Secure Control for Network Systems: Theory, Algorithms and Applications

Qian Xie
NYU Tandon School of Engineering

Network systems rely on connected sensing and actuating devices for computation, communication, and coordination. Examples include transportation, logistics, manufacturing, and communication networks. State-of-the-art network systems have many fancy features, such as high mobility, real-time responses, and cooperativity. However, the lack of secure-by-design features makes them susceptible to various security failures. One real-world instance is the Internet of Vehicles (IoV), where vehicles not only communicate with each other but also with pedestrians and infrastructures. The vehicles typically make decisions based on real-time routing guidance services such as Google Maps and Waze. Such services heavily depend on data collection and transmission but also face risks of random malfunctions and malicious attacks. It has been reported that an artist used phones to create a phantom traffic jam on navigation apps. Under such circumstances, the information provided by such services can be faulty, and the misled travelers may suffer extra travel times. Nevertheless, the impact of random and strategic sensing faults has not been well understood, and practical fault-tolerant mechanisms have not been developed either. Trip advisory providers, transportation agencies, and the public are in general concerned with the security of IoV. To address such concern, my proposed research develops theoretical foundations and practical insights for building secure-by-design network systems including IoV. The modeling and analysis approach for strategic sensing attacks can be extended to other real-world applications in smart city such as ride-sharing, public transit, smart supply chain and smart grid. The research outcomes will support the deployment and operations of network systems in the following aspects: identification of vulnerable components, allocation of security resources, and mitigation of security failures.

In this project, I will utilize my expertise in game theory, queuing theory, and stochastic dynamic programming to evaluate security risks existed in ubiquitous network systems and design corresponding protection/ detection/ mitigation mechanisms. In particular, I aim to design feedback control strategies that are both cost-efficient and reliable under the impact of random faults and malicious attacks. I will consider a Markovian queuing network model with dynamic routing that applies to a variety of network systems and design defending strategies based on a security game model. Under this setting, the system operator (defender) protects the routing guidance for incoming jobs dynamically based on the system status (queue lengths). The attacker manipulates the routing guidance so that the jobs are wrongly allocated to servers. Attacking and defending both induce technological costs, so the defender has to balance the technological cost and queuing cost. Tools in queuing theory and stochastic process will be applied to study the dynamics and the stability of the queuing system. By formulating infinite-horizon dynamic programming, I can analyze the structure of the optimal defending strategies and compute them numerically. I will also characterize the equilibria of the attacker-defender game and analyze the best responses for both players.

Secure Control for Network Systems: Theory, Algorithms and Applications

Qian Xie
NYU Tandon School of Engineering

1 Introduction

My PhD study develops knowledge and insights on the analysis and design of secure feedback control strategies for network systems. Feedback control strategies rely on connected sensing and actuating components, subject to random malfunctions and malicious attacks. Since vulnerable components are connected via wired/wireless communications but physically distributed, it is hard to predict when a component will be attacked, and which component will be attacked. It can be seen that it is not economically infeasible and technically unnecessary to completely prevent security failures. Yet, it is crucial to understand the risk level under various scenarios and to design proactive and reactive mechanisms for the system. My research will consider the efficient allocation of security resources such as redundant communication channels and diagnosis capabilities, as well as real-time decision-making strategies such as secure dynamic routing. To achieve this goal, I consider a novel Markovian queuing network model with random/strategic disruptions, which is applicable to a variety of network systems and design defending strategies based on a security game model. The theoretical basis of this work includes queuing theory, game theory, and stochastic optimization. I will use our expertise in such areas to characterize the theoretical properties of secure routing strategies and develop algorithms to compute such strategies. The expected results will also provide a solid foundation for applications on the internet of vehicles, smart supply chains, and communication networks.

2 Motivation

The operation of network systems relies heavily on data collection and transmission, which is vulnerable to remote and/or on-site attacks that bring security risk. For example, in the internet of vehicles, researchers have found that traffic sensors and traffic lights can be easily intruded and manipulated [Ghena et al. 2014, Chen et al. 2019]; communication between connected vehicles are also vulnerable to various forms of attacks [Sakiz and Sevil 2017, Al-Kahtani 2012]. Similar security risk also exists in production lines [Lee 2008] and communication networks [Deng et al. 2002]. However, such security risk has not been well studied in conjunction with the dynamics of network systems, which is typically modeled as queuing processes. Moreover, appropriate proactive and/or responsive mechanisms should be designed so that network systems can tolerate a certain level of attacks.

3 Related Work

Dynamic routing refers to a class of optimal control strategy to route jobs (such as vehicles, products, data packets, etc.). It has been studied for a variety of network systems, including transportation [Daganzo 1998, Osorio and Bierlaire 2009], production lines [Yao and Pei 1990, Govil and Fu 1999], and communications [Tamir and Frazier 1992, Orda et al. 1993]. The idea of most routing policies is that a job is allocated to a server with a shorter queue when it arrives. In particular, the shortest-queue policy has been proved to be optimal if the system operator has a perfect observation of the system states and perfect implementation of the policy [Ephremides et

al. 1980]. Numerous results have been developed for the queuing system with perfect sensing plus perfect actuating [Foley and McDonald 2001, Eschenfeldt and Gamarnik 2018]. Although some of these results provide hints for our problem, they do not directly apply to the security setting with imperfect sensing and/or actuating.

Game theory is a powerful tool for security risk analysis that has been extensively used in various engineering systems [Manshaei et al. 2013, Etesami and Başar 2019], and game-theoretic approaches have been applied to studying the security of routing in transportation [Laszka et al. 2019] and communications [Bohacek et al. 2002, Guo et al. 2016]. This project will be the basis for a synthesis of game theory and queuing theory, which is essential for capturing the interaction between the players' decisions and queuing dynamics.

4 Research Objectives

This project aims to evaluate the security risk of network systems and design resilient control algorithms against random faults or strategic attacks. The specific questions to be addressed include:

- How to quantify the attacker's incentive and the impact of attacks?
- How to allocate limited resources for recovering compromised sensing components?
- How to design algorithms that fully or partially protect feedback control capabilities from various types of sensing faults/attacks?
- How can our method be applied to specific scenarios?

I will study the evolution of network flows under the influence of sensing attacks based on the stochastic stability theory of Markov chains and queuing theory. The equilibrium strategies of the attackers and the system operator will also be characterized. I will particularly focus on quantifying the incentive of launching attacks and designing secure-by-design mechanisms. Furthermore, I can synthesize the idea of learning-based methods with the results from this research to design secure control strategies that are adaptive to the non-stationarities in system dynamics; learning-based methods are also relevant in security games with incomplete information.

5 Research Plan

I will first consider a network of parallel servers with homogeneous service rates and extend to a more general network with heterogeneous service rates later. As shown in Fig. 1, arriving jobs follow the routing instruction to join the queues. The routing instruction is generated based on the real-time traffic state of all servers. If sensing and actuating are normal, the routing instruction will guide the incoming jobs to the shortest queue. However, a malicious attacker is able to compromise the state observation and the transmission of routing instruction and thus cause inefficiency (e.g., jobs allocated to the longest queue). The system operator (SO) can deploy additional resources to protect the state observation and instruction transmission, but the resources may be limited or costly. The SO can also select the routing policy in anticipation of malicious attacks. The interaction between the malicious attacker and the SO is modeled as a security game. I will formulate a security game to capture the interaction between the attacker and the defender, viz. the SO.

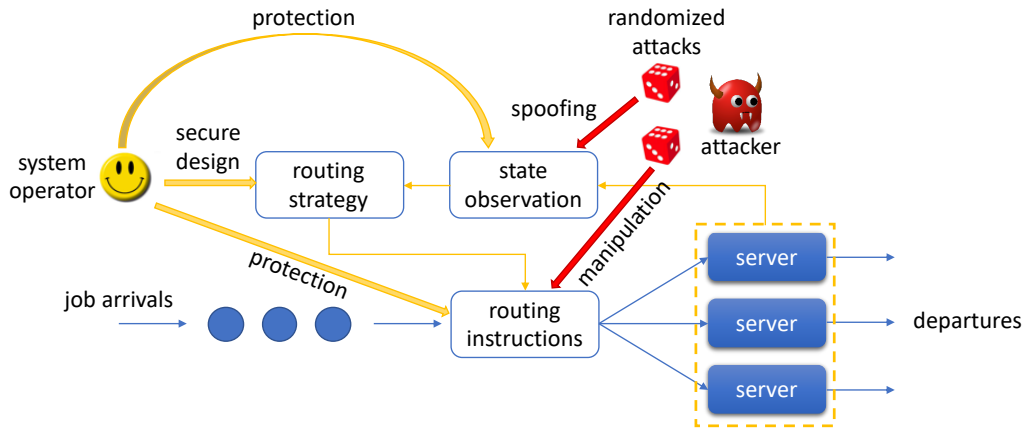

Fig. 1: Security game over a network of parallel queuing servers.

I will address the following questions in our research.

How to model security vulnerabilities?

Three types of malicious attacks can be considered: Denial-of-Service (DoS), data spoofing, and instruction manipulation. More specifically, DoS can cut off observations, then the system is overwhelmed by large amounts of data and cannot handle more; thus the observations would be lost until they are recovered. Data spoofing refers to the injection of malicious data into the state observation, causing the SO to make wrong decisions. Instruction manipulation refers to the interception and modification of the routing instruction sent to individual jobs. The difference among them will be reflected in the attacking probability; it should be state-independent (constant) for DoS and state-dependent (based on queuing states) for spoofing. They all induce technological costs that include human labor and investments in software/hardware on the attacker. Importantly, I assume that the attacking time is randomized. It is practically relevant since deterministic attacking times will allow the SO to get optimally prepared. The attacker's objective is to balance the queuing cost and the attacking cost.

The defender also faces a similar tradeoff when securing the routing. The defense can take the form of redundant components, diagnosis mechanisms, human inspectors, etc. Like the attack, it also induces technological cost. The routing is compromised or failed if and only if it is attacked and not defended.

As opposed to conventional queuing models where the state transition rates only depend on arrival and service rates, our model's transition rates result from the interaction between the attacker and the defender. Essentially, the players' actions will be selecting the transition rates in the Markov chain underlying the queuing process.

The security game is formulated as an infinite-horizon dynamic game, which can be summarized in the following form:

attacker's decision: attacking and manipulating strategy
attacker's objective: max expected cumulative discounted (queuing cost - attacking cost)
defender's decision: defending and routing strategy
defender's objective: min expected cumulative discounted (queuing cost + defending cost)
constraint: queuing dynamics

How to evaluate the security risk?

The security risk of the queuing system can be quantified based on the queuing delay and throughput loss. To this end, I need to study the long-term properties of the queuing system, including stability and equilibrium.

For classical queuing processes (e.g., M/M/1), stability analysis is straightforward: the queue is stable if and only if the arrival rate is strictly less than the total service rate. However, for feedback-controlled queuing processes, the analysis can be involved [Foley and McDonald 1992]. Furthermore, in the case of state-dependent attacking and defending strategies, it is even impossible to obtain analytical sufficient and necessary condition for stability. To meet this challenge, I will use Lyapunov function-based approach for deriving stability criteria.

I will also characterize the best response of both players and the equilibria structure of the security game. Then one way to define the security risk is as follows:

security risk = SO's utility under equilibrium – queuing cost without attacks.

How to design a secure queuing system?

Note that some queuing states are "riskier" than the others in the sense that being attacked in those states is more costly. For example, if the queues are severely unbalanced, then a wrongly routed job will make the imbalance more severe; if all servers are idling, then an attack leads to no benefit for the attacker. Although such arguments are intuitive, quantification is not easy, and obtaining an analytical solution is very hard. Hence, I will use stochastic dynamic programming as tools to compute optimal strategies and equilibrium strategies analytically. Since the state space can be countable infinite, I may also need learning-based methods. Stability criteria can also be used to refine the search space.

6 Expected Outcomes

The main products of this project will be (i) models and methods for systematical risk evaluation of network systems with dynamic routing and (ii) practical network control algorithms that ensure system resilience in the face of bogus information. They will be the basis for allocating recovery resources and designing reliable failure-tolerant routing algorithms. The expected results will support the design of resilient transportation and logistics systems. Specific applications include app-based routing, signal-free intersection control, and packet routing.

Take app-based routing as an example; it is reported that an artist used 99 phones to fake a traffic jam on Google Maps [Holmes 2020]. I can expect that in the near future, hackers may spoof traffic sensor data or create phantom traffic jams in navigation apps for selfish or malicious intent (e.g., leading other vehicles to take a different road). Meanwhile, trip advisory providers, transportation agencies, and the public are in general concerned with the security of intelligent transportation system that heavily relies on data, and our research outcomes are directly relevant for this concern. The implementation of our products will enable transportation system operators to identify vulnerable components, efficiently allocate security resources, and mitigate security failures.

References

Al-Kahtani, M. S. (2012, December). Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In *2012 6th International Conference on Signal Processing and Communication Systems* (pp. 1-9). IEEE.

Bohacek, S., Hespanha, J.P., Obraczka, K., Lee, J. & Lim, C. (2002, October). Enhancing security via stochastic routing. In *Proceedings. Eleventh International Conference on Computer Communications and Networks* (pp. 58-62). IEEE.

Chen, Q.A., Yin, Y., Feng, Y., Mao, Z.M. and Liu, H.X. (2018, February). Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control. In *NDSS*.

Daganzo, C.F. (1998). Queue spillovers in transportation networks with a route choice. *Transportation Science*, *32*(1), pp.3-11.

Deng, H., Li, W. & Agrawal, D.P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications magazine*, *40*(10), pp.70-75.

Foley, R.D. & McDonald, D.R. (2001). Join the shortest queue: stability and exact asymptotics. *The Annals of Applied Probability*, *11*(3), pp.569-607.

Ephremides, A., Varaiya, P. & Walrand, J. (1980). A simple dynamic routing problem. *IEEE transactions on Automatic Control*, *25*(4), pp.690-693.

Eschenfeldt, P. & Gamarnik, D. (2018). Join the shortest queue with many servers. The heavy-traffic asymptotics. *Mathematics of Operations Research*, *43*(3), pp.867-886.

Etesami, S.R. & Başar, T. (2019). Dynamic Games in Cyber-Physical Security: An Overview. *Dynamic Games and Applications*, pp.1-30.

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J. & Halderman, J.A. (2014). Green lights forever: Analyzing the security of traffic infrastructure. In *8th {USENIX} Workshop on Offensive Technologies ({WOOT} 14)*.

Govil, M.K. & Fu, M.C. (1999). Queueing theory in manufacturing: A survey. *Journal of manufacturing systems*, *18*(3), pp.214-240.

Guo, H., Wang, X., Cheng, H. & Huang, M. (2016). A routing defense mechanism using evolutionary game theory for Delay Tolerant Networks. *Applied Soft Computing*, *38*, pp.469-476.

Holmes, A. (2020, February). An artist wheeled 99 smartphones around in a wagon to create fake traffic jams on Google Maps. *Business Insider*. Retrieved from https://www.businessinsider.com/.

Laszka, A., Abbas, W., Vorobeychik, Y. & Koutsoukos, X. (2019). Detection and mitigation of attacks on transportation networks as a multi-stage security game. *Computers & Security*, *87*, p.101576.

Lee, E.A. (2008, May). Cyber physical systems: Design challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)* (pp. 363-369). IEEE.

Manshaei, M.H., Zhu, Q., Alpcan, T., Bacşar, T. & Hubaux, J.P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, *45*(3), p.25.

Meyn, S.P. & Tweedie, R.L. (1993). Stability of Markovian processes III: Foster–Lyapunov criteria for continuous-time processes. *Advances in Applied Probability*, *25*(3), pp.518-548.

Orda, A., Rom, R. & Shimkin, N. (1993, March). Competitive routing in multi-user communication networks. In *IEEE INFOCOM'93 The Conference on Computer Communications, Proceedings* (pp. 964-971). IEEE.

Osorio, C. & Bierlaire, M. (2009). An analytic finite capacity queueing network model capturing the propagation of congestion and blocking. *European Journal of Operational Research*, *196*(3), pp.996-1007.

Sakiz, F. & Sevil S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Networks* 61, 33-50.

Tamir, Y. & Frazier, G.L. (1992). Dynamically-allocated multi-queue buffers for VLSI communication switches. *IEEE Transactions on Computers*, *41*(6), pp.725-737.

Xie, Q., & Jin, L. (2020, July). Resilience of Dynamic Routing in the Face of Recurrent and Random Sensing Faults. In *2020 American Control Conference (ACC)* (pp. 1173-1178). IEEE.

Xie, Q., & Jin, L. Stabilizing Queuing Networks with Model Data-Independent Control. Submitted to *IEEE Transactions on Automatic Control*.

Xu, S. J., Xie, Q., Chow, J. Y., & Liu, X. (2019). Empirical validation of network learning with taxi GPS data from Wuhan, China. Accepted by *IEEE Intelligent Transportation Systems Magazine*.

Yao, D.D. & Pei, F.F. (1990). Flexible parts routing in manufacturing systems. *IIE transactions*, *22*(1), pp.48-55.