5-2018

OpenICE-lite: Towards a Connectivity Platform for the Internet of Medical Things

Radoslav Ivanov
University of Pennsylvania, rivanov@cis.upenn.edu

Hung Nguyen
University of Pennsylvania, hungng@cis.upenn.edu

James Weimer
University of Pennsylvania, weimerj@cis.upenn.edu

Oleg Sokolsky
University of Pennsylvania, sokolsky@cis.upenn.edu

Insup Lee
University of Pennsylvania, lee@cis.upenn.edu

Recommended Citation

Radoslav Ivanov, Hung Nguyen, James Weimer, Oleg Sokolsky, and Insup Lee, "OpenICE-lite: Towards a Connectivity Platform for the Internet of Medical Things", *IEEE ISORC 2018* . May 2018.

IEEE ISORC 2018, Singapore, May 29 - 31, 2018

OpenICE-lite: Towards a Connectivity Platform for the Internet of Medical Things

Abstract

The Internet of Medical Things (IoMT) is poised to revolutionize medicine. However, medical device communication, coordination, and interoperability present challenges for IoMT applications due to safety, security, and privacy concerns. These challenges can be addressed by developing an open platform for IoMT that can provide guarantees on safety, security and privacy. As a first step, we introduce OpenICE-lite, a middleware for medical device interoperability that also provides security guarantees and allows other IoMT applications to view/analyze the data in real time. We describe two applications that currently utilize OpenICE-lite, namely (i) a critical pulmonary shunt predictor for infants during surgery; (ii) a remote pulmonary monitoring systems (RePulmo). Implementations of both systems are utilized by the Children's Hospital of Philadelphia (CHOP) as quality improvements to patient care.

Disciplines

Computer Engineering | Computer Sciences

Comments

IEEE ISORC 2018, Singapore, May 29 - 31, 2018

OpenICE-lite: Towards a Connectivity Platform for the Internet of Medical Things

Radoslav Ivanov, Hung Nguyen, James Weimer, Oleg Sokolsky, and Insup Lee
PRECISE Center
Computer and Information Science Department
University of Pennsylvania
Email: {rivanov, hungng, weimerj, sokolsky, lee}@cis.upenn.edu

Abstract—**The Internet of Medical Things (IoMT) is poised to revolutionize medicine. However, medical device communication, coordination, and interoperability present challenges for IoMT applications due to safety, security, and privacy concerns. These challenges can be addressed by developing an open platform for IoMT that can provide guarantees on safety, security and privacy. As a first step, we introduce OpenICE-lite, a middleware for medical device interoperability that also provides security guarantees and allows other IoMT applications to view/analyze the data in real time. We describe two applications that currently utilize OpenICE-lite, namely (i) a critical pulmonary shunt predictor for infants during surgery; (ii) a remote pulmonary monitoring systems (RePulmo). Implementations of both systems are utilized by the Children's Hospital of Philadelphia (CHOP) as quality improvements to patient care.**

I. Introduction

Technology has revolutionized the medical landscape, serving as a force multiplier in the mission to save lives. The Internet of Medical Things (IoMT) is evolving rapidly as medical devices become smaller, often implantable, with embedded intelligence, and with the ability to (wirelessly) transmit information [12]. The IoMT framework would make it possible to continuously monitor vital physiological functions without disrupting normal lifestyle and, crucially, implement timely corrective actions.

Developing such a broad IoMT framework requires building two components that are currently in early stage: 1) the IoMT infrastructure that ensures proper medical device interoperability and secure data management; 2) data analytics techniques for processing medical data and providing guaranteed performance regardless of the physiology/context of the specific person who generated the data. Although some aspects of both components exist in other fields, simply adopting existing solutions would be insufficient to satisfy the strict requirements of the medical setting as well as to ensure the emergent safety and security properties of the composed system.

In this paper, we describe the main challenges with building the first of the above components, namely an IoMT infrastructure for ensuring the proper interoperability and communication between all IoMT entities. To be effective, such a platform must support both computer security "best" practices (e.g., encryption, secure key distribution) as well as plug-and-play medical devices from different manufacturers with different message types and built-in security features. In addition, this system must provide real-time communication and performance guarantees since medical systems are inherently safety- and time-critical. Finally, it is essential to store all IoMT data safely and securely to enable retrospective and forensic analysis while ensuring the privacy of the stored data.

With the above challenges in mind, we developed OpenICE-lite, a general-purpose IoMT middleware for safe and secure medical device interoperability. OpenICE-lite evolved as a lightweight and modular version of OpenICE, an open-source medical device interoperability platform that satisfies the Integrated Clinical Environment (ICE) framework [2]. OpenICE-lite separates device drivers from IoMT communication protocols (e.g., although OpenICE-lite uses the lightweight Message Queuing Telemetry Transport (MQTT) protocol, it can also work with the Data Distribution Service (DDS) protocol used in OpenICE). Thus, OpenICE-lite enables the addition of applications that analyze medical data in real time and potentially close the loop as well as applications for safe and secure data storage. Furthermore, OpenICE-lite provides strong security guarantees, with end-to-end message encryption and the capability of secure data logging and storage.

To demonstrate the usefulness of OpenICE-lite, we describe two applications that use the proposed infrastructure and illustrate the benefit of a general-purpose IoMT middleware. The first is the implementation of the critical pulmonary shunt predictor for predicting shunt-induced hypoxia events during surgery [8], [9], [10]. The critical pulmonary shunt predictor was originally applied on retrospective data and was subsequently implemented (using OpenICE-lite to communicate with the anesthesia machine in real time) in an operating room (OR) at the Children's Hospital of Philadelphia (CHOP). The second application supports the Bronchopulmonary Dysplasia Saturation TARgeting (BPD STAR) pilot trial; in this trial, oxygen saturation (SpO2) data is collected from babies who experience BPD in an effort to determine whether long-term supplemental oxygen might reduce intermittent hypoxemia. This trial utilized a remote pulmonary monitoring system (named RePulmo), where OpenICE-lite is installed in each patient's home and communicates with the pulse oximeter that provides SpO2; the collected data is eventually securely

This work was supported in part by NSF CNS-1505799 and the Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy.

transmitted to a server in CHOP for permanent storage.

II. Current Challenges in Building an IoMT Connectivity Platform

This section presents the current challenges associated with building a general purpose IoMT infrastructure.

A. Medical Device Communication and Interoperability

The first challenge has to do with the current state of medical devices. Most devices used in modern ORs were developed a few decades ago and do not have sophisticated communication capabilities. The standard way of obtaining their measurement data is through a serial port at the back of the device. What is more, the measurements usually arrive at low time granularity (e.g., once a second) and are often numeric only (i.e., the "raw" waveform data is rarely available). Thus, low data quality is still a major obstacle to building reliable data analytics systems in the medical space.

In addition to the data quality issue, medical devices often have proprietary communication protocols and are not setup to share information with each other (especially if they are not produced by the same vendor). In addition, patient health records and demographic information are not even accessible through medical devices (but are rather stored in central hospital servers). This makes it challenging to collect all the data in a centralized location and have a holistic view of the patient. As a result, several interoperability platforms (e.g., OpenICE) as well as health record integration platforms (Smart on FHIR [4]) have been proposed but none has so far been widely adopted (partially due to vendors' concerns that they might lose their market share).

B. Security and Privacy

Several attacks have been carried out over the last decade showing that medical devices have poor or no security guarantees [7], [13], [17]. This issue is bound to become more pronounced as medical devices begin to communicate remotely and wirelessly such that attacks might no longer require physical access or domain expertise. Furthermore, since medical devices often contain personal information about the patient, concerns about the privacy of the transmitted data have started to emerge. Although no privacy attacks similar to the movie database attack have been performed yet [15], it might be possible to identify people based on unique physiological patterns (e.g., a heart murmur).

C. Real-time Guarantees

Since the IoMT systems will ultimately be used in a closed-loop fashion, real-time guarantees are essential for the correct functioning of such a system. Real-time analysis is especially challenging given the distributed and wireless setting of IoMT, coupled with some variant of a publish-subscribe framework where nodes are allowed to enter and leave the network as necessary.

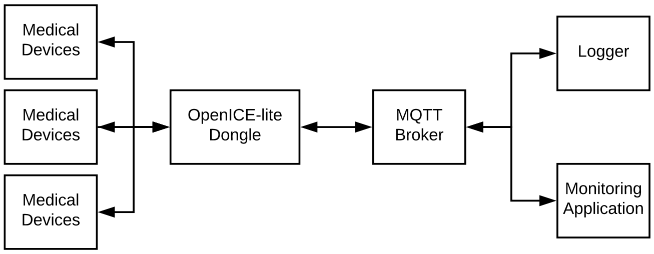

Fig. 1. Overview of OpenICE-lite.

D. Availability and Quality of Service

Due to their safety-critical nature, IoMT systems need to always have high availability and guarantee a certain quality of service. This is especially true in emergency situations where high-volume data might be generated and timely measures might be required. Current IoT systems do not have any provisions for such scenarios and usually provide "best effort" type of guarantees.

III. OpenICE-lite: A Lightweight Safe and Secure IoMT Platform

In order to address some of the challenges presented in Section II, we developed OpenICE-lite, an IoMT platform for medical device interoperability that also provides security guarantees and allows other IoMT applications to view/analyze the data in real time and possibly close the loop. This section provides a brief description of OpenICE-lite as it pertains to the challenges listed above.

A. Medical Device Interoperability

To enable medical device interoperability, OpenICE-lite provides a dongle for each medical device. The dongle is a small device (e.g., a Raspberry Pi) that is connected to the respective medical device and implements its communication protocol in order to receive all measurement data. Once the dongle receives a message from the device, it transmits it to the rest of the OpenICE-lite system as detailed in the next subsections.[1]

B. Publish/Subscribe Communication

Since OpenICE-lite operates in the IoMT, it needs to allow nodes, i.e., medical device/dongle pairs, to enter and leave the network as desired. The most flexible way to enable such a framework is through a publish/subscribe protocol where new nodes announce the type of data they provide whereas existing ones can subscribe to the newly transmitted data. The current OpenICE-lite implementation uses the MQTT [3] protocol.[2] MQTT was chosen due to its lightweight nature in comparison with other existing publish/subscribe middlewares (e.g., DDS [1]), which is an essential property in the dynamic

[1] Note that the interoperability part of OpenICE-lite is the only part that is similar to the original OpenICE in the sense that the medical device communication drivers are mostly identical.

[2] OpenICE-lite is designed to be modular with respect to the underlying middleware so that other middlewares (e.g., [1], [5] can also be used.

environment of the IoMT. MQTT consists of a centralized broker that manages all communication and individual clients who are the users of the infrastructure. Note that although the broker is centralized, it is possible to use a cluster instead of a single machine, thereby addressing scalability concerns that might arise in an IoMT setting. Furthermore, MQTT provides certain quality-of-service guarantees (e.g., guaranteed message delivery) that also make it suitable for the medical setting.

With the above framework in mind, the MQTT clients (i.e., nodes on the network) are two types: 1) dongles, i.e., clients that serve as a proxy between MQTT and the medical devices themselves, and 2) applications, i.e., clients that use the medical device data (either to log it or to analyze it) and potentially close the loop (if the medical device supports such a function). OpenICE-lite supports dongles for almost all medical devices currently in use (e.g., Philips bedside monitors, Drager ventilators/anesthesia machines, Puritan Bennett ventilators). Two example application clients we have developed, namely the PAIN detector and RePulmo, are described in Sections IV-A and IV-B, respectively.

C. *Secure Communication*

As noted in Section II, secure communication is one of the main requirements for any IoMT platform. Since the vanilla version of MQTT does not support secure communication, we augmented the protocol with a security wrapper. In particular, we use the Transport Layer Security (TLS) protocol in order to establish a secure communication between any two MQTT clients.[3] TLS is a widely adopted communication protocol as it combines symmetric and asymmetric encryption and provides strong security guarantees if the keys are periodically refreshed.

With the TLS-augmented communication protocol, OpenICE-lite is able to defend against most known information attacks such as eavesdropping and replay attacks. Since decrypting a TLS message (with fresh keys) is infeasible with modern computers, it is impossible for an eavesdropper to learn anything about a message's payload; similarly, replay attacks are prevented by adding sequence numbers in the encrypted message. Finally, the distributed nature of MQTT also makes it harder to perform a denial-of-service (DoS) attack, although effectively defending against DoS attacks is still an active research area.

IV. Applications Utilizing OpenICE-lite

This section describes two applications that employ OpenICE-lite: (i) a critical pulmonary shunt predictor for infants during surgery; (ii) a remote pulmonary monitoring systems (RePulmo). Both systems are implemented within CHOP.

A. *Critical Pulmonary Shunt Predictor*

This subsection describes the first application of OpenICE-lite, namely the critical pulmonary shunt predictor for infants and as implemented in an OR in CHOP.

1) Pulmonary Shunts during Surgery: During surgery, blood oxygen content is perhaps the most closely monitored physiological variable, as values that are too low can lead to organ failure (e.g., brain damage), and values that are too high can cause atelectasis (e.g., collapse of the lungs). Pulmonary shunts, which occur when a patient is breathing with only one lung, can cause dangerous drops in oxygen levels. Shunts can be caused by a physical disorder, such as pulmonary edema, or may occur accidentally in patients being mechanically ventilated, if ventilation tubes are improperly placed. Occasionally, one-lung ventilation is intentionally induced via a shunt at the request of a surgeon to keep a lung still for operation. Infants are especially vulnerable to accidental shunts because they have small, underdeveloped lungs. In these patients, breathing with one lung may not supply enough oxygen to the body, and the oxygen content may quickly drop to dangerously low levels.

Though it is one of the most closely monitored physiological variables during surgery, blood oxygen content is also one of the most challenging to monitor, as it cannot currently be measured non-invasively or in real time. Instead, clinicians must monitor proxy variables. One popular proxy is the hemoglobin oxygen saturation in the peripheral capillaries, denoted by S_pO_2. While it is a good non-invasive measure of the oxygen content in the location at which it is measured (usually a fingertip, or the foot in small infants), S_pO_2 is a delayed measure of the oxygen content in other parts of the body (e.g., the arteries), as blood takes time to circulate.

2) The Critical Pulmonary Shunt Predictor: It is possible to predict drops in a patient's oxygen content before these drops are observed through the current low S_pO_2 approach by developing a detector using multiple pulmonary measurements that are available through an anesthesia machine, namely the partial pressures of oxygen and carbon dioxide, tidal volume, and respiratory rate [9], [10]. We developed a parameterized model of the circulation of the partial pressures of oxygen and carbon dioxide around the cardiovascular and pulmonary systems for the purposes of critical pulmonary shunt detection in infants. Since the model parameters vary drastically across patients and cannot be reliably estimated from data, we used a Parameter Invariant (PAIN) detector which provides a near-constant false alarm rate for all patients regardless of the specific values of the physiological parameters. The PAIN detector was originally evaluated on retrospective data. Over 61 patients experiencing a drop in blood oxygen concentration, the detector achieves a detection rate of about 85% with an early warning of 90 seconds on average. In addition, it achieves a false alarm rate of 0.95 false alarms per hour (about 0.5% of the tests) across 314 patients who did not experience a pulmonary shunt.

3) The Critical Pulmonary Shunt Predictor as an OpenICE-lite Application: Given the predictor's impressive performance on retrospective data, we implemented it in an OR in CHOP in order to aid clinicians in real time. We developed a dongle that connects to the anesthesia machine and publishes the required measurements to the MQTT broker. The predictor

[3] The TLS (public and private) encryption keys are distributed by a key distribution server as each node enters the network.

is implemented on another machine in the OR that subscribes to the dongle measurements and outputs its decision. Finally, the predictor's decision is displayed on a large screen such that clinicians are alerted when a pulmonary shunt might result in a drop in oxygen levels. Although the predictor's actual performance cannot be revealed due to data privacy reasons, our clinical collaborators assured us that the real-time performance is in line with the retrospective one.

B. Remote Pulmonary Monitoring System (RePulmo)

This subsection describes a second application of OpenICE-lite, namely the remote pulmonary monitoring system (RePulmo) as part of a clinical trial at CHOP.

1) Bronchopulmonary Dysplasia (BPD) in Infants: Bronchopulmonary dysplasia (BPD) is a chronic lung disease of prematurity that is associated with poor long-term outcomes, yet no therapies have been proven to improve the outcomes of children with BPD. Frequency of intermittent hypoxemia (IH) in extremely preterm infants during the newborn period is associated with death or developmental disability at 18 months, and infants with BPD may be at risk for continued IH, even after hospital discharge. The risks and benefits of using supplemental oxygen to target different oxygen saturation levels have been evaluated extensively in preterm infants during the initial hospitalization, but have not been studied in infants with established lung disease as they approach term corrected age and are discharged home. To answer this question, the Bronchopulmonary Dysplasia Saturation TARgeting (BPD STAR) pilot trial conducted at CHOP aims to collect oxygen saturation (SpO2) data from infants who experience BPD in an effort to determine whether long-term supplemental oxygen might reduce intermittent hypoxemia.

2) RePulmo as an OpenICE-lite Application: To collect SpO2 data remotely from infants at home, we developed RePulmo system which employs two parts: (a) a remote collector device for each patient to continuously measure SpO2 data and send to CHOP, and (b) a back-end infrastructure to receive data from all collector devices and securely store data to a database. The collector device is a Masimo Rad-8 Pulse Oximeter with an attached dongle running OpenICE-lite to publish data to the MQTT broker via an LTE 4G hotspot. With the widely used Masimo device for hospital bedside monitoring, the setup ensures that the collected data are aligned with hospital-grade accuracy and also provides the seamless experience for the patient. Collected data are encrypted within MQTT network and can only be decrypted by the logger running inside CHOP infrastructure. Given the decrypted data, the logger performs sanity checks and writes to an embedded relational database for further analysis. RePulmo is currently under deployment at CHOP and we are expecting to support 42 patients over the course of 6 months continuous monitoring.

V. Discussion and Future Research Directions

This paper presented the OpenICE-lite platform for IoMT applications. As outlined in Section II, there are many open research challenges in developing systems for IoMT. Future work includes (1) providing a medical-application development language with tools to assure the correctness and safety of medical applications; (2) extending OpenICE-lite to utilize the Mobile Edge Computing (MEC) paradigm to manage the security, privacy, QoS, and high availability of solutions based on the Integrated Clinical Environment (ICE); (3) extending MQTT to provide real-time guarantees. The combination of MEC [16] with new technologies as Network Function Virtualization (NFV) and Software Defined Networking (SDN) [11], [14] can provide a new flexible, efficient, and fault-tolerant platform suitable for IoMT challenges. Specifically, the MEC paradigm will enable the management of the components defined by the ICE framework in the edge of the network, which is a critical aspect in order to ensure the low-latency associated to the QoS [6].

References

[1] Data Distribution Services (DDS). https://www.omg.org/dds/.

[2] Integrated Clinical Environment (ICE) Standard. http://mdpnp.org/uploads/F2761_completed_committee_draft.pdf.

[3] OASIS Message Queuing Telemetry Transport. www.mqtt.org.

[4] Smart on FHIR. http://docs.smarthealthit.org/.

[5] aloma Rubio-Conde, D. Villarn-Molina, and M. Garca-Valls. Measuring performance of middleware technologies for medical systems: Ice vs amqp. *SIGBED review*, 14(2):8–14, 20017.

[6] L. Gu, D. Zeng, S. Guo, A. Barnawi, and Y. Xiang. Cost efficient resource management in fog computing supported medical cyber-physical system. *IEEE Transactions on Emerging Topics in Computing*, 5(1):108–119, 2017.

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

[8] R. Ivanov, J. Weimer, and I. Lee. Context-aware detection in medical cyber-physical systems. In *Proceedings of the ACM/IEEE Ninth International Conference on Cyber-Physical Systems (ICCPS)*, 2018. Accepted.

[9] R. Ivanov, J. Weimer, A. Simpao, M. Rehman, and I. Lee. Early detection of critical pulmonary shunts in infants. In *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems (ICCPS)*, pages 110–119, 2015.

[10] R. Ivanov, J. Weimer, A. F. Simpao, M. A. Rehman, and I. Lee. Prediction of critical pulmonary shunts in infants. *IEEE Transactions on Control Systems Technology*, 24(6):1936–1952, Nov 2016.

[11] A. L. King, S. Chen, and I. Lee. The middleware assurance substrate: Enabling strong real-time guarantees in open systems with openflow. In *Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), 2014 IEEE 17th International Symposium on*, pages 133–140. IEEE, 2014.

[12] I. Lee, O. Sokolsky, S. Chen, et al. Challenges and research directions in medical cyber–physical systems. *Proceedings of the IEEE*, 100(1):75–90, 2012.

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

[14] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob. Toward an sdn-enabled nfv architecture. *IEEE Communications Magazine*, 53(4):187–193, 2015.

[15] A. Narayanan and V. Shmatikov. How to break anonymity of the netflix prize dataset. *arXiv preprint cs/0610105*, 2006.

[16] R. Roman, J. Lopez, and M. Mambo. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78:680–698, 2018.

[17] R. Van Der Togt, E. J. van Lieshout, R. Hensbroek, E. Beinat, J. M. Binnekade, and P. Bakker. Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment. *Jama*, 299(24):2884–2890, 2008.