ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

A BEHAVIOR RULE SPECIFICATION BASED TECHNIQUE FOR INTRUSION DETECTION IN A MEDICAL CYBER PHYSICAL SYSTEM (MCPS)

M.SUGAPRIYA
PG Student
Department of CSE
Rajas Engineering College
Vadakkangulam
akshayasri2114@gmail.com

V.SHEEJA KUMARI, M.Tech,MBA,(PhD)
ASSISTANT PROFESSOR
Department of CSE
Rajas Engineering College
Vadakkangulam
ammusheeja@rediffmail.com

Abstract—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. We propose and analyze a behavior-rule specification-based technique for intrusion detection of medical devices embedded in a medical cyber physical system (MCPS) in which the patient's safety is of the utmost importance. In this project, 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. However, an IDS technique for MCPSs is still in its infancy with very little work reported. Intrusion detection techniques in general can be classified into four types: signature, anomaly, trust, and specification-based techniques. In this project, we consider specification rather than signature and anomaly based detection to deal with unknown attacker patterns 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.

I. INTRODUCTION

1.1 Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). The NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS. On-line NIDS deals with the network in real time and it analyses the Ethernet packet and applies it on the some rules to decide if it is an attack or not. Off-line NIDS deals with a stored data and pass it on a some process to decide if it is an attack or not. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system.

Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

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 a vulnerability represents an exposure, which carries the potential for an attack or intrusion. The difference between an attack and a vulnerability, then, is that an attack exists at a particular time, while a vulnerability exists independently of the time of observation. Another

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

way to think of this is that an attack is an attempt to exploit a vulnerability (or, in some cases, a perceived vulnerability). This leads us to categorize various types of intrusion detection systems.

1.2 Types of IDS

There are five different categories of IDS covered in this guide. Not all of these categories represent "classical intrusion detection" but they play a role in the overall goal of detecting or preventing intrusions on a corporate network. The categories are:

- Network Based Intrusion Detection System
- Host Based Intrusion Detection System
- File Integrity Checker
- Network Vulnerability Scanner
- Host Vulnerability Scanner

An intrusion detection system (IDS) examines system or network activity to find possible intrusions or attacks. Intrusion detection systems are either network-based or host-based; vendors are only beginning to integrate the two technologies. Network based intrusion detection systems are most common, and examine passing network traffic for signs of intrusion. Host-based systems look at user and process activity on the local machine for signs of intrusion. Each type has it own specific strengths and weaknesses. You might ask, Three kinds of commercially available analysis engines:

- Event or Signature-based Analysis
- Statistical Analysis
- Adaptive Systems

The event, or signature-based, systems function much like the anti-virus software with which most people are familiar. The vendor produces a list of patterns that it deems to be suspicious or indicative of an attack; the IDS merely scans the environment looking for a match to the known patterns. The IDS can then respond by taking a user-defined action, sending an alert, or performing additional logging. This is the most common kind of intrusion detection system.

A statistical analysis system builds statistical models of the environment, such as the average length of a telnet session, then looks for deviations from "normal". After over 10 years of government research, some products are just beginning to incorporate this technology into marketable products. The adaptive systems start with generalized rules for the environment, then learn, or adapt to, local conditions that would otherwise be unusual. After the initial learning period, the system understands how people interact with the environment, and then warns operators about unusual activities. There is a considerable amount of active research in this area.

You should keep in mind that any IDS will both miss some kinds of suspicious activity (false negatives) and signal alarms when there is nothing wrong (false positives). This is why organizations must have a strong human process that interacts with the IDS to evaluate the operating environment. The machine intelligence of most intrusion detection systems is still evolving, though current research is working to improve this. Remember, when reading these sections, that the discussion deals with generalizations. Each specific product has strengths and weaknesses, and some tools use multiple technologies to accomplish their goals.

II. EXISTING METHODS AND SYSTEM ANALYSIS

2.1 Redundancy Management

Hamid Al-Hamadi and Ing-Ray Chen has proposed a paper Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks. In this paper they propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of the redundancy management is to exploit.The tradeoff between energy consumption vs. the gain in reliability,timeliness, and security to maximize the system useful lifetime. They formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Furthermore, they consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect.Evict malicious nodes in a HWSN. For the issue of intrusion tolerance through multipath routing, there are two major problems to solve: (1) how many paths to use and (2) what paths to use. To the best of our knowledge, we are the first to address the "how many paths to use" problem. For the "what paths to use" problem, our approach is distinct from existing work in that we do not consider specific routing protocols (e.g., MDMP for WSNS or AODV for MANETs)

2.2 Host-Based Anomaly

B. Asfaw, D. Bekele, B. Eshete, A. Villafiorita, and K. Weldemariam, has proposed a paper "Host-based anomaly detection for pervasive medical systems". Intrusion detection systems are deployed on hosts in a computing infrastructure to tackle undesired events in the course of usage of the systems. One of the promising domains of applying intrusion detection is the healthcare domain. A typical healthcare scenario is characterized by high degree of mobility, frequent interruptions and above

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

all demands access to sensitive medical records by concerned stakeholders.Migrating this set of concerns in pervasive healthcare environments where the traditional characteristics are more intensified in terms of uncertainty, one ends up with more challenges on security due to nature of pervasive devices and wireless communication media along with classic security problems for desktop based systems. Despite evolution of automated healthcare services and sophistication of attacks against such services, there is a reasonable lack of techniques, tools and experimental setups for protecting hosts against intrusive actions.This paper presents a contribution to provide a host-based, anomaly modeling and detection approach based on data mining techniques for pervasive healthcare systems. The technique maintains normal usage profile of pervasive healthcare applications and inspects current workflow against normal usage profile so as to classify it as anomalous or normal. The technique is implemented as a prototype with sample data set and the results obtained revealed that the technique is able to perform classification of anomalous activities.

2.3 Trust-Based Intrusion

F. Bao, I. Chen, M. Chang, and J.H. Cho, has proposed a paper "Trust-based intrusion detection in wireless sensor networks". They propose a trust-based intrusion detection scheme utilizing a highly scalable hierarchical trust management protocol for clustered wireless sensor networks. Unlike existing work, they consider a trust metric considering both quality of service (QoS) trust and social trust for detecting malicious nodes.By statistically analyzing peer-to-peer trust evaluation results collected from sensor nodes, each cluster head applies trust-based intrusion detection to assess the trustworthiness and maliciousness of sensor nodes in its cluster. Cluster heads themselves are evaluated by the base station. They develop an analytical model based on stochastic Petri nets for performance evaluation of the proposed trust-based intrusion detection scheme. A statistical method for calculating the false alarm probability. They analyze the sensitivity of false alarms with respect to the minimum trust threshold below which a node is considered malicious. Further, the optimal trust threshold differs depending on the anticipated wireless sensor network lifetime.

2.4 Trust Management

Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho has proposed a paper Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection. They propose a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. Unlike prior work, we consider multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. A novel probability model, we describe a heterogeneous WSN comprising a large number of sensor nodes with vastly different social and quality of service (QoS) behaviors with the objective to yield "ground truth" node status. This serves as a basis for validating our protocol design by comparing subjective trust generated as a result of protocol execution at runtime against objective trust obtained from actual node status. To demonstrate the utility of our hierarchical trust management protocol, they apply it to trust-based geographic routing and trust-based intrusion detection. For each application, they identify the best trust composition and formation to maximize application performance.

2.5 Reliability Of Systems

F. B. Bastani, I. R. Chen, and T. W. Tsao, has proposed a paper "Reliability of systems with fuzzy-Failure criterion". In many situations, such as robot path planning and automated manufacturing systems, the output for a given input cannot be simply classified as being either correct (no failure) or incorrect (failure). Instead of an ad hoc binary classification of the correctness of the output, it is more intuitive to use a fuzzy set based classification scheme. One approach is to let the value of the fuzzy set membership function denote the degree of acceptability (i.e., correctness) of the output. In this paper, they investigate several such fuzzy-failure criteria and their effects on system reliability in embedded computer systems. They first model the fuzzy output level of a response to a sensor event as a random variable in the range of [0,1] with 0 indicating that the output is completely acceptable and 1 indicating that the output is completely unacceptable. Then they derive analytical expressions for the reliability of systems for various fuzzy-failure criteria and compare their numerical solutions. They conclude that the reliability of such systems depends significantly on the fuzzy-failure criterion defined by the system designer.

2.6 Critical State Analysis

A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Fovino, and A. Trombetta, has proposed a paper "A Multidimensional critical state analysis for detecting intrusions in SCADA systems". A relatively new trend in Critical Infrastructures (e.g., power plants, nuclear plants, energy grids, etc.) is the massive migration from the classic model of isolated systems, to a system-of-systems model, where these infrastructures are intensifying their interconnections through Information and

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

Communications Technology (ICT) means. The ICT core of these industrial installations is known as Supervisory Control And Data Acquisition Systems (SCADA). Traditional ICT security countermeasures (e.g., classic firewalls, anti-viruses and IDSs) fail in providing a complete protection to these systems since their needs are different from those of traditional ICT. This paper presents an innovative approach to Intrusion Detection in SCADA systems based on the concept of Critical State Analysis and State Proximity. The theoretical framework is supported by tests conducted with an Intrusion Detection System prototype implementing the proposed detection approach.

2.7 Artificial-Intelligence

I. R.ChenandF. B. Bastani, has proposed a paper "Effect of artificial-intelligence planning procedures on system reliability". For an embedded real-time process-control system incorporating artificial-intelligence programs, the system reliability is determined by both the software-driven response computation time and the hardware-driven response execution time. A general model, based on the probability that the system can accomplish its mission under a time constraint without incurring failure, is proposed to estimate the software/hardware reliability of such a system.

The factors which influence the proposed reliability measure are identified, and the effects of mission time, heuristics and real-time constraints on the system reliability with artificial-intelligence planning procedures are illustrated. An optimal search procedure might not always yield a higher reliability than that of a non-optimal search procedure. Hence, design parameters and conditions under which one search procedure is preferred over another, in terms of improved software/hardware reliability, are identified.

.

2.8 Adaptive Fault-Tolerant

Ing-Ray, Anh Phan Speer, and Mohamed Eltoweissy has proposed a paper Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks. Data sensing and retrieval in wireless sensor systems have a widespread application in areas such as security and surveillance monitoring, and command and control in battlefields. In query-based wireless sensor systems, a user would issue a query and expect a response to be returned within the deadline.

While the use of fault tolerance mechanisms through redundancy improves query reliability in the presence of unreliable wireless communication and sensor faults, it could cause the energy of the system to be quickly depleted. Therefore, there is an inherent trade-off between query reliability versus energy consumption in query-based wireless sensor systems. In this paper, they develop adaptive fault-tolerant quality of service (QoS) control algorithms based on hop-by-hop data delivery utilizing "source" and "path" redundancy.

The goal to satisfy application QoS requirements while prolonging the lifetime of the sensor system. That is they have developed an adaptive fault-tolerant QoS control (AFTQC) algorithm which incorporates path and source redundancy mechanisms to satisfy query QoS requirements while maximizing the lifetime of query-based sensor networks. They develop a mathematical model for the lifetime of the sensor system as a function of system parameters including the "source" and "path" redundancy levels utilized.

2.9 Analyzing dynamic voting

I. R. Chen and D. C. Wang, has proposed a paper "Analyzing dynamic voting using petri nets". Dynamic voting is considered a promising technique for achieving high availability in distributed systems with data replication. To date, stochastic analysis of dynamic voting algorithms is restricted to either site or link Markov models, but not both, possibly because of the difficulty in specifying the state-space which grows exponentially as the number of sites increases.

Furthermore, to reduce the state-space, the assumption of "frequent updates" was normally made, which results in an overestimation of the availability. In this paper, they develop a Petri net model that considers both site and link failures and also relaxes the modeling assumption of frequent updates. They test their Petri net model on ring and star network topologies to analyze if availability under dynamic voting can be seriously degraded if updates are not frequent under various site and link failure/repair situations.

Finally, they use the Petri net developed in the paper to determine the maximum achievable improvement in availability when null updates are introduced to augment regular updates to keep the status of availability up-to-date

2.10 Dynamic Threshold

Sheng-Tzong Cheng and Chi-Ming Chen has proposed a paper Performance Evaluation of an Admission Control Algorithm: Dynamic Threshold with Negotiation. An admission control algorithm for a multimedia server is responsible for determining if a new request can be accepted without violating the QoS requirements of the existing requests in the system. Most admission control algorithms treat every request uniformly and hence optimize the system performance by maximizing the number of admitted and served requests.

In practice, requests might have different levels of importance to the system. Requests offering high contribution or reward to the system performance

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

deserve priority treatment. Failure of accepting a high-priority request would incur high penalty to the system. A novel threshold-based admission control algorithm with negotiation for two priority classes of requests is proposed in our previous study. The server capacity is divided into three partitions based on the threshold values: one for each class of requests and one common pool shared by two classes of requests.

Reward and penalty are adopted in the proposed system model. High-priority requests are associated with higher values of reward as well as penalty than low-priority ones. In this paper, given the characteristics of the system workload, the proposed analytical models aim to finds the best partitions, optimizing the system performance based on the objective function of the total reward minus the total penalty. The negotiation mechanism reduces the QoS requirements of several low-priority clients, by cutting out a small fraction of the assigned server capacity, to accept a new high-priority client and to achieve a higher net earning value.

2.11 Existing System

Intrusion detection system (IDS) design for cyber physical systems (CPSs)Intrusion detection system (IDS) design for cyber physical systems (CPSs) has attracted considerable attention. he fundamental difference in designing IDSs for safety critical CPSs and other systems is that the intrusion detection is closely tied with the physical components of the CPS. The detection is less about communication protocol compliance but more about behavior compliance specific to the physical components to be controlled in the CPS.

Monitoring packet routing or packet loss data for misbehavior detection of communication protocol compliance during packet transmission, IDSs for MCPSs may test medical sensor measurements and actuator settings for misbehavior detection of physical properties manifested because of attacks.

Disadvantages

- IDS techniques for MCPSs is still with very little work reported A challenge is to provide a high detection rate without introducing high false positives.
- The existing IDS design based on the compliance threshold can not effectively distinguish normal abnormalities from malicious attacks.
- To the best of our knowledge, there is no prior work discussing the difference between CPS intrusion detection and communication systems intrusion detection.

2.12 PROPOSED SYSTEM

Intrusion detection techniques in general can be classified into four types: signature, anomaly, trust, and specification-based techniques. specification rather than signature-based detection to deal with unknown attacker patterns. 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.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 accommodate resource-constrained sensors. Actuators in an MCPS, we propose behavior-rule specification based intrusion detection (BSID) which uses the notion of behavior rules for specifying acceptable behaviors of medical devices in an MCPS. Rule-based intrusion detection thus far has been applied only in the context of communication networks which have no concern of physical environments and the closed-loop control structure as in an MCPS.

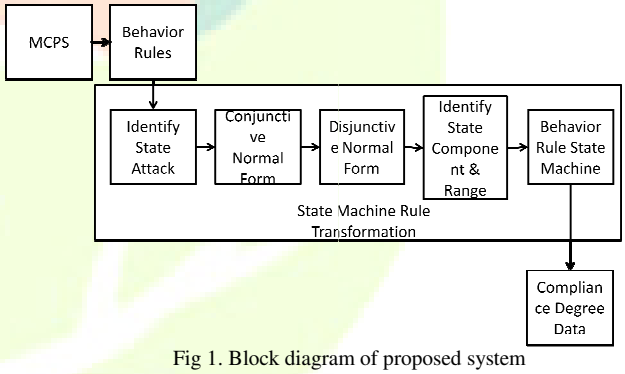


Fig 1. Block diagram of proposed system

Advantages

- specifically consider behavior rules for MCPS actuators controlling patient treatment algorithms as well as for physiological sensors providing information concerning the physical environment.
- A device that is being monitored for its behavior can easily be checked against the transformed state machine for deviation from its behavior specification.
- Attacks that violate the integrity of an MCPS that harm a patient.

2.13 MODULES DESCRIPTION

Implementation is the stage of the project in which the theoretical design is turned out into the working system.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

Thus it can be considered to be the most critical stage in developing the successful new system. It provides the confidence to the user that the new system will work more effectively.This implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve change over and evaluation of change over methods.

MODULE

The system implementation consists of the login page and the main modules of the system are given below:

1. MCPS Creation
2. MCPS View
3. Behaviour Rule Generation
4. Monitor
5. Data Reading
6. Actuator
7. Intrusion Detection

MCPS Creation

The MCPS creation module allows the user to create the number of Medical Cyber Physical System. It also consists of the following buttons

- CD
- PCA
- VSM

The CD button displays the three mode of operation in the Cardiac Device. They are the passive, pacemaker and defibrillator mode. The PCA displays its control type as Analgesic request. The VSM button displays the type of the sensor that it provides. They are temperature sensor, blood pressure sensor, pulse rate sensor, respiration rate sensor and oxygen saturation sensor.

MCPS View

The MCPS view displays the number of MCPS that has been created by the user. It also displays the name of the sensor and the actuators provided in each units.

Behaviour Rule Generation

The Behaviour Rule Generation module provides the default rules that are created during the generation of the MCPS. It displays the rule combinations that are to be checked during the process.

Monitor

The monitor module provide the facility for the user select the trustee MCPS and the monitor MCPS. The monitor MCPS check the reading of the trustee MCPS reading whether the reading and the control provided by the trustee MCPS is reliable or not.

Data Reading

The data reading module provide the facility for the user to choose the corresponding MCPS ID. Then it displays the reading of all the sensor in that sensor unit.

Actuator

The actuator module also allows the user to select the trustee MCPS. It then displays the control of the actuators.

Intrusion Detection

The intrusion detection module consists of three buttons. They are the CD, PCA and VSM. When these buttons are selected it displays the details of the trustee and the monitor MCPS. The intrusion status is displayed. Three type of intrusion status is displayed they are safe, warning and unsafe. The intruder in each unit can be displayed separately. The status is safe in case of no intruder. If there is slight variation in the reading of the trustee and the monitor then the status is displayed as warning. The unsafe status specifies the presence of the intruder in the trustee MCPS.

IV. EXPERIMENTAL RESULTS ANDDISCUSSIONS

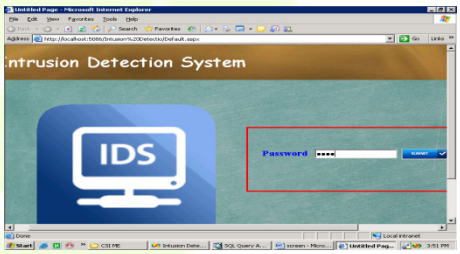


Fig 2. Login Page

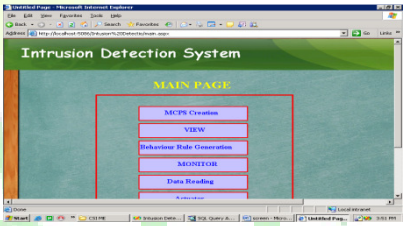


Fig 3. MCPS Creation

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

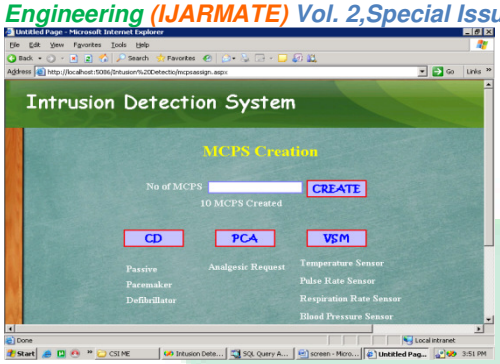


Fig 4.View

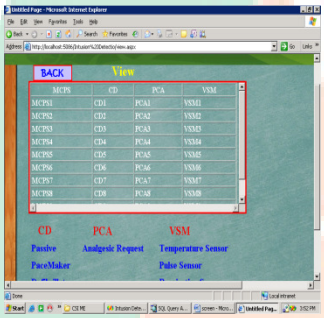


Fig 5.Behaviour Rules

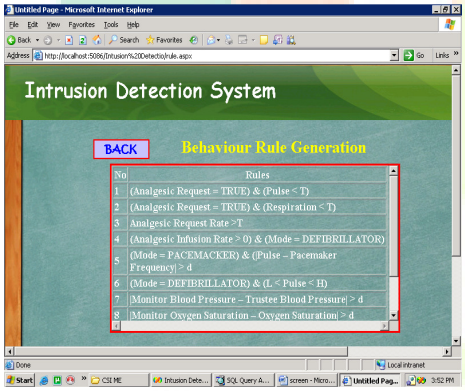


Fig 6.Monitor

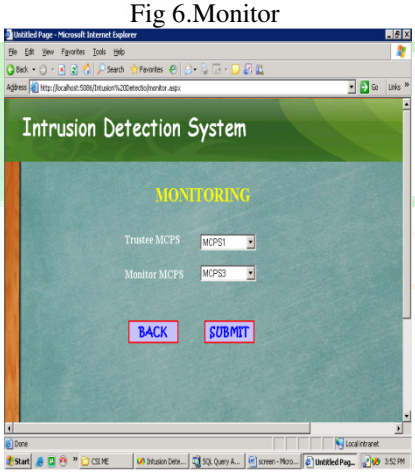


Fig 7.Data Reading

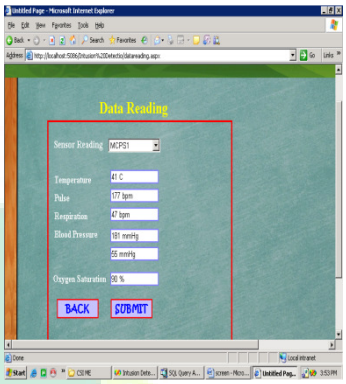


Fig 8.Actuator

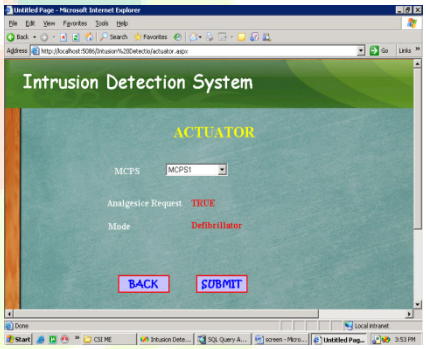


Fig 9.Intrusion Detection(DC)

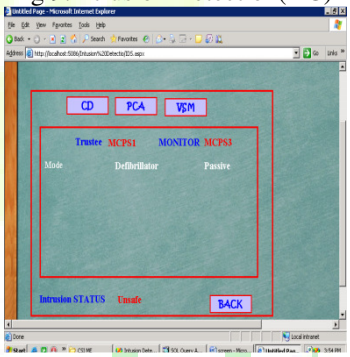
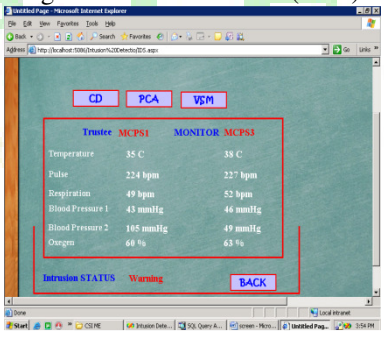


Fig 10.Intruction Dection(PCA)



ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

Fig11.Intrusion Detction(VSM)

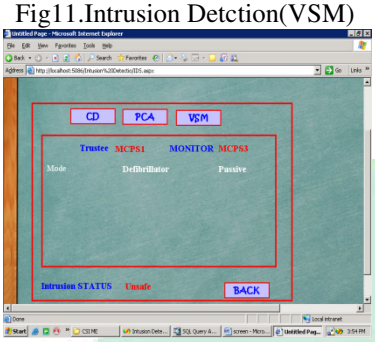


Fig12.Instruction Status

V. 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 project we have proposed a behavior-rule specification-based IDS technique for intrusion detection of medical devices embedded in a MCPS. We exemplified the utility with VSMs and demonstrated that the detection probability of the medical device approaches one (that is, we can always catch the attacker without false negatives) while bounding the false alarm probability to below 5 percent for reckless attackers and below 25 percent for random and opportunistic attackers over a wide range of environment noise levels. This system provides three output denoting three stages in the system they are the safe, warning and the unsafe state. The warning state shows that there are chances for an intruder and the unsafe state says that there is an intruder. Thus the presence of the intruder can be detected effectively using the proposed behavior-rule specification-based IDS technique.

REFERENCES

1. H. Al-Hamadi and I. R. Chen, "Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensor networks," IEEE Trans. Netw. Service Manage., vol. 10, no. 2, pp. 189–203, Jun. 2013.
2. M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Security challenges in next generation cyber physical systems," Beyond SCADA: Netw. Embedded Control for Cyber Phys. Syst., Pittsburgh, PA, USA, Nov. 2006.
3. B. Asfaw, D. Bekele, B. Eshete, A. Villafiorita, and K. Weldemariam, "Host-based anomaly detection for pervasive medical systems," in Proc. 5th Int. Conf. Risks Security Internet Syst., Oct. 2010, pp. 1–8.
4. F. Bao, I. Chen, M. Chang, and J.H. Cho, "Trust-based intrusion detection in wireless sensor networks," in Proc. IEEE Int. Conf. Commun., Jun. 2011, pp. 1–6.
5. F. Bao, I. R. Chen, M. Chang, and J. H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manage., vol. 9, no. 2, pp. 169–183, Jun. 2012.
6. F. B. Bastani, I. R. Chen, and T. W. Tsao, "Reliability of systems with fuzzy-failure criterion," in Proc. Annu. Rel. Maintainability Symp., Anaheim, CA, USA, Jan. 1994, pp. 442–448.
7. 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 Trans. Ind. Inf., vol. 7, no. 2, pp. 179–186, May 2011.
8. A. C_ardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in Proc. 1st Workshop Cyber-Phys. Syst. Security DHS, 2009, pp. 1–4.
9. I. R.ChenandF. B. Bastani, "Effect of artificial-intelligence planning procedures on system reliability," IEEE Trans. Rel., vol. 40, no. 3, pp.364–369,Aug.1991.
10. I. R. Chen, F. B. Bastani, and T. W. Tsao, "On the reliability of AI planning software in real-time applications," IEEE Trans. Knowl. Data Eng., vol. 7, no. 1, pp. 4–13, Feb. 1995.
11. I. R. Chen and T. H. Hsi, "Performance analysis of admission control algorithms based on reward optimization for real-time multimedia servers," Perform. Eval., vol. 33, no. 2, pp. 89–112, 1998.
12. I. R. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive fault tolerant QOS control algorithms for maximizing system lifetime of query-based wireless sensor networks," IEEE Trans. Dependable Secure Comput., vol. 8, no. 2, pp. 161–176, Mar./Apr. 2011.
13. I. R. Chen and D. C. Wang, "Analysis of replicated data with repair dependency," The Comput. J., vol. 39, no. 9, pp. 767–779, 1996.
14. I. R. Chen and D. C. Wang, "Analyzing dynamic voting using petri nets," in Proc. 15th IEEE Symp. Rel. Distrib. Syst., Niagara Falls, Canada, Oct. 1996, pp. 44–53.
15. S.-T. Cheng, C.-M. Chen, and I. R. Chen, "Dynamic quota-based admission control with sub-rating in multimedia servers," Multimedia Syst., vol. 8, no. 2, pp. 83–91, 2000.
16. S.-T. Cheng, C.-M. Chen, and I. R. Chen, "Performance evaluation of an admission control algorithm: Dynamic threshold with negotiation," Perform. Eval., vol. 52, no. 1, pp. 1–13, 2003.
17. S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

detection for SCADA networks," in Proc. SCADA Secur. Sci. Symp., Miami, FL, USA, Jan. 2007, pp. 127–134.

18. J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," IEEE Trans. Rel., vol. 59, no. 1, pp. 231–241, Mar. 2010.

19. J.-H. Cho, A. Swami, and I.-R. Chen, "Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks," in Proc. Int. Conf. Comput. Sci. Eng., Aug. 2009, pp. 641–650.

20. J.-H. Cho, A. Swami, and I. R. Chen, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 1001–1012, 2012.