International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Intrusion Detection in Medical Cyber Physical System (MCPS) Based On Behavior Rule Specification Method

Palisetti Sree Keerthi
PG Scholar
Department of CSE,
DIET, ANAKAPALLE, Visakhapatnam

Addala Vasudeva Rao
Associate Professor,
Department of CSE,
DIET, ANAKAPALLE, Visakhapatnam

Abstract- *Medical cyber physical systems (MCPS) are getting popular now a days. Every advanced healthcare hospitals use the help of MCPS to ease otherwise complicated tasks. These systems analyze the patient status using physical sensors and employ corresponding reaction using actuators. An array of sensor devices is attached to the patient which reads real time data and analyses it. Actuators provide corresponding action with respect to the values sensed. Nowadays these cyber physical systems (CPS) are used as tool for cyber-attacks. This can relatively harm the patient or may even cause a direct or indirect threat to life. Since the CPS work based on sophisticated and more complex algorithms, intrusion detection in such system can be really complicated task. Behavior-rule specification-based technique is analyzed for intrusion detection of medical devices embedded in a medical cyber physical system (MCPS) where patient's safety is of the utmost importance. Medical cyber physical systems (MCPS) are used as tool for cyber attacks. This can relatively harm the patient or may even cause a direct or indirect threat to life. Intrusion detection technique helps to detect secret attackers to support safe and secure MCPS applications. In this dissertation research we aim to design and validate intrusion detection system (IDS) protocols for a medical cyber physical system (MCPS) comprising sensors, actuators, control units, and physical objects for controlling and protecting physical infrastructures. The design part includes host IDS, system IDS and IDS response designs.*

The validation part includes a novel model-based analysis methodology with simulation validation. Our objective is to maximize the MCPS reliability or lifetime in the presence of malicious nodes performing attacks which can cause security failures. Our host IDS design results in a lightweight, accurate, autonomous and adaptive protocol that runs on every node in the CPS to detect misbehavior of neighbor nodes based on state-based behavior specifications. Our system IDS design results in a robust and resilient protocol that can cope with malicious, erroneous, partly trusted, uncertain and incomplete information in a MCPS. Our IDS response design results in a highly adaptive and dynamic control protocol that can adjust detection strength in response to environment changes in attacker strength and behavior. The end result is an energy-aware and adaptive IDS that can maximize the MCPS lifetime in the presence of malicious attacks, as well as malicious, erroneous, partly trusted, uncertain and incomplete information. We develop a probability model based on stochastic Petri nets to describe the behavior of a MCPS incorporating our proposed intrusion detection and response designs, subject to attacks by malicious nodes exhibiting a range of attacker behaviors, including reckless, random, insidious and opportunistic attacker models. We identify optimal intrusion detection settings under which the MCPS reliability or lifetime is maximized for each attacker model.

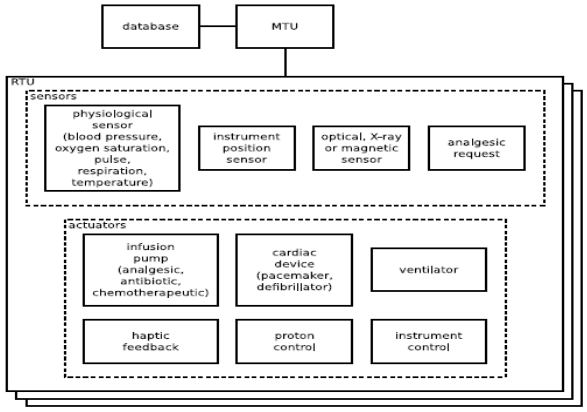
Keywords: intrusion detection, sensor actuator networks, medical cyber physical systems, healthcare, security, safety.

1. INTRODUCTION

Medical Cyber Physical System is used in advanced healthcare hospitals to do any complicated tasks. This system can analyze the patient status using physical sensors and perform corresponding action using actuators. An array of sensor devices is attached to the patient who reads real time data and analyses it. Actuators provide corresponding action with respect to the values sensed. Medical Cyber Physical System becomes a tool for cyber-attacks. IDS is used to detect unknown attack/attacker patterns. IDS Uses behavioral rule specification for this purpose. MCPS sensor/actuator networks are highly resource constrained. Therefore To enclose an intrusion detection system in MCPS sensor/actuator networks is difficult. To overcome this problem a new methodology for intrusion detection is Introduced which is based on behavioral rule specifications which utilizes behavioral rules for defining normal behavioral patterns for a medical device. These behavioral patterns represent acceptable behaviors of that particular CPS. Further, these behavioral rules are then transformed into a state machine, so that any deviation from normal state to an unsafe state can be easily monitored. The most prominent characteristic of a medical cyber physical system (MCPS) is its feedback loop that

acts on the physical environment. In other words, the physical environment provides data to the MCPS sensors whose data feed the MCPS control algorithms that drive the actuators which change the physical environment. MCPSs are often characterized by sophisticated patient treatment algorithms interacting with the physical environment including the patient. In this paper, we are concerned with intrusion detection mechanisms for detecting compromised sensors or actuators embedded in an MCPS for supporting safe and secure MCPS applications upon which patients and healthcare personnel can depend with high confidence. Intrusion detection system (IDS) design for cyber physical systems (CPSs) has attracted considerable attention because of the dire consequence of CPS failure The Basic difference between creating an IDSs for medical devices and other systems is that the attacker may attack the physical component rather than the network or communication protocols. Thus IDS should be closely coupled with the physical equipment of the Cyber Physical System. IDSs for MCPSs may test medical sensor measurements and actuator settings to detect misbehavior of physical properties visible because of attacks. In this paper, we consider specification rather than signature-based detection to deal with unknown attacker patterns. We consider specification rather than anomaly based techniques to avoid using resource constrained sensors or actuators in an MCPS for profiling anomaly patterns (e.g., through learning) and to avoid high false positives. We consider specification rather than trust based techniques to avoid delay due to trust aggregation and propagation to promptly react to malicious behaviors in safety critical MCPSs. To embed an intrusion detection system in MCPS sensor/actuator networks brings further challenges. These sensor/actuator networks are highly resource constrained. Adding an intrusion detection system should bypass these challenges. With all these in mind a new methodology for intrusion detection is put-forward which uses behavioral rule specification-based Intrusion detection (BSID) which utilizes behavioral rules for defining normal behavioral patterns for a medical device. These behavioral patterns represent acceptable behaviors of that particular CPS. Further, these behavioral rules are then transformed into a state machine, so that any deviation from normal state to an unsafe state can be easily monitored. The impact of various attackers is also investigated to benchmark the effectiveness of MCPS Intrusion Detection System. This methodology has also been proved to display higher true positives for a reduced false negative as well as false positive rate. This can further help to identify more complex and invisible attackers. A peer to peer architecture provides an additional uninterrupted operation of Intrusion Detection System. The goal of an intrusion detection system is to provide an indication of a potential or real attack. An attack or intrusion is a transient event, whereas vulnerability represents an exposure, which carries the potential for an attack or intrusion. The difference between an attack and vulnerability, then, is that an attack exists at a particular time, while vulnerability exists independently of the time of observation.

2. SYSTEM ARCHITECTURE



Medical Physical Components in the Reference MCPS.

3. RELATED WORK

The mixture of embedded software controlling the devices, networking capabilities, and complicated physical dynamics that patient bodies reveal makes modern medical device systems a distinct class of cyber-physical systems, which is referred as medical CPS(MCPS). Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things are satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system. In the context of intrusion detection for MCPSs or healthcare systems, Asfaw et al. studied anomaly-based IDS for MCPSs. The authors studied attacks that violate privacy of an MCPS. A trust-based IDS scheme giving a hierarchical trust management protocol for Wireless Sensor Networks is used. A composite trust metric deriving from both social trust (honesty) and QoS trust (energy and coop-erativeness) as an indicator of maliciousness is considered. A probability model based on stochastic Petri nets techniques to describe the behaviors of Sensor Networks or Cluster Heads for trust evaluation

and intrusion detection, as well as a statistical method to predict the false alarm probabilities of the trust-based IDS scheme. The experimental results shows that a node with high compromising rate can be easily detected, thus were supporting the idea of using trust to implement IDS.

4. OVERVIEW OF INTRUSION DETECTION

1. Threat Model:

We focus on defeating inside attackers that violate the integrity of the MCPS with the objective to disable the MCPS functionality. Our design is also effective against attacks such as subtle manipulations that change medical doses slightly to cause long term harm to patients or medical or billing record exhilarations which violate privacy. There are two distinct stages in an attack: before a node is compromised and after a node is compromised. Before a node is compromised, the adversary focuses on the tactical goal of achieving a foothold on the target system.

2. Attacker Archetypes:

We differentiate two attacker archetypes: reckless, random and opportunistic. A reckless attacker performs attacks whenever it has a chance to impair the MCPS functionality as soon as possible. A random attacker, on the other hand, performs attacks only randomly to avoid detection. It is thus insidious and hidden with the objective to cripple the MCPS functionality. We model the attacker behavior by a random attack probability pa. When pa = 1 the attacker is a reckless adversary. Random attacks are typically implemented with on off attacks in real-world scenarios, so pa is not a random variable drawn from uniform distribution U(0, 1) but rather a probability that a malicious node is performing attacks at any time with this on-off attack behavior. An opportunistic attacker is the third archetype. An opportunistic attacker exploits ambient noise modeled by per (probability of miss-monitoring)to perform attacks.

3. Behavior Rules:

Behavior rules for a device are specified during the design and testing phase of an MCPS. Our intrusion detection protocol takes a set of behavior rules for a device as input and detects if a device's behavior deviates from the expected behavior specified by the set of behavior rules. Since the intrusion detection activity is performed in the background, it allows behavior rules to be changed if incomplete or imprecise specifications are discovered during the operational phase without disrupting the MCPS operation. Our IDS design for the reference MCPS model relies on the use of lightweight specification-based behavior rules for each sensor or actuator medical device. For each device, its behavioral rules are predefined during the design and testing phase.

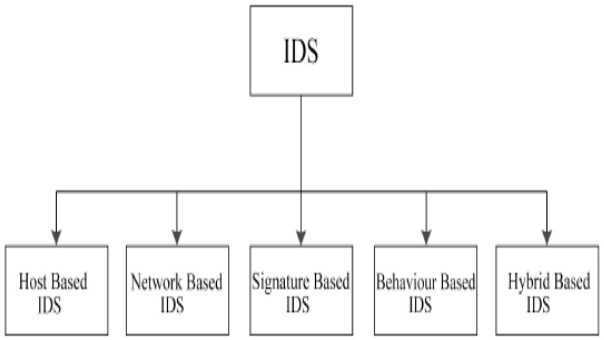
This method takes in behavioral rules for specific devices and analyze whether if that device is being deviated from expected behavior specified by behavioral rule set. Isolated from the functional modules of MCPS, modification of behavioral rules are possible during its normal functioning without interrupting its operation. Since the sensor and actuators are resource constrained, this method uses a lightweight specification based behavior rules for each and every component. The method uses a peer to peer approach such that each and every device performs monitoring of their neighboring nodes. That means a sensor/actuator might be monitoring other dissimilar sensor/actuator nodes. Thus failure of IDS can be reduced to a greater extend. While specifying behavior rules, the acceptable numerical parameters for IDS may vary for different patients.

4. Intrusion detection system:

Intrusion detection system (IDS) design for cyber physical systems (CPSs) has attracted considerable because of the dire consequence of CPS failure. In this paper, we consider specification rather than signature-based detection to deal with unknown attacker patterns. We consider specification rather than anomaly based techniques to avoid using resource constrained Sensors or actuators in an MCPS for profiling anomaly patterns (e.g., through learning) and to avoid high false positives. We consider specification rather than trust based techniques to avoid delay due to trust aggregation and propagation to promptly react to malicious behaviors in Safety critical MCPSs.

5. Hybrid Intrusion Detection System.

Hybrid approach uses a combination of both signature based and behavior based intrusion detection. This method can help us to detect both known as well as unknown attacks and further reduces the false alerts currently generated by behavioral based intrusion detection design



Categories of IDS

5. Conclusion

For safety-critical MCPSs, being able to detect attackers while limiting the false alarm probability to protect the welfare of patients is of utmost importance. In this paper we proposed a behavior-rule specification-based IDS technique for intrusion detection of medical devices embedded in a MCPS. We framework the security maintenance of computer networks as a Stackelberg random two-player game during which the intruder and response engine attempt to maximize their own benefits by taking best soul and response actions, respectively. Through a comparative analysis, we demonstrated that our behavior-rule specification-based IDS technique outperforms existing techniques based on anomaly intrusion detection. The comparison between various intrusion detection methods will allow security professionals to effectively and efficiently find best technique that suits a particular system or organization. It can also assist in making acceptable tradeoffs among sometimes conflicting goals such as True Positives, True Negatives, False positives and False negatives and to allocate valuable sensor/actuator energy resource based on the security requirements

6. Future Work

In future work, we plan to analyze the overheads of our detection techniques such as the various distance-based methods in comparison with contemporary approaches. We also plan to deepen adversary modeling research based on stochastic Petri net techniques such that the system can dynamically adjust CT to maximize intrusion detection performance in response to changing attacker behaviors at runtime. As a result of our efforts, it is seen that security research is far from mature for the newly-emerged cyber physical systems and there are still many challenges facing designers, operators and researchers. This is unsatisfactory, and hopefully, by providing an overview of the literature efforts done, the overview will contribute in providing reference for researcher in the area of CPS security. For safety-critical MCPSs a behavior-rule specification-based IDS technique is used for intrusion detection of medical devices contained in a MCPS.In future, plan is to analyze the overheads of current detection techniques by using comparison with contemporary approaches.

References

[1] H. Al-Hamadi and I. R. Chen. Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensornetworks. IEEE Transactionson Network and Service Management, 10(2):189–203,2013.

[2] M. Aldebert, M. Ivaldi, and C. Roucolle. Telecommunications Demand and Pricing Structure: An Econometric Analysis. Telecommunication Systems, 25:89–115, 2004.

[3] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee. Security challenges in next generation cyber physical systems. Beyond SCADA: Networked Embedded Control for Cyber Physical Systems, 2006.

[4] B. Asfaw, D. Bekele, B. Eshete, A. Villafiorita, and K. Weldemariam. Host-based anomaly detection for pervasive medical systems. In Fifth International Conference on Risks and Security of Internet and Systems, pages 1–8, October 2010.

[5] F. Bao, I. R. Chen, M. Chang, and J. H. Cho. Hierarchical Trust Management forWireless Sensor Networks and its Applications to Trust- Based Routing and Intrusion Detection. IEEE Transactions on Network and Service Management, 9(2):169–183, 2012.

[6] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Fovino, and A. Trombetta. A multidimensional critical state analysis for detecting intrusions in scada systems. IEEE Transactions on Industrial Informatics, 7(2):179 – 186, May 2011.

[7] A. C´ardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry. Challenges for securing cyber physical systems. In First Workshop on Cyber-physical Systems Security, DHS, 2009.

[8] I. R. Chen and T. H. Hsi. Performance analysis of ad-mission control algorithms based on reward

optimization for real-time multimedia servers. Performance Evalua-tion, 33(2):89–112, 1998.

[9] I. R. Chen, A. P. Speer, and M. Eltoweissy. Adaptive fault tolerant qos control algorithms for maximizing sys-tem lifetime of query-based wireless sensor networks. IEEE Transactions on Dependable and Secure Comput-ing, 8(2):161–176, 2011.

[10] I. R. Chen and D. C. Wang. Analysis of replicated data with repair dependency. The Computer Journal, 39(9):767–779, 1996.

[11] I. R. Chen and D. C. Wang. Analyzing Dynamic Vot-ing using Petri Nets. In 15th IEEE Symposium on Re-liable Distributed Systems, pages 44–53, Niagara Falls, Canada, October 1996.

[12] S.-T. Cheng, C.-M. Chen, and I. R. Chen. Dynamic quota-based admission control with sub-rating in multi-media servers. MultimediaSystems, 8(2):83–91, 2000.

[13] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes. Using model-based intrusion de-tection for SCADA networks. In SCADA Security Sci-entific Symposium, pages 127–134, Miami, FL, USA, January 2007.

AUTHORS

Palisetti Sree Keerthi
PG Scholar
Department of CSE,
DIET, ANAKAPALLE,
Visakhapatnam

Addala Vasudeva Rao
Associate Professor,
Department of CSE,
DIET, ANAKAPALLE,
Visakhapatnam