillator information: magnets," www.medtronic.com/rhythms/downloads/3215ENp7magnetsonline.pdf.
[7] D. Panescu, "Emerging technologies: wireless communication systems for implantable medical devices," *Engineering in Medicine and Biology Magazine*, vol. 27, pp: 96-101, Mar.-Apr. 2008.
[8] K. Fu, "Inside risks: reducing risks of implantable medical devices," *Communications of the ACM*,vol. 52, pp: 25-27, Jun. 2009.
[9] K. Malasri and L. Wang, "Securing wireless implantable devices for healthcare: ideas and challenges," *IEEE Communications*, vol. 47, pp: 74-80, Jul. 2009.
[10] A. Juels, "RFID security and privacy: a research survey," *IEEE JSAC*, vol. 24, pp: 381-394, Feb. 2006.
[11] D. Raymond and S. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," *IEEE Pervasive Computering*, vol.7, pp: 74-81, Jan.-Mar. 2008.
[12] D. Raymond , "Effects of denial of sleep attacks on wireless sensor network MAC protocols," in *Proc. of the 7th Ann. IEEE Systems, Man, and Cybernetics, Information Assurance Workshop*, pp: 297-304, 2006.
[13] D. Halperin et al., "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, vol. 7, pp: 30-39, Jan.-Mar. 2008.
[14] Mica2 mote sensor, Crossbow Technology, http://www.xbow.com.
[15] 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.
[16] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: new directions for implantable medical device security," in *Proc. of Hot Topics in Security*, pp: 1-7, 2008.
[17] 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.
[18] D. Halperin et al., "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, pp: 30-39, 2008.
[19] USPTO Patent Application 20080044014, "Secure telemetric link," http://www.freshpatents.com.
[20] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "RFID guardian: a battery-powered mobile device for RFID privacy management," in *Proc. of 10th Australasian Conf. on Information Security and Privacy*, pp: 184-194, 2005.
[21] K. B. Rasmussen et al., "Proximity-based access control for implantable medical devices," in *Proc. of ACM CCS*, pp: 410-419, 2009.
[22] D. Halperin et al., "Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses," in *Proc. of the 2008 IEEE Symp. on Security and Privacy*, pp: 129-142, 2008.
[23] A. Ferreira et al., "How to break access control in a controlled manner," in *Proc. of the 19th IEEE Symp. on Computer-Based Medical Systems*, pp: 847-854, 2006.
[24] M. Aizerman, E. Braverman, and L. Rozonoer, "Theoretical foundations of the potential function method in pattern recognition learning," *Automation and Remote Control*, vol. 25, pp: 821-837, 1964.
[25] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," in *Proc. of the 5th Annual ACM Workshop on COLT*, pp: 144-152, 1992.