International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 9, No.6 (Nov-2020)

http://dx.doi.org/10.12785/ijcds/0906020

Cyber-Attacks on Medical Implants: A Case Study of Cardiac Pacemaker Vulnerability

Muhammad Muneeb Ur Rehman[1], Hafiz Zia Ur Rehman[1] and Zeashan Hameed Khan[1]

[1]*Department of Mechatronics and Biomedical Engineering, Air University, Islamabad, Pakistan*

Received 10 Apr. 2020, Revised 2 May 2020, Accepted 15 Jul. 2020, Published 1 Nov. 2020

Abstract: This paper describes the vulnerability of the medical implants due to cyber-attacks, which can result in unexpected behavior of these devices thus causing severe damage to human safety. Although, it seems hard to believe that someone's implantable medical device (IMD), e.g. pacemaker or insulin pump can be hacked by an eavesdropper, in reality, researchers have demonstrated that these embedded medical devices can turn into assassination weapons by modifying the operation through remote access. It is therefore important to address these issues to ensure safety and security in medical cyber physical systems. Model based control is implemented in MATLAB/Simulink to demonstrate the control of pacemaker device. Moreover, certain attack models are used to visualize the effects of cyber-attacks on cardiac pacemaker.

Keywords: Implantable Medical Device, Cyber-Attack, Cardiac Pacemaker, Cyber Physical System

1. Introduction

Due to rapid growth of micro and nanotechnology, miniature devices are getting popular to control human biological systems e.g. artificial pancreas, pacemaker etc. A medical cyber physical system (CPS) is a network of regulator, communication, sensing and actuation of the embedded components to monitor and control the physical process of patients [1]. However, as for a typical CPS, safety and security are equally important aspects and these complex systems are responsible to control biological process of a human organ. As future healthcare systems are heading towards "e-health", more focus is required to establish trust as these embedded systems are vulnerable to cybersecurity threats that can jeopardize patient health and safety [2].

Implantable cardioverter defibrillators (ICDs) and pacemakers are examples of IMDs used to control the heart rhythms by sending electrical impulses to heart for synchronization [3]. External devices connected remotely to access the data from ICDs where patient need not to come to the hospital and physicians are kept informed about the functioning of pacemaker implants. An artificial pancreas also functions the same way by continuously monitoring the blood sugar level and controlling an insulin pump to inject appropriate amount of insulin to the blood stream [4, 5]. Due to wireless link connectivity, an intended attacker can hack into the signal to alter the device functioning. One such concern was documented by Department of Homeland Security industrial control system advisories who highlighted the security breach, which can be easily accessed in case of Medtronic insulin pump over-dosage resulting in sudden hypoglycemic condition mortal for the patient [6].

Although, in the medical history, until present, no patient died due to cyber-attack on IMDs, experts demonstrated several times that such devices can be accessed and reprogrammed remotely by a malicious intruder, which can be fatal for the safety of the patient using it. In 2008, a team of researchers revealed for the first time that implantable cardiac defibrillators (ICD) can be reprogrammed using a low cost, commercially available programmer to deny service i.e. making them useless for the patient [7]. After that, several others have demonstrate d different scenarios for hacking embedded medical devices including pacemakers and insulin pumps [8-10]. Securing such safety critical systems for instance, may require multi-factor biometric template generation for authentication to device programming and interconnected adapter nodes for secure access to human interface [11-13].

E-mail:engrzee@gmail.com, mnburrahman2@gmail.com, hzia05@gmail.com

2. IMPLANTABLE MEDICAL DEVICES (IMDS)

IMDs aim to address various malfunctioning of human organs in order to ensure correct operation necessary for the quality of life. Due to wireless connection with the external world, these devices are potential candidate for cyber-attacks, which can risk a victim's life. Nowadays, there are very few efficient solutions to these attacks, which could address the issues of reliability, security and power consumption. There have been efforts to secure the communication link of medical implants [14]. One such approach proposes using optical secure communication for data exchange between IMD and external world with minimal packet size and energy overheads [15]. Some examples of IMDs include biosensors, open loop IMDs and closed loop IMDs.

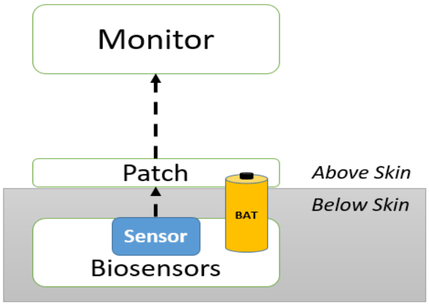

Figure 1. Biosensor patch based monitoring

Biosensors periodically transmit measurements to the patch, which then sends the measurement to a peripheral monitoring segment as shown in Fig. 1.

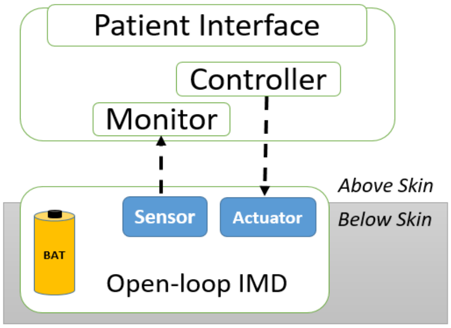

Figure 2. Open-loop implantable medical device

Open-loop IMDs often combine the monitor and controller to form a patient interface. Based on the data from the sensor, the patients are able to monitor their health status as shown in Fig. 2. Based on the status, commands are issued so that the open loop IMD can work as required. The communication between the implant and the peripheral interface is usually not encrypted.

In closed-loop IMDs, the control is established on the interconnection between the sensor and these actuator inside the body as shown in Fig. 3. While patients do not have access to monitor them, they do require skilled configurations from the hospital/clinic. Due to power consumption considerations, the communication is typically not encrypted. Typically, the battery cannot be charged and surgery is required to remove it.

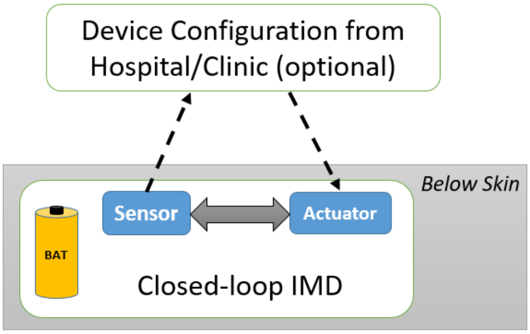

Figure 3. Closed-loop implantable medical device

3. PACEMAKER IMPLANTS

A progressive debility in maximum heart rate (mHR) in humans and other mammals is a fundamental phase of aging [16]. The drop in mHR is independent of class, health and lifestyle, affecting women and men equally from all traits of life. Notably, mHR deterioration is the major factor of age-dependent aerobic capacity decline that eventually restricts functional independence for many older people. The continuing reduction in mHR with age imitates a slackening of the intrinsic pacemaker action of the sinoatrial (S/A) node of the heart, which is the outcome of electrical transformation of individual pacemaker cells along with structural remodeling and a blunted β-adrenergic response.

Continuous cardiac functioning is essential for human beings. Therefore, patients with abnormal heart rhythms are advised to get a pacemaker implanted in their body, which are expected to be robust and fail-safe device with durable battery life ending up to a decade. Thus, various problems in the natural conduction system of the heart are addressed by using an artificial pacemaker, which constantly observes and corrects the heart rate whenever required. A pacemaker is an electronic device used to generate pacing signals for the heart in order to correct irregular heart beat [17]. Irregular heartbeat (arrhythmia) can may result in stroke, heart failure and other complications related to the heart. Pacemaker therapy in atrial fibrillation is also very effective [3]. Pacemaker implants are placed under the skin near left or right collarbone through surgical procedure. Insulated leads are inserted in the heart chambers through cephalic or subclavian veins, which supply electrical impulses from the implantable pulse generator (IPG) to the heart as shown in Fig. 4. Moreover, it also senses the cardiac depolarization [18]. Pacemaker is in fact, a real time computer-controlled system with predefined tasks precedence. A low-power, robust microcontroller interfaced with required memory space is chosen as the core component of this intelligent machine [19].

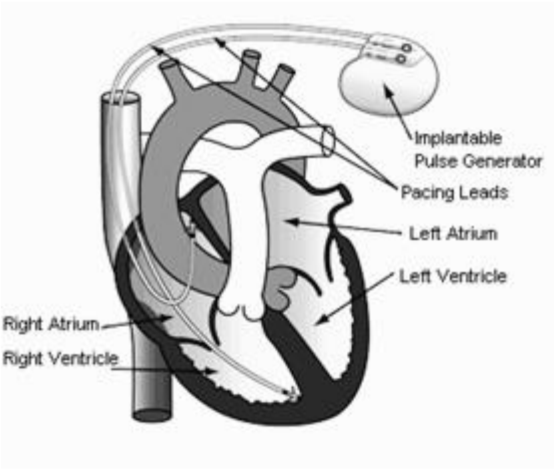

Figure 4. Cardiac pacemaker implant with pacing leads

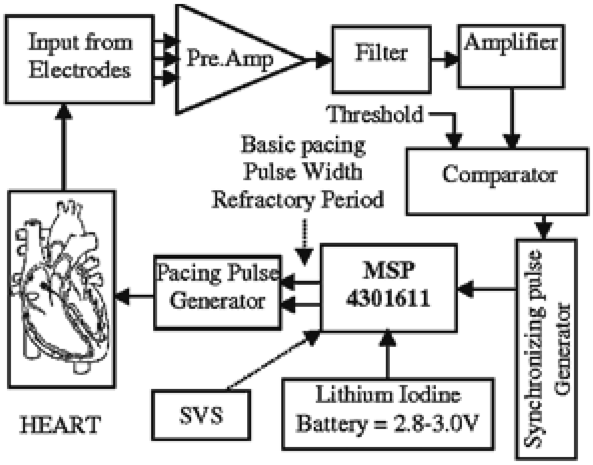

Figure 5. Inside block diagram of cardiac pacemaker [19]

Effectively, a cardiac pacemaker is composed of an implantable pulse generator (IPG) connected to leads (cathode/anode). The IPG is further composed of a battery, analog/digital circuitry and sensing/actuation connectors as shown in Fig. 5. A pacemaker can have unipolar or bipolar electrode configuration in case one or two leads are connected to the heart muscles. Several sensing and control algorithms for pacemakers have been proposed in the literature. For example, a wavelet-based ECG detector for implantable cardiac pacemaker is discussed in [20] while a novel PID controller with adaptive correction factor for heart rate control is presented in [21].

Modern pacemaker's durability allows them to be used for pacing as well as for other cardiac diagnostic applications. Low energy electrical pulses generated by pacemaker can speed up a slow heart rhythm, thus helping to maintain a constant heart rate by harmonizing electrical signaling between the upper and lower chambers as well as between the ventricles of the heart.

A. *Schematic of Pacemaker*

Typically, a microcontroller-based pacemaker design involves related circuitry to sense and actuate the heart muscle activity through electronics [17]. The basic functionality of this electronics is to generate appropriate pacing pulses based on the input from the electrodes. A schematic of cardiac pacemaker is shown in Fig. 5.

B. *Telemetry link*

Pacemakers can transmit and receive information through a wireless telemetry connection. The baud rate of this two-way communication is around 300 bps. Using this link, important data for example pulse amplitude and duration, lead current, lead impedance and battery condition can be assessed in real time [22]. An external programmer is supplied to modify any of the programmable parameters using encoded instruction set and to retrieve diagnostic data.

The telemetry link provides an essential interface for data exchange; however, it also results in the vulnerability of the overall system. It is recommended to incorporate encryption and password protection in the link to avoid information breach by a malicious extruder.

4. Cyber Attack Types and Mechanisms

As discussed above, due to lack of security mechanisms, wireless-enabled IMDs are susceptible to different security threats [15]. In general, the target of adversary attack aims to impact on confidentiality, integrity and availability of the IMDs [13]. It is important to analyze the medical CPS for resilience by modeling and simulating cyber-attacks. Following attack models are described as the possible threats to the medical CPS [23].

A. *Basic Attack Models*

In this type of attack, an attacker may use physical alteration in order to disrupt signals of a medical CPS [24]. The original or the intended signal is u_s and v_s is the attacked signal. We assume that the attacker employs high-energy radiation/electromagnetic signals directed to the system's sensors or communication devices. The attack duration is assumed to be during the period [τ_{start}, τ_{end}].

1) Denial of service (DoS) attack model: Also known as the interruption attack model, DoS service attack results in no data communication during the period of attack. It is represented as:

$$v_s = \begin{cases} 0 & \tau_{start} \prec \tau \prec \tau_{end} \\ u_s & else \end{cases} \qquad (1)$$

2) Man in the middle (MIM) attack model: This attack refers to the action of a human evasdropper in the loop. The intended signal u_s is transformed to the manipulated signal u_m controlled by the eavesdropper during the attack duration. It is represented as:

$$v_s = \begin{cases} u_m & \tau_{start} \prec \tau \prec \tau_{end} \\ u_s & else \end{cases} \qquad (2)$$

3) Down-sampling attack model: This attack type reduces the sampling rate of the intended signal. This means that the quality of control (QoC) will be considerably reduced due to this attack.

$$u_{low} = \begin{cases} u_s & \tau \bmod rate_{down} = 0 \\ u_{low} & else \end{cases} \qquad (3)$$

$$v_s = u_{low}$$

B. Control parameter attack

In this type of cyber-attack, the invader directly get access to the system controller in order to modify the control parameters. Altering the control parameters to arbitrary values induces an incorrect operation of the device.

In this discussion, we assume that an attacker is able to break into the system and is able to get access of the control parameters directly thus bypassing the details of the cybersecurity break-in to the system. Therefore, in the control parameter attack, the attacker is able to destabilize the system by amending the control parameters as follows:

$$v_{par} = \begin{cases} atk_{par} & \tau_{start} \prec \tau \prec \tau_{end} \\ u_{par} & else \end{cases} \qquad (4)$$

Where, u_{par} and v_{par} are the intended and the modified parameters respectively. Moreover, atk_{par} denotes the modified parameter value. The vulnerable control parameters of the device will be changed by the attacker's supplied parameter because of this attack.

C. Coordinated Attack

In an attempt to design robust medical CPS, such safety critical systems are equipped with redundant physical components to withstand basic cyber-attacks. Thus, attackers plan to execute a coordinated attack that is a combination of two or more basic attack mechanisms in order to sabotage the correct operation of an embedded medical implant. As an example, we consider a coordinated attack comprising of man-in-the-middle attack coordinated with a control parameter attack.

$$v_s, v_{par} = \begin{cases} u_m, atk_{par} & \tau_{start} \prec \tau \prec \tau_{end} \\ u_s, u_{par} & else \end{cases} \qquad (5)$$

5. Simulation Results

The system model is simulated in MATLAB/Simulink to demonstrate the impact of cyber-attack on the performance of cardiac pacemaker control. The closed loop control of heart rate is achieved by a pacemaker sub-system using a feedback loop [21]. The complete system is shown in Fig. 6 where R(s) is the desired heart rate and Y(s) is the actual heart rate. The sensing of heart rate is taken as ideal with no delay or lag. Thus, its transfer function H(s) is assumed as unity. It is important to note that the set-point heart rate varies in human w.r.t age.

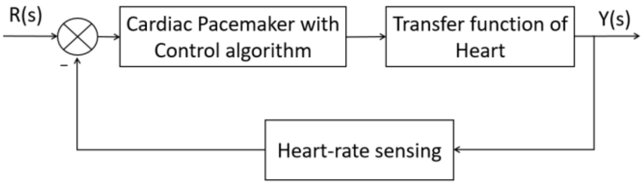
R(s)
-
Cardiac Pacemaker with Control algorithm
Transfer function of Heart
Y(s)
Heart-rate sensing

Figure 6. Block diagram of cardiac pacemaker

A. Control design for Pacemaker

The heart transfer function included in the cardio-vascular system is taken as a second order under-damped model as follows [25]:

$$G_h(s) = \frac{169}{s^2 + 20.8s} \qquad (6)$$

The pacemaker dynamics are represented as a first order lag model as follows:

$$G_p(s) = \frac{8}{s+8} \qquad (7)$$

The desirable range is between 60-100 beats per minutes (bpm). If the heart rate is slower than 60 bpm, it is known as bradycardia, while if it is higher than 100 bpm, it is characterized as tachycardia. Both these abnormalities require an appropriate correction. We have designed three different control schemes i.e. Proportional Integral derivative (PID), Pole Placement Control (PPC) and Linear Quadratic Regulator (LQR) to demonstrate the tracking behavior of pacemaker on heart rate. The time response behavior of these controllers is tested to see if the desired heart rate is higher or lower than the nominal heart rate of 72 bpm.

1) PID Controller

A base line PID controller is applied for heart rate tracking control. The PID compensator is simulated in Simulink as follows:

$$G_{PID}(s) = P + I\frac{1}{s} + D\frac{N}{1 + N\frac{1}{s}} \qquad (8)$$

Following gains are used: Proportional (P) = 1.792, Integral (I) = 0.231, Derivative (D) = 0.302 and the filter coefficient (N) =1727.04.

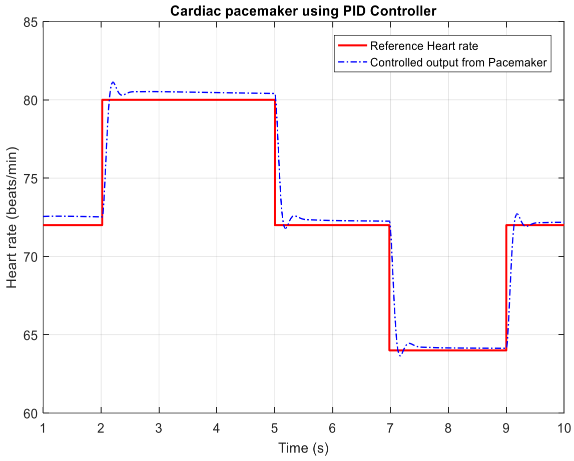

Figure 7. Control performance with PID Controller

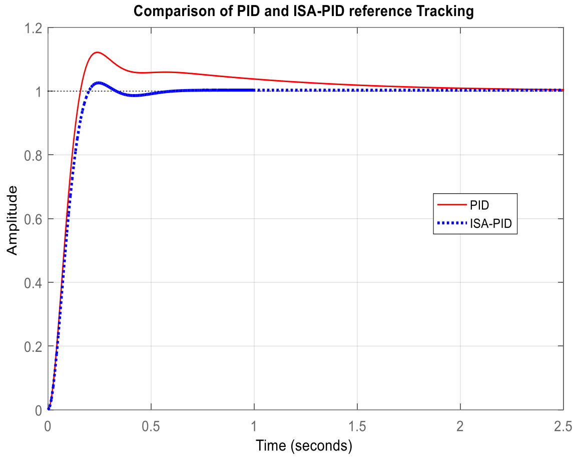

Figure 8. Performance comparison of PID and ISA-PID controllers

As seen from the step response, the performance of the PID controller even after gains tuning is not good. We next try to add an ISA-PID controller for both reference tracking and disturbance rejection. A pre-filter F(s) involves the PID gains from the original controller and a set-point weight “b” as follows:

$$F(s) = \frac{bK_p s + K_i}{K_p s + K_i} \qquad (9)$$

The performance comparison of both PID and ISA-PID controllers is shown in Fig. 8. It is evident that ISA-PID offers reduced overshoot and quick convergence with improved set-point tracking.

2) Pole placement Controller

Pole placement controller permits the designer to place the closed loop dynamics as required. Out of three closed loop poles, dominant pair is placed such that the rise time (tr) is less than 0.15 sec, settling time (ts) is less than 0.5 sec, the overshoot is less than 5% while steady state error is zero. These requirements are met with poles placed at [-10.5±10.71i, -20]. The controller gains to shift these poles to the desired locations are found to be Kc = [12.2 478 450].

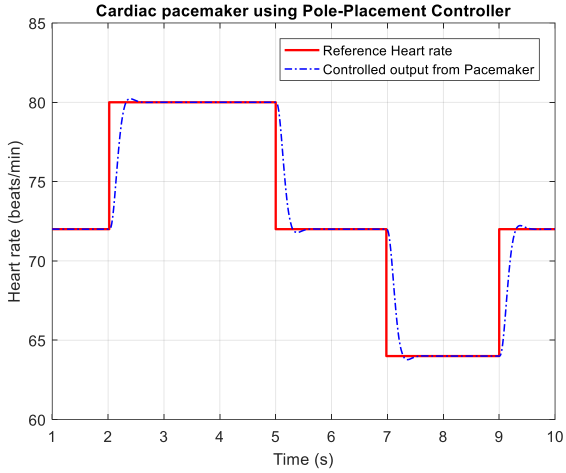

Figure 9. Control performance with Pole Placement Controller

1) LQR Controller

Linear quadratic control is used as an optimal controller for pacemaker heart rate tracking by minimizing the following quadratic cost function:

$$J = \int (x^T Qx + u^T Ru)dt \qquad (10)$$

The weighting matrices ‘Q’ and ‘R’ are adjusted to penalize the state variables and the control signals. For higher values of these matrices, these signals are more penalized. After multiple iterations, the closed loop system is best seen with rise time of 0.22 sec and overshoot of 3.67% using these Q and R weighting matrices as shown in Eq. 9.

$$Q = \begin{bmatrix} 10 & 0 & 0 \\ 0 & 10^2 & 0 \\ 0 & 0 & 10^5 \end{bmatrix}, \quad R = 10^{-5} \qquad (11)$$

From Fig. 7, 8, 9, it is clear that although the base line PID controller shows faster response, there is more than 5% overshoot in the response and the steady state error is non-zero. However, the PPC and LQR control results are quite similar in terms of transient and steady state characteristics with PPC showing a faster response as compared to LQR.

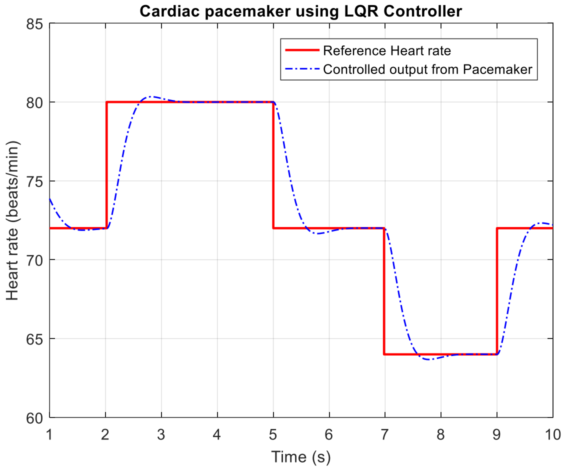

Figure 10. Control performance with LQR Controller

B. *Cyber attack simulation on Pacemaker*

We aim to generate different scenarios of cyber-attack for the vulnerability analysis of our closed loop pacemaker. We considered only the base line PID controller to simply the analysis. The case study describes a patient with age related bradycardia whose heart rate drops below 60 bpm. His cardiologist advised for the pacemaker implant, which enables a normal heart rate of 72 bpm. The man-in-the-middle (MIM) attack during 8 to 14 sec alters the correct reference value for the pacemaker control and the heart rate drops back to 52 bpm during this period.

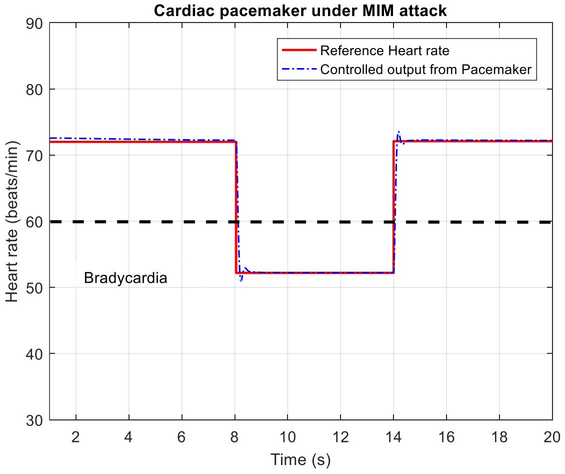

Figure 11. Pacemaker under man-in-the-middle attack during 8≤ t ≤14

In the second scenario, a coordinated attack is simulated in which the reference heart rate is altered by MIM attack as well as the control parameter change (by reducing the derivative gain (K_d) up to 90% of its nominal value) resulting in pronounced overshoot in the response. The simulated cyber-attack is successful in disabling the pacemaker during attack period and generating bradycardia.

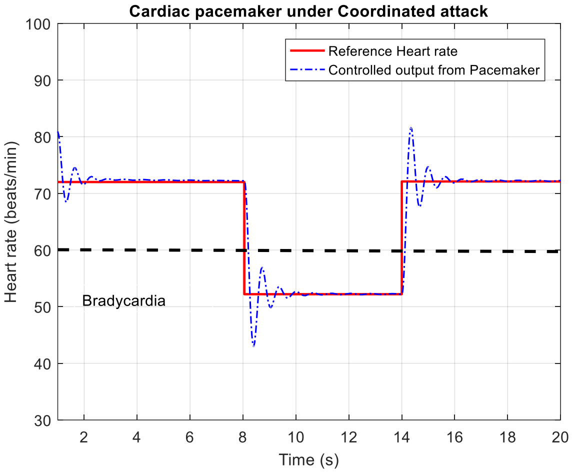

Figure 12. Pacemaker under coordinated attack combining MIM and Control parmeter attack during 8≤ t ≤14

These two scenarios depict the vulnerability of the pacemaker devices to cyber-attack. These vulnerability effects are more evident in the presence of coordinated attacks. Thus, in addition to the electromagnetic interference (EMI) effects, cardiac implants may fail to provide therapy when it is needed or delivering therapy when it is not needed (resulting in tachycardia/bradycardia) due to cyber-attacks.

6. CONCLUSION

In the present work, different control techniques are analyzed to design Heart Rate controller for the embedded control of pacemaker. Initially, a baseline PID controller is tuned to satisfy different performance parameters. The PID controller response is improved by using ISA-PID so that a better tracking response with disturbance rejection can be obtained. Moreover, in order to compare the performance, an optimal LQR and state feedback pole placement controller (PPC) are also simulated. It is observed that the response of pole placement controller is better among all other designs. Next, analysis is done to simulate cyber-attack on the closed loop system. Two cyber-attacks, namely MIM and Coordinated attack are simulated to see the performance. Results have shown that the cyber-attacks are capable of deteriorating the response of pacemaker by injecting a variation in set point tracking or by varying any of the control parameter of the closed-loop system. In future, extensive simulation models will be developed to understand the effect of cyber-attacks as well as adaptive strategies to detect and counter such cyber-attacks on medical devices.

REFERENCES

[1] P. Bogdan, S. Jain, and R. Marculescu, "Pacemaker Control of Heart Rate Variability: A CPS Perspective," ACM Transactions on Embedded Computing Systems, 05/01 2013.

[2] I. Skierka, The governance of safety and security risks in connected healthcare, 2018.

[3] S. Park, P. J. Wang, P. C. Zei, H. H. Hsia, M. Turakhia, M. Perez, et al., "Pacemaker Therapy in Atrial Fibrillation," jcvm, vol. 1, pp. 1-5, 12/04 2013.

[4] S. H. Khan, A. H. Khan, and Z. H. Khan, "Artificial Pancreas Coupled Vital Signs Monitoring for Improved Patient Safety," Arabian Journal for Science and Engineering, vol. 38, pp. 3093-3102, 2013/11/01 2013.

[5] S. Ata and Z. H. Khan, "Model based control of artificial pancreas under meal disturbances," in 2017 International Symposium on Recent Advances in Electrical Engineering (RAEE), 2017, pp. 1-6.

[6] L. h. Newman. (2018, 25th Dec). A New Pacemaker Hack Puts Malware Directly on the Device. Available: https://www.wired.com/story/pacemaker-hack-malware-black-hat/

[7] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, et al., "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in 2008 IEEE Symposium on Security and Privacy (sp 2008), 2008, pp. 129-142.

[8] W. Burleson, S. Clark, B. Ransford, and K. Fu, Design Challenges for Secure Implantable Medical Devices, 2012.

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

[10] E. Marin, D. Singelée, F. Garcia, T. Chothia, R. Willems, and B. Preneel, On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them, 2016.

[11] S. H. Khan, M. Ali Akbar, F. Shahzad, M. Farooq, and Z. Khan, "Secure biometric template generation for multi-factor authentication," Pattern Recognition, vol. 48, pp. 458-472, 2015/02/01/ 2015.

[12] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K.-D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," Computers in Industry, vol. 97, pp. 132-145, 2018/05/01/ 2018.

[13] E. Hamadaqa, A. Abadleh, A. Mars, and W. Adi, "Highly Secured Implantable Medical Devices," in 2018 International Conference on Innovations in Information Technology (IIT), 2018, pp. 7-12.

[14] L. Bu, M. G. Karpovsky, and M. A. Kinsy, "Bulwark: Securing implantable medical devices communication channels," Computers & Security, vol. 86, pp. 498-511, 2019.

[15] A. Mosenia and N. K. Jha, "OpSecure: A Secure Unidirectional Optical Channel for Implantable Medical Devices," IEEE Transactions on Multi-Scale Computing Systems, vol. PP, pp. 1-1, 11/08 2017.

[16] C. Peters, E. Sharpe, and C. Proenza, "Cardiac Pacemaker Activity and Aging," Annual Review of Physiology, vol. 82, 02/10 2020.

[17] M. Sayahkarajy, E. Supriyanto, M. H. Satria, and H. Samion, "Design of a microcontroller-based artificial pacemaker: An internal pacing device," in 2017 International Conference on Robotics, Automation and Sciences (ICORAS), 2017, pp. 1-5.

[18] D. Fitzpatrick, "Chapter 6 - Pacemakers and Implantable Cardioverter Defibrillators," in Implantable Electronic Medical Devices, D. Fitzpatrick, Ed., ed Oxford: Academic Press, 2015, pp. 75-97.

[19] S. D. Chede and K. D. Kulat, "Design Overview Of Processor Based Implantable Pacemaker," JCP, vol. 3, pp. 49-57, 2008.

[20] Y. Min, H. Kim, Y. Kang, G. Kim, J. Park, and S. Kim, "Design of Wavelet-Based ECG Detector for Implantable Cardiac Pacemakers," IEEE Transactions on Biomedical Circuits and Systems, vol. 7, pp. 426-436, 2013.

[21] K. R. A. Govind and R. A. Sekhar, "Design of a novel PID controller for cardiac pacemaker," in 2014 International Conference on Advances in Green Energy (ICAGE), 2014, pp. 82-87.

[22] G. Brooker, "Chapter Fourteen - Pacemakers," in Handbook of Biomechatronics, J. Segil, Ed., ed: Academic Press, 2019, pp. 567-589.

[23] N. Rashid, J. Wan, G. Quiros, A. Canedo, and M. A. Al Faruque, "Modeling and simulation of cyberattacks for resilient cyber-physical systems," in 2017 13th IEEE Conference on Automation Science and Engineering (CASE), 2017, pp. 988-993.

[24] J. Wan, A. Canedo, and M. A. A. Faruque, "Security-aware functional modeling of cyber-physical systems," in IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), 2015.

[25] A. D. S.C Biswas, P.Guha, "Mathematical Model of Cardiovascular System by Transfer function Method," Calcutta Medical Journal, 2010.

Muhammad Muneeb Ur Rehman is pursuing his M.S in Mechatronics Engineering from Air University, Islamabad, Pakistan. Previously, he obtained his Bachelor of Mechatronics Engineering from the same university in 2019. His interests include modeling and simulation, design of robots and mechatronic systems, control design etc. He is a student member of IEEE.

Hafiz Zia Ur Rehman is working as an Assistant Professor in the department of Mechatronics and Biomedical Engineering, Air University, Islamabad, Pakistan. He obtained his Ph.D. in mechatronics engineering from Hanyang University, South Korea in 2019. His research interests include medical image processing, computer vision and adaptive filtering. He is a member of Pakistan Engineering Council (PEC).

Zeashan Hameed Khan is working in the department of Mechatronics and Biomedical Engineering, Air University, Islamabad, Pakistan as an Associate Professor. He obtained his Ph.D. in control systems from University of Grenoble, France in 2010. His research interests include robust control, networked control systems, cyber physical systems, and biomedical control. He has written more than 50 papers including journal papers, conference papers and book chapters. He is a member of IEEE and PEC.