Chapter 6

Conclusion and Future Direction

This chapter summarizes the research works done in the previous chapters of this thesis and highlights the significant contributions and findings. This chapter also gives future directions for the researchers by explaining the open research challenges of security in CPSs.

6.1 Conclusion

In this thesis, we have worked on the modeling and organization problem of the CPS security and brought out some pertinent observations. Security threats are quite pertinent and observable as (1) the system needs to facilitate external entities (hardware and software) to obtain extreme privileges to operate on resources and execute functionality, and (2) interconnectivity of devices, systems and infrastructures and their possibilities of being network-ready. These factors increase the security risks by opening the doors for attackers. They could be used to launch attacks to compromise the system by exploiting existing vulnerabilities that may arise due to inappropriate policy, facilitation to external entities, inefficient and inaccurate protection mechanisms and procedures. Moreover, during development, functionality often takes priority over security. Security measures were implemented late as an add-on resulting in brittle designs that lack proper integration.

Several approaches have been proposed to perform the security analysis in the early phases of system development. Most of these present a qualitative assessment rather than a quantitative assessment. Even where security is assessed quantitatively, it was evaluated separately from functionality. This thesis presents the security modeling and arrangement approaches to overcome these research gaps in the early phases by (1) Considering the known modeling techniques for some representative CPS with the purpose of enhancing those model for integration of security consideration, and (2) Considering a moderately large distributed CPS, which may have arrangements similar to distributed systems, for integration of security arrangements along with modules/ components/ subsystems responsible for delivery of functionality.

In this direction, the main contributions are as follows -

1. A model based security verification framework is proposed to model the CPS with security, where security is analyzed qualitatively and quantitatively using fundamental properties of the Stochastic Petri Net. The proposed methodology may benefit the practitioners and academicians to understand the modeling power of a widely adopted Petri Net and its properties to filter out broad security issues at the modeling level in the early phases of the system life cycle.

2. There is a need for early-stage formal models to analyze the integrated impact of intrusion prevention and responsive measures on the availability of Safety Critical Cyber Physical System (SC-CPS) like NPP. However, with the increasing complexity of industrial control systems and their interactions with the attacker, the state space of the corresponding finite state-transitions models grows rapidly, leading to state explosion. As GSPN deals with the state explosion problem well, our second work proposes a GSPN based model to analyze the combined effect of intrusion prevention and responsive measures on the system's dynamic behavior under attack and its availability. Moreover, it is challenging to test cyber-attacks experimentally in NPPs or simulate them virtually. Hence, the transition rates of the stochastic model are difficult to

obtain, and so is determining the failure probabilities of preventive and responsive security measures. The proposed work overcomes this problem by performing the sensitivity analysis to analyze the effect of defense measures on the strength and prioritize these measures and select the optimal secure designs.

3. As CPS is generally a kind of distributed system with safety-critical functionalities which may be targeted by attackers. An architectural arrangement is proposed for integration of security arrangements along with modules/ components/ subsystems responsible for delivery of functionality.

   On the line of distributed computing, such systems require the identification of leaders for distribution of work, aggregation of results, etc. Depending upon the enormity and complexity of event monitoring for security and functionality delivered in a CPS, a single leader or separate leaders may handle the functionality and security responsibilities. By nature, CPSs are complex and large real-time systems like rail management or smart city. If security and functionality are handled by one and the same leader, the leader node may face a heavy load to coordinate all the functionality and security activities simultaneously. Consequently, the deadline of the functional tasks may be overlooked, or security events may be missed, which is considered a failure in hard real-time systems. Moreover, monitoring and events related to security are pretty different from functionality and may be needed to integrate and update the existing system. By looking at the exigency and grave consequences of security and the time criticality of security mechanisms and using the understanding developed at the modeling level in previous proposed works, we propose a multi-tier architectural model of a CPS with logical and physical separation between functionality and security. Further, we propose a fault-tolerant leader election algorithm that can independently elect the functional and security leaders. The proposed election algorithm identifies a list of potential leader capable nodes to reduce the leader election overhead. It keeps identifying the highest potential node as the leader, whenever needed, including the situation when

one has failed. We also explain the proposed architecture and its management method through a case study. Moreover, the general leader election process is itself vulnerable to initiate unnecessary leader election process. The proposed algorithm can also deal with this scenario, where a malicious node tries to initiate the election process unnecessary to target an unbiased leader. It achieves consensus among leader-capable nodes to start the election process. Further, several experiments are performed to evaluate the system performance. The experimental results show that the proposed architectural model improves the system performance in terms of latency, average response time, and the number of real-time tasks completed within the deadline.

6.2 Future Research Directions

There are many research efforts going on at various levels for dealing with security aspects in systems, including Cyber-Physical Systems. Some of the research issues warrant concerted effort concentrating on security aspects of CPSs. This needs to be done purposefully to ensure that security and other non-functional concerns are taken care of along with the system design for functionality rather than keeping them as an afterthought.

1. The problem description and corresponding modeling for a secure system may consist of ambiguities and vagueness, such problem may be viewed as uncertainties and necessary handling of the situation becomes an important challenge to be tackle.

2. The present work in this thesis has considered safety-critical systems modeling for security. In future, the impact of cyber risk on overall dependability, defined in term of aggregation of usability, fault-tolerance *etc.* may also be explored.

3. Mostly a system is tested for delivery of functionality. It is interesting to consider and explore security oriented testing for CPSs.

4. It will always be useful to consider estimation and optimization for secure system design so as to be able to workout a proposition that provides a secure system as per the budgetary needs.

5. Security algorithms may at times make use of heavily the processing time available in the system and hence it will always be prudent to strive for obtaining such algorithms that implement the security with light weight algorithm in terms of resource consumption.

6. In a CPS, threats are identified in terms of vulnerabilities and possibilities of their exploitation, during the operation of the system attacks may occurs. It would be useful to monitor occurrence of such attacks over time and data regarding their detection and responses for the purpose of application of data analytics which may identify the pattern of such attacks which may help in making use of this knowledge for strengthening the security of the system.