DOI 10.12694/scpe.v17i3.1178
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 17, Number 3, pp. 155–170. http://www.scpe.org

IMPROVEMENT STRATEGIES FOR DEVICE INTEROPERABILITY MIDDLEWARE USING FORMAL RELIABILITY ANALYSIS

USMAN PERVEZ*, ASIAH MAHMOOD*, OSMAN HASAN*, KHALID LATIF† AND AMJAD GAWANMEH‡

Abstract. Ensuring the correctness of middleware that ensures interoperability of various medical devices is one of the biggest challenges in the e-health domain. Traditionally, these Device Interoperability Middleware (DIM) are analyzed using software testing. However, given the inherent incompleteness of testing and the randomness of the user behaviours, the analysis results are not guaranteed to be accurate. Some of these inaccuracies in analysis results could even put human life at risk. In order to overcome these limitations, we propose to use a probabilistic model checker PRISM for analyzing DIM. The proposed approach allows us to rigorously verify reliability properties of the given DIM and thus allows the designers to make appropriate measures to design more reliable systems. For illustration, we formally analyze a middleware that uses the HL7 FHIR and ontology-based description of the devices and a communication protocol to bridge the gap in heterogeneity for dealing with different vendors and incompatible data formats.

Key words: Reliability Analysis, Health Information System (HIS), Device Interoperability Middleware (DIM), Markov Chain, PRISM

AMS subject classifications. 92C50, 92-08, 68Q60, 60J05, 60J25

1. Introduction.

With the fast growing technology in the world, a lot of effort has been put to automate the worksflows, ranging from domestic to industrial workflows, with the aim to enhance the performance of work and shorten the completion time. Hospital workflows have also drawn the attention of the researchers and thus many medical equipments and devices have been developed to perform the work, such as performing medical tests and data capturing, storing, management or transmission. These medical devices and systems have been categorized as Health Information System (HIS) [9] and are increasingly found in almost every hospital now-a-days. Although, the workflows that are composed of HIS systems are better than manual workflows, yet there are many inherit problems, such as device interpretability. Conc univ

Device Interoperability problem refers to the lack of communication between the HIS systems due to the lack of standardization in the manufacturing of medical devices and thus it has become one of the biggest problem that needs to be incorporated in order to setup a hospital workflow or upgrade the existing workflow. The medical devices are diverse in nature and their functionality differs from device to device and the communication mechanism may also be different (e.g., Wifi, Bluetooth or Serial Port). To understand the impact of the interoperability problem, consider a hospital that aims to setup its workflow using HIS systems. This new setup can only be established if we are able to find medical devices that work on the same standards and support the same device integration mechanisms. Similarly, if a hospital aims to upgrade its existing e-health based medical system by adding a new medical device, such as a urine testing device, blood testing device or sugar testing device, then the new medical device must be compatible with the existing electronic environment and must follow the same standard that the other medical devices are following. In case of an unavailability of such a device, the hospital may have to upgrade all of its existing medical devices, which would certainly be a very undesirable solution for most hospitals.

One of the promising solutions to the above-mentioned problem is the development of a middleware that completely resolves the problem by bridging the gap between different standards of the medical devices. For example, if a device using the serial port and ASTM E1394 [7] or its replacement CLSI LIS01 standard [14] required to communicate with the HL7 FHIR based laboratory information system, then the communication can take place by introducing a middleware between them in such a way that it translates the output of the device coming on the serial port to HL7 FHIR compatible data so that it can be received by the laboratory

*School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan. ((usman.pervez, asiah.mahmood, osman.hasan)@seecs.edu.pk).

†Department of Computer Science, COMSATS Institue of Information Technolgy, Islamabad, Pakistan. (khalid.latif@comsats.edu.pk).

‡Department of Electrical and Computer Engineering, Khalifa University, UAE, and Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada. (amjad.gawanmeh@kustar.ac.ae).

information system. Similarly, the middleware will also be responsible to translate the requests of the laboratory information systems into serial data so that it can be received by the device. This paradigm shift of overcoming the device interoperability problem from standardization of the workflows to the development of the Device Interoperability Middleware (DIM) [6] has shown a significant potential to solve the interoperability problem.

Considering the safety-critical nature of the medicine domain, ensuring the correct functionality of DIM is very important. In particular, if the middleware fails to translate the data from one communication standard to another standard, then this may lead to false results and hence false diagnostic reports of the patients will be produced which is extremely undesirable. Therefore, these medical procedures are considered critical, since faults and errors in the medical system may lead to loss of lives, and in the best cases, loss of money and reputations [16]. Traditionally, the functionality of a middleware is checked by software testing. However, given the enormous number of possible scenarios in these DIM, they cannot be exhaustively tested due to computational power and memory constraints. Thus, the quality of DIM is judged based on a set of test vectors. This kind of incomplete testing of DIM can have serious consequences, including human deaths.

To overcome the above-mentioned inaccuracy limitations of simulations, formal methods have been proposed as a viable solution[19]. They are primarily based on computer-based mathematical analysis methods to model and analyse the given system. A lot of work has been done in the domain of analyzing heathcare systems using formal methods. Some notable examples include the verification of electrocardiogram (ECG) biosensors in event-B [5, 3]. The work is then extended to formalize the rules that reflects the construction of the ECG wave specifications [4, 21]. In addition, reliability analysis of FHIR standard based e-health system was addressed in [34]. Other works include the verification of software components in medical devices [36, 41], ambient assisted systems [24] or healthcare requirements [1] and the verification of collaborative and agent based workflows in healthcare [10, 29]. A formal model for e-Healthcare readiness assessment was also proposed in [38]. Similarly, formal methods have also been used for the verification of system engineering lifecycle where the Communication Sequential Processes (CSP) have been adopted as a formal method language with an aim to formalize the system specifications [33]. Other work related to managing workflow was presented in [32] and [12].

Probabilistic model checking technique, which is a sub domain of formal methods, has also been used for the verification of the healthcare systems that exhibit probabilistic behaviour, such as modeling and verification of the treatment therapies of Tuberculosis and HIV [35]. Some other model based reliability analysis of the systems include the verification and reliability analysis of the software used in medical devices for infusion pump [22]. Moreover, some generic test cases have also been generated for healthcare systems using model based testing [31]. Despite the above-mentioned formal methods work in ascertaining the correctness of healthcare systems, their usage for analyzing the functionality and performance of healthcare systems, like HIS, has been very rare. Similarly, to the best of our knowledge, formal methods have never been used to assess the recently proposed DIM based HIS system.

Given the safety-critical nature of the DIM, it is a dire need to assess its functionality, reliability and performance using formal methods. As a first step towards this direction, we propose to conduct the reliability analysis of DIM using probabilistic model checking. The usage of a probabilistic model checker allows us to capture the natural randomness found in the DIM models. The considered DIM has been developed as a middleware to integrate various medical devices that run on different communication mediums, including serial port, Wifi and bluetooth. This DIM has been installed in different hospitals of Pakistan and it enables automatic up-gradation of the medical systems by adding any new medical device that runs on either of the three communication mediums.

In this paper, we aim to develop a Markovian model of simple DIM based and fault tolerant based DIM medical systems in the language of the PRISM model checker [30], to analyse the reliability and performance of the respective systems. In particular, we use the Markov Decision Processes (MDP) [40] in PRISM to find the probability of occurrence of wrong results (failures) in the considered system having DIM installed. Moreover, we also use Continuous Time Markov Chain (CTMC) [15] to model the real-time workflow of the medical system and evaluate the real-time failure probabilities. The proposed approach provides more accurate results than traditional counterparts due to the exhaustive exploration of a state-based model of the DIM based medical system and allow the designers to find the failures and weaknesses in the underlying system and to make appropriate measures on the basis of these results, in order to make the system more reliable. In addition, this

works extend our previous work in [39] by providing reliability improvement strategies based on probabilistic analysis method conducted in this work. The presented strategies are expected to enhance the probability of success for several workfow operations.

The rest of paper is organized as follows: Section 2 describes some preliminaries about model checking and PRISM to facilitate the understanding of the paper. The considered health information system along with its reliability analysis is described in Section 3. This is followed by the reliability analysis of two versions of the MDP and CTMC based models of the considered health information system in Sections 4 and 5, respectively. Finally, Section 6 concludes the paper.

2. Probabilistic Model Checking and PRISM. Model checking [2] is used to model and verify the systems that exhibit time or decision based behaviour. Some of the examples of these systems include communication protocols and controllers of digital circuits. The given system is first modeled with a finite-state Markovian state machine and the required verification specifications are defined as system properties, which are expressed in temporal logic. The state machine along with its defined properties are then implemented in a model checking tool that verifies either the given properties hold for the system or not. Moreover, if the properties do not hold, the tool also provides the error traces. Based on the size of the given system, the corresponding size of the state machine may also vary i.e., for a large system, its corresponding state machine will also be large. Therefore, for very large systems, the state machines also grow quite large and thus, its verification become impossible with limited resources of memory and time. This problem is termed as the state-space explosion problem and is usually resolved by developing less complex, abstract models, of the system to facilitate analyses. Moreover, to enhance the memory and computational handling power of the model checking tool, several other symbolic and bounded model checking techniques have also been proposed.

Probabilistic model checking [26] is a special branch of model checking that is precisely used for the verification of the systems that exhibit probabilistic behaviour. The properties verified against these systems are also probabilistic. Many probabilistic model checking tools, such as ETMCC [17], VESTA [25], PRISM [30], MRMC [23] and YMER [18], have been proposed and each has its own pros and cons. Among these tools, PRISM best suits our work as it supports the verification of the steady-state probabilities and is also efficient in terms of memory consumptions, whereas YMER and VESTA are less efficient and do not support the verification of steady-state probabilities [27]. PRISM also supports a wide range of models, such as Discrete Time Markov Chain (DTMC), Continuous Time Markov Chain (CTMC) and Markov Decision Process (MDP) and thus has been selected for our work for analysing the reliability and performance of fault tolerant based DIM HIS system [30].

PRISM model checker has its own modeling language, i.e., the PRISM language, in which the underlying system is modeled. A system may have multiple modules. A state at a given time is represented by local variables, which are defined in those modules whereas, the values of all the local variables of those modules represent the overall state of the system. Modules contains a number of instructions and each instruction has its own guarded commands, which defines the behaviour of the system. PRIMS supports various kinds of properties specifications, such as PCTL, LTL and CSL. $S_{\geq 0.99}[\text{“}normal\text{”}]$ is the steady state probability of *normal* state ≥ 0.99. PRISM also supports verification and analysis of time based properties which we use for the time based analysis of Markovian models. These properties are analyzed by associating a certain reward with each state of the model through a reward structure.

2.1. Markov Decision Process (MDP). MDP [8] based modelling is used for the systems where the behaviour of the system changes on the basis of certain decisions. Eac transition in MDP, i.e., from state $\boldsymbol{S}$ to a state $\boldsymbol{S'}$ is based on a probabilistic decision and depends on the present state $\boldsymbol{S}$ of the system. Mathematically, the equation that is used to find the transitional probability of the transition form state $\boldsymbol{S}$ to state $\boldsymbol{S'}$ is represented below,

$$P_a(S, S') = P_r(S_{t+1} = S' | S_t = S, a_t = a) \tag{2.1}$$

where P_r defines the transition probability and $\boldsymbol{a}$ is the action performed by the decision maker. Similarly, the mathematical equation that expresses the system is termed as Transition Probability Matrix $\boldsymbol{P}$ [11], which represents various transition rates from one state to other state. Similarly, the mathematical equation that is

used to calculate the probability of next state is given below

$$P_r(S') = P_r(S) * P \tag{2.2}$$

MDPs are used to evaluate the systems whose behaviour depends on transitional decisions. The corresponding properties of such systems are defined in terms of probability of failures and success and the model and properties are expressed in the language of the PRISM model checker. The PRISM model checker can then be used to verifiy the properties against the system and calculate the overall probabilities of success and failures.

2.2. Continuous Time Markov Chain (CTMC). CTMC [15] models are used for the mathematical modeling of the workflows, in which each event of the workflow is continuous with respect to the time. A CTMC model includes the total number of states $\boldsymbol{S}$, initial probability distribution of states and the transition rate matrix $\boldsymbol{Q}$. The next transition state probabilities are calculated in the CTMC as follows:

$$P'_t = P_t * Q \tag{2.3}$$

Once the given system is modeled with CTMC and is implemented in PRISM, the reliability *properties* are defined according to the needs and are verified to find the results.

2.3. Discrete Time Markov Chain (DTMC). DTMC [37] are used for the mathematical modeling of the workflows in which each event of the workflow is discrete with respect to time. The DTMC also includes the total number of states $\boldsymbol{S}$, initial probability distribution of states and the transition rate matrix $\boldsymbol{P}$, just like in case of CTMC. The next transition state probabilities are calculated in the DTMC as follows:

$$P'_t = P_t * P \tag{2.4}$$

For the reliability analysis of the workflows that exhibit discrete transitional events w.r.t. time, the given system is modeled with DTMC and the intended properties are verified in PRISM.

3. Reliability analysis of a Typical Health Information System. The reliability of a typical Health Information System (HIS) is expected to increase when the DIM is used as a middleware to overcome Device Interoperability problem. To observe this increase in reliability, we first present a manual HIS system, as depicted in the Fig 3.1. which is typically found in the hospitals and evaluate its reliability by using the proposed model checking approach. This system provides the means of communication between various stake holders.

As presented in the figure, when a patient visits the doctor, the doctor examines the patient and refers him to the medical lab in order to undergo medical tests, such as blood test, urine test and glucose test. The lab collects the information of the patient, including his blood sample and generates his bar code. The blood sample is then fed in the medical device which performs the medical test. However, if the blood sample is found to be clotted or of low quantity, the patient's request is rejected. Upon successful completion of the medical test of the blood sample, the test reports are given to the person in charge of delivering them to a pathologist. During this process, the medical device may fail to perform the tests due to some hardware or software failures. Similarly, the reports may get lost while being delivered to the pathologist by the person in charge. Finally, the reports will be delivered to the patient after being successfully examined by pathologist.

The behaviour of the underlying medical system is probabilistic due to the fact that the workflow transitions occur with some probabilities. In order to analyse the reliability of the overall medical system, which is the probability of successful delivery of the medical reports to the patient by the pathologist, the medical system is modeled with MDP. It allows probabilistic decisions by including the appropriate state transition probabilities. The Markov Chain (MC) of the underlying health system is presented in Fig 3.2 and its transitional probabilities, which present the failure and successful probabilities of the transitional events, are depicted in the Table 3.1. These transitional probabilities have been taken based on the statistics reported in [20] [13], and the probability of the reports being lost by the person in charge is considered to be 0.4.

By using the transition probabilities, as mentioned in Table 3.1, we find the probability of success and failure of all the undergoing transitional events of the considered medical system by verifying the properties

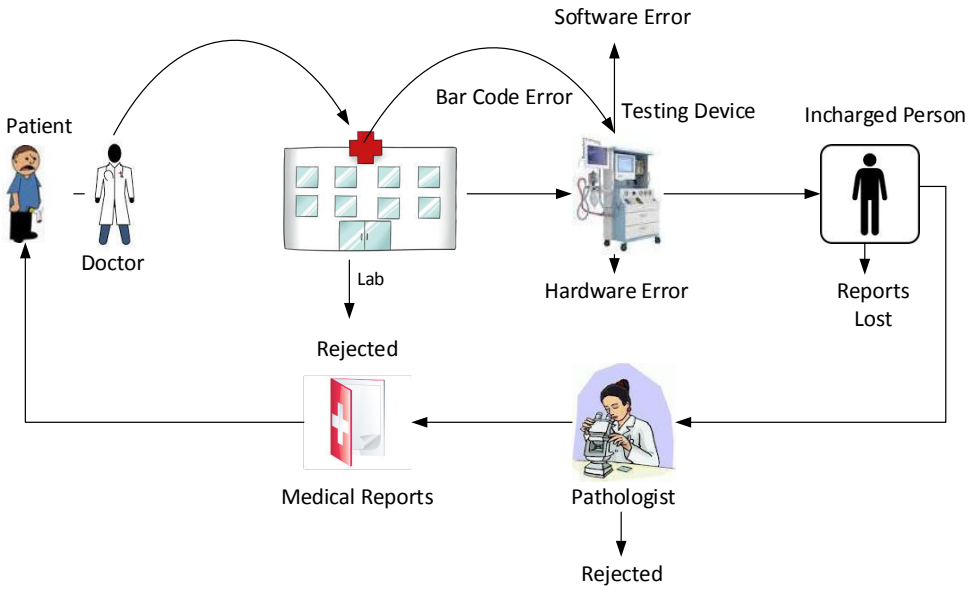

FIG. 3.1. *A Typical Health Information System (HIS)*

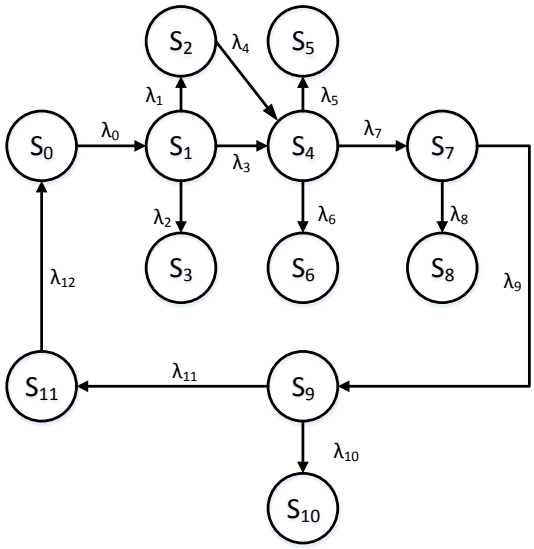

FIG. 3.2. *State Machine of the manual HIS system*

mentioned in Eq 3.1 and 3.2, and the results are presented in the Table 3.2. These results show that the probability of the successful delivery of the medical reports to the patient by the pathologist is 0.41777.

$$Pmax = ?[F\ succ = 1] \tag{3.1}$$

$$Pmax = ?[F\ fail = 1] \tag{3.2}$$

TABLE 3.1
Transitional Probabilities

State Transitions	Probabilities	State Transitions	Probabilities
λ_0	1.0	λ_7	1-λ_5-λ_6=0.93
λ_1	0.02826	λ_8	0.4
λ_2	0.00174	λ_9	1-λ_8=0.6
λ_3	1-λ_1-λ_2=0.97	λ_{10}	0.25
λ_4	1.0	λ_{11}	0.75
λ_5	0.035	λ_{12}	1.0
λ_6	0.035		

TABLE 3.2
Probability of Success and Failure

Lab Rejection	0.002	Human Error	0.637
Bar Code Error	0.047	Human Success	0.557
Device Hardware Error	0.060	Pathologist Rejection	0.239
Device Software Error	0.060	Pathologist Acceptance	0.417
Machine Success	0.928	Successful Delivery	0.417

where ***Pmax*** is the output probability, ***F*** indicates eventually in the future, ***succ*** and ***fail*** are the variables whose values are updated to 1 during the transition from state S_a to S_b. To find the probability of successful medical testing by the machine, the variable ***succ*** is updated during the transition from state S_4 to state S_7. Similarly, to find the probability of failure of delivery of the medical reports to the pathologist by the person in charge, the variable ***fail*** is updated during the transition from state S_7 to S_8. The other probabilities are calculated in the same way.

Reliability analysis of HIS system using MDP allows us to evaluate the general probabilities of success and failure of the underlying system. To increase the depth of evaluation, we use CTMC to model a real-time workflow of the medical system to calculate the probabilistic success as well as failures with respect to time. The CTMC model of the HIS system is just like the MDP model as presented in Fig. 3.2, but with the difference of transitional probabilities. The transitional probabilities are presented in Table 3.3. These probabilities refer to the probability of occurrence of the events with in a time period of 1 hour. For example, the transitional probability λ_0 means that the total number of patients visiting the lab during the time period of 1 hour are 10.

The CTMC model of the above system is implemented in PRISM and the property, as mentioned in Eq 3.3, is verified.

$$P = ? \ [F <= T \ count = K] \tag{3.3}$$

where ***P*** is the output probability, ***F*** indicated future, ***T*** is the time in hours and ***count*** is a variable that acts like a counter which counts the total number of path transitions. This variable is set to count the total number of transitions that occur from state S_9 to S_{11}, which means that the ***count*** variable will count the total number of patient's reports which are successfully delivered to the patients by the pathologist. ***K*** is a variable whose value will be set manually to find the probability of occurrence of ***K*** numbers of count. For testing purposes, the variable ***K*** is set to ***K=1***, and the model is executed for 10 hours, by setting ***F=10*** and results are obtained, as presented in Fig 3.3. From the graph, we conclude that the probability of successful delivery of the medical reports to a single patient by the pathologist during the time period of 1 hour is almost 0.23.

4. Reliability analysis of DIM based Health Information System. After evaluating the reliability of a typical HIS system, we now move on to evaluate the reliability of a DIM based HIS [6] system with the aim to observe the increase in the reliability of the underlying HIS system. The workflow of a DIM based HIS system is presented in the Fig 4.1. This workflow is as same as that of a typical HIS system with the difference that the responsibility of the person, who is in charge of delivering the medical reports to the pathologist, is now

TABLE 3.3
Transitional Probabilities

State Transitions	Probabilities	State Transitions	Probabilities
λ_0	10	λ_7	10-λ_5-λ_6=9.3
λ_1	0.2826	λ_8	4
λ_2	0.0174	λ_9	1-λ_8=6
λ_3	10-λ_1-λ_2=9.7	λ_{10}	2.5
λ_4	10	λ_{11}	7.5
λ_5	0.35	λ_{12}	10
λ_6	0.35		

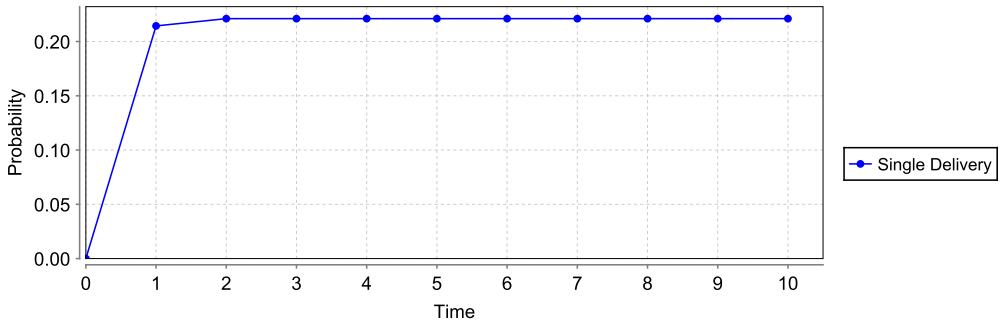

FIG. 3.3. *Probability of successful delivery of a single patient's reports w.r.t time*

performed accurately by the automatic DIM middleware. The DIM in this example is composed of mainly two operations, which include a communication channel and a data mapping. The communication channel, which might be a serial port interface, a WiFi interface or a bluetooth interface, provides the medium to transfer the data taken from the medical machine output to the data mapper. The selection of the communication interface, i.e., serial port, WiFI or bluetooth, depends on the communication standard of the medical machine installed. If the machine has been designed to communicate through a serial port, the serial port interface will be used as a communication channel to communicate the data. Similarly, the wifi interface and the bluetooth interface will be used for the wifi and bluetooth compatible devices, respectively. This automatic selection of the communication interface has significantly resolved the device interoperability problem and thus facilitates new setups as well as easy up-gradation of the existing HIS systems. For example, if the HIS system of a hospital only posses a blood testing medical device, which communicates only by a serial port, then this HIS system can be easily upgraded by adding any new medical device, such as a urine testing medical device, without taking care of the communication standard (i.e., serial port, Wifi, or bluetooth) being followed by the new device. The device mapper finally maps the raw data, as received from the communication channel, to the HL7 standard based diagnostic reports. It has the capability to understand the received raw data regardless of the format of the data i.e., serial port data format, Wifi data format or bluetooth data format. The diagnostic reports are then delivered to the pathologist automatically.

The underlying HIS system is very efficient in terms of automatic reports delivery but it does not guarantee accuracy and perfection. Failures in the system, such as communication failure and data mapping failure, may result into a fatal loss. To avoid these failures, the system must be pre-tested before installation. We propose a reliability evaluation mechanism of the considered system by utilizing MDPs in the proposed methodology. We have developed the MC of the system, presented in the Fig 4.2, and its transitional probabilities are depicted in Table 4.1. These transitional probabilities have been taken based on the statistics reported in [20] [13], whereas the probability of the communication channel failure has been considered to be 0.1.

We verified the reliability of the DIM based HIS system in terms of successful delivery of the diagnostic

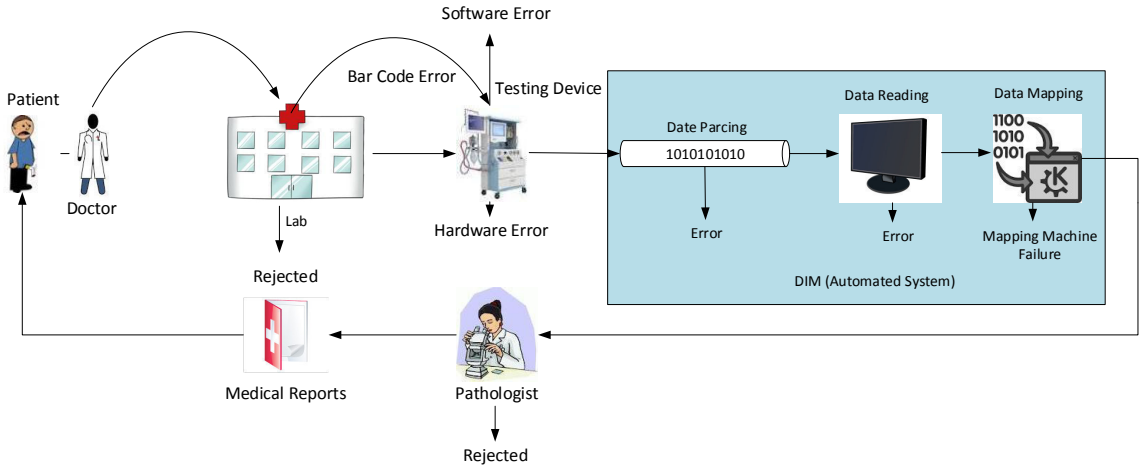

FIG. 4.1. *DIM based HIS System*

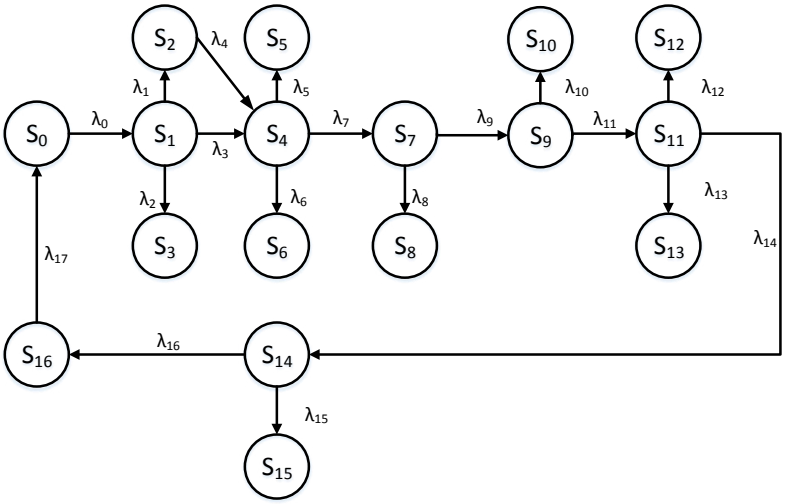

FIG. 4.2. *State Machine of DIM based HIS system*

TABLE 4.1
Transition Probabilities

State Transitions	Probabilities	State Transitions	Probabilities
λ_0	1.0	λ_9	1-λ_8=0.9
λ_1	0.02826	λ_{10}	0.2
λ_2	0.00174	λ_{11}	1-λ_{10}=0.8
λ_3	1-λ_1-λ_2=0.97	λ_{12}	0.065
λ_4	1.0	λ_{13}	0.065
λ_5	0.035	λ_{14}	1-λ_{12}-λ_{13}=0.87
λ_6	0.035	λ_{15}	0.25
λ_7	1-λ_5-λ_6=0.93	λ_{16}	1-λ_{15}=0.75
λ_8	0.1	λ_{17}	1.0

TABLE 4.2
Probability of Success and Failure

Lab Rejection	0.00308	Data Reading Failure	0.29637
Bar Code Error	0.04904	Data Reading Success	0.66843
Device Hardware Error	0.06196	Mapping Machine Error	0.07705
Device Software Error	0.06196	Mapping Algorithm Failure	0.07705
Machine Success	0.92838	Mapping Success	0.58153
DIM Success	0.58153	Pathologist Rejection	0.25784
Communication Failure	0.16465	Pathologist Acceptance	0.43615
Communication Success	0.83554	Successful Delivery	0.43615

TABLE 4.3
Transition Probabilities

State Transitions	Probabilities	State Transitions	Probabilities
λ_0	10	λ_9	10-λ_7=9
λ_1	0.2826	λ_{10}	2
λ_2	0.0174	λ_{11}	10-λ_{10}=9
λ_3	10-λ_1-λ_2=9.7	λ_{12}	0.65
λ_4	10	λ_{13}	0.65
λ_5	0.35	λ_{14}	10-λ_{12}-λ_{13}=8.7
λ_6	0.35	λ_{15}	2.5
λ_7	10-λ_5-λ_6=9.3	λ_{16}	10-λ_{15}=7.5
λ_8	1	λ_{17}	10

report to the patient using PRISM as follows:

$$Pmax = ?[F\ succ = 1] \tag{4.1}$$

The value of the variable ***succ*** is updated to 1 during the transition form state S_{14} to state S_{16}. Similarly, we can find the probabilities of other successful as well as failure transitions by updating the value of the variable **succ** to 1, during those particular transitions. Table 4.2 presents the probability of success as well as failure of all the events in the DIM based HIS. The results indicate that the reliability of the DIM based HIS system, which is the probability of successful delivery of the diagnostic reports to the patient, is 0.43615.

For the reliability evaluation of the real-time workflow of the DIM based HIS system, we developed its CTMC model and analysed the intended property to find the probability of successful delivery of the medical reports to the patient. The CTMC model is just like its MDP model as presented in Fig 4.2, whereas the input transitional probabilities are presented in Table. 4.3. The output results are presented in Fig 4.3. From the graph, we conclude that the probability of successful delivery of the medical reports to a single patient by the pathologist during the time period of 1 hour is almost 0.24.

It has been observed that the MDP as well as CTMC based reliability analysis of the DIM based HIS system is higher than the reliability analysis of the typical HIS system, given in the previous section.

5. Reliability analysis of TMR enabled DIM based Health Information System. Based on the obtained results, as presented in the previous section, the DIM middleware has resulted in increasing the overall reliability of the system, but it has been noticed that this increase in reliability is not significant. Since, the HIS systems are very sensitive and require high accuracy due to the fact that its performance and reliability has a direct effect on the lives of the patients, there is a dire need to increase this reliability up to some acceptable level. For this purpose, we propose some modifications in the DIM system by leveraging upon the strengths of the Triple Modular Redundancy (TMR) mechanism [28].

TMR is a fault tolerating mechanism that is used frequently in safety-critical systems where a single fault in the system may lead to some drastic situations. This mechanism has the capability to tolerate a single

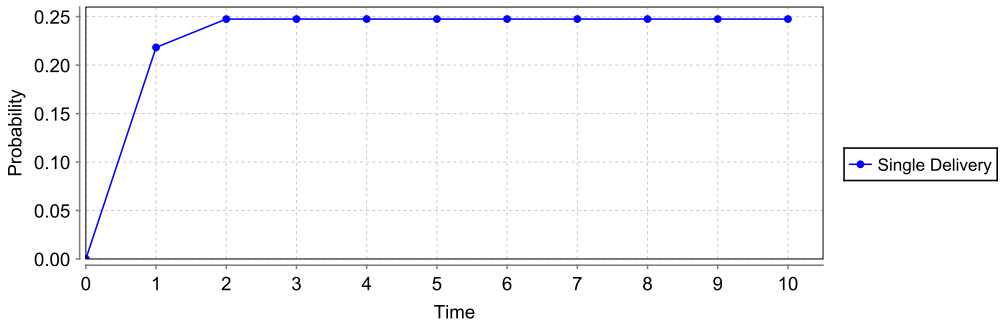

FIG. 4.3. *Probability of successful delivery of a single patient's reports w.r.t time*

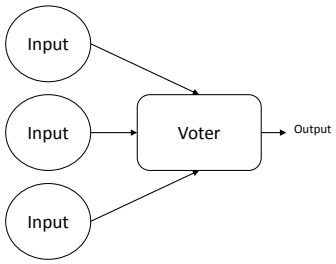

FIG. 5.1. *Triple Modular Redundancy*

fault in the system and thus the reliability of the underlying system increases. A typical TMR mechanism has been presented in Fig 5.1. In TMR, the critical process is performed separately by three identical resources functioning in parallel, whereas the output of all the three resources are fed into a voter. The voter checks these outputs and decides the final output on the basis of a majority voting system. If all the three resources produce the same output, the voter will consider the system flawless and produce the same output, as produced by the resources. However, if any one of the resource produces a different output, due to some unknown fault, in comparison to the remaining two resources, the voter will consider this resource faulty. It will tolerate this fault by masking it and keep the system functioning by producing the output, as produced by the remaining two resources. For the case, when all the resources produce different outputs, the voter will consider the whole system faulty. The MC of a common TMR mechanism is presented in Fig 5.2. In the figure, state 1 shows that all the three resources are functioning properly. State 2 shows that only one system is faulty, however the whole system is still functioning. If any other resource fails from this point, the whole system goes into state $\boldsymbol{F}$. In the figure, the term λ represents the failure rates.

As discussed in the previous section, the communication channel of the DIM middleware can communicate through any of the three communication interfaces i.e., serial port, Wifi and bluetooth. Moreover, only one communication interface is used at a time to communicate the data from medical device output to the data mapping. With the aim to increase the reliability of communication channel in terms of successful communication, we propose to use all the three communication channels in parallel, while using the concepts of TMR mechanism. This proposed modification of the DIM middleware can significantly increases the reliability of the underlying HIS system by enhancing the reliability of the communication channel. This choice would obviously need devices that can communicate via all three communication mediums and is thus the cost of the additional reliability gained. The Markov chain of the modified DIM based HIS system is presented in the Fig 5.3 and its transitional probabilities are presented in the Table 5.1, whereas the failure probabilities of all the communication interfaces are considered to be 0.1.

In Fig 5.3, the state S_4 represents the status of the medical device machine. If the tests are successful, the state machine moves to the state S_7, which indicates that all the three communication channels are functioning

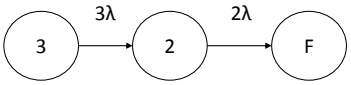

FIG. 5.2. *MC of a TMR mechanism*

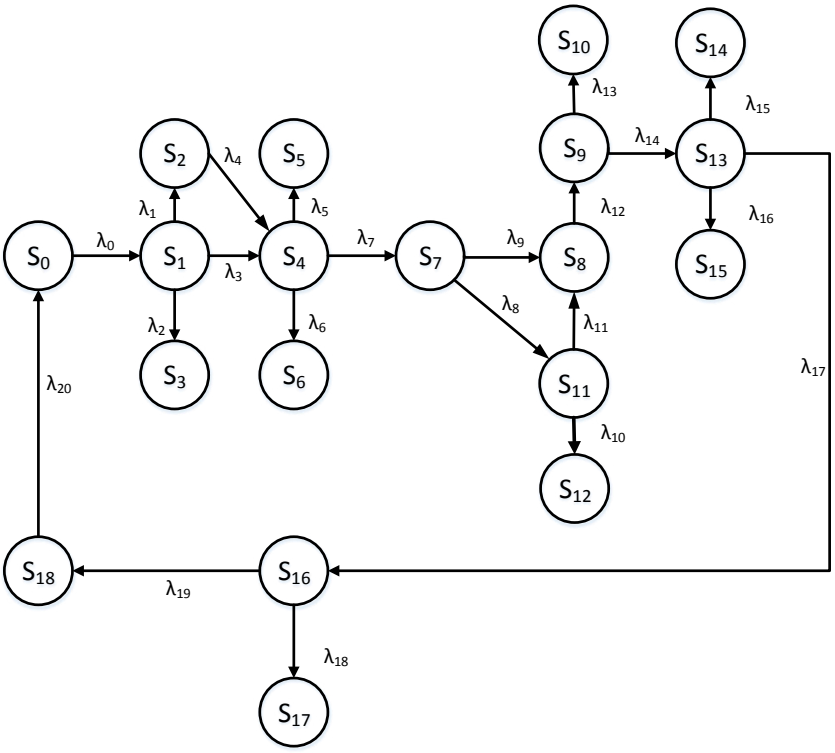

FIG. 5.3. *State Machine of Modified DIM based HIS system*

TABLE 5.1
State Transitional Probabilities

State Transitions	Probabilities	State Transitions	Probabilities
λ_0	1.0	λ_{11}	1-2λ=0.8
λ_1	0.02826	λ_{12}	1.0
λ_2	0.00174	λ_{13}	0.2
λ_3	1-λ_1-λ_2=0.97	λ_{14}	1-λ_{13}=0.8
λ_4	1.0	λ_{15}	0.065
λ_5	0.035	λ_{16}	0.065
λ_6	0.035	λ_{17}	1-λ_{15}-λ_{16}=0.87
λ_7	1-λ_5-λ_6=0.93	λ_{18}	0.25
λ_8	3λ=0.3	λ_{19}	1-λ_{18}=0.75
λ_9	1-λ_8=0.7	λ_{20}	1.0
λ_{10}	2λ=0.2		

TABLE 5.2
Probability of Success and Failure

Lab Rejection	0.00319	Data Reading Failure	0.32056
Bar Code Error	0.0507	Data Reading Success	0.6981
Device Hardware Error	0.06417	Mapping Machine Error	0.08334
Device Software Error	0.06417	Mapping Algorithm Failure	0.08334
Machine Success	0.92838	Mapping Success	0.60738
DIM Success	0.60738	Pathologist Rejection	0.27889
Channel Failure	0.4215	Pathologist Acceptance	0.4555
Communication Failure	0.1023	Successful Delivery	0.4555
Communication Success	0.87263		

TABLE 5.3
State Transitional Probabilities

State Transitions	Probabilities	State Transitions	Probabilities
λ_0	10	λ_{11}	10-2λ=8
λ_1	0.2826	λ_{12}	10
λ_2	0.0174	λ_{13}	2
λ_3	10-λ_1-λ_2=9.7	λ_{14}	10-λ_{13}=8
λ_4	10	λ_{15}	0.65
λ_5	0.35	λ_{16}	0.65
λ_6	0.35	λ_{17}	10-λ_{15}-λ_{16}=8.7
λ_7	10-λ_5-λ_6=9.3	λ_{18}	2.5
λ_8	3λ=3	λ_{19}	10-λ_{18}=7.5
λ_9	10-λ_4-λ_5-λ_6=7	λ_{20}	10
λ_{10}	2λ=2		

successfully. If one of the communication channel fails, the state machine will enter the state S_{11}. Finally, if more than one communication channel fail, the state machine will move to the fail state, which is represented by S_{12}. By using the transitional probabilities, presented in the Table 5.1, we obtained the reliability results which are depicted in the Table 5.2.

For the reliability evaluation of a real-time workflow of the underlying system, we developed its CTMC model and analysed the intended property to find the probability of successful delivery of the medical reports to the patient. The CTMC model is just like its MDP model as presented in Fig 5.3, whereas the input transitional probabilities are presented in Table. 5.3. The output results are presented in Fig. 5.4. From the graph, we conclude that the probability of successful delivery of the medical reports to a single patient by the pathologist during the time period of 1 hour is almost 0.36. These results indicate that the overall reliability of the modified DIM based HIS system has been increased.

6. Reliability Improvement Strategies. As discussed earlier, HIS systems have been increasingly used in many hospitals and are considered to be the fundamental systems of the hospital workflows. Their functionality must be reliable due to the fact that a single fault in the system may lead to a human death. For example, if a blood analyser or a urine testing device produces incorrect results of a particular patient, the results may be mistakenly incorporated as correct results and may eventually cause a serious damage to the patient's health. It is highly recommended to perform the reliability analysis of a workflow as it helps to find the failures and weaknesses in the system and thus some appropriate measures can be taken to incorporate such failures and to increase the overall reliability. In this paper, we conducted the reliability analysis of a typical hospital workflow as well as a DIM based workflow and highlighted the achieved automation and increased reliability in Sections 3 and 4. We further declared in Section 5 that the overall success rate of the workflow can be further increased by adopting the TMR approach within the system and presented the MDP and CTMC based reliability results.

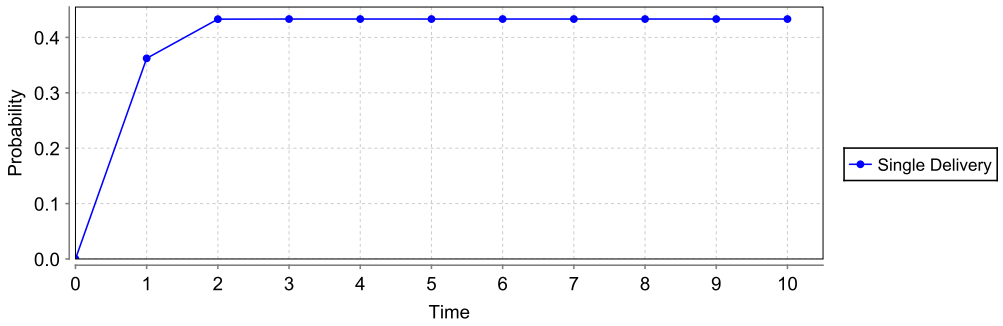

FIG. 5.4. *Probability of successful delivery of a single patient's reports w.r.t time*

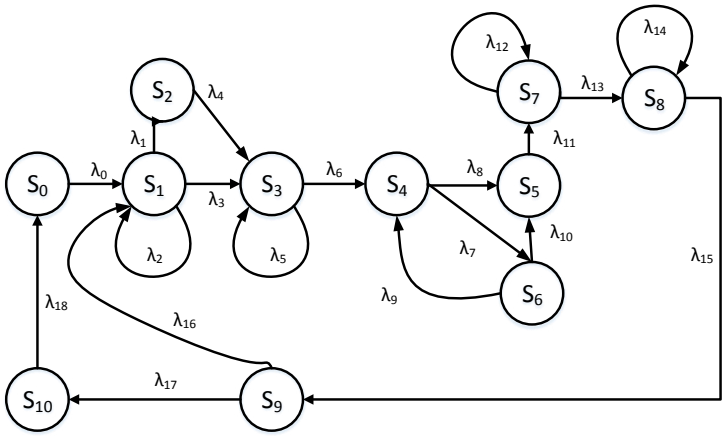

FIG. 6.1. *State Machine*

It has been noted that the overall reliability is not increased up to an acceptable level even after applying TMR approach within the DIM based HIS system and thus there is a dire need to increase this reliability by using some other reliability improvement strategies.

We propose some strategies that have a significant impact on the overall reliability as well as success rate of the hospital workflow and we present a CTMC based reliability analysis of the workflow with these strategies enabled. One of the strategy is to use *verifiers* after every transitional event, such as blood test, urine test, data communication, data reading, data mapping etc., that will verify the correctness of the output result of each event, where a *verifier* can either be an automatic computer system or a human resource. If a *verifier* identifies a mistake, it will notify its event to carry out the process again, and thus the event will eventually produce correct results and will never go into a fail state. Therefore, if all the transitional events produce correct results, the system will never go into a fail state and the overall reliability will greatly increase. Fig 6.1 presents the Markov Chain of TMR enabled DIM based HIS system where no transitional state goes into a fail state due to the applied *verifier*. The other strategy refers to buying highly reliable HIS systems in such a way that their failure rates are very low. For example, if the failure probability of the blood analyzer or urine testing device is very low, it will help to enhance the overall system reliability. Similarly, a highly reliable DIM middleware will greatly improve the overall success rate of the hospital workflow. By using low failure rates, we assume the state transitional probabilities as presented in the Table 6.1, where the failure probability of the communication medium has been assumed to be 0.01. By using these transitional probabilities, we conducted the CTMC based reliability analysis of the workflow, mentioned in the Fig 6.1, and the results are depicted in

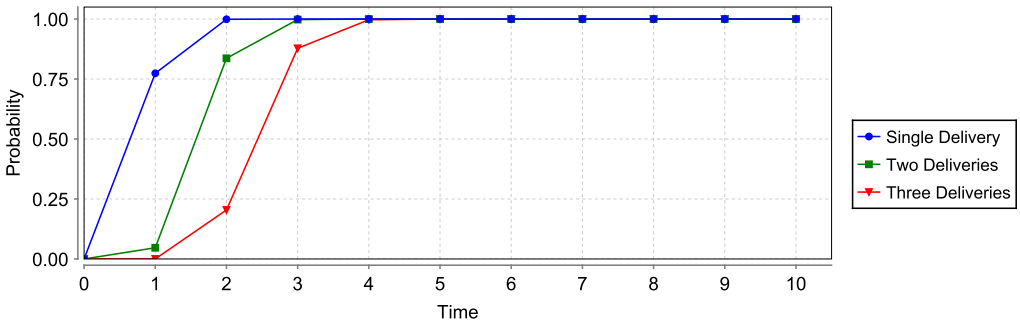

FIG. 6.2. *Probability of Successful Delivery of the Medical Report*

TABLE 6.1
State Transitional Probabilities

State Transitions	Probabilities	State Transitions	Probabilities
λ_0	10	λ_{10}	10-2λ=9.998
λ_1	0.001	λ_{11}	10
λ_2	0.001	λ_{12}	0.002
λ_3	10-λ_1-λ_2=9.998	λ_{13}	10-λ_{12}=9.998
λ_4	10	λ_{14}	0.002
λ_5	0.01	λ_{15}	10-λ_{14}=9.998
λ_6	10-λ_5=9.99	λ_{16}	0.001
λ_7	3λ=0.003	λ_{17}	10-λ_{16}=9.999
λ_8	10-3λ=9.997	λ_{18}	10
λ_9	2λ=0.002		

the Fig 6.2. These results indicate that the overall reliability has been significantly improved. For example, the probability of successfully delivery of the medical reports to a single patient is 0.76 within a time period of 1 hour and this probability increases w.r.t. time, as presented by blue colored graph. Similarly, the probability of successfully delivery of the medical reports to two patients is 0.01 within a time period of 1 hour but this probability considerably increases w.r.t. time, as presented in the green colored graph.

To the best of our knowledge, the underlying DIM based HIS system has not been analysed before using formal methods and the results presented in this paper are accurate and provide detailed information about the system before deployment. On the contrary, the traditional reliability analysis approaches, including numerical methods and simulations, cannot match the rigour and soundness of the results obtained in the presented work.

7. Conclusion. The paper presents a formal reliability analysis of a typical DIM based HIS system using probabilistic model checking technique. The main contribution of the paper includes the MDP and CTMC models development of the traditional HIS system, the DIM based system and the fault tolerant based DIM system and the identification of the corresponding system properties. The analysis is conducted using the PRISM tool and thus the models and properties are implemented for the above-mentioned systems in the language of PRISM. The reliability analysis approach, presented in this paper, was found to be more scalable and accurate compared to the traditional simulation based analysis techniques. We aim to evaluate other DIM middlewares as well using the proposed technique. Similarly, we also aim to find the reliability improvements by using **n** level-redundancy within the DIM HIS system.

REFERENCES

[1] A. Gawanmeh, *An Axiomatic Model for Formal Specification Requirements of Ubiquitous Healthcare Systems*, in Consumer Communications and Networking, IEEE, 2013, pp. 898–902.

[2] W. Ahmad, M. Jongerden, M. Stoelinga, and J. van de Pol, *Model checking and evaluating QoS of batteries in MP-SoC dataflow applications via hybrid automata (extended version)*, Centre for Telematics and Information Technology, University of Twente, 2016.

[3] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, *Theorem proving verification of privacy in WBSN for healthcare systems*, in International Conference on Electronics, Circuits, and Systems, IEEE, 2013, pp. 100–101.

[4] H. Al Hamadi, A. Gawanmeh, and M. Al-Qutayri, *A Verification Methodology for a Wireless Body Sensor Network Functionality*, in Biomedical and Health Informatics (BHI), 2014, pp. 635–639.

[5] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, *Formalizing Electrocardiogram (ECG) Signal Behavior in Event-B*, in e-Health Networking, Applications and Services (Healthcom), IEEE, 2014, pp. 55–60.

[6] A.Mahmood, F.Ahmed, K.Latif, H.Mukhtar, and A.Raza, *Middleware for Medical Device Interoperability using Ontology-based Description and Mapping*, Technical Report, National University of Sciences and Technology, Pakistan, (2015). http://semr.seecs.nust.edu.pk/downloads/middleware.pdf.

[7] ASTM E1394-97, *Standard Specification for Transferring Information Between Clinical Instruments and Computer Systems*, 1997. http://www.astm.org/Standards/E1394.htm.

[8] Y. Aviv and A. Pazgal, *A partially observed Markov decision process for dynamic pricing*, Management Science, 51 (2005), pp. 1400–1416.

[9] S. Brown, *Networked Health Information System for Monitoring Food Intake*, Oct. 7 2003. US Patent App. 10/605,548.

[10] C. Bertolini, Z. Liu, M. Schaf, and V.Stolz, *Towards a Formal Integrated Model of Collaborative Healthcare Workflows*, in Foundations of Health Informatics Engineering and Systems, vol. 7151 of LNCS, Springer, 2012, pp. 57–74.

[11] R. Cerqueti, P. Falbo, C. Pelizzari, F. Ricca, and A. Scozzari, *A mixed integer linear program to compress transition probability matrices in Markov chain bootstrapping*, Annals of Operations Research, (2016), pp. 1–25.

[12] O. Choudhury, N. Hazekamp, D. Thain, and S. Emrich, *Accelerating Comparative Genomics Workflows in a Distributed Environment with Optimized Data Partitioning and Workflow Fusion*, Scalable Computing: Practice and Experience, 16 (2015), pp. 53–70.

[13] J. Dale and D. Novis, *Outpatient phlebotomy success and reasons for specimen rejection*, Archives of pathology & laboratory medicine, 126 (2002), pp. 416–9.

[14] A. K. David Chou, *LIS01-A2: Specification for Low-Level Protocol to Transfer Messages Between Clinical Laboratory Instruments and Computer System; Clinical and Laboratory Standards Institute (CLSI)*, 2008. http://shop.clsi.org/automation-documents/LIS01.html.

[15] R. P. Dobrow, *Continuous-Time Markov Chains*, Introduction to Stochastic Processes With R, pp. 265–319.

[16] A. Gawanmeh, H. Al-Hamadi, A. Al-Qutayri, S.-K. Chin, and K. Saleem, *Reliability Analysis of Healthcare Information Systems: State of the Art and Future Directions*, in IEEE International Conference on e-Health Networking, Applications and Services, IEEE, 2015, pp. 68–74.

[17] J. M.-K. H. Hermanns, J. Katoen and M. Siegle, *ETMCC: Model Checking Performability Properties of Markov Chains*, in Dependable Systems and Networks, 2003, pp. 673–673.

[18] H. Younes, *Ymer: A Statistical Model Checker*, in Computer Aided Verification, vol. 3576 of LNCS, Springer, 2005, pp. 429–433.

[19] O. Hasan and S. Tahar, *Formal Verification Methods*, Encyclopedia of Information Science and Technology, IGI Global, (2015), pp. 7162–7170.

[20] R. Hawkins, *Managing the pre-and post-analytical phases of the total testing process*, Annals of laboratory medicine, 32 (2012), pp. 5–16.

[21] Hussam Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, *Formal Validation of QRS Wave within ECG*, in IEEE Int. Conf. on Information and Communication Technology Research, May 2015, pp. 190–193.

[22] J. F. Groote, A. Osaiweran, and J. H. Wesselius, *Analyzing the Effects of Formal Methods on the Development of Industrial Control Software*, in Software Maintenance, IEEE, 2011, pp. 467–472.

[23] M. K. J. Katoen and I. Zapreev, *A Markov reward Model Checker*, in *Quantitative Evaluation of Systems*, 2005, pp. 243–244.

[24] K. Benghazi, M. V. Hurtado, M. L. Rodrguez, and M. Noguera, *Applying Formal Verification Techniques to Ambient Assisted Living Systems*, vol. 5872 of LNCS, Springer, 2009, pp. 381–390.

[25] M. V. K. Sen and G. Agha, *VESTA: A Statistical Model-Checker and Analyzer for Probabilistic Systems*, in Quantitative Evaluation of Systems, 2005, pp. 251–252.

[26] M. Kwiatkowska, G. Norman, and D. Parker, *PRISM: probabilistic model checking for performance and reliability analysis*, ACM SIGMETRICS Performance Evaluation Review, 36 (2009), pp. 40–45.

[27] A. Legay, B. Delahaye, and S. Bensalem, *Statistical Model Checking: An Overview*, in Runtime Verification, H. Barringer, Y. Falcone, B. Finkbeiner, K. Havelund, I. Lee, G. Pace, G. Rou, O. Sokolsky, and N. Tillmann, eds., vol. 6418 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2010, pp. 122–135.

[28] R. Lyons and W. Vanderkulk, *The use of triple-modular redundancy to improve computer reliability*, IBM Journal of Research and Development, 6 (1962), pp. 200–209.

[29] M. Hoogendoorn, M. C. Klein, Z. A. Memon, and J. Treur, *Formal Verification of an Agent-Based Support System for Medicine Intake*, 25 (2009), pp. 453–466.

[30] M. Kwiatkowska, G. Norman, and D. Parker, *PRISM 4.0: Verification of Probabilistic Real-time Systems*, in Computer

Aided Verification, vol. 6806 of LNCS, Springer, 2011, pp. 585–591.
[31] M. Vieira, X. Song, G. Matos, S. Storck, R. Tanikella, and B. B. Hasling, *Applying Model-Based Testing to Healthcare Products: Preliminary Experiences*, in Software Engineering, ACM, 2008, pp. 669–672.
[32] E. Marzini, P. Mori, S. Di Bona, D. Guerri, M. Lettere, and L. Ricci, *A tool for managing the X1. V1 platform on the cloud*, Scalable Computing: Practice and Experience, 16 (2015), pp. 103–120.
[33] O. Faust, U. R. Acharya, and T. Tamura, *Formal Design Methods for Reliable Computer-Aided Diagnosis: A Review*, IEEE Revisions in Biomedical Engineering, 5 (2012), pp. 15–28.
[34] U. Pervez, O. Hasan, K. Latif, S. Tahar, A. Gawanmeh, and M. Hamdi, *Formal Reliability Analysis of a Typical FHIR Standard based e-Health System using PRISM*, in e-Health Networking, Applications and Services, IEEE, 2014, pp. 43–48.
[35] R. Jetley, S. PurushothamanIyer, and P. L. Jones, *A Formal Methods Approach to Medical Device Review*, IEEE Computer Journal, 39 (2006), pp. 61–67.
[36] S. M. Babamir and M. Borhani, *Formal Verification of Medical Monitoring Software Using Z Language: A Representative Sample*, Journal of Medical Systems, 36 (2012), pp. 2633–2648.
[37] B. Sericola, *Discrete-Time Markov Chains*, Markov Chains, pp. 1–87.
[38] S.O. Oio, O. Olugbara, G. Ditsa, M. Adigun, and S. Xulu, *Formal Model for e-Healthcare Readiness Assessment in Developing Country Context*, in Innovations in Information Technology, 2007, pp. 41–45.
[39] U. Pervez, A. Mahmood, O. Hasan, K. Latif, and A. Gawanmeh, *Formal Reliability Analysis of Device Interoperability Middleware (DIM) based E-Health System using PRISM*, in International Conference on E-health Networking, Application Services (HealthCom), IEEE, Oct 2015, pp. 108–113.
[40] K. Ugurlu, *Controlled Markov Decision Processes with AVaR Criteria for Unbounded Costs*.
[41] Z. Daw, R. Cleaveland, and M. Vetter, *Formal Verification of Software-Based Medical Devices considering Medical Guide-lines*, Computer Assisted Radiology and Surgery, 9 (2014), pp. 145–53.

Edited by: Kashif Saleem
Received: Feb 1, 2016
Accepted: May 27, 2016