Open Access
Full Length Article

ORIGINAL ARTICLE

Formal Verification of Safety and Liveness Properties using Coloured Petri-Nets: A Flood Monitoring, Warning, and Rescue System

Nadeem Akhtar[1], Abdul Rehman[2], Dost Muhammad Khan[3]

[1,3] Department of Computer Science and IT, The Islamia University of Bahawalpur, Pakistan
[2] Department of Computer Science and IT, Virtual University of Pakistan

ABSTRACT

Annual floods after rainy monsoon season are the most dangerous natural disaster in Pakistan that affects millions of people. It is important to specify, design, model, and implement a correct system for flood monitoring, and after-flood rescue services. The correctness of the proposed system is of vital importance. We have proposed an approach for the analysis, design, and modeling of a flood monitoring system centered on formal modeling and verification. Flood monitoring which requires the environment data starts from flood sensors, independent observers and meteorological forecasts. Information is processed to determine flood status and in real-time, this information is shared among the general public, meteorological departments and disaster management authorities. The early warning and preventions alert can minimize the aftershocks of disaster. The recommended approach uses formal modeling and verification to ensure the correctness of the system. The model takes input and systemically ensures that the liveness and safety properties hold for the proposed system. Model checking technique ensures high-quality, reliable model constructions.

Keywords: Flood monitoring, Formal modeling, Formal verification, Safety property, Liveness property, Coloured Petri Nets (CPNs), Event-B, Rodin.

Author`s Contribution
[1]Data analysis, Data collection, Conception, interpretation and manuscript writing
[2]Conception, synthesis, and manuscript writing
[3]Conception, Interpretation and discussion

Address of Correspondence
Nadeem Akhtar
Email: nadeem.akhtar@iub.edu.pk

Article info.
Received: January 11, 2018
Accepted: June 03, 2018
Published: June 30, 2018

Cite this article: *Akhtar N, Rehman A, Khan DM. Formal Verification of Safety and Liveness properties using Coloured Petri-Nets: A Flood Monitoring, Warning, and Rescue System Confirmation J. Inf. commun. technol. robot. appl.2018; 9(1):80-88.*

Funding Source: *Nil*
Conflict of Interest: *Nil*

INTRODUCTION

Pakistan is an agriculture country, where the economy depends upon crops, and crops depend on irrigation water. In Pakistan, one of the world's biggest irrigation canal system is running, consisting of five major rivers and a large number of small rivers, and canals. Agriculture is the back-one of Pakistan economy, and irrigation water is the back-bone of agriculture. So without Irrigation water the economy simply cannot sustain itself. The river system depends on the northern glaciers for water, and each year after monsoon season the water levels in rivers, dams, and canals increase to dangerous levels, and this results into floods after every couple of years. These floods cause human lives loss, animal lives loss, destroy millions of hectors of crops. It's of critical

importance for the flood warning system to warn people on time about intensity and degree of floods. And if the system is not able to warn people on time then it can result in high human casualties, crops loss as well as very high material and financial loss.

Formal modeling is an important approach for the analysis, design, verification, and implementation of a correct software system. A model is created and the correctness properties of safety, liveness of the system is verified by applying mathematical proofs on that model. This model helps to exhaustively write the specifications as well as to rigorously prove the correctness properties. We have constructed the formal models using a well-defined formal language having a mathematical based syntax, semantics, and grammar. This formal model

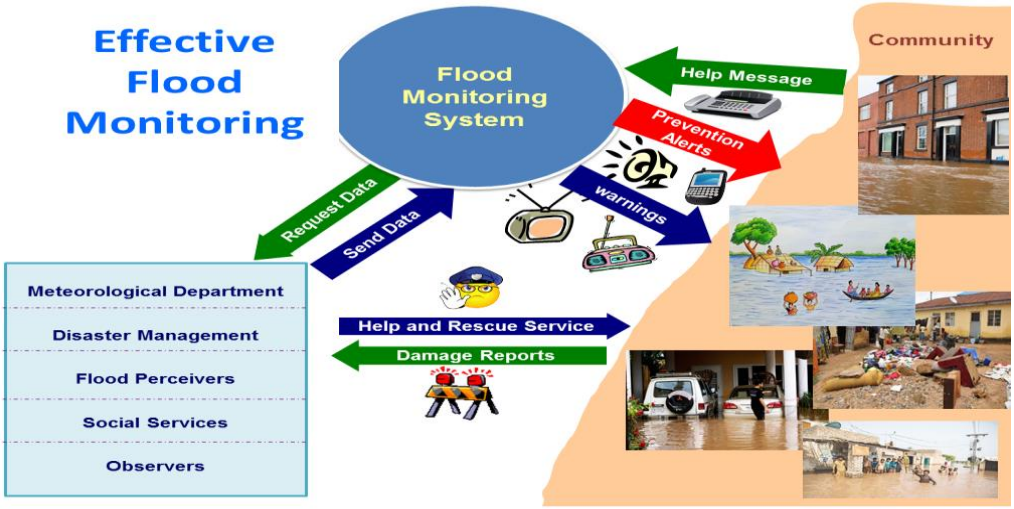

Fig. 1. Stakeholders of the Flood Monitoring System

provides the real-time simulation of the actual working system and verifies whether or not the system is working correctly (i.e. correct behavior) according to its desired specifications. This formal modeling plays a fundamental role in understanding the requirements of the system as well as designing and implementing a correct system. This formal modeling also plays a key role in the exhaustive verification and validation of the system. Theorem Provers can be used with this formal modeling.

The flood monitoring, warning, and rescue system is a critical system as human lives depend on it. Therefore it must be correct. Formal modeling using CPN simulates the control flow as well as data flow for the flood monitoring system. In the next step the critical parts of the flood monitoring system are specified in Event-B (Abrial, 2010)1 method using Rodin tool for the theorem proving and proof obligations. This results in a heavyweight exhaustive formal verification of the safety and liveness properties.

***Why flood monitoring*?**

Pakistan has an agriculture-centered economy. It has seven major rivers, and out of these rivers originate hundreds of small and large canals. These canals constitute one of the biggest canal irrigation system of the world. This canal system is central to the economy, which in turn is vital for the survival of Pakistan. Irrigation water plays a central role. But each year after monsoon rain seasons, floods arise in rivers and canals. These floods vary from low flooding to very high-level floods. These floods result into human lives loss, and complete destruction of houses, crops, agriculture lands and cattle. Our major objective is to devise correct methods, techniques, and tools to give real-time floods warnings, future flood predictions, as well as rescue services after the floods.

***Why formal modeling*?**

Formal modeling is based on automated construction of a mathematically based model of the actual system. It allows to study the system exhaustively and specify complete requirements. Most of the formal modeling methods and techniques also have model-checking tools integrated into them for formal verification.

Why model checking?

One of the major methods for formal verification is model checking. Model checking is based on exhaustive

verification and mathematical proofs. In software development, the correctness of the system is important. If the system is incorrect then it's of no use. The first and foremost goal of using formal modeling and verification is to ensure the correctness of the system. The correctness of the proposed model is verified using model checking techniques. Model checking performs automatic verifications of the systems. The model takes input and systemically checks whether or not, the safety and liveness properties hold. The proposed system is a critical system, as without the correct working of the system human life can be lost, and millions of hectors of lands, properties, and buildings can be destroyed.

Why correctness?

The role of correctness is fundamental, an incorrect system is of no use. The proposed system is a critical system i.e. if the system is incorrect and not able to warn general public at the time of flood then it can lead to human life loss, property loss, crops damaged, and animal loss.

Why safety and liveness?

Safety means something bad does never happen i.e. a certain minimum level of state of affairs is maintained. Safety property can be ensured through analysis of the functionality (i.e. behavior), and formal tools as model checkers can be used to ensure safety property. Liveness states that something good eventually happens. Safety and liveness both complement each other, and for the correct working of the system, both safety and liveness are equally important. Both safety and liveness ensure the correctness of the system.

1.1. Research Hypothesis

"Is it possible to design and specify a correct methodology based on the standard of the flood monitoring system, damage reduction, and disaster management operation; formal modeling and verifications of the methodology to ensure correctness properties?"

1.2. Research Questions

The fundamental research questions are:

RQ.1. *How can the correctness of a system be ensured to make it reliable?*

RQ.2. *How formal verification can improve quality assurance by checking the correctness through model checking techniques?*

RQ.3. *How formal verification is beneficial to be used for flood monitoring and disaster management?*

LITERATURE REVIEW

(Menon & Kala, 2017)[13] proposed a system of three major components; a processing unit, sensor network, and database of applications. The water level is monitored by using wireless sensors that use mobiles radio service communication to broadcast the information towards the web-based server.

Smith et al. (2017)[18] presented a community-based warning system for floods in Nepal. It includes the present status of the community-based system, development of robust operations for forecasting and proper strategies to utilize the flood by the Nepal hydrological and meteorological department to provide early flood warnings on time. This system uses the database to generate the probability of flood forecast, which is represented by a simple visual platform.

A system was developed by Alipio et al. (2017)[3] called ArRoad that analyzes and monitors rush-hour traffic and water-logged regions via sensors and image processing which uses machine learning techniques to first forecast traffic congestion and substitute redirecting traffic routes. Water sensor nodes are located to monitor and analyzes the flooded locations whereas real-time video images of cameras are used to detect the traffic capacity on the roads.

Amagsila et al. (2017)[4] presented an Android application for motor vehicle owners that use smart-phones. They can receive real-time flood alerts during traveling in their motor vehicles. Identification of flood is done by specific Arduino device while Global Positioning System (GPS) is used for detection of the user location. Motor vehicle passengers are informed about flood thorough voice messages. The main focus of this research is to use mobile application for the flood warning to save people from the floods during traveling.

Yumang et al. (2017)[21] proposed a flood monitoring system for Philippine centered on the areas having high flood victims. The system programmed and developed using Arduino Uno technology. The sensors and the global mobile system powered by a generator or solar panel are used. The system sends SMS alerts to the residence of the flood affected area. The system tested

through simulation of floods models after the analysis of result shows that the design satisfies the requirement of the user.

Noar & Kamal (2017)[19] presented the idea of a smart flood monitoring system having platform named Blynk, which is used as a standard for data communication. Blynk is based on two nodes multipoint control unit using an Android application. The first node multipoint control unit is located at the flood zone, while the second node multipoint control unit performed as the control room. The information is rapidly collected and kept in a committed database for copy purposes. The individual in charge of the controller room sends the information to the second node multipoint control unit through Blynk Bridge to activate the signal and the light emitting diode.

Research by Panganiban & Cruz (2017)[20] designed and developed a method to determine the status of flood water level on the roads through the use of the analytical model. The flood level is measured at different stages. The data is collected from the rain gauges and websites. PAGASA platform sends color coded flood levels that are easily understood.

Siregar et al. (2017)[17] proposed a network monitoring system in order to understand the flow of data packets in a flood monitoring system. This monitoring system evaluated and recognized different types of packet losses via early detection algorithm. Early detection algorithm technique matches the packet's counter value using its type through a user well-defined starting point value. This system is executed and exhaustively evaluated for a number of days in a continuous fashion. This system involved user data protocol, transmission control protocol, and internet. This network system was used as the main component of a flood monitoring system.

Khan et al. (2016)[11] proposed a flood monitoring system that gets data from the government departments, independent observers and flood associated departments and processes that data to generate warning and preventions alerts to the people of that area and also emergency services. It describes the architecture of the smart flood monitoring system. The smart flood monitoring system emphasized continuous communication among the citizens, police, media and official authorities.

Mousa et al. (2016)[14] have suggested a novel recognizing tool that concurrently monitors traffic over-crowding and flash floods in inner-city areas. The proposed algorithm is used with low-power consumption wireless sensor tools. The water level can be checked for half of the year by comparing different sensors, the result shows that the inner-city water level is predictable.

Sakib et al. (2016)[15] proposed one of safest techniques neuro-fuzzy approach for a flood monitoring system which uses a wireless network sensor for flood monitoring. The node is created using a low-cost wireless network which gathers information as water level, wind speed, rainfall, and air pressure from a particular location in order to validate the suggested approach for the flood monitoring system. The wireless network is linked though mesh topology that can send data to distant places.

In India Shiravale et al. (2015)[16] have recommended a system that generates flood alerts via wireless network sensors. These wireless sensors also perform weather forecasting. The older systems used data from satellites for generating flood alerts, therefore it used to take long time intervals to send flood alerts, also in a number of cases the information sent by satellites were incomplete and thus insufficient to generate and send alerts. This proposed system consisting of a network of wireless sensors identify, monitor, and report the flood situation using water level and rainfall measure.

A low-cost flood monitoring system based on Arduino and Android phone was proposed by Intharasombat & Khoenkaw (2015)[6] The system can measure water level by techniques that gather information through sensors and forward it to server mobile network or Wi-Fi. Some other high-level structures are extracted at the server to determine the types of floods.

(Akhtar, 2014)[2] has proposed an approach for the requirement specification, formal verification, and transformation from a requirement model to a verification model based on multi-agent systems. This approach can also be used for the analysis, design, verification, and implementation of a flood monitoring system.

A system that consisted of the Pressure sensor and rain gauge are linked using general packet radio service network is presented by Garcia et al. (2015)[5]. Data from network stations are received through transmission control protocol to provide information and floods updates using mobile SMS network as well as website. Flood

arrival time is implemented using forecast Random algorithm to get an early flood alerts system.

BACKGROUND STUDIES

Formal modeling and Formal Verification

The correctness of the model is verified by constructing a formal model of the system. One of the methods of formal modeling is model checking. Model checking is the process of automatic verifications of the systems. The model takes input and systemically checks whether this property holds by the system or not. A formal model of the system is constructed by using Coloured Petri-Nets (CPNs).

Formal verification is the process of ensuring the correctness of the system, which evaluates whether or not the functionality (i.e. behavior) of the system is according to its requirement specifications. It can also be used to verify the sub-properties of correctness i.e. safety and liveness. Formal verification ensures correctness by using mathematical constructs of mathematics i.e. set theory, relations, functions, axioms, invariants, pre-condition, post-condition, propositional calculus, first-order predicate calculus etc. The major methods and techniques for formal verification are model checking, theorem proving, automated generation of proof obligations etc.

Coloured-Petri Nets (CPNs)

Coloured Petri nets[7] [8] [9] [10] [12] is a formal, discrete mathematics based graphical language that creates an executable model of the system. This model consists of places, transitions, and tokens flowing between places through transitions. These formal models can be compiled and executed. They are ideal to model the behavior of real-time critical software systems. A system can be modeled in the form of CPNs and its correctness properties of safety and liveness can be exhaustively studied and verified. The CPN has a graphical as well as textual syntax, it can exhaustively verify a system, in which concurrency, communications, and synchronizations play the main role.

PROPOSED APPROACH

The Proposed approach for a flood monitoring system to ensure correctness properties for safety and liveness is shown in the figure. 2. It has three major phases of Data input, formal modeling, and formal verification. In order to implement the model and verify the correctness properties of safety and liveness CPN is used. In addition to this verification, the Event-B (Abrial, 2010)[1] based formal theorem proving is done for heavyweight exhaustive verification and validation.

Workflow model

Workflow model as shown in the figure. 1 shows the major process, and put-forth the relationship between the general public, meteorological department, and crisis management authorities. This model helps to understand the flow of information to facilitate task completion. The data-flow model is very helpful and enhances the understanding of the system. The given rich picture indicates the data-flow of flood monitoring approach before and after the flood and determines the flood status.

Formal CPN Model

In order to check the status of river floods, prediction

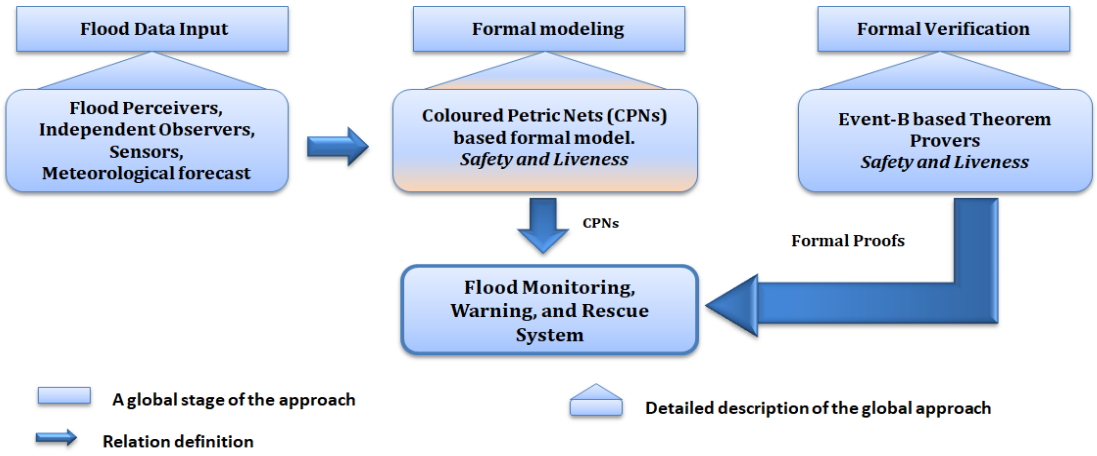

Fig.2. The proposed Flood Monitoring Approach centered on formal modeling and verification

and initial signs of the flood are vital. All the flood indicators (i.e. rainfall, river water level, the storage capacity of water in dams and ponds, water speed, water direction etc.) are analyzed. These indicators describe flood status. CPN models are designed and developed. These CPN models, formally specify the different aspects of flood monitoring as:

- Communication with the population of areas that are in the danger zone and therefore can be affected by floods
- Communication with the population of areas already affected by floods
- Preventive warnings to the affected population
- After-flood rescue services information to the affected population
- After-flood information about the distribution of first-aid to the affected population
- After-flood information about shelter houses for flood victims
- After-flood information about the food distribution sites for the affected population
- Send victims location information to the crisis management authorities
- Creation of flood damage reports, then the distribution of these reports to the administrator to inform affected people on time.

The damage reports are as follows

- People killed during the flood
- People injured during the flood
- Basic health unit destroyed
- Number of cattle killed in each affected area
- Electricity supply disconnect
- School building destroyed
- Hospital destroyed
- Crops destroyed.

The queries to the admin from the flood-affected area are

- Where to find medical treatment and medicines
- When the electricity supply will be connected
- Where to live during a disaster

The admin forward these damage reports to the concerned authorities and also send a rescue and help service message for the flood-affected area. The CPN model of the flood information gathering system is shown in figure-3. After the determination of flood status, different values of flood attributes are analyzed to predict flood warning.

RESULTS AND DISCUSSION

Answers to Research Questions

RQ-1. *How can the correctness of a system be ensured to make it reliable?*

The Correctness of a critical system like a flood monitoring system is important. The correctness property

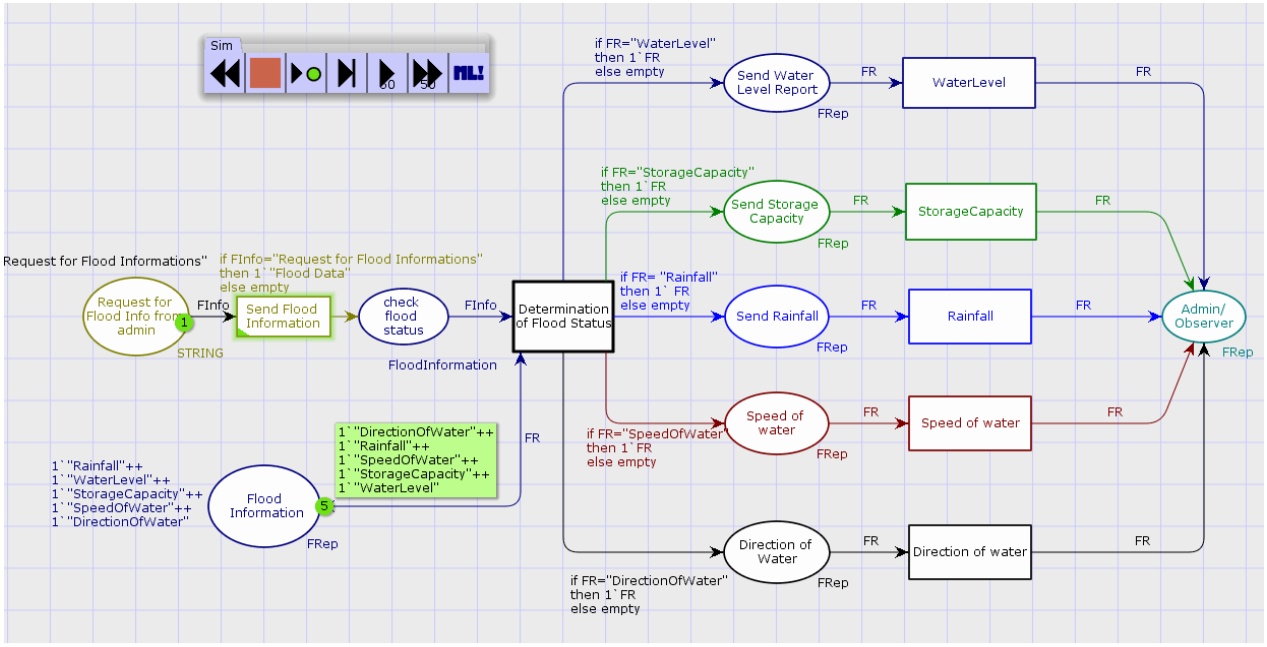

Fig. 3. CPN of Flood Information Gathering

directly influences the reliability and robustness of the system. We have concentrated on the two most important sub-properties of correctness i.e. safety and liveness. These two properties are formally specified, modeled, and verified by using CPNs and ultimately by Event-B. This paper is centered on the CPN portion of the formal verification. The CPN specification model the liveness of the system. The evaluation of safety property is done by using the Proof Obligations of the Event-B method using the Rodin platform. This process is centered on behavior modeling, consisting of sets, axioms, theorems, machines, invariants, pre-conditions, post-conditions, events, and guards. These formal proofs of safety properties of the system are not presented in the current paper and would be presented in future work.

RQ-2. *How formal verification can improve quality assurance by checking the correctness through model checking techniques?*

Model checking is one of the most important formal technique for formal verification. It performs exhaustive verification of the system state space of the proposed model. The Flood Monitoring System is specified as exhaustive CPN specifications. This CPN model of the system performs system space evaluation. As Flood Monitoring is a critical system, it must be correct, error in it can cause high human life losses.

RQ-3. *How formal verification is beneficial to be used for flood monitoring and disaster management?*

Formal verification is beneficial for ensuring the correctness properties of safety and liveness. It makes the system reliable. The reliability of the system is important for flood monitoring and disaster management in flood-affected areas. This system can save the lives and properties of millions of people living in flood-affected areas. The proposed system gets important data from sensors, process this raw data into useful information, and share this critical information with all the stakeholders i.e. flood department, meteorological forecast department, independent observers, rescue services, and the general population. This approach is beneficial because it uses

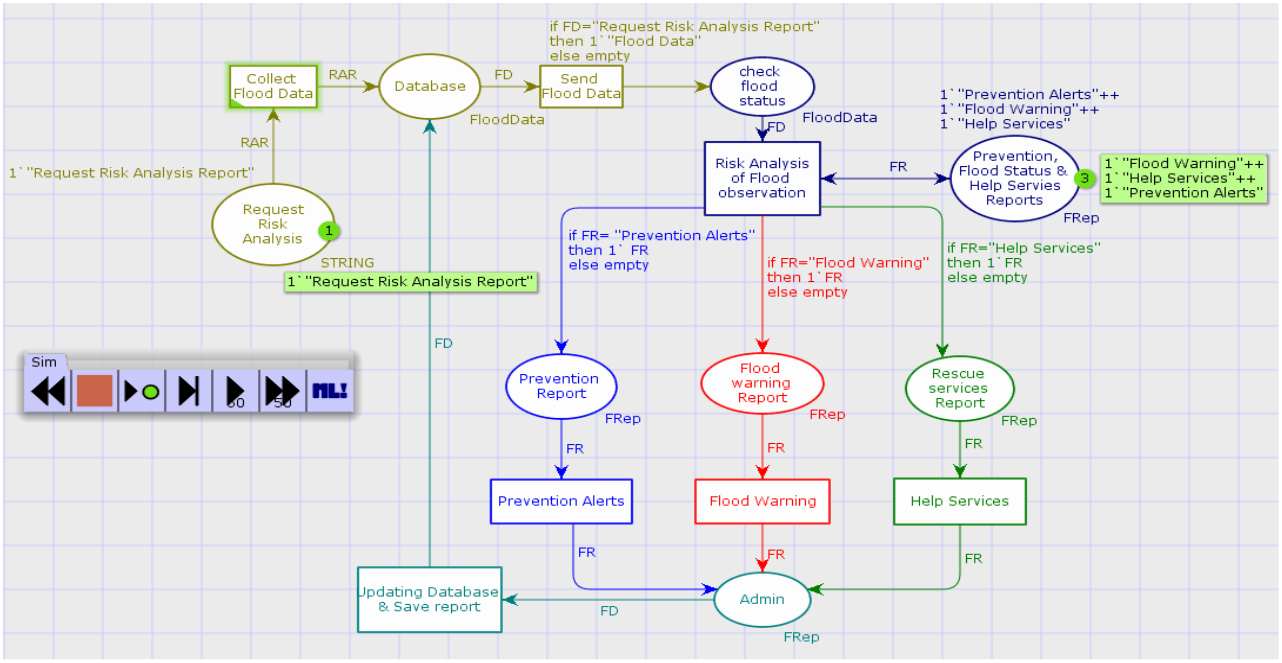

Fig. 4. CPN of Risk Analysis of Flood observation

exhaustive state space evaluation by CPN and heavy-weight theorem proving based on an Event-B method which uses the platform Rodin

CONCLUSION

The proposed flood monitoring system is designed then formally modeled, and formally verified. The detailed model is specified using CPNs. In order to implement the formal verification of safety properties, the theorem-prover of the Event-B method is used. Event B method has a very mature, stable, exhaustive and modern platform Rodin for Proof Obligations. It performs the simulations by

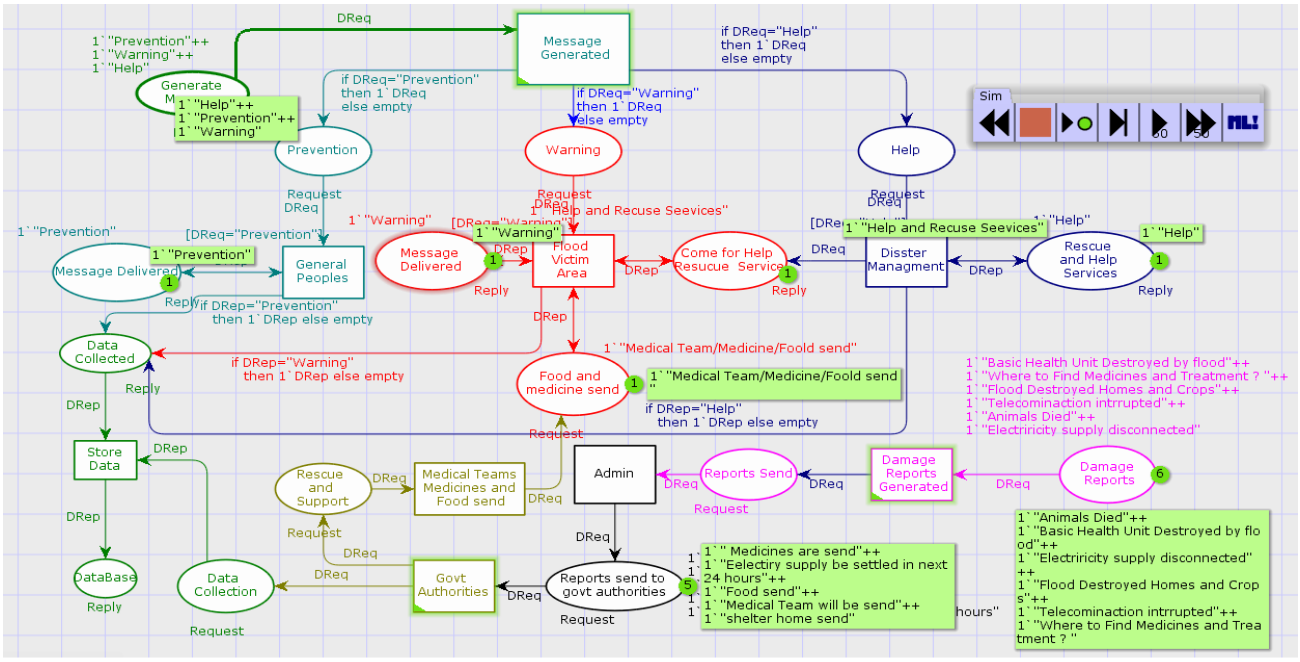

Fig. 5. CPN of after-flood Disaster Management Services i.e. Rescue and Help services

creating mathematical models that are exhaustively analyzed and proved.

FUTURE WORK

In the future, there are short term, medium term, and long-term future objectives. These three types of objectives constitute the three major axes of future work.

The short-term future objective is the exhaustive theorem proving of safety properties of the Flood Monitoring System. This exhaustive proving would be done by the Event-B method, and this process would be centered on automated as well as manual creation of Proof Obligations of the system.

The middle-term objective is the generation of high-level implementation code as a result of the refinements and transformation of the Event-B model of this Flood Monitoring System.

The long-term objective is to design, formally model, formally verify, a disaster management system for earthquakes for Pakistan.

REFERENCES

1. Abrial, J. R. (2010). Modeling in Event-B System and Software Engineering. Cambridge University Press.
2. Akhtar, N. (2014). Requirements Formal Verification and Model transformations of an Agent-based System. Computer Engineering and Intelligent Systems ISSN 2222-1719 ISSN 2222-2863 (Online) Vol.5, No.3, 1501-05120.
3. Alipio, M. I., Bayanay, J. R. R., Casantusan, A. O., & Dequeros, A. A. (2017). Vehicle traffic and flood monitoring with reroute system using Bayesian networks analysis. In Consumer Electronics (GCCE), IEEE 6th Global Conference, 1-5.
4. Amagsila, G. A., Cabuhat, M. E., Tigbayan, J. E., Uy, E., & Ramirez, E. (2017). A framework for the mobile application of flood alert monitoring system for vehicle users using the Arduino device. In Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (Hnicem), IEEE 9th International Conference, 1-6.
5. Garcia, F. C. C., Retamar, A., & Javier, J. (2015). A real-time urban flood monitoring system for Metro Manila. In Tencon IEEE Region 10 Conference, 1-5.
6. Intharasombat, O., & Khoenkaw, P. (2015). A low-cost flash flood monitoring system. In Information Technology and Electrical Engineering (ICITEE), IEEE 7th International Conference, 476-479.
7. Jensen, K., Kristensen, L. M., Wells, L., Coloured Petri Nets and CPN Tools for modeling and validation of concurrent systems Published online: 13 March 2007 © Springer-Verlag 2007.
8. Jensen, K.: Coloured Petri Nets. Basic Concepts, Analysis Methods, and Practical Use. Practical use, vol. 3. Springer, Berlin (1997).
9. Jensen, K.: Coloured Petri Nets. Basic concepts, analysis methods, and practical use. Analysis Methods, vol. 2. Springer, Berlin (1994).
10. Jensen, K.: Coloured Petri Nets. Basic concepts, analysis methods, and practical use. Basic Concepts, vol. 1. Springer, Berlin (1992).
11. Khan, S., Anwar, M., & Akhtar, N. (2016). Analysis, Design, Architecture, Specification and Formal Verification of a Smart Flood Monitoring Systems of Systems.

Sci.Int.(Lahore),28(1),221-226, ISSN 1013-5316; CODEN: SINTE 8.
12. Kristensen, L.M., Christensen, S., Jensen, K. (1998). The Practitioner's Guide to Coloured Petri Nets. Int. J. Softw. Tools Technol. Transf. 2(2), 98–132.
13. Menon K, P., & Kala, L. (2017). A Review on Flood monitoring: Design, Implementation and Computational Modules. International Journal of Innovative Research in Computer ISSN(Online): 2320-9801.
14. Mousa, M., Zhang, X., & Claudel, C. (2016). Flash flood detection in urban cities using ultrasonic and infrared sensors. IEEE Sensors Journal, 16(19), 7204-7216.
15. Sakib, S. N., Ane, T., Matin, N., & Kaiser, M. S. (2016). An intelligent flood monitoring system for Bangladesh using wireless sensor network. In Informatics, Electronics and Vision (ICIEV), IEEE 5th International Conference, 979-984.
16. Shiravale, S., Sriram, P., & Bhagat, S. M. (2015). Flood Alert System by using Weather Forecasting Data and Wireless Sensor Network. International Journal of Computer Applications, 124(10).
17. Siregar, B., Manik, M. S., Rahmat, R., Andayani, U., & Fahmi, F. (2017). Implementation of network monitoring and packets capturing using random early detection (RED) method. In Communication, Networks, and Satellite (Comnetsat), IEEE International Conference, 42-47.
18. Smith J. P., Brown, S., & Dugar, S. (2017). Community-based early warning systems for flood risk mitigation in Nepal. Nat. Hazards Earth Syst. Sci., 17, 423–437.
19. Noar, N. A. Z. M., & Kamal, M. M. (2017). The development of smart flood monitoring system using an ultrasonic sensor with blynk applications. In Smart Instrumentation, Measurement and Application (ICSIMA), IEEE 4th International Conference, 1-6.
20. Panganiban, E. B., & Cruz, J. C. D. (2017). Rainwater level information with flood warning system using a flat clustering predictive technique. In Region 10 Conference, Tencon IEEE, 727-732).
21. Yumang, A. N., Paglinawan, C. C., Paglinawan, A. C., Avendaño, G. O., Esteves, J. A. C., Pagaduan, J. R. P., & Selda, J. D. S. (2017). Real-time flood water level monitoring system with SMS notification. In Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), IEEE 9th International Conference, 1-3.