Systematic Threat Analysis of Modern Unified Healthcare Communication Systems

AKM Iqtidar Newaz, Ahmet Aris, Amit Kumar Sikder, and A. Selcuk Uluagac
Cyber-Physical Systems Security Lab
Florida International University, Miami, Florida, USA
{anewa001, aaris, asikd003, suluagac}@fiu.edu

GLOBECOM 2022 - 2022 IEEE Global Communications Conference | 978-1-6654-3540-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/GLOBECOM48099.2022.10001605

***Abstract*—Recently, smart medical devices have become prevalent in remote monitoring of patients and the delivery of medication. The ongoing Covid-19 pandemic situation has boosted the upward trend of the popularity of smart medical devices in the healthcare system. Simultaneously, different device manufacturers and technologies compete for a share in a smart medical device's market, which forces the integration of diverse smart medical devices into a common healthcare ecosystem. Hence, modern unified healthcare communication systems (UHCSs) combine ISO/IEEE 11073 and Health Level Seven (HL7) communication standards to support smart medical devices' interoperability and their communication with healthcare providers. Despite their advantages in supporting various smart medical devices and communication technologies, these standards do not provide any security and suffer from vulnerabilities. Existing studies provide stand-alone security solutions to components of UHCSs and do not cover UHCSs holistically. In this paper, we perform a systematic threat analysis of UHCSs that relies on attack-defense tree (ADTree) formalisms. Considering the attack landscape and defense ecosystem, we build an ADTree for UHCSs and convert the ADTree to stochastic timed automata (STA) to perform quantitative analysis. Our analysis using UPPAAL SMC shows that the Man-in-the-Middle and unauthorized remote access attacks are the most probable attacks that a malicious entity could pursue, causing mistreatment to patients. We also extract valuable information about the top threats, the likelihood of performing different individual and simultaneous attacks, and the expected cost for attackers.**

***Index Terms*—Smart Medical Device, Healthcare Communication, ISO/IEEE-11073, HL7**

I. Introduction

In recent years, the healthcare industry has seen a dramatic increase in the utilization of smart medical devices. Smart medical devices are highly interconnected entities capable of performing traditional healthcare operations while enabling remote monitoring and transmission of health data. Currently, millions of smart medical devices (e.g., blood pressure monitors, pulse oximeters, insulin pumps, etc.) are remotely monitoring the patients, and that number is projected to reach 80.3 billion by 2027 [1]. Along the same line, the ecosystem of smart medical devices got considerably vast as over half a million different medical devices were manufactured in recent years [2].

Given this emerging interest, different device manufacturers offer myriads of smart medical devices to compete for a share in a smart medical device's market, which use different communication technologies (e.g., Bluetooth/BLE, WiFi, etc.). Similarly, the standardization organizations proposed a multitude of standards to support the interoperability of devices and their communications with healthcare providers. Among the communication standards, ISO/IEEE-11073 [3] and HL7-FHIR (Health Level Seven (HL7) International-Fast Healthcare Interoperability Resources) [4] are the most widely used standards [5] that complement each other in modern *unified healthcare communication systems* (UHCSs).

Although ISO/IEEE-11073 and HL7-FHIR standards provide interoperability and communication flexibility to UHCSs, they have become lucrative targets for attackers since both standards do not provide any security mechanisms. In fact, security pitfalls of HL7-FHIR [6] and ISO/IEEE-11073 [7] have already been shown in the literature, putting thousands of UHCSs at great risk. Although there have been attempts to secure those protocols [6], [7], or harden individual devices or communication technologies [8], [9], such solutions have been stand-alone and have not been covering UHCSs holistically with consideration of the wide attack landscape and existing defense ecosystem.

In this paper, we analyze the security of UHCSs and perform systematic threat analysis that relies on attack-defense tree (ADTree) formalisms. ADTree is a well-established approach for systematic security analysis [10]. We build an ADTree for UHCSs considering the wide landscape of threats and ecosystem of defenses. To perform quantitative security analysis and understand the top threats and the minimal attack time and the cost values, we follow the state-of-the-art and convert our ADTree to stochastic timed automata (STA). Our quantitative analysis with UPPAAL SMC shows that Man-in-the-Middle (MitM) and unauthorized remote access attacks are the most probable attacks that a malicious entity could pursue, causing mistreatment to patients.

Contributions: Our contributions are three-fold:

- We methodically identify the threats against UHCSs, existing defenses and build an ADTree.
- We transform the ADTree to STA models to perform quantitative security analysis.
- By means of the quantitative security analysis, we extract the top threats, the success probability of performing individual and simultaneous attacks, and the expected cost for attackers to achieve their goals in UHCSs.

Organization: The rest of the paper is organized as follows:

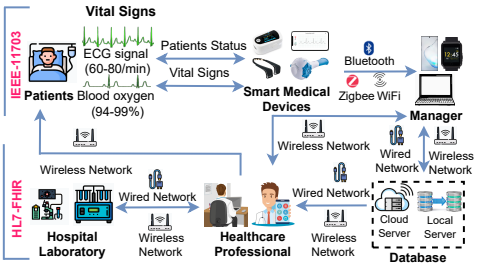


Fig. 1: An example of a UHCS.

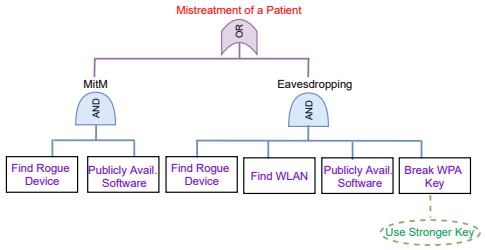


Fig. 2: An example of an ADTree.

Section II provides the background information on UHCSs, ADTree, and STA. Section III defines the threat model, presents the ADTree modeling and the conversion process of the ADTree to STA. Section IV performs quantitative analysis. Section V reviews the related work. Finally, Section VI concludes the paper.

II. Background

In this section, we provide background information on UHCSs. Also, we explain how attack trees and STA can be used for threat analysis in a UHCS.

A. Modern Unified Healthcare Communication Systems

Modern unified healthcare communication systems provide real-time data integration and interoperability for smart medical devices, healthcare providers, and external systems to provide seamless services to patients. The communication in UHCSs is divided into two segments where the communication between a healthcare device and a manager (e.g., smartphone, smartwatch, etc.) is followed by ISO/IEEE-11073 standard and from the manager to the healthcare professional/hospital is followed by HL7-FHIR communication standard. An example UHCS is shown in Figure 1. It consists of a single or a group of smart medical devices that can be used both at home and in hospital networks. These smart medical devices are equipped with different physiological sensors to collect data from a patient's body and send it to a manager via wireless communication protocols (i.e., Bluetooth, WiFi, etc.). A manager can be an intermediate device (e.g., smartphone, laptop, or smartwatch) that works as a user interface and forwards data to a database deployed in a cloud and/or local server or directly sends to the healthcare professional. The communication between the smart medical device and the manager is based on the ISO/IEEE-11073 communication standard. Healthcare professionals can further analyze patients' health status by obtaining patients' data from the database/manager via wired or wireless networks. Finally, healthcare professionals examine those data at the hospital laboratory and send feedback to the patients. Here, the communication starting from the manager to the hospital laboratory is based on the HL7-FHIR standard.

Security of Communication Standards: The ISO/IEEE 11073 standard is transport-layer agnostic; it is supported by almost any datagram-based technology such as TCP/IP and Bluetooth Low Energy (BLE). However, it does not provide any security for healthcare data exchange, and patient monitoring [7]. It relies on the transport layer implementations of known protocols for security. Similarly, FHIR does not define any security-related functionality and depends on transport layer security and OAuth for communication security and authentication, respectively [11]. Since both standards do not provide security, their security pitfalls have been shown in [7], [12] which puts thousands of UHCSs at great risk.

B. Attack(-Defense) Trees

Attack trees [13] provide a formal, systematic way of describing complex systems' security based on various attacks. They have hierarchical structures that graphically display attacker goals, sub-goals, and a series of steps that make it possible for attackers to reach these goals. It is possible to perform quantitative analysis of attack trees and assess the severity of attacks thanks to their hierarchical structure [10]. In an attack tree, the root node represents attacker's goal and is divided into subgoals by *logic gates* until subgoals cannot be processed further and reached *basic attack steps (BASs)* constituting only the leaves of the tree. *BASs* are individual atomic steps within a composite attack that appear as leaves of the attack tree. Boolean *AND* gate is used to state whether a node in a tree requires achieving all of its sub-nodes or *OR* gate for any of its sub-nodes.

The limitation of attack trees is that they cannot capture the interaction between attackers and defenders on a system. To overcome this, attack-defense trees (ADTrees) were introduced as an extended security formalism [14]. ADTree describes how an attacker might attack a system and the defenses that a defender can employ against. It has two types of nodes: attack nodes and defense nodes that correspond to attacker's and defender's goals respectively. An example ADTree in a UHCS is shown in Figure 2. As shown in the figure, the root node of the ADTree is the mistreatment of a patient. An attacker can reach the goal of causing mistreatment to a patient via performing eavesdropping attacks on the hospital network or MitM attacks on the medical device. Hence, these two attacks are connected with the root node as an *OR* gate. For performing an eavesdropping attack, an attacker needs a rogue device, a wireless LAN, publicly available software, and then break WPA-key, which are represented as leaf nodes *(BASs)* that are connected with an *AND* gate to the eavesdropping node. As a defense mechanism, a defender can use a strong WPA key against the key-breaking attack.

C. Stochastic Timed Automata

Timed automaton is a formal notation to model the behavior of real-time systems, which provides a simple way to annotate state-transition graphs with timing constraints using finitely many real-valued clock variables [15]. STA is a stochastic process based on timed automata where the constraints on the edges and the invariants on the locations are used to enable or force certain transitions at certain times [16]. These invariants and constraints are specified as clocks that can increase linearly over time but may be reset when a transition is taken. To understand how STA works in case of an eavesdropping and MitM attack scenarios shown in Figure 2, we assume leaf nodes *(BASs)* have different parameters as an input, such as the success probabilities of different attacks, the cost of attacks, and the time required to perform attacks. Here, the time works as an invariant for each BAS that puts constraints on reaching the AND gate of eavesdropping and MitM attacks. Similarly, the cost of each BAS performs as an update action, and probability works as a way of defining the transition steps from one location to another in STA. Based on these parameters of leaf nodes, attackers' success rate to reach the root node varies.

III. Attack-Defense Tree Models

In this section, we first define our threat model and then explain how we generate the ADTree models of UHCSs and convert the trees to STA.

A. Threat Model

In this study, we perform a systematic threat analysis of UHCSs. As UHCSs employ ISO/IEEE-11073 and HL7-FHIR communication standards to enable seamless communication of smart medical devices and transfer of patient data from smart medical devices to healthcare providers and external systems, *we consider an adversary profile who targets the communication of a UHCS in this study*. The attacker is assumed to be knowledgeable about performing the attacks, obtaining the required hardware and software, and using his resources efficiently to perform the attacks given in our ADTree in Section III. The attacks that directly target the devices or people are not considered in this study which include bribing or threatening people, the physical attacks (i.e., node capturing and reprogramming), or attacks applied in the supply chain of medical devices. Moreover, we do not consider the major side-channel attacks (i.e., time, power, and electromagnetic radiation analysis) in this study. Lastly, phishing attacks and social engineering attacks on the patients or healthcare employees are not considered in this study since they do not directly target the communication in a UHCS.

B. ADTree Models of UHCSs

The construction of ADTrees is usually initiated by determining the attackers' goals in the target system, considering the system components and processes. In order to determine the goals of the attackers in UHCSs, we considered the goals of the communication standards that enable seamless communication in UHCSs. While ISO/IEEE-11073 aims to capture and transfer patient data from various devices [3], HL7-FHIR intends to enable the electronic exchange of health data [4]. As both standards focus on the transfer of patient data, we concluded that attackers in a UHCS could target either the privacy or the security of patient data. As a result, we devised two attacker goals for a UHCS. Specifically, an attacker can aim to *Disclose Sensitive Information* of patients or cause *Mistreatment of Patients*. Although both of the attacks can cause detrimental effects and it is very vital to analyze them, *we focus only on the attacker goal of Mistreatment of Patients in this study*, and left the investigation of Disclose Sensitive Information goal of attackers in UHCSs as a future work. Using the ADTool [17] we constructed the ADTree model of *Mistreatment of Patient* that is shown in Figure 3. In this subsection, we first explain our ADTree model, then provide the characterization of BASs in our ADTree, and finally explain the conversion process of our ADTree to STA.

Mistreatment of Patient ADTree. The ADTree model of Mistreatment of Patients is shown in Figure 3. In UHCSs, an attacker can achieve this goal either via compromising the devices or performing Denial-of-Service (DoS) attacks. An attacker can compromise a device by firstly gaining unauthorized access to the networks (home network and hospital network) in ISO/IEEE-11073 or HL7 communication, then exploiting a software vulnerability, and then running a malicious script. To gain unauthorized access to the home network, an attacker has two options: WiFi or Bluetooth/BLE network. If the attacker targets the WiFi network, then as shown in P1 Subtree, he can either apply MitM attack by performing the BASs of i) obtaining a rogue device such as a laptop, ii) obtaining publicly available software (e.g., Ettercap, Hydra, etc.) to apply the attack, and iii) performing MitM attack; or gain unauthorized access and eavesdrop by i) obtaining a rogue device, ii) acquiring publicly available software, iii) finding a WLAN to attack, and iv) breaking the encryption key of the WLAN via the obtained software. If the attacker targets the Bluetooth/BLE network at home, then he/she would have to perform the attacks (thus the BASs) in the P2 Subtree.

To gain unauthorized access to the hospital network, an attacker can target either the HL7 communication or the ISO/IEEE-11073 communication. For the ISO/IEEE-11073 communication at the hospital, the attacker can follow the similar steps mentioned for accessing the home network. However, for gaining unauthorized access to HL7 communication, the attacker can either try to gain unauthorized access to WiFi (thus P1 Subtree) or try to gain unauthorized access remotely. In this case, the attacker would have to find a rogue device and a network and then try to break OAuth 2.0 authentication. In terms of DoS attacks, an attacker can perform such attacks either locally or remotely. In the former case, an attacker who is in the vicinity of the WiFi or Bluetooth/BLE network can apply DoS attack to ISO/IEEE-11073 communication at home or hospital environments. In the latter case, a remote attacker can perform Distributed DoS (DDoS) attacks to HL7 communication. For the local DoS attacks applied to WiFi

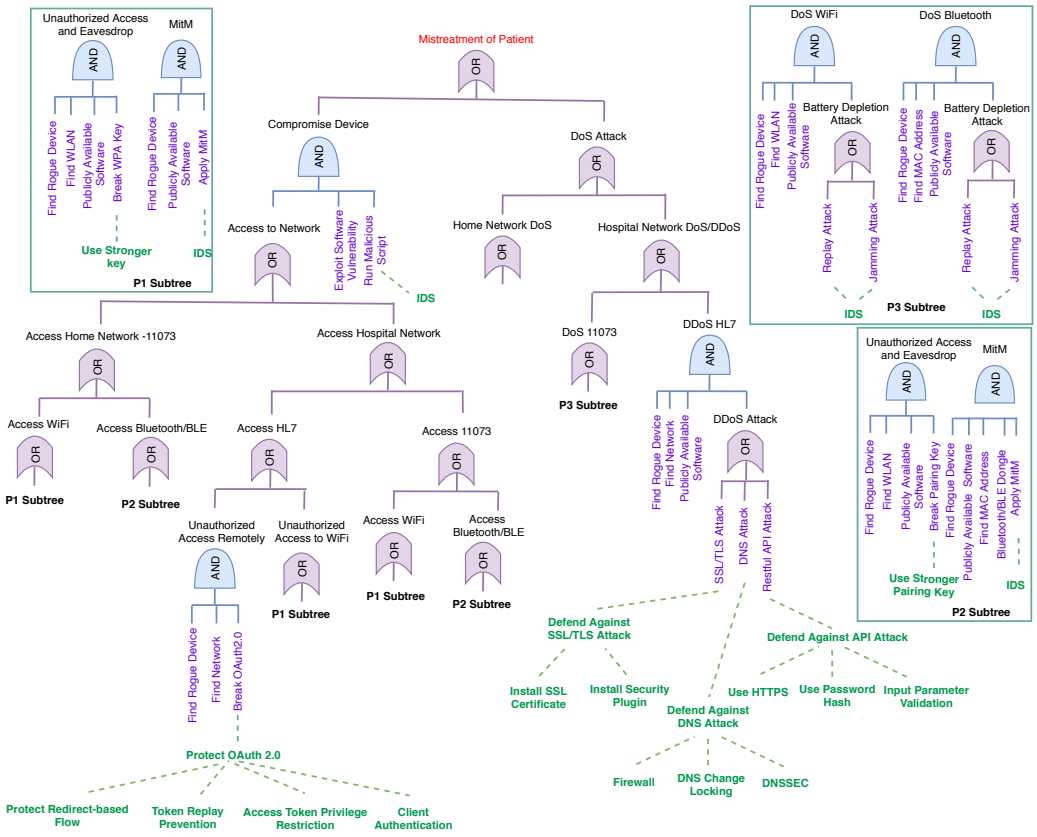


Fig. 3: Attack-Defense Tree model for the attacker goal of Mistreatment of Patients.

and Bluetooth/BLE networks, we consider replay and jamming, which can be performed by an attacker to deplete the batteries of the medical devices, hence cause mistreatment of patients. To perform those attacks, an attacker can have a rogue device, find publicly available software, and determine the network to apply jamming or replay. For the DDoS attacks applied by remote attackers, we consider DNS attacks, attacks to Restful APIs and SSL/TLS that are the most common DDoS attacks on the healthcare industry to interrupt patients' treatment [18].

Figure 3 also shows the defense solutions against the attacks. SSL certificates and security plugins can be installed against SSL/TLS-based DDoS attacks [19]. For DNS-based attacks, firewall, DNS change locking, or DNSSEC can be employed [20]. API-based attacks can be prevented via the use of HTTPS, password hashing, and input parameter validation [21]. An IDS can be used to monitor unauthorized access/eavesdropping, MitM, and DoS attacks in the communication network. For preventing OAuth2.0 attacks, redirect-based flow protection, token replay prevention, access token privilege restriction, or client authentication can be used [22].

Characterization of Basic Attack Steps (BASs). In this study, we characterize the BASs of our ADTree by three parameters: *Probability of Success, Minimal Time* and *Minimal Cost*. The probability of success signifies the success probability of the BAS. Every BAS requires a certain amount of time of an attacker that is represented by minimal time. In addition,

TABLE I: Characterization of Variable Basic Attack Steps

Basic Attack Step	Probability of Success	Minimal Time (mins)	Minimal Cost ($)
Apply MitM Bluetooth /BLE	0.68	15	15
Exploit Software Vulnerability	0.56	50	50
Apply MitM WiFi	0.68	20	20
Jamming Attack	0.65	25	25
Break OAuth2.0	0.59	60	60
Replay Attack	0.65	25	25
Break Pairing Key	0.68	30	30
Restful API Attack	0.59	45	45
Break WPA Key	0.68	40	40
Run Malicious Script	0.65	15	15
DNS Attack	0.59	60	60
SSL/TLS Attack	0.81	90	90

every BAS needs an attacker to invest resources of hardware, software, and time. Investment of those resources required for a BAS is represented by a minimal cost. One of the most crucial parts of quantitative threat analysis via ADTrees is the assignment of parameter values that characterize BASs. We characterized the probability of success, minimal time, and minimal cost for every BAS in our ADTree as outlined in Table I and Table II. Here, for presentation purposes, we categorize the BASs into two groups as *invariable* and *variable*. Here, invariable BASs are the ones whose parameters do not differ much from one attack to another. For instance, the BASs of *Find Network* and *Find Rogue Device* are almost always possible for attacks. Invariable BASs in this regard contribute to the success of other BASs, which we refer to as *variable* BASs. Variable BASs on the other hand have different properties for distinct attacks, and every variable BAS can have different parameter values. We explain how we set these parameter values for the invariable and variable BASs as follows.

TABLE II: Characterization of Invariable Basic Attack Steps

Basic Attack Step	Probability of Success	Minimal Time (mins)	Minimal Cost ($)
Find Bluetooth/BLE Dongle	0.99	30	30
Publicly Avail. Software	0.99	15	15
Find MAC Address	0.99	5	5
Find Rogue Device	0.99	15	500
Find Network	0.99	1	1
Find WLAN	0.99	1	1
Publicly Avail. Sniffer	0.99	100	100

Assignment of Probability of Success. In order to set the probability of success values for the variable BASs, we researched the studies that apply/analyze such attacks. However, the studies [23]–[25] do not report probability of success values for the attacks. Since those attacks affect confidentiality, integrity, or availability of a UHCS, we decided to benefit from the Common Vulnerability Scoring System (CVSS) to assign the probability of success [26]. CVSS provides metrics such as *Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality, Integrity, Availability* that enable the severity score calculation for threats. Each metric has a few value options which contribute to the overall severity score. For instance the options for Attack Vector metric are *network, adjacent, local* and *physical*. Different metric value combinations result in a different severity score between 0 and 10. For those variable BASs, we logically set the metrics in the CVSS for each BAS and converted the calculated score to a probability value via dividing by 10. For instance, for *Break WPA Key* BAS, we set *Attack Vector: Adjacent, Attack Complexity: High, Privileges Required: None, User Interaction: None, Scope: Unchanged, Confidentiality: High, Integrity: High, Availability: None* which signifies that the attack is applied by an attacker that must be in the vicinity of the network, the attack has high complexity, does not require privileges or user interaction, has a scope of affecting only the resources of the target system, can have a big impact on confidentiality and integrity of the target, and does not affect availability. This assignment resulted in a severity score of 6.8. We converted this severity score to a probability of success value of 0.68 and assigned it to Break WPA Key BAS. For the invariable BASs, we did not use CVSS to set the probability values. The underlying reason is that those BASs do not affect the confidentiality, integrity, or availability of UHCSs and rather act as contributing attack steps that are needed to achieve other attacks. Since those BASs can be successfully performed at will, we decided to apply a small uncertainty and set the probability of success values to 0.99.

Assignment of Minimal Time. Similar to the case in Probability of Success, the studies attacking WiFi [23], Bluetooth [24], and OAuth [25] are not reporting the amount of time needed to apply such attacks. Among the studies, only the BIAS attack [24] on Bluetooth was stated to be applied in the order of minutes. Hence, we set the minimal time values between $15 - 90$ minutes for those BASs. For the invariable BASs (Table II), we set the minimal time values based on the time required to perform the action. For instance, finding a network or WLAN is possible within a minute. On the contrary, finding a Bluetooth/BLE dongle will require more time as an attacker has to buy the hardware to apply an attack.

TABLE III: Probability of success and expected cost for the ADTree

Performance Metric	Time Intervals (minutes)			
	30	60	120	240
Attacker Success Probability	0 - 0.0029	0.3243 - 0.3845	0.4705 - 0.5334	0.4446 - 0.5074
Expected Max. Cost ($)	4534 - 4657	4562 - 4695	4551 - 4675	4619 - 4745

Assignment of Minimal Cost. We used two procedures to assign the minimal cost values. For the BASs that require hardware, such as *Find Rogue Device, Find Bluetooth/BLE Dongle,* and *Publicly Available Sniffer* listed under invariable BASs, we estimated the minimal cost based on the market values of the hardware. For the rest of the BASs (invariable and variable), we determined the minimal cost values based on the time an attacker is required to spend. Specifically, we assumed that the wage of the attacker is $\$60$ per hour. We assigned the cost values for those BASs by multiplying the minimal time by the hourly wage of the attacker.

C. Conversion of the ADTree to STA

In order to perform quantitative analysis, we need to convert our ADTree to STA, which enables the statistical model checking of the ADTree, thus provide statistical evidence on the analyzed properties. For the conversion process, we used the only publicly available conversion tool, ATTop [27]. Although ATTop can convert attack trees, it cannot convert ADTree to STA. So as to use ATTop, we had to transform our ADTree model to an attack tree model. We performed this transformation via a reduction process on our ADTree in which we removed the defense nodes from the tree, reduced the probability of success values for the corresponding BASs by 50% and doubled the minimal time required for the BAS, so as to reflect the effect of defenses on the success of attacks. To be more specific, we assumed that existing defense solutions would reduce the probability of success values of their associated variable BASs by 50% and double the time that is required for the success of the BAS. Although these amounts can vary among different attack-defense pairs, we considered to employ these changes as the average effectiveness of defense solutions. For instance, Break OAuth 2.0 BAS in our ADTree has the probability of success value of 0.59 and a minimal time of 60 mins as outlined in Table I. There are four defense mechanisms that can be employed against this attack, as shown in the ADTree. Our reduction operation reduces the probability of success value of Break OAuth 2.0 BAS by 50% and doubles the minimal time as an effect of the existing defense solutions, and in the conversion process of ATTop tool, the probability of success value for this BAS is converted as 0.29 and minimal time is converted as 120 mins in the resulting STA.

IV. Quantitative Analysis of UHCS

In this section, we do quantitative analysis of our ADTree. We consider the following research questions:

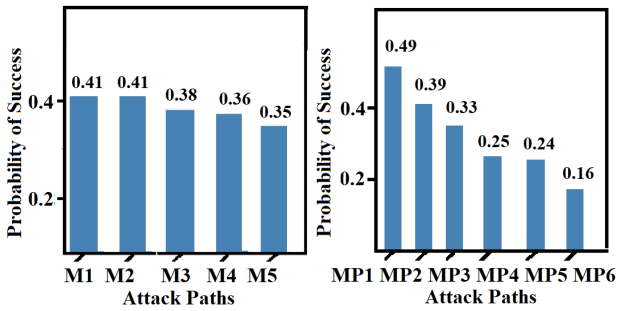
- **RQ1** How likely is it for attackers to perform a successful attack? (Section IV-A)
- **RQ2** What are the most likely threats against UHCS? (Section IV-B)

- **RQ3** How likely is it for an attacker to perform multiple attacks simultaneously in UHCSs? (Section IV-C)

We performed quantitative analysis using UPPAAL SMC to answer these questions. We constructed queries to either estimate the probabilities or the expected values of stochastic model-specific expressions for the ADTree on UPPAAL SMC. For the probability estimation queries, we instructed UPPAAL SMC to perform 1000 simulation runs to obtain meaningful results with a 95% confidence interval.

A. Likelihood and Cost Analysis of Successful Attacks

In this analysis, we investigate how likely it is for attackers to cause mistreatment of patients and the corresponding cost of attackers. To determine the likelihood and cost values, we constructed UPPAAL SMC queries for the ADTree with respect to different time intervals. Table III outlines the probability of success and expected cost values for the ADTree with respect to different time intervals. As shown in Table III, it is almost impossible for the attacker to reach his/her goal in 30 minutes since the probability of success values is very close to zero. However, in a time interval of 120 minutes, probability of success reaches the highest of 0.5334 for the goal of causing mistreatment. Regarding the expected maximum cost for the attacker, Table III shows that the cost of the attack the highest to be applied in a time interval of 60 minutes.



(a) Top 5 attacks on ADTree **(b)** Simultaneous multiple Attacks

Fig. 4: Probability of top 5 and simultaneous attacks on the ADTree.

B. Top Threat Analysis

In this analysis, we investigate the top threats against the treatment security for patients. We constructed UPPAAL SMC queries to determine the likelihood of BASs and find the top five threats for the ADTree. During the queries' construction, we focused on individual BASs while disabling the rest of the subtrees that include the rest of the attack steps. Figure 4(a) shows the top five attacks on the ADTree. We enumerated the attacks with Mi for Mistreatment of Patient ADTree where i represents the rank of the attack for each tree. Table IV outlines the top five attacks for the ADTree with their corresponding IDs and attack paths. As shown in Figure 4(a), the probability of success values of the top attacks are close to each other, with MitM applied to Bluetooth/BLE at home network having the highest probability. Considering the top five attacks that target the treatment security of patients, Table IV shows that four out of five attacks are targeting the ISO/IEEE-11073 communication. The top threats for the security of patient treatment are *MitM attack* targeting ISO/IEEE-11073 Bluetooth/BLE network at home and *Unauthorized access remotely* targeting HL7 network at hospital which have the same probability of success values as shown in Figure 4(a). The rest of the top attacks are *Unauthorized access and eavesdrop* and *MitM* attacks targeting WiFi and Bluetooth/BLE networks at home and hospital. We would like to note that all of the top attacks are applied under the *Compromise Device* subtree of the ADTree shown in Figure 3. For this reason, as the figure shows, they require *Exploit Software Vulnerability* and *Run Malicious Script* BASs to be successfully completed to cause mistreatment of patients.

TABLE IV: Paths of top five attacks and simultaneous attacks

Evaluation	ID	Attack Path
Top Threat Analysis	**M1**	Compromise device -> Access to network -> Access home network (**11073**) -> Bluetooth/BLE -> **MitM**
	M2	Compromise device -> Access to network -> Access hospital network -> **Access HL7** -> **Unauthorized access remotely**
	M3	Compromise device -> Access to network -> Access home network (**11073**) -> WiFi -> **Unauthorized access and eavesdrop**
	M4	Compromise device -> Access to network -> Access hospital network -> **Access 11073** -> WiFi -> **Unauthorized access and eavesdrop**
	M5	Compromise device -> Access to network -> Access hospital network -> **Access 11073** -> Bluetooth/BLE -> **MitM**
Multiple Simul. Attacks Analysis	**MP1**	Compromise Device -> Access to Network -> Access to Home Network -> **WiFi** and **Bluetooth/BLE**
	MP2	DoS Attack -> Hospital Network DoS/DdoS -> **DdoS HL7**
	MP3	DoS Attack -> Home Network Dos -> **DoS WiFi** and **DoS Bluetooth/BLE**
	MP4	Compromise Device -> Access to Network -> Access to Hospital Network -> Access to HL7 -> **Remote Unauthorized Access** and **Unauthorized Access to WiFi**
	MP5	Compromise Device -> Access to Network -> Access to Hospital Network -> Access to 11073 -> **WiFi** and **Bluetooth/BLE**
	MP6	DoS Attack -> Hospital Network DoS/DdoS -> DoS 11073 -> **DoS WiFi** and **DoS Bluetooth/BLE**

C. Simultaneous Multiple Attacks Analysis

The quantitative analysis performed earlier in this paper considered the scenarios of an attacker performing only one BAS. However, an attacker can simultaneously target multiple communication points to achieve his goal quicker. For this reason, investigating how likely it is for the attacker to achieve his goals in such scenarios can provide vital information. Our analysis of the ADTree given in Figure 3 shows that there are six such cases in a UHCS that are outlined in Table IV. For instance, an attacker can try to gain unauthorized access to the home network in ISO/IEEE-11073 communication by attacking both WiFi and Bluetooth/BLE networks simultaneously that is given on the first row of the table with the ID of $MP1$. Based on the outlined multiple attack scenarios, we constructed queries on UPPAAL SMC to analyze the likelihood of such cases. Figure 4(b) shows the probability of success values for the multiple attack cases outlined in Table IV. As shown in the figure, probability of success values for multiple attack scenarios vary between 0.49 and 0.16. While attacking both WiFi and Bluetooth/BLE networks at home environment ($MP1$) in ISO/IEEE-11073 communication provides an attacker the highest probability of success, the lowest probability of success is achieved via performing DoS attacks on both WiFi and Bluetooth/BLE networks at hospital environment ($MP6$).

V. Related Work

In this section, we discuss the related work on threat analysis using attack tree and ADTree security formalisms in modern healthcare systems and other domains.

Attack trees. Asif et al. proposed an attack tree model to evaluate the privacy risks associated with an IoT ecosystem [28]. An attack tree-based security framework for modeling IoT was proposed in [29]. Siddiqi et al. proposed a threat-modeling based on attack trees to evaluate the security of implantable medical devices (IMDs) [30]. In [31], a methodology was proposed to enable the automated generation of attack trees for IMDs based on a description of the IMD operational workflow. In [32] how Isabelle model checking might help the IoT healthcare system to improve the detection of attack traces and refinement of attack tree analysis was investigated.

ADTrees. Researchers employed ADTree for risk assessment in different domains such as multi-UAV networks [33] and ATM [34]. A game-theoretic scheme was proposed for risk assessment in multi-UAV networks and evaluated against DoS attacks [33]. In [34], ADTree was used to model and analyze ATMs' security. A continuous risk assessment methodology was proposed for smart grid based on ADTrees [35].

Differences from existing work: The main differences between the prior works and our work are as follows: (1) While the existing studies mostly performed threat assessment for narrower domains such as IMDs and IoT, we conduct threat analysis for UHCS that consists of two healthcare standards, numerous types of smart medical devices, various communication technologies, and several different types of attacks. (2) The prior works which employed ADTree-based threat analysis did not target UHCS, unlike our study.

VI. Conclusion

In this study, we performed a systematic threat analysis of UHCS. Our analysis relied on the ADTree formalisms and quantitative analysis of stochastic timed automata. We methodically identified the threats against UHCSs and built an ADTree. Our ADTree shows the series of steps of an attacker to successfully compromise the treatment security of patients, as well as existing defense solutions. To perform quantitative analysis and determine the likelihood of various attack scenarios, we converted our ADTree to stochastic timed automata. Our results indicated both MitM and unauthorized remote access attacks are the most probable attacks that a malicious entity could pursue, causing mistreatment to patients.

Acknowledgments

This work was partially supported by the U.S. National Science Foundation (Award: NSF-CAREER CNS-1453647, and NSF-2219920) and a Microsoft Research Grant. The views are those of the authors only.

References

[1] "Global medical devices market trajectory," https://www.businesswire.com/news/home/20210113005785/en/Global-80-Billion-Portable-Medical-Devices-Market-Trajectory-Research.com/, January 2021.
[2] H. Ronte, K. Taylor, and H. John, "How connected medical devices are transforming healthcare," Tech. Rep., 2018.
[3] "Ieee 11073 personal health devices," http://11073.org/.
[4] "Hl7 international," https://www.hl7.org/.
[5] S. Lee and H. Do, "Comparison of ieee 11073, ihe pcd-01, and hl7 fhir messages for personal health devices," *Healthcare infor. research*, 2018.
[6] D. Haselhorst, "HL7 Data Interfaces in Medical Environments: Attacking and Defending Healthcare," 2017. [Online]. Available: https://www.sans.org/reading-room/whitepapers/vpns/paper/38010
[7] A. I. Newaz, A. K. Sikder, L. Babun, and A. S. Uluagac, "Heka: A novel ids for attacks to personal medical devices," in *IEEE CNS*, 2020.
[8] A. Newaz, A. Sikder, M. A. Rahman, and A. S. Uluagac, "Healthguard: A ml-based security framework for shs," in *IEEE SNAMS*, 2019.
[9] H. Rathore, A. Mohamed, and M. Guizani, "Deep learning-based security schemes for implantable medical devices," in *Energy Efficiency of Medical Devices and Healthcare Applications*, 2020.
[10] W. Wideł, B. Audinot, and S. Pinchinat, "Beyond 2014: Formal methods for attack tree–based security modeling," *ACM Comput. Surv.*, 2019.
[11] "Fhir security," https://www.hl7.org/fhir/security.html/.
[12] C. Dameff, M. Bland, K. Levchenko, and J. Tully, "Pestilential protocol: How unsecure hl7 messages threaten patient lives," in *BlackHat*, 2018.
[13] "Schneier on security," https://www.schneier.com/academic/archives/1999/12/attack_trees.html/, December 1999.
[14] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, "Attack–defense trees," *Journal of Logic and Computation*, 2014.
[15] R. Alur, "Timed automata," in *Intl. Conference on Verification*, 1999.
[16] A. David, K. G. Larsen, A. Legay, M. Mikučionis, and D. B. Poulsen, "Uppaal smc tutorial," *International Journal on Software Tools*, 2015.
[17] B. Kordy, S. Mauw, and P. Schweitzer, "Adtool: Security analysis with attack–defense trees," in *Quantitative Eval. of Systems*. Springer, 2013.
[18] "Denial-of-service attacks on healthcare," https://www.healthcareitnews.com/news/denial-service-attacks-healthcare-poised-explode/, 2017.
[19] "Rest api security," https://securityboulevard.com/2020/01/how-to-prevent-cookie-stealing-and-hijacking-sessions-easiest-guide, May 2020.
[20] "How to prevent dns attacks," https://www.esecurityplanet.com/networks/how-to-prevent-dns-attacks/, October 2017.
[21] "Rest api security," https://restfulapi.net/security-essentials.
[22] "Oauth 2.0 security best current practice," https://tools.ietf.org/html/draft-ietf-oauth-security-topics-16/.
[23] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *ACM CCS*, 2017.
[24] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "Bias: Bluetooth impersonation attacks," in *IEEE S&P*, 2020.
[25] X. Wang, W. C. Lau, and S. Shi, "Make redirection evil again: Url parser issues in oauth," in *BlackHat Asia 2019*, 2019.
[26] "Common vulnerability scoring system version 3.1 calculator," https://www.first.org/cvss/calculator/3.1/.
[27] R. Kumar, E. Ruijters, B. M. Yildiz, and M. Stoelinga, "Effective analysis of attack trees," in *Fundamental Approaches to Soft. Eng.*, 2018.
[28] W. Asif, I. G. Ray, and M. Rajarajan, "An attack tree based risk evaluation approach for the internet of things," in *IoT*, 2018.
[29] D. Beaulaton, I. Said, and S. Sadou, "Security analysis of iot systems using attack trees," in *Graphical Models for Security*, 2019.
[30] M. A. Siddiqi, R. M. Seepers, and C. Hamad, "Attack-tree-based threat modeling of medical implants." in *PROOFS@ CHES*, 2018, pp. 32–49.
[31] J. Xu, K. K. Venkatasubramanian, and V. Sfyrla, "A methodology for systematic attack trees generation for imds," in *IEEE SysCon*, 2016.
[32] F. Kammüller, "Formal modeling with humans in infrastructures for iot healthcare," in *Conf. on Information Security and Privacy*, 2017.
[33] S. Garg, G. S. Aujla, and Kumar, "Attack-defense model for risk assessment in multi-uav networks," *IEEE Consumer Electronics*, 2019.
[34] M. Fraile, M. Ford, and R. Trujillo-Rasua, "Using adtrees to analyze threats and countermeasures in an atm," in *Enter. Modeling*, 2016.
[35] E. Rios, E. Rego, M. Higuero, and X. Larrucea, "Continuous quantitative risk management in smart grids using adtrees," *Sensors*, 2020.