REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
23-07-2023	Final Report	16-Jul-2022 - 15-Jan-2024

4. TITLE AND SUBTITLE
Final Report: 2022 ARO Workshop on Network Security

5a. CONTRACT NUMBER
W911NF-22-1-0168

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES

Temple University
3340 N. Broad Street
Student Faculty Center Suite 427
Philadelphia, PA 19140 -5102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
80200-NC-CF.1

12. DISTRIBUTION AVAILIBILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jie Wu
UU	UU	UU	UU		19b. TELEPHONE NUMBER 215-204-8888

RPPR Final Report
as of 24-Jul-2023

Agency Code: 21XD

Proposal Number: 80200NCCF **Agreement Number: W911NF-22-1-0168**
INVESTIGATOR(S):

Name: PHD Jie Wu
Email: jiewu@temple.edu
Phone Number: 2152048888
Principal: Y

Organization: **Temple University**
Address: 3340 N. Broad Street, Philadelphia, PA 191405102
Country: USA

DUNS Number: 057123192 EIN: 231365971
Report Date: 20-Aug-2023 Date Received: 23-Jul-2023
Final Report for Period Beginning 16-Jul-2022 and Ending 15-Jan-2024
Title: 2022 ARO Workshop on Network Security
Begin Performance Period: 16-Jul-2022 **End Performance Period:** 15-Jan-2024
Report Term: 0-Other

Submitted By: PHD Jie Wu Email: jiewu@temple.edu
Phone: (215) 204-8888

Distribution Statement:

STEM Degrees: **STEM Participants:**

Major Goals: Information assurance in network science must provide authentic, accurate, secure, reliable, and timely information to warfighters to achieve information dominance, regardless of threat conditions. Computing and information processes may be carried out over distributed and heterogeneous systems, which include mobile edge, mobile computing and communications systems, and high-performance information process systems that are inter-connected through both tactical and strategic communication systems. The advancement of machine intelligence has led to new opportunities for efficient tactical communication systems but also brought in new vulnerabilities.

This project focused on a network security workshop on various threat models and adversarial behaviors while exemplifying the corresponding countermeasures under the era of artificial intelligence (AI) and machine learning (ML).

Accomplishments: The project focused on the following aspects:

1.5 days of ARO workshop at Philadelphia. The workshop was co-organized by Professors Yingying Chen from Rutgers University and Professor Jie Wu from Temple University under the direction of Dr. Paul Yu, ARO program director. The workshop was held November 17-18, 2022, at Temple University Center City Campus, Philadelphia.

The topics of the workshop were futuristic forward looking on AI/ML-enabled security in spectrum management, mobile networks, and next-generation wireless access under the era of artificial intelligence. Topics include, but not limited to, robust and trusted wireless and mobile networks, models and metrics for next generation robust systems, cyber deception, principle of moving target defense, trusted learning for cyber autonomy, spectrum management, and network forensics.

A comprehensive workshop summary report. This report (see attached summary) was collectively generated by all participants (with a total of 32 participants from academia and government agencies, ARO, ARL, and NSF, see attached summary). It is a summary of presentations and discussions from 4 sessions (2 invited talks and 2 panels) and 4 round-tables.

Training Opportunities: Nothing to Report

RPPR Final Report
as of 24-Jul-2023

Results Dissemination: As a result of this workshop, the workshop organizers and program directors of ARO/NSF decided to compile a book titled “Network Security Empowered by Artificial Intelligence” to be edited by Yingying Chen, Jie Wu, Paul Yu, and Cliff Wang.

Around 16 chapters will be contributed by participants of the workshop and a few experts in the field. Springer has agreed to publish the book. The book is expected to complete before the end of 2023 and to be published at the beginning of 2024.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Jie Wu
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Co PD/PI
Participant: Yingying Chen
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Partners

,

RPPR Final Report

as of 24-Jul-2023

I certify that the information in the report is complete and accurate:
Signature: Jie Wu
Signature Date: 7/23/23 3:33PM

ARO Workshop Summary

Scope

Information assurance in network science must provide authentic, accurate, secure, reliable, and timely information to warfighters in order to achieve information dominance, regardless of threat conditions. Computing and information processes may be carried out over distributed and heterogeneous systems, which include mobile edge, mobile computing and communications systems, and high-performance information process systems that are inter-connected through both tactical and strategic communication systems. The advancement of machine intelligence has led to new opportunities for efficient tactical communication systems but also brought in new vulnerabilities. This network security workshop focuses on various threat models and adversarial behaviors while exemplifying the corresponding countermeasures under the era of artificial intelligence (AI) and machine learning (ML).

This workshop focuses on fundamental scientific study and discussion directed toward advancing the scientific state of the art and increasing basic knowledge and understanding. The technical scope is exclusively extramural basic research, which matches well with the research vision of federal programs.

The topics are futuristic and forward-looking on security in spectrum management, mobile networks, and next-generation wireless access under the era of AI/ML. Topics include robust and trusted wireless and mobile networks, models and metrics for next-generation robust systems, cyber deception, the principle of moving target defense, trusted learning for cyber autonomy, spectrum management, and network forensics.

Workshop Organization

The workshop is organized by co-organizers Jie Wu and Yingying Chen, and local arrangements Yan Wang. Professor Chen is a faculty member from Rutgers University, and Professors Jie Wu and Yan Yang are faculty members from Temple University. There were two local student volunteers from Temple University.

Cognizant ARO TPOC/Program Manager

Dr. Paul Yu, ARO Program Manager for Information Assurance.

Invited Participants

Name	**Affiliation**
Avinash Srinivasan	US Navy Academy
Jiacheng Shang	Montclair State University
Loukas Lazos	The University of Arizona
Marwan Krunz	The University of Arizona
Ness Shroff	Ohio State University
Quanyan Zhu	New York University
Selcuk Uluagac	Florida International University
Angelos Stavrou	Virginia Tech
Zhuo Lu	University of South Florida
Dipankar Raychaudhuri	Rutgers University
David Mohaisen	University of Central Florida
Guevara Noubir	Northeastern University
Kang Shin	The University of Michigan
Kun Sun	George Mason University
Narayan Mandayam	Rutgers University
Rui Zhang	University of Delaware
Shiwen Mao	Auburn University
Wenjing Lou	Virginia Tech
Xiaonan Guo	George Mason University
Ning Zhang	Washington University at St. Louis
Patrick Traynor	University of Florida
Jason Li	Trusted Science and Technology
Tao Li	Indiana and Purdue University at Indianapolis
Cliff Wang	National Science Foundation
Organizers	
Jie Wu	Temple University
Yingying Chen	Rutgers University
Yan Wang	Temple University

ARO/ARL	
Paul Yu	ARO
Venkateswara Dasari	ARO
Ananthram Swami	ARL
Brian Rivera	ARL
Michael Frame	ARL
Michael De Lucia	ARL

Agenda

Thursday, November 17

8:30 – 9:00	Opening remarks by ARO Program Managers, Yingying Chen, Jie Wu			
9:00 – 10:30	**Panel 1: AI/ML Enabled Security in Cyber Physical Systems** Moderator: Yingying Chen, Scribe: Ning Zhang Jason Li, David Mohaisen, Kang Shin, Angelos Stavrou, Patrick Traynor			
10:30 – 10:45	Coffee Break			
10:45 – 12:00	**Session 1 (Invited talks): New Security Problems in Next Generation Networks** (Moderator: Yingying Chen, Scribe: Zhuo Lu) Loukas Lazos, Wenjing Lou, Guevara Noubir			
12:00 – 13:00	Lunch (one hour)			
13:00 – 14:30	**Panel 2: AI/ML Enabled Security in Wireless Networks** Moderator: Jie Wu, Scribe: Rui Zhang Michael De Lucia, Narayan Mandayam, Avinash Srinivasan, Kun Sun, Selcuk Uluagac			
14:30 – 15:45	**Session 2 (Invited talks): Information Assurance and Theory to Practice** (Moderator: Jie Wu, Scribe: Yan Wang) Marwan Krunz, Dipankar Raychaudhuri, Ness Shroff			
15:45 – 16:00	Coffee Break			
16:00 – 18:00	**World Café**			
	Table 1	**Table 2**	**Table 3**	**Table 4**
16:00 – 16:30	Group 1	Group 2	Group 3	Group 4
16:30 – 17:00	Group 4	Group 1	Group 2	Group 3
17:00 – 17:30	Group 3	Group 4	Group 1	Group 2
17:30 – 18:00	Group 2	Group 3	Group 4	Group 1
18:00	Dinner			

World Café Table and Group Assignment	
Table 1	**Theory to Practice** (Host: Shiwen Mao, Scribe: Avinash Srinivasan)

Table 2	**AI/ML Enhanced Defense** (Host: Cliff Wang, Scribe: Xiaonan Guo)
Table 3	**AI/ML in Cyber Physical Systems and Wireless Networks** (Host: Yingying Chen, Scribe: Tao Li)
Table 4	**Open Topics: Autonomous Systems, AR/VR, Benchmarking** (Host: Jie Wu, Scribe: Jiacheng Shang)

Group 1	Loukas Lazos, Wenjing Lou, Guevara Noubir, Angelos Stavrou, Quanyan Zhu
Group 2	David Mohaisen, Kang Shin, Patrick Traynor, Yan Wang, Rui Zhang
Group 3	Marwan Krunz, Jason Li, Narayan Mandayam, Selcuk Uluagac
Group 4	Dipankar Raychaudhuri, Ness Shroff, Kun Sun, Ning Zhang, Zhuo Lu

Friday, November 18

8:30 – 8:40	Debrief by Yingying Chen and Jie Wu
8:40 – 9:45	**Presentations from ARO and ARL**
	Paul Yu and Brian Rivera
9:45 – 10:45	**Panel / Session Summaries and Discussion**
9:45 – 10:00	Session 1 Summary and Discussion
10:00 – 10:15	Session 2 Summary and Discussion
10:15 – 10:30	Panel 1 Summary and Discussion
10:30 – 10:45	Panel 2 Summary and Discussion
10:45 – 11:00	Coffee Break
11:00 – 12:00	**World Café Summaries and Discussion**
11:00 – 11:15	Table 1
11:15 – 11:30	Table 2
11:30 – 11:45	Table 3
11:45 – 12:00	Table 4
12:00 – 12:10	Concluding remarks by ARO Program Manager, Paul Yu
12:10 – 13:10	Wrap up and box lunch

Session, Panel, and Table Summaries

Panel I Summary on AI/ML Security in Cyber Physical Systems

1 Panel Organization

The first panel discussion on 11/17/2022, with the title "AI/ML Enabled Security in Cyber-Physical Systems," consists of five panelists, Dr. Jason Li from Trusted Science and Technology,

Dr. David Mohaisen from the University of Central Florida, Dr. Kang Shin from University of Michigan, Dr. Angelos Stavrou from Virginia Tech, and Dr. Patrick Traynor from University of Florida. It was moderated by Dr. Yingying Chen from Rutgers University and scribed by Dr. Ning Zhang from Washington University in St. Louis.

2 Scope, Definition, and Formulation of CPS

Scope and Definition. With recent advances in embedded devices and communication, our cyber world and physical world are increasingly intertwined. Cyber-physical systems (CPS) can be defined as systems where cyber components and physical systems are tightly-coupled and deeply-integrated. A collective vision of the CPS ecosystem is shown in Fig. 1, where besides the common consideration of computation elements, human and physical components are also essential for the safety and security consideration of CPS. While the application of control theory in these systems is well understood, emerging CPS often has artificial intelligence (AI) / machine learning (ML) as key enablers, and how AI/ML impacts the security landscape of CPS remains an active research area. There are three commonly agreed-upon observations on the impact of recent breakthroughs of AI/ML on CPS. First, AI/ML components are integrated into both the front end and the back end of the CPS. At the front end, AI/ML enables more intuitive controls for non-experts through voice/gesture recognition, natural language processing, etc. At the back end, AI/ML is also widely used in autonomous systems to form the perception of the physical world. There are also recent developments in utilizing AI to control actuation in CPS. Second, CPS systems are often highly diverse (heterogeneous), where there is a full spectrum of different computation, storage, and network capabilities, as well as the scale of problems in time and system. Third, besides the evolving attack surface due to the involvement of AI/ML components in CPS design, AI/ML can also be used as a tool for attacks (such as inferring private information and finding vulnerabilities automatically) and defenses.

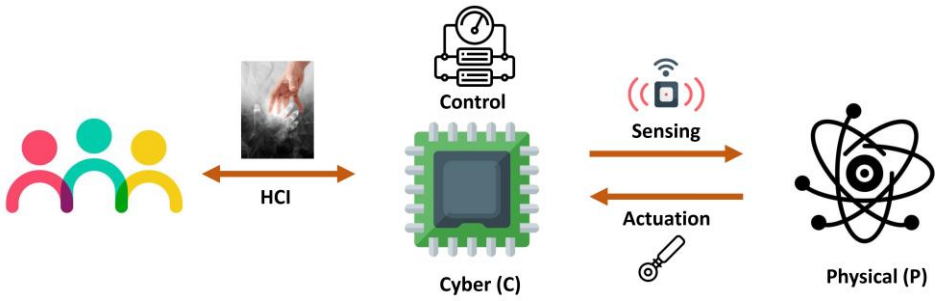

Fig. 1: Overview of CPS

Unique Threat Landscape for CPS. The strong coupling between cyber and physical components in CPS not only gives rise to a set of new constraints on the computation but also opens up new dimensions on the attack surface in addition to the cyber-only attacks. Recent physical world attacks include signal injection attacks, such as injecting inaudible commands via ultrasound or laser, fault injection using power or repeated memory access, or even physically sabotaging the system. Cyber threats include the AI vulnerabilities (such as stealing attacks against model

confidentiality, adversarial samples against model integrity, and sponge examples against model availability), network vulnerabilities (such as replay and spoof attacks), platform vulnerabilities (such as software exploitation and microarchitectural side-channel attacks), and management vulnerabilities (such as insider threats).

Key Principles in CPS Design. Four fundamental design principles emerged in the discussion. First, in CPS, physics rules, and cyber is often a slave of physical process. Hence, when a defense is considered for CPS, it has to be placed in the context of the CPS mission and taken into the tight coupling and deep integration nature between the cyber and physical components. Second, bridging the gap of abstractions between cyber and physical is key, since strong inter-dependencies exist among different assurance dimensions and abstraction layers. Third, domain customization of context/mission offers new opportunities to tackle the complexity of the design of AI/ML in large-scale CPS. Lastly, human-AI collaboration is essential not only for the efficiency of AI-enabled CPS but also for establishing trust between human and machine.

3 Discussion Questions

What's critical in CPS Security? There are three key critical aspects. First, domain-specific customization and context awareness empower effective solutions that can strike a balance between security protection and performance. Second, data is essential in AI/ML-enabled CPS, where both reliability and trustworthiness can significantly influence the system's effectiveness. Lastly, timing is important. Untimely computation results may be useless or even harmful to the system.

Other important properties of CPS include the consideration for usability, the decision on prioritization order for human-in-the-loop CPS, the use of multimodal sensing to improve robustness in perception, and the corresponding false sense of security due to its potential amplification of impacts from vulnerabilities.

What CPS security cannot do without AI/ML? AI/ML is a powerful tool to understand, identify, and model adversarial behaviors, either in the cyber or the physical domain, enabling a more accurate estimation of the window of superiority. Additionally, AI/ML tools can also be used to effectively gather intelligence (by inferring private and hidden information), search for vulnerabilities in targets (by automatically exploring network and software system input spaces,) or even automatically weaponize vulnerability (by constructing mission payloads based on the found vulnerability), enabling a deeper understanding on the window of vulnerability. From the control perspective, cyber-enabled (with AI/ML) control hardening can be indispensable when there is no closed-form relationship between input and output. It is capable of enabling the CPS to cover unknown gaps between the designed range of operations through reinforcement learning, which enables structured trial-n-error exploration. Lastly, it can also be used to mediate physical world signals to either inject adversarial signals or mitigate attacks that originate from the physical world. It is also possible to use this capability to aid non-experts in the operation of complex CPS.

What unique aspects can AI/ML help that conventional approach may not be? Human-AI collaboration is a unique aspect that conventional approaches may not be able to support. More specifically, along the lines of human for AI, by embedding human in the loop, there is an opportunity to massively reduce model complexity while improving the effectiveness of the workflow. From the perspective of AI for human, it may be possible to leverage AI to complement user expertise to make systems more usable or use AI to enable user-specific customization of multimodal data visualization.

To what extent can AI/ML improve CPS security? There are limitations regarding what AI/ML can do for CPS. In AI-enabled CPS, the reliance on AI/ML exposes new attack surfaces. Fortunately, this attack surface often moves when domain customization is applied, significantly limiting the transferability of the attacks. There are also many challenging problems, such as the composability of security properties in CPS, holistic patching and mitigation of system vulnerabilities, and integration of fault tolerance in multiple subsystems, where it is unclear if AI/ML can be part of the solution.

Panel 2 Summary on AI/ML Enabled Security in Wireless Networks

1 Panel Organization

The panel on "AI/ML Enabled Security in Wireless Networks" was held on 11/27/2022 from 13:00 to 14:30 and moderated by Dr. Jie Wu from Temple University. Panelists include Dr. Michael De Lucia from Army Research Lab, Prof. Narayan Mandayam from Rutgers University, Prof. Avinash Srinivasan from US Navy Academy, Prof. Kun Sun from George Mason University, and Prof. Selcuk Uluagac from Florida International University. The summary, done by Rui Zhang, was based on the key questions discussed by the panelists.

2 Discussion Questions

How Can AI/ML Learn by Interacting with the Environment? AI/ML learns by interacting with the environment from the feedback from its own actions and experiences in a trial-and-error fashion.

What Can be Learned by AI/ML? Current AI/ML technology is well suited to learning a broad range of capabilities. Examples include object and event detection and recognition, situation awareness, such as perception of entities in the environment, device/user activities, and behaviors. AI/ML can also learn forensically valuable information about events and activities from interactions between devices, users, and apps. In military settings, AI/ML can learn normal baseline operations under different conditions, which may evolve over time. They can also learn layer-specific Indicators of Attack (IOA) and Key Performance Indicators (KPI). Generally speaking, whether AI/ML systems can learn anything effectively requires us to have the right AI system and datasets and pose the right questions.

What Cannot be Learned by AI/ML? While much can be learned by AI/ML, current AI/ML technologies face some noticeable challenges. First, since current AI/ML systems have fundamentally different cognitive qualities and abilities than biological systems, they cannot reason as human beings. Second, it is often difficult, even for the designer of an AI system, to explain why the AI arrived at a specific decision. There is thus a pressing need for developing explainable or interpretable AI techniques to allow humans to understand the decisions or predictions made by the AI, especially for high-stake mission-critical military applications. Third, AI is limited to detecting and recognizing events present in the training data and is unable to detect unforeseen events or unknown attacks. Last but not least, even though machine learning models can make quick decisions, the action taken by AI/ML-powered cyber-physical systems in response to a detected event or attack is often limited by the agility of related physical components.

What Can AI/ML Do for Future Networks? The rapid advance in AI/ML technologies presents a wide range of opportunities for future networks. First, AI/ML will catalyze the transition from traditional hardware-driven networks to software-driven networks. Unlike traditional networks that use dedicated hardware devices (i.e., routers and switches) to control network traffic, software-driven networks, a.k.a. software-defined networks, use software-based controllers to communicate with underlying commoditized hardware infrastructure and direct traffic on a network. Such a transition will bring many advantages, including increased control with greater speed and flexibility, customizable network infrastructure, and more robust network security. Second, AI/ML techniques have great potential to drive network automation by automating network and security provisioning and management for increasing network speed, reducing power consumption, improving network efficiency and functionality, and alleviating network operators' network planning and deployment challenges. Third, AI/ML can also help manage large-scale networks that are difficult to manage, e.g., billions of IoT devices, by traditional rule-based methods. Fourth, AI/ML allows continuous real-time optimization in various network applications such as spectrum sensing, app-based traffic steering, dynamic network slicing, etc. Fifth, AI/ML can greatly improve network operations by providing network operators with situation and context awareness. Moreover, AI/ML techniques can be used for developing physical-layer security mechanisms that complement upper-layer security defenses. Examples include directional modulation with metamaterial antenna and spoof defense, e.g., hybrid classification based on physics-based statistical models and learning-based classifiers. Finally, it is possible to improve network security by incorporating human subjectivity and intervention into AI/ML's decision-making.

Meanwhile, AI/ML technologies also bring new challenges to defending future networks. Specifically, an adversary can also exploit AI/ML techniques for attack automation. In addition, the AI/ML techniques will also introduce new attack surfaces.

What Can Future Networks Do for AI/ML? Future networks can also benefit AI/ML in multiple ways. First, the expanding deployment of 5G networks will bring higher data speeds, ultra-low latency, more reliability, and massive network capacity. In addition, emerging Trusted Execution Environments have great potential to safeguard both user data and machine learning models from malicious attacks. Moreover, it is possible to design new network architectures that support in-situ AI/ML by design. In addition, future networks can also improve AI/ML performance by establishing contextual awareness through monitoring both network devices' software and

physical components and environment. Last but not least, future networks will be able to provide the right data and ask the right questions to better harness the power of AI/ML.

How Can We Leverage Rich IoT Signals to Enhance Security? The rich IoT signals of large volume, variety, and diverse quality generated by vast IoT devices present unique opportunities for enhancing network security. One such opportunity is to improve system security by cross-checking signals from different sensors. Examples include multi-factor authentication, secure in-vehicle automatic speech recognition, and device fingerprinting and tracking via continuous authentication. Another opportunity lies in privacy protection. Recent works have shown that we can detect information leakage by devices and identify if user activities is being tracked by analyzing IoT signals. Moreover, rich IoT signals can be exploited to create contextual awareness for improved attack detection and collect forensically valuable information.

What Measures Can We Take to Improve Cyber-attack and Forensics Readiness in Future? Several actions were suggested to be taken for improving cyberattacks and forensics readiness in the future. First, there is a pressing need for collecting and sharing high-quality network traffic datasets for AI/ML research. Second, it is important to obtain a better understanding of users' needs, as different users and stakeholders may have conflicting demands. Third, we should explore AI/ML, such as Reinforcement Learning and VR/AR technologies for cyber training. Third, since most current network traffic is encrypted, it is necessary to develop better AI/ML techniques to better classify encrypted network traffic. Fourth, current IoT devices suffer from hardcoded and weak credentials, lack of built-in secure software and firmware update capabilities, and limited visibility to network operators, which have made a major attack vector. It is, therefore, important to secure IoT software supply chains. Last but not least, it is necessary to investigate effective approaches for involving human subjectivity in AI/ML decision-making, such as human intervention in reinforcement learning, for improved security defense capability.

Session 1 Summary: Information Assurance and Theory to Practice

Moderator: Yingying Chen, Rutgers University

Scribe: Zhuo Lu, University of South Florida

Speakers: Loukas Lazos (The University of Arizona), Wenjing Lou (Virginia Tech), Guevara Noubir (Northeastern University)

Topic 1: New Security Problems in Next-Generation Networks

There are four evolution pillars: network architecture, PHY Layer technologies, business models, and applications. Each is associated with different security requirements, threat models, trust models, defense capabilities, and main research challenges. There are many architecture innovations in NextG networking, including softwarization and virtualization of network functions that can run on commodity hardware, capability for openness and re-programmability (e.g., rApps and xApps in the O-RAN architecture), data-driven network optimization at different time scales,

access to fine-grained key performance indicators (KPIs), and application-driven network slicing for supporting heterogeneous services. For the new PHY-layer technologies, there are dynamic spectrum management, operations in mmWave and THz frequencies, and flexible numerology. Business models include new stakeholders and relationships that need to be built in a mutual trust environment. The applications involve human-centric models, including intelligent transportation, AR/VR, and healthcare.

From the taxonomy perspective, there are external adversaries, internal adversaries, and application threats. Three New PHY layer threat examples have been discussed: 1) passive eavesdropping (e.g., in more difficult yet possible mmWave/THz beamforming), 2) active eavesdropping in which an attacker manipulates the beam sweeping algorithm to attract transmissions towards its direction. And 3) intelligent DoS attacks (e.g., introducing delay for time-critical applications, attacking CSI and FO estimations, targeting AI-based beam tracking, and using PHY-layer attacks to control the reward in resource allocation optimization).

The threats in data-driven resource allocation are particularly discussed. For example, a machine learning agent may enforce a policy to allocate wireless resources according to its observation of the operational state and a set of certain actions. An attacker may try to manipulate the resource requests, alter the reward observed by the agent, or change the radio frequency environment. There are many other machine learning-based threats, including attacks against reinforcement learning, model inversion attacks, poisoning attacks, inference attacks, and trojan attacks. We need to thoroughly understand their conditions, access level, and impacts on the network and services.

Topic 2: Security and Privacy Problems in Next-Generation Wireless Networks

We observe several important new technological trends in 5G and beyond networks. The first new technological trend is softwarization and cloudification of telecom infrastructure. With the development of SDN and NFV, SW and HW are increasingly disaggregated. Radio, edge, and network as a service become increasingly possible. This has led to reduced equipment costs and power consumption, and economics of scale of IT industry time-to-market from HW dev to SW dev. The second trend we have seen is integration of AI/ML learning in network functions, which has been used to help with air interface design, localization, channel estimation, radio resource management, interference mitigation, network optimization for QoE improvement, network monitoring, and intrusion detection. And the third trend is the desire to have an open ecosystem to achieve full interoperability of different vendors' equipment and to allow better network flexibility and lower the operational cost.

The blockchain technology has been intensively discussed. There are many benefits to moving from a centralized to a decentralized management model for network service. However, the challenges of designing blockchain for wireless networking include cost and scalability, resource centrality and impact of consensus protocols, HW centrality, SW/developer centrality, selfish mining, eclipse attacks, the truthfulness of external data (i.e., the blockchain oracle problem), the confidentiality of external data, protocol and software vulnerabilities, and anonymization and deanonymization. Two examples were given in the session, and they are 1) Blockchain-based

Decentralized Spectrum Access and 2) Blockchain-based Provable Resource Allocation that ensures verification of resource transactions among mutually distrusting parties.

Topic 3: Civilian Wireless Technologies for DoD and Private Networks: Challenges and Opportunities

5G+ systems provide multiple opportunities for DoD, which can leverage the developments in the commercial world. If we focus on pre-authentication signaling in 5G networks, we can see that they are essential to initialize/maintain network control. There is potential leakage from signaling (e.g., PSS, SSS, PBCH/MIB), which broadcasts constant values, predictable values, or predictably repeating values. Several attacks have been identified, evaluated, and demonstrated. They are significantly more efficient than naive attacks, and these adversaries can be miles away (10s of dB gains) to perform traffic analysis. Experiments were conducted to show the feasibility of the long-range detection of 3GPP LTE via parabolic grid high directional antenna with 26 dB gain and wide spectrum (600-6500MHz). In addition to the 5G signal sniffing, valuable information can be inferred by using side information of the 5G protocol. The privacy leaking attacks are able to cause a wide range of problems, including rogue infrastructure; denial of service attacks (e.g., the disappearance of networks, cell barring), and tracking. Several mitigation and defense mechanisms have been developed. Their requirements are from no-modification to standard to minimal modifications to standard and impact on implementation.

RF situational awareness for potential military applications was briefly mentioned. It motivates creating deep learning models capable of detecting, classifying, and precisely locating RF emissions in time and frequency. A framework and techniques for reasoning and driving proactive and autonomous defense mechanisms, including mechanism hopping (randomization) at different network layers (e.g., PHY, link/MAC, network, transport), using game theory-guided approaches (strategies for a variety of utility functions including deception). The overall objective is always to let an adversary suffer a low success probability to attack the right mechanism.

Session 2 Summary: Information Assurance and Theory to Practice

Moderator: Jie Wu, Temple University

Scribe: Yan Wang, Temple University

Speakers: Marwan Krunz (The University of Arizona), Dipankar Raychaudhuri (Rutgers University), Ness Shroff (The Ohio State University)

Topic 1: When Adversarial Machine Learning Meets Signal Classifiers

Currently, signal classification in software-defined radio mainly uses machine-learning classifiers. They are known to be vulnerable to adversarial machine learning (AML) attacks such as 1) Misclassification Attacks: The attacker estimates the defender’s classifier and generates low-

power AML perturbations that cause the defender's classifier to assign wrong labels to captured samples. This type of attack can be either targeted or untargeted attacks. 2) Spoofing/Impersonation Attack: The attacker transmits a mimicked signal that would be classified by the defender as a legitimate signa. Attackers can use multi-agent GAN-based synthesizers to generate fake signals based on legitimate signals.

In these attacks, the attacker may not have perfect (or even any) knowledge of the defender's classifier, resulting in unique challenges in wireless communications. For example, the attacker and defender may use different training datasets. They may have imperfect synchronization between legitimate signals and attacker's perturbations. In addition, channel noise may be totally different between the attacker and the defender (i.e., Alice-to-Bob, Alice-to-Eve, and Eve-to-Bob channels). Moreover, the attacker may not act persistently (to avoid detection). However, we have observed that with just the knowledge of perturbation, attackers can still cause significant misclassification when they have zero knowledge of the structure of defenders' classifiers, without perfect synchronization, and even with non-persistent efforts.

Along this direction, there are many open research issues. For example, the theoretical analysis of AML attacks in generalized settings is an interesting topic. We still lack a theory of how to attack using adversarial ML using different types of perturbation. In addition, online detection and classification of AML attacks are important and worth studying. It is important to develop methods for detecting the attacks or determining the type of perturbation just based on the signal strength of perturbation. Moreover, defense mechanisms are an essential goal of achieving system security. We need to answer research problems, such as whether the reactive defense is better or proactive defense is better. Keep in mind that the security community currently lacks datasets for certain waveforms (e.g., radar waveforms and passive systems). Therefore, datasets are also valuable assets in this research domain.

Interesting questions were raised during the discussion. For example, "Can we determine the bound of perturbation for different models?" "How close does the zero-knowledge attack performance compared to the random noise attack performance?" "Can the RF data factory generate the data that we need?" The data missing is non-commercial waveform data. When considering the synchronization problems in attacks, skipping the data part of the frame may have degraded performance but still works. The high sampling rate in signal classification allows attackers to launch attacks using continuous/intermittent perturbations.

Topic 2: Information Assurance in Next-Gen Wireless Networks

Compared to the current generation of wireless networks, the next-gen wireless networks will provide ultra-high bandwidth, low latency, and powerful edge computing that will enable important new classes of real-time applications. The application domain of the next-gen wireless network includes AR, VR, connected cars, smart cities (with high-bandwidth sensing), industrial control, etc. The emerging next-gen mobile core network architecture is based on open, programmable cloud-native architecture. It usually consists of native cloud, software-defined networks (SDN)/software-defined radio (SDR), virtual network function (VNF), and edge computing integrated with access networks. The next-gen wireless networks use Open-Radio Access Networks (O-RAN) as the foundation for custom designs.

Next-gen networks face various security challenges, including attacks by the mobile end, attacks on the radio interface, attacks with physical access to the transport network, virtualization attacks by third party VNF, insider attacks, API-based attacks, attacks from roaming networks, and attacks from the Internet and other networks. There are also challenges to information assurance in next-gen networks. Protection is needed for spectrum/radio signals, PHY spec extensions for Low Probability of Detection (LPD), and Low Probability of Interception (LPI). Since radio signal is open by nature, we need to consider both hardware and software. Open APIs and programmability in O-RAN provide multi-vendor flexibility but also enable various software-based attacks, particularly for the implementation of 5G PHY. This is more like software-engineering problems than network design problems. Emerging AR/VR or CPS applications require tight QoS/latency bounds (~10ms) that are susceptible to DOS attacks. Real-time ML inference in distributed edge cloud scenarios should also pay attention to such attacks since data sharing and all kinds of related problems, e.g., edge offloading (data or model slicing), are time-sensitive.

Topic 3: Machine Learning and Information Assurance for Emerging Network Systems

Machine learning (ML) has also been adopted in network design and control. Traditional network design and control approaches usually start with a set of assumptions, then develop a policy. Such approaches are often "Open Loop," meaning that policies do not affect assumptions. In the recent study of ML for network design and control, we usually have fewer assumptions in modeling. The learning policies are designed based on feedback data and converge to the optimal settings. It is a "Closed loop" process that is more adaptive to network conditions and a good place for reinforcement learning. In particular, ML for network design and control is good for predicting implicit relationships across networks. Edge caching strategies guided by online learning principles can be developed to adaptively learn the cost of missing each future data item, which can significantly improve state-of-the-art control systems to minimize overall miss costs. ML is also useful in handling non-stationarity network dynamics. For example, in designing beam alignment methods for mmWave, it is possible to reproduce the kernel Hilbert function to model the RSS, appropriately discard old data and start afresh to counter the non-stationarity.

Summary for Discussions on Table 1

Topic: Theory-to-practice

Host: Dr. Shiwen Mao

Scribe: Dr. Avinash Srinivasan

At table-1, we discussed the challenges with transitioning from theory to practice, specifically focusing on AI/ML. In particular, we answered the following three important questions during the discussion.

1. What are the key challenges to bridge the gap from theory to practice?

The gap that exists in transitioning from theory-to-practice is a long-standing, yet to be well understood challenge facing all areas of research, especially with modern technology. Some of the key gaps that significantly hinder the transition from theory-to-practice include technical-, knowledge-, and semantic-gap. Theoretical models developed in labs and academic settings are often developed under strong assumptions. These assumptions are a key-hurdle in transitioning such models to practice and render them ineffective for real-world deployment. Theoretical models that eventually transition to practical solutions – both hardware and software – are faced with challenges during installation and deployment in the real-world.

Models that are developed for a highly specific application's scenarios will minimize their practicality, regardless of how well the model requirements are defined. This is primarily due to the narrow scope of applications for which the models are developed. Most theoretical models are often not repeatable, which once again makes the transition unjustifiable for the stakeholders' return on investment (ROI). Ideas also often fail to transition when the Intellectual Property (IP) office of an organization is highly inflexible. There are no incentives for researchers to go the extra mile to publish/share their dataset or to pursue commercialization efforts. Private industries are also overly cautious, due to fear of liability, with using university-developed technologies unless it is fully protected.

A *testbed* can be a great enabler in transitioning from theory-to-practice as it supports prototype implementation and testing. However, a key challenge with current *testbeds* is their steep learning curve, and without support from personnel who maintain the testbed, researchers need substantial amount of time to implement and test their models on a testbed. *NSF PAWR testbed* and *USENIX artifact evaluation* are two classic examples of testbeds faced with the above discussed challenges.

Another challenge facing testbeds is that academic testbeds have a short shelf-life. Such short shelf-life testbeds go obsolete by the time researchers are ready to implement and test their models. When it comes to funded research, it is critical that program managers and their teams are cognizant of the importance of applied AI/ML. Agency personnel involved with go/no-go funding decisions should not dismiss applied AI/ML research in favor of foundational AI/ML research. While the concept of transition from theory-to-practice and its challenges are more readily recognized, it is important to note that there are situations that may warrant transition of ideas and concepts from practice to theory.

2. Can Benchmarking support the transition from theory-to-practice?

Benchmarking is a critical requirement that can alleviate the gap that exists between theory and practice. However, developing a good and meaningful benchmark that has a good representation of the target domain is extremely hard and challenging. Repeatability is a key requirement since every AI/ML model invariably works best on the dataset it is modeled for. Therefore, a common dataset to compare performance of different models is required. However, creating benchmarks for all possible workloads is neither scalable nor practical.

It is not possible to have good, labeled data for all security scenarios. Additionally, creating good benchmarks that remain current and relevant at the pace at which system architectures are evolving is not possible. To overcome these limitations, it is imperative to move toward models that can

learn with limited training data with little to no labeling. Finally, it is not just the quantity of the data, but also the quality and relevance that impact the model. Additionally, benchmarking may not always be helpful since success in some scenarios can be probabilistic.

3. How can past lessons learned help transition from theory to practice?

Much can be learned from previous experiences. It is important to note that learning and gains are the highest when problem complexity is the highest. Past experiences also teach us a valuable lesson that *asymmetry* is a big part of attacker utility, with the attacker's objective being *maximum gains with minimum effort.* It is important to note that changing from *model-based systems* to *AI/ML-based systems* decreases the cost for the attacker and is bound to introduce new attack surfaces and vectors.

One such key learning came from AI/ML Image analysis for malware detection that *uncovered cryptojacking*, a new botnet ecosystem that uses edge systems for crypto mining. Another learning comes from *autonomous driving,* where poor real-time decision-making leads to crashes.
A model trained for one scenario (dataset) can fail in a different scenario. For instance, an AI/ML model on self-driving cars that is trained for sunny weather is very likely to fail in overcast weather.

Generalizability is very important for AI/ML applications. Past experience indicates that Neural Networks have higher success because of their generalizability. It takes time to predict what will translate into practice and what will remain theoretical and academic. For example, *Shannon's* work, which was initially considered theoretical and academic, eventually transitioned to being the very foundation of today's digital communications. Similarly, MANETs that started as academic interests with the likelihood of success in the commercial realm ended up being more successful in the military. Compared to the military, which is poorly understood, the commercial domain is ROI driven. Commercial domains also prefer *false negatives* over *false positives* since the system will be blamed for the false positive-induced operator fatigue.

The potential future direction of AI/ML model development can benefit from closed-loop architecture which will support *continuous-learn-continuous-use* philosophy. Such models will be incremental but provide continuous improvements. AI/ML models can also benefit by leveraging a game-theory approach with offensive and defensive security aspects. Finally, it would be highly beneficial to move toward *multiscale* and *generalizable* AI/ML models.

Summary for Discussions on Table 2

Topic: AL/ML Enhanced Defense

Host: Dr. Cliff Wang

Scribe: Dr. Xiaonan Guo

Artificial intelligence (AI) and machine learning (ML) have been widely used in a broad spectrum of applications in the past decade. To understand AL/ML enhanced defense, we discussed a series of questions from different perspectives among all the discussion groups.

1. Is AI/ML just Tool or Game Changer?

We first discussed whether AI/ML is just a tool or a game changer. Most of the current research is adopting AI/ML as a tool. On the one hand, many AL/ML algorithms have been developed to facilitate different application scenarios. For example, AI/ML can be used to assist building efficient models to accelerate tasks such as gesture recognition, autonomous driving, etc. On the other hand, AI/ML could be a game changer in cyber defense. There are successful examples in other domains, such as chess playing, where the problem is well-bounded, state space is well-defined, and the problem/solution space is not open-ended. A complete understanding of context and domain is critical to applying AI/ML to solve challenging problems such as cyber defense. Consequently, if we know the context and domain constrain better, it helps us define problem boundaries and confine state space, making it easy to adopt AI/ML as a game changer.

2. Does AI/ML Bring more Advantages or Disadvantages to Cyber Defense?

There is also a discussion on whether AI/ML brings more advantages or disadvantages to the cyber defense. Due to the asymmetric nature of cyber defense where defenders have to protect the whole attack space, while an adversary only needs to make one penetration to succeed. If AI/ML models are adopted without careful security protection, it may potentially increase more risk by enlarging attack surface and introducing more vulnerability. Existing research showed that training data could poison ML algorithms. The adversary could use a lot of data to hijack the system, where the learner will suffer a significant loss. In addition, the security of AI/ML model is the most important. To deal with the advanced adversaries that can attack ML algorithms, we need to reconsider the possible attacking types and knowledge of the adversaries. The system should have a fallback plan so that when ML-based security countermeasure does not work, the system could still be under protection. However, current AI/ML is quite often introduced without complete rigorous security analysis making finding new attacks on AI/ML systems a popular way to generate papers. Although we have lots of AI/ML data, if they are not properly structured or labeled, these data can be manipulated to bring harm, such as to launch poisoning attacks. Therefore, we need to do it proactively and autonomously to have security by design against capable, strategic, and determined adversaries. We need to find systematic approaches to model security threats and defenses. The vision is that we should utilize elasticity for seamless adaptivity.

Although AI/ML has been widely used in different application domains, the use of AI/ML brings both advantages and disadvantages. Currently, there is a lack of understanding of high-order statistics or dynamics of these data, which leads to an increase in the risk of this AI/ML augmented system. To gain an advantage in cyber defense, we need to develop algorithms to learn from

unstructured data. Moreover, to gain an advantage in cyber defense, we need to build scalable solutions for a complex system. Generic AI/ML models may not be applicable to every domain. In addition, to gain an advantage in cyber defense, we need to incorporate domain knowledge and context. In addition, the knowledge gained in one domain should be transferred to another domain so that the efforts in building the AL/ML can be significantly reduced. But this is extremely challenging, even for similar (but unidentical) domains.

3. Relationship between Human and AI/ML for Cyber Defense

It is critical to identify the strength and capability boundary between AI/ML system and human players such that we can make intelligent and optimized task delegation or decision choices. In a typical system within the domain of cyber defense, there is a close relationship between human player and the system. The role of the human player is to make decisions based on the data collected from the system along with the output from the AI/ML models, and the human players can take full control of the system if there are abnormal happens. Ideally, if we can bound the problem properly, AI/ML systems could outperform human players. We could leverage AI/ML to help the human player for better input and more efficient multitasking. The cost of switching between human and AI/ML systems should be taken into consideration. It is important to define optimum role switching. It is critical for research to build an interface between AI/ML and human player. It is critical to create human-AI interaction model such that we can facilitate human in-the-loop or human on-the-loop. AI/ML should collect and present information in a way that optimize human player performance. It is also critical to build inherited trust between AI/ML system and human players.

4. Data Driven Approach V.S. Protocol Driven Approach

We can use protocol-driven settings as an initial start and leverage reinforcement learning and online learning to further enhance cyber defense. By exploiting reinforcement learning (RL), we can significantly improve system performance. For example, in the network domain, it gives the machine the ability to learn dependencies/correlations, shared links, similar locations, and channel conditions. These dependencies would result in much better network performance, e.g., the shortest path performance could substantially be improved if exploring the correlation between two paths. The data-driven approach can potentially help us to capture high-order dynamics while the protocol-driven approach can only capture the average cases. The challenge is whether we have complete knowledge of the data space. The second challenge is that the data space can be trusted and malicious data be identified and eliminated. If the data space is too large or non-stationary, then the data-driven-based learning may potentially fail. Human expertise could potentially help data-driven approach by determining initial search point and follow-on search path (Reducing the search space). We can also use GAN type of approach to help traverse the whole data search space minimizing blind spot.

Summary for Discussions on Table 3

Topic: AI/ML in Cyber Physical Systems and Wireless Networks

Host: Dr. Yingying Chen

Scribe: Dr. Tao Li

We discussed new directions and opportunities that AI/ML techniques bring for cyber-physical systems and wireless networks. We answered the following three important questions during the discussion.

1. What are the new directions in cyber-physical systems?

AI/ML solved some problems that stuck cyber-physical systems for many years. For example, AI/ML techniques can be used to detect anomalies and optimize the process in large-scale CPS. But AI/ML techniques cannot replace traditional control theories because AI/ML techniques do not always outperform traditional controllers. Sometimes, the AI controllers fail to balance multiple requirements in cyber-physical systems. Strategically combining traditional control theories and AI/ML algorithms is a promising future research direction.

Despite a lot of AI/ML research, we still need more fundamental AI/ML contributions to networked systems and applications instead of just applying existing AI/ML techniques. The existing AI/ML techniques were not initially designed for cyber-physical systems. AI/ML algorithms that consider unique features in CPS are necessary for further performance improvement. Special needs and features in CPS may also stimulate new AI/ML research.

Current AI/ML techniques are not good enough to be used in many cyber physical systems. For example, the mistake of AI in autonomous driving or medical systems may cause severe problems. The real physical world is too complex for existing AI/ML systems to understand. AI/ML cannot learn everything like many corner cases in autonomous driving, so humans have to make final decisions sometimes. Though both human and AI make mistakes, many people do not trust AI/ML to make decisions when they are in danger. Therefore, we need to consider both benefits and risks of AI/ML. How to mitigate the risks brought by AI/ML is a good research topic. It is also meaningful to understand and compare the decisions made by AI/ML and humans in CPS.

In addition to the false negatives in the above examples that cause fatal accidents, false positives in many AI-enabled devices may cause inconvenience for users. For example, the user may have to see the doctor because of the false health diagnosis of the smartwatch. Developing usable wearable devices with accurate AI/ML algorithms is an important topic for researchers in both industry and academia.

Context-aware AI/ML solutions are very necessary in cyber-physical systems. It is better to design new models or customize existing models according to the context to achieve better performance.

Since CPS sensors generate too much data, AI/ML may be used to guide the data collection. We can also save bandwidth by uploading only the data that we need.

AI/ML can be used to transform the data and extract the semantic meaning of the data. Since online training is very hard, offline training is a safe way for many applications. Synthesized data can help the training process in many scenarios which do not have enough data. For example, it is better to use synthesized data in applications that require users to generate large training data manually.

CPS may have very limited normal traffic patterns but very diverse abnormal traffic patterns. How to design a model that can handle diverse abnormal patterns is a good direction.

2. What are the new opportunities for wireless networks?

AI/ML enabled many wireless applications. For example, the devices can be identified by the AI model based on their signal fingerprints. AI/ML can also be used to detect malicious wireless signals to secure the network in protected facilities. Next-generation wireless networks which support high bandwidth and low-latency communications will create more opportunities for AI/ML techniques.

Compared with CPS, it is more challenging to apply AI/ML to wireless networks because of the lack of perfect training data. Since wireless signals can be affected by many factors in the open channel, the signals change over time, even with the same environment layout. Therefore, the data in wireless networks are not as simple or reliable as the CPS data. A model trained in one environment can hardly be used in another environment. How to reduce model retain efforts is an important direction for AI/ML applications in wireless networks.

Currently, all the networks are designed by humans and consist of some hidden vulnerabilities, especially in large and complex networks. AI/ML has the potential to enable automatic network design and substantially increase network design quality and delivery speed. The automatically designed networks may have fewer risks and better performance.

3. How can network layers be benefited from AI/ML? Top-down or bottom-up?

AI/ML can be used in all the network layers, but we need to consider the context in every layer and customize the model for every layer. The network may not get real-time decisions from the AI algorithms, but the results are useful for the network in the long run. Lower layers of the network benefit more from AI/ML. There are many AI/ML applications in the physical layer because it generates more data. For example, the devices can be identified based on their signal fingerprints. But many problems still have not been solved.

The current AI/ML solutions target only a single network layer. Cross-layer holistic solutions may be very useful to solve security problems in the whole network. It is a good direction to consider a global view of network security. Cross-layer approaches may also improve the performance of the whole network in addition to the security. It is a good direction to consider the data in different layers to solve the bottleneck problem in each layer.

Summary for Discussions on Table 4

Topic: Open Topics: Autonomous Systems, AR/VR, Benchmarking

Host: Dr. Jie Wu

Scribe: Dr. Jiacheng Shang

This report is a summary of the discussion on table 4 during the World Cafe event of the ARO workshop. Four groups of participants from industry, academia, and the army shared their insights on two major topics: security benchmarks of security systems and security and privacy of AR/VR.

1. Whether it is possible to find a group of general metrics for measuring the security levels of systems? And if the answer is yes, what metrics could be used?

One benchmark that could be used to measure the security level is how many detected vulnerabilities have been fixed. However, this metric is based on a strong assumption that all vulnerabilities have been detected, which is usually false in practice. Moreover, this metric cannot measure the impact and the cost to recover from an attack, which could be more challenging.

We are still having a problem understanding the impacts and costs of different attacks under different scenarios, and it is extremely hard to have such metrics. It is already challenging to develop benchmarks in order to measure the security level even for two systems in the same network. Even a security protection system is trained based on the current estimation of attackers' behaviors may fail in the future due to the dynamic signatures of attacks. Also, when comparing the security levels of several systems, it is too hard to find what the measurable quantity is.

2. How to measure system security in practice?

System security should be measured case by case using concrete measurements. However, different people may still have different interpretations of the same measurements. We need to choose a baseline attack model when comparing the security of two systems. Also, we should consider different variables (e.g., the number of used resources, accuracy, and time) to determine whether the system is both effective and usable. Moreover, system security can only be measured based on the defined objectives. Therefore, we should use different metrics for different goals.

3. How can we design the evaluation to get such concrete measurements?

Current security evaluation has many limitations. For example, we cannot inject all attacks into practice since some of them are harmful and dangerous, and we must put them in toy systems. As a result, we may not collect enough data or concrete measures for some attacks. Many existing security evaluations were conducted based on threats that are designed by human beings, which cannot reflect the real attacks in practice. For good evaluation, we need to expose the system to

the same stress test across the whole evaluation. However, we currently do not have a good solution to expose the system to continuous threats. One possible solution to this problem is to have the evaluation system tied to the real-world system. The system should allow people to gather data and inject experimental attacks to get scenarios-specific benchmarking or data for training and understanding the information.

4. What are the security and privacy problems of AR/VR?

Besides current commercial applications, AR/VR has already been used for soldier training. Therefore, the security and privacy of AR/VR are more important in such scenarios. Also, it would be helpful to use AR/VR to help improve network security by involving human beings in the loops to help identify attacks.

Recent research works have shown that attackers can manipulate sensor signals by controlling ambient signals. Due to the unique hardware features (e.g., unique sensors) and special use cases of AR, the threat models in AR are different from those in traditional mobile devices.

There are a group of attacks that aim to control AR users' perception in their cyber worlds, which is unique and only exist in AR/VR. Also, the potential long-term impacts of using AR/VR on the users. For example, it will impact neural response, which could be the new attacking surface.

The privacy issues of AR/VR will be more user-centered. For example, data generated by AR/VR is largely impacted by users' behaviors and operations, and sensor data contains rich and sensitive information about the users.

In conclusion, the network security workshop studies various threat models and adversarial behaviors and explores corresponding countermeasures by using cyber-physical systems and future networks as two example domains under the era of artificial intelligence (AI) and machine learning (ML). The attendees provide insightful discussions ranging from philosophical thoughts to detailed technical approaches. Both theoretical and practical aspects of AI on information assurance in network science have been presented and discussed. The outcome of the workshop generates many interesting research topics and worth-exploring directions, which can help to advance the information assurance of network science under AI and machine learning.