A games-in-games approach to mosaic command and control design of dynamic network-of-networks for secure and resilient multi-domain operations

Chen, Juntao, Zhu, Quanyan

Juntao Chen, Quanyan Zhu, "A games-in-games approach to mosaic command and control design of dynamic network-of-networks for secure and resilient multi-domain operations," Proc. SPIE 11017, Sensors and Systems for Space Applications XII, 110170P (29 July 2019); doi: 10.1117/12.2526677

SPIE.

Event: SPIE Defense + Commercial Sensing, 2019, Baltimore, Maryland, United States

A Games-in-Games Approach to Mosaic Command and Control Design of Dynamic Network-of-Networks for Secure and Resilient Multi-Domain Operations

Juntao Chen[a] and Quanyan Zhu[a]

[a] New York University, 2 MetroTech Center, Brooklyn, NY, USA

ABSTRACT

This paper presents a games-in-games approach to provide design guidelines for mosaic command and control that enables the secure and resilient multi-domain operations. Under the mosaic design, pieces or agents in the network are equipped with flexible interoperability and the capability of self-adaptability, self-healing, and resiliency so that they can reconfigure their responses to achieve the global mission in spite of failures of nodes and links in the adversarial environment. The proposed games-in-games approach provides a system-of-systems science for mosaic distributed design of large-scale systems. Specifically, the framework integrates three layers of design for each agent including strategic layer, tactical layer, and mission layer. Each layer in the established model corresponds to a game of a different scale that enables the integration of threat models and achieve self-mitigation and resilience capabilities. The solution concept of the developed multi-layer multi-scale mosaic design is characterized by Gestalt Nash equilibrium (GNE) which considers the interactions between agents across different layers. The developed approach is applicable to modern battlefield networks which are composed of heterogeneous assets that access highly diverse and dynamic information sources over multiple domains. By leveraging mosaic design principles, we can achieve the desired operational goals of deployed networks in a case study and ensure connectivity among entities for the exchange of information to accomplish the mission.

Keywords: Multi-Domain Operation, Dynamic Games, Games-in-Games, System of Systems, Network Systems, Mosaic Design, Security and Resilience

1. INTRODUCTION

Security and resilience of networked systems become increasingly critical nowadays due to the prevailing adversarial threats from both cyber and physical domains.[1] A number of approaches have been proposed in literature to enhance the system performance under adversarial environment through strategic trust,[2–5] resilient control,[6–11] moving target defense,[12–15] proactive deception,[16–21] and contracts and insurances.[22–25] With the adoption of Internet of things (IoT) devices and information and communications technologies (ICTs), different systems are integrated together, creating network-of-networks (NoN).[26–28] On one hand, NoN improves the system dependability and interoperablity.[29] On the other hand, the network interdependency introduces new challenges for the system operator to maintain the NoN performance as the interconnection provides extra opportunity for the propagation of attacks from one network to another, e.g., through lateral movement in advanced persistent threat (APT).[30] Traditional defensive strategies for networked systems are no longer sufficient in this emerging NoN framework. Therefore, our goal in this paper is to propose an efficient and flexible way to achieve mission objectives while ensuring the security and resilience of NoN through a new paradigm called *mosaic design*. The associated concept of mosaic warfare has been recently proposed by DARPA.[31]

Mosaic distributed system design refers to engineering agents with flexible interoperability and the capability of *self-adaptability*, *self-healing*, and *resiliency*. Specifically, systems can achieve its objective when one node goes away or fails.[32,33] Furthermore, systems can respond to other systems in a non-deterministic/stochastic way and increases the composability and modularity of the system design. For example, agents can randomly

Further author information: (Send correspondence to Quanyan Zhu)
Juntao Chen: E-mail: jc6412@nyu.edu; Quanyan Zhu: E-mail: qz494@nyu.edu, Telephone: 1-646-997-3371

Sensors and Systems for Space Applications XII, edited by Genshe Chen, Khanh D. Pham, Proc. of SPIE
Vol. 11017, 110170P · © 2019 SPIE · CCC code: 0277-786X/19/$18 · doi: 10.1117/12.2526677

arrive and respond in a stochastic but structured way to other agents in an uncertain environment. However, the structured randomness leads to emerging system behaviors that manifest desirable properties for the objective of entire mission. Systems that have such properties are easily composable and resilient-by-design. Without a pre-planned integration among agents, the agents can adapt their response and reconfigure their own systems based on the type of agents that they interact with. For example, in the decision-making of battlefield scenario, the unmanned ground vehicle (UGV) network should intelligently coordinate its actions with the heterogeneous unmanned aerial vehicle (UAV) network and the soldier network in a self-adaptive manner. Thus, in the paradigm of mosaic design, agents can be easily composed to achieve a prescribed objective through an unprescribed path. In addition, under the adversarial environments, the agents can reconfigure their response and roles to achieve the global mission in spite of failures of nodes and communication links. Returning to the battlefield example, a single removal of UGV or UAV should not interrupt the action of other agents, and the whole system should still be operable when one piece is missing to achieve the global mission. These features of agile self-recovery ability and autonomous composability are the epicenter of the mosaic designs.

Mosaic design is a migration from a pre-defined protocol for distributed systems that aim to achieve a single objective. Classical design has a prescribed objective and then uses a top-down design methods to decentralize the operations. For example, the operator of the entire battlefield first designs optimal strategies for the agents globally and then inform each agent how to act based on their local information. However, when one agent leaves the battlefield which modifies the system, the previous designed strategy is not globally optimal anymore. Therefore, the loss of one piece will loose the entire effect in the classical top-down design. Mosaic design is also different from the classical deterministic bottom-up approach in which agents are programmed to behave in a designed way offline which losses the adaptivity.

In this work, we develop a games-in-games approach to provide a system-of-systems science for mosaic distributed design of large-scale systems. Different from previous works in designing resilient operational strategy for interdependent networks based a single game,[34–37] the games-in-games approach allows an automated composition of systems to achieve flexible interoperability.[33,38] Agents can adapt to their neighboring ones and integrate themselves into the environment. The game-theoretic approach also enables the integration of threat models and achieve self-mitigation/resilience capabilities.

Related Work: Game-theoretic approaches have been extensively adopted for resilient control of networked system and critical infrastructures.[1,7,34,37,39] To analyze strategic interactions between attackers and defenders, a large number of works have focused on the security modeling and design through game-theoretic frameworks.[23,30,35,36,38,40] Furthermore, researchers have also used game-theoretic methods to enable decentralized multi-layer network/network-of-networks design.[29,32,41,42] Due to the integration between heterogeneous system components, interdependent security and trust mechanisms become critical and they have been addressed through game-theoretic methods from a system-of-systems perspective.[2,3,22,24] When the number of agents in the network grows, secure and resilient control needs to incorporate the feature of large-scale complex systems, e.g., multi-layer IoT networks and epidemic networks.[43–46]

2. GAMES-IN-GAMES APPROACH FOR MOSAIC DESIGN

In this section, we develop a games-in-games framework which enables multi-layer and multi-scale decision-making over network systems. Then, we design the mosaic control based on this games-in-games framework.

2.1 Games-in-Games Framework

The games-in-games principle is a framework that provides a theoretical underpinning and a guideline for mosaic control designs. Specifically, the proposed games-in-games approach integrates three layers of design for each agent: strategic layer, tactical layer, and mission layer. At the strategic layer, the agents learn and respond to their environment quickly to unanticipated events such as attacks, disruptions, and changes of other agents. At the tactical layer, the agents plan for a longer period of time by taking into account the long-term interactions with the environment and other agents. The agents can make a goal-oriented planning at each stage. At the mission layer, the agents develop a stage-by-stage planning of multi-stage objectives to achieve the mission despite the uncertainties and online changes.

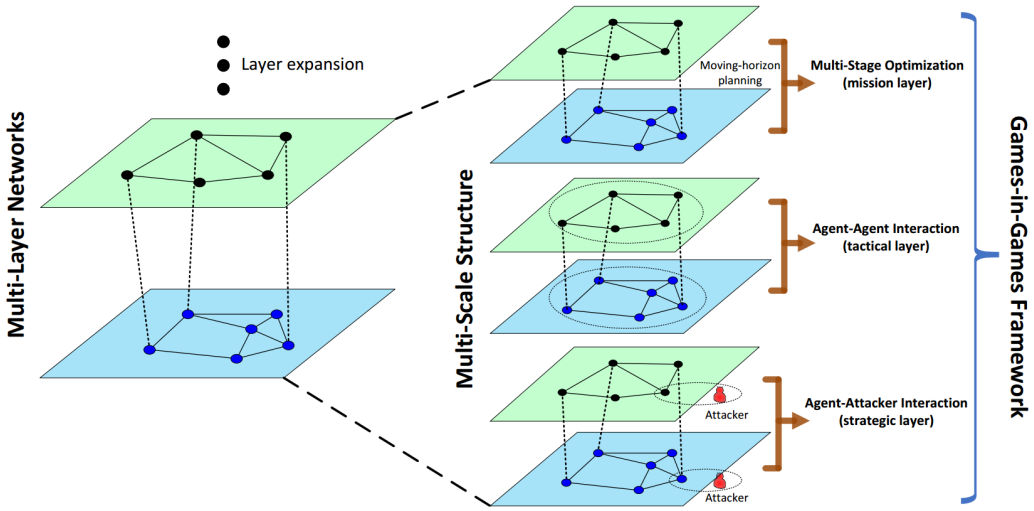


Figure 1. Games-in-Games framework for mosaic command and control design of secure and resilient networks-of-networks. The games-in-games framework contains three layers: strategic layer for attack and disruption consideration of each agent; tactical layer for interaction consideration between agents within and across different layers at each stage; and mission layer for moving-horizon planning to achieve multi-stage objective. Games at different layers can be composed together, leading to a flexible mosaic control design.

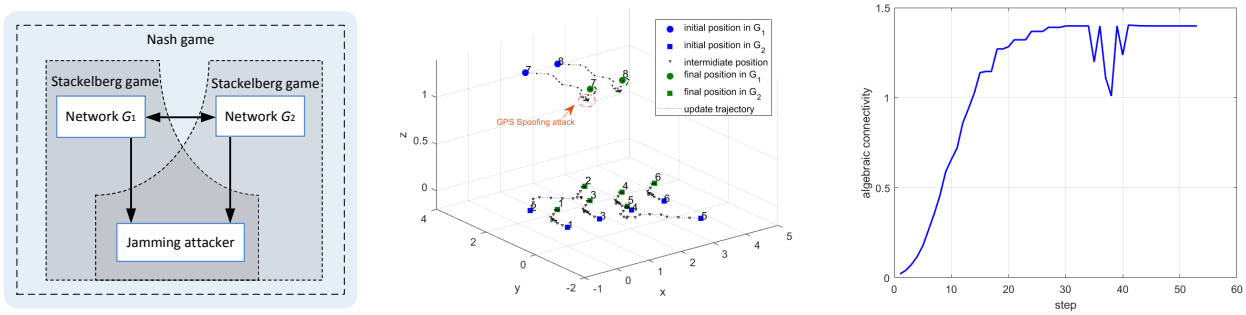
Each layer in the established model corresponds to a game of a different scale. 1): At the strategic layer, a game associated with an agent describes its interaction with an adversary, e.g. a jammer, a spoofer, or a sudden loss of neighboring node. Solutions to this game can prepare nodes for unanticipated attacks and secure the agents. 2): At the tactical layer, an N-person dynamic game describes the longer-term interactions among cooperative agents, each seeking control policies to achieve individual stage objectives. The individual control would lead to achieving global objectives such as connectivity and network formation. 3): At the mission layer, each agent plans at each stage their stage objectives at the tactical layer. This planning is obviously under a lot of uncertainties and need to be achieved in a moving-horizon way.

In sum, games-in-games framework describes a multi-layer and multi-scale game-theoretic framework. Furthermore, the games at each layer can be composed together. For example, an N-person game can be composed with an M-person game to create an $N+M$-person game. Such composition leads to a resolution of the games at each layer. The games across the layers can also be composed together. For example, an N-person tactical layer game is nested in an N-person mission-layer game. In addition, the security game at the strategic layer can be nested in the tactical layer games. For clarity, the games-in-games framework is illustrated in Fig. 1.

2.2 Mosaic Command and Control Design

The developed games-in-games framework can be adopted to address the mosaic control design as the composability of the framework provides agility required by the mosaic control objective. This framework is inherently secure and resilient by design. First, the games-in-games framework anticipates the attack behavior and designs a control policy that would prepare to defend against the anticipated attacks. The framework provides a clean-slate design and provides a built-in security for each system component that would lead to security of the integrated system. Second, the games-in-games framework enables each system to respond to the unanticipated events at each time instant. Each agent can respond to events that inflict damages on the agent and go through a self-healing process that can recover itself from the attacks and failures if possible. If the full recovery is not achievable, the agents will develop control strategies that will allow a graceful performance degradation. Therefore, the multi-layer mosaic control enables the agents to achieve mission despite of failures, uncertainties, and unstructured behaviors. Note that the mosaic control is a fully integrated design which differentiates itself from current existing designs in which only partial aspects are considered, e.g., security, but not all key issues.

The solution concept of the developed multi-layer and multi-scale mosaic design is characterized by Gestalt Nash equilibrium (GNE).[40,47] Nash equilibrium provides a solution concept to a well defined static or dynamic



(a) (b) (c)

Figure 2. (a) depicts a games-in-games framework for two-layer autonomous systems. (b) shows the iterative configuration of a two-layer autonomous network under mosaic control. (c) shows the corresponding network connectivity. The spoofing attack launches at step 35 and lasts for 6 steps. The network recovers and reaches a GNE quickly afterward.

game in strategic or extensive forms. We extend this solution concept to GNE for games-in-games framework where multiple games can be composed to capture heterogeneous interactions among different types of players. The GNE solution concept follows the definition of NE and describes an equilibrium concept in which no agent has incentives to deviate away from not only the local game, which captures the local agent-agent level interactions, but also the composed game, which captures the global system-system level interactions. The development of GNE provides a solution concept for multi-scale interactions, provides a way to assess system-level performance, and enables the design of mosaic control systems.

Mosaic control design is suitable for multi-domain operations (MDO).[48,49] MDO refers to a cross-domain integration of information and assets across air, space, sea, land, and cyber domains to provide a holistic situational awareness and decision-making. We can leverage mosaic control design to provide a framework to develop a modular, functional, and composable design of command and control systems that can autonomously achieve the mission objectives.

2.3 Examples and Results

In this subsection, we study a case study of a multi-layer network of autonomous systems,[32] in which UAVs and UGVs act collaboratively, intelligently, and adaptively to achieve a high connectivity. Furthermore, the designed decentralized MDO command and control algorithms enable a synchronized response for each layer to respond to others to maintain real-time connectivity despite the adversarial environment. Here, we present numerical results of a two-layer mobile autonomous systems using mosaic design principles. Maintaining connectivity between different agents is critical which improves the network situational awareness.[41,42] In the case studies, the objective of two network operators is to optimize the global network algebraic connectivity by anticipating the existence of adversary.[32] As shown in Fig. 2, the network is robust to jamming attack and maintains connectivity with the presence of a jammer at every step which demonstrates the security of the mosaic control algorithm. In addition, the nodes can respond quickly to the spoofing attack and achieve agile resilience through the proposed control design. Interested readers can find more results and discussions of case studies in external references.[33,50]

REFERENCES

[1] Chen, J., Touati, C., and Zhu, Q., "A Dynamic Game Analysis and Design of Infrastructure Network Protection and Recovery," *ACM SIGMETRICS Performance Evaluation Review* **45**, 125–128 (Oct. 2017).

[2] Pawlick, J. and Zhu, Q., "Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control," *IEEE Transactions on Information Forensics and Security* **12**(12), 2906–2919 (2017).

[3] Pawlick, J., Chen, J., and Zhu, Q., "iSTRICT: An interdependent strategic trust mechanism for the cloud-enabled internet of controlled things," *IEEE Transactions on Information Forensics and Security* **14**(6), 1654–1669 (2019).

[4] Zhu, Q., Fung, C., Boutaba, R., and Başar, T., "Guidex: A game-theoretic incentive-based mechanism for intrusion detection networks," *Selected Areas in Communications, IEEE Journal on* **30**(11), 2220–2230 (2012).

[5] Fung, C. J. and Zhu, Q., "Facid: A trust-based collaborative decision framework for intrusion detection networks," *Ad Hoc Networks* **53**, 17–31 (2016).

[6] Chen, J., Zhou, L., and Zhu, Q., "Resilient control design for wind turbines using markov jump linear system model with lévy noise," in [*IEEE International Conference on Smart Grid Communications (SmartGridComm)*], 828–833 (2015).

[7] Chen, J. and Zhu, Q., "Interdependent strategic cyber defense and robust switching control design for wind energy systems," in [*IEEE Power & Energy Society General Meeting*], 1–5 (2017).

[8] Xu, Z. and Zhu, Q., "A Game-Theoretic Approach to Secure Control of Communication-Based Train Control Systems Under Jamming Attacks," in [*Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles*], 27–34, ACM (2017).

[9] Xu, Z. and Zhu, Q., "Secure and practical output feedback control for cloud-enabled cyber-physical systems," in [*Communications and Network Security (CNS), 2017 IEEE Conference on*], 416–420, IEEE (2017).

[10] Xu, Z. and Zhu, Q., "A cyber-physical game framework for secure and resilient multi-agent autonomous systems," in [*Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*], 5156–5161, IEEE (2015).

[11] Xu, Z. and Zhu, Q., "Secure and resilient control design for cloud enabled networked control systems," in [*Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*], 31–42, ACM (2015).

[12] Jajodia, S., Ghosh, A. K., Swarup, V., Wang, C., and Wang, X. S., [*Moving target defense: creating asymmetric uncertainty for cyber threats*], vol. 54, Springer Science & Business Media (2011).

[13] Zhu, Q. and Başar, T., "Game-theoretic approach to feedback-driven multi-stage moving target defense," in [*International Conference on Decision and Game Theory for Security*], 246–263, Springer (2013).

[14] Maleki, H., Valizadeh, S., Koch, W., Bestavros, A., and van Dijk, M., "Markov modeling of moving target defense games," in [*Proceedings of the 2016 ACM Workshop on Moving Target Defense*], 81–92, ACM (2016).

[15] Jafarian, J. H., Al-Shaer, E., and Duan, Q., "Openflow random host mutation: transparent moving target defense using software defined networking," in [*Proceedings of the first workshop on Hot topics in software defined networks*], 127–132, ACM (2012).

[16] Al-Shaer, E. S., Wei, J., Hamlen, K. W., and Wang, C., [*Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings*], Springer (2019).

[17] Jajodia, S., Subrahmanian, V., Swarup, V., and Wang, C., [*Cyber deception*], Springer (2016).

[18] Huang, L. and Zhu, Q., "Dynamic bayesian games for adversarial and defensive cyber deception," in [*Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings*], Al-Shaer, E., Wei, J., Hamlen, K. W., and Wang, C., eds., 75–97, Springer International Publishing, Cham (2019).

[19] Pawlick, J., Colbert, E., and Zhu, Q., "Modeling and analysis of leaky deception using signaling games with evidence," *IEEE Transactions on Information Forensics and Security* (2018).

[20] Pawlick, J., *A Systems Science Perspective on Deception for Cybersecurity in the Internet of Things*, PhD thesis (2018). Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2018-08-09.

[21] Pawlick, J., Colbert, E., and Zhu, Q., "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *arXiv preprint arXiv:1712.05441* (2017).

[22] Chen, J. and Zhu, Q., "Optimal contract design under asymmetric information for cloud-enabled internet of controlled things," in [*International Conference on Decision and Game Theory for Security*], 329–348, Springer (2016).

[23] Zhang, R., Zhu, Q., and Hayel, Y., "A bi-level game approach to attack-aware cyber insurance of computer networks," *IEEE Journal on Selected Areas in Communications* **35**(3), 779–794 (2017).

[24] Chen, J. and Zhu, Q., "Security as a service for cloud-enabled internet of controlled things under advanced persistent threats: a contract design approach," *IEEE Transactions on Information Forensics and Security* **12**(11), 2736–2750 (2017).

[25] Chen, J. and Zhu, Q., "A linear quadratic differential game approach to dynamic contract design for systemic cyber risk management under asymmetric information," in [*2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*], 575–582, IEEE (2018).

[26] Kurian, V., Chen, J., and Zhu, Q., "Electric power dependent dynamic tariffs for water distribution systems," in [*Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks*], 35–38, ACM (2017).

[27] Zimmerman, R., Zhu, Q., de Leon, F., and Guo, Z., "Conceptual modeling framework to integrate resilient and interdependent infrastructure in extreme weather," *Journal of Infrastructure Systems* **23**(4), 04017034 (2017).

[28] Zimmerman, R., Zhu, Q., and Dimitri, C., "A network framework for dynamic models of urban food, energy and water systems (fews)," *Environmental Progress & Sustainable Energy* **37**(1), 122–131 (2018).

[29] Chen, J. and Zhu, Q., "Interdependent network formation games with an application to critical infrastructures," in [*American Control Conference (ACC)*], 2870–2875, IEEE (2016).

[30] Huang, L. and Zhu, Q., "Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks," *ACM SIGMETRICS Performance Evaluation Review* **46**(2), 52–56 (2019).

[31] DARPA, "Darpa tiles together a vision of mosaic warfare: Banking on cost-effective complexity to overwhelm adversaries."

[32] Chen, J. and Zhu, Q., "Resilient and decentralized control of multi-level cooperative mobile networks to maintain connectivity under adversarial environment," in [*Conference on Decision and Control (CDC)*], 5183–5188, IEEE (2016).

[33] Chen, J. and Zhu, Q., "Control of multi-layer mobile autonomous systems in adversarial environments: A games-in-games approach," *IEEE Transactions on Control of Network Systems, submitted* (2019).

[34] Huang, L., Chen, J., and Zhu, Q., "A factored MDP approach to optimal mechanism design for resilient large-scale interdependent critical infrastructures," in [*Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), CPS Week*], 1–6 (2017).

[35] Huang, L., Chen, J., and Zhu, Q., "A large-scale markov game approach to dynamic protection of interdependent infrastructure networks," in [*International Conference on Decision and Game Theory for Security*], 357–376, Springer (2017).

[36] Huang, L., Chen, J., and Zhu, Q., "Factored markov game theory for secure interdependent infrastructure networks," in [*Game Theory for Security and Risk Management*], 99–126, Springer (2018).

[37] Huang, L., Chen, J., and Zhu, Q., "Distributed and optimal resilient planning of large-scale interdependent critical infrastructures," in [*Winter Simulation Conference (WSC)*], 1096–1107 (2018).

[38] Zhu, Q. and Basar, T., "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine* **35**(1), 46–65 (2015).

[39] Chen, J. and Zhu, Q., "A game-theoretic framework for resilient and distributed generation control of renewable energies in microgrids," *IEEE Transactions on Smart Grid* **8**(1), 285–295 (2016).

[40] Chen, J. and Zhu, Q., "Security investment under cognitive constraints: A gestalt Nash equilibrium approach," in [*52nd Annual Conference on Information Sciences and Systems (CISS)*], 1–6 (2018).

[41] Chen, J., Touati, C., and Zhu, Q., "Heterogeneous multi-layer adversarial network design for the IoT-enabled infrastructures," in [*IEEE Global Communications Conference*], 1–6 (2017).

[42] Chen, J., Touati, C., and Zhu, Q., "Optimal secure two-layer IoT network design," *IEEE Transactions on Control of Network Systems* (2019).

[43] Chen, J., Zhang, R., and Zhu, Q., "Optimal quarantining strategy for interdependent epidemics spreading over complex networks," *IEEE Transactions on Signal and Information Processing over Networks, submitted* (2019).

[44] Farooq, M. J. and Zhu, Q., "On the secure and reconfigurable multi-layer network design for critical information dissemination in the internet of battlefield things (IoBT)," *IEEE Transactions on Wireless Communications* **17**(4), 2618–2632 (2018).

[45] Farooq, M. J. and Zhu, Q., "A multi-layer feedback system approach to resilient connectivity of remotely deployed mobile Internet of things," *IEEE Transactions on Cognitive Communications and Networking* **4**(2), 422–432 (2018).
[46] Hayel, Y. and Zhu, Q., "Epidemic protection over heterogeneous networks using evolutionary poisson games," *IEEE Transactions on Information Forensics and Security* **12**(8), 1786–1800 (2017).
[47] Chen, J. and Zhu, Q., "Interdependent strategic security risk management with bounded rationality in the internet of things," *IEEE Transactions on Information Forensics and Security* (2019).
[48] Perkins, D. G., "Multi-domain battle: driving change to win in the future," *Military Review* **97**(4), 6 (2017).
[49] Perkins, D. G., "Multi-domain battle: The advent of twenty-first century war," *Military Review* **97**(6), 8 (2017).
[50] Chen, J. and Zhu, Q., [*A Game- and Decision-Theoretic Approach to Resilient Interdependent Network Analysis and Design*], Springer (2020).