# Adaptive and Dynamic Security in AI-Empowered 6G: From an Energy Efficiency Perspective

Shuaiqi Shen, Chong Yu, Kuan Zhang, Jianbing Ni, and Song Ci

## Abstract

Emerging AI-empowered services and techniques, such as connected vehicle, intelligent industry, and smart city, are forthcoming with the sixth generation (6G) cellular network to benefit daily life, industry, and society. However, the increasing integration of the 6G network with the physical world leads to a plethora of new scenarios that bring new challenges to 6G, especially from the security and energy aspects. In 5G networks, security solutions across all devices and base stations are configured with universal settings for certain types of attacks. This one-size-fit-all strategy no longer suits 6G security due to the higher diversity in device capabilities, service features, energy conditions, attack vulnerabilities, and other time-varying attributes. Since each scenario may have unique security requirements and energy availability, the selection and configuration of security strategies need to be optimized for 6G networks in an adaptive and dynamic manner. In this article, we explore 6G security from an energy efficiency perspective by balancing the trade-off between security and energy consumption in various scenarios. Specifically, we first investigate the AI-empowered 6G network architecture with promising applications and visions. Then we identify the challenges for adaptive and dynamic security optimization in 6G from the aspects of heterogeneity, dynamics, and modeling complexity. To balance security-energy trade-off, we propose an optimization framework that provides customized recommendations of security strategy to different user devices and base stations. Finally, open issues are discussed on 6G security from an energy efficiency perspective.

## Introduction

With the worldwide commercialization of the fifth generation (5G) cellular network, global interest in the sixth generation (6G) cellular network is starting to grow with the maturity and broad utilization of artificial intelligence (AI). Except for the continuous improvements of data rate, latency, reliability, and network coverage, 6G eyes revolutionary advancement by realizing ubiquitous intelligence as an essential part of 6G architecture [1]. From autonomous network management to a plethora of intelligent services, AI can be deeply involved in the era of 6G from various aspects, such as daily life, industry production, and city governance. Billions of intelligent devices are broadly deployed, covering ground, airborne, underwater, and space regions to interact with the surrounding environment to make decisions anywhere and anytime. Services such as autonomous driving, intelligent robotics, and smart agriculture/industry production can be enhanced by AI-empowered 6G networks without unnecessary human intervention to achieve reduced manual labor and faster response to various demands.

However, the promising 6G network raises a series of security issues due to the increasing autonomy of intelligent services and their deep integration with our daily life [2]. Besides traditional vulnerabilities, attacks on the AI training process bring new challenges to the 6G network. For instance, attackers can inject falsified data into the model training pool to make the learned decision boundary useless. A poisoned model may infect other clients' models in federated learning caused by unsupervised training parameter uploading, integrating, and updating among untrusted users. To this end, adequate security should be guaranteed across billions of connected devices and millions of base stations. Although 5G security schemes [3] already consider different types of attacks, 5G networks often configure security schemes with universal settings (e.g., cryptographic algorithms and their key lengths) in all scenarios.

This one-size-fits-all strategy is easy to launch, but no longer fits 6G security for two reasons. First, user devices in the 6G network have more diverse hardware capabilities and are deployed in more complex environments uncovered by 5G, requiring security to be adapted accordingly. For example, underwater devices usually have more limited power supply than devices on land, so lightweight security schemes are preferred for longer operating time. Second, 5G security lacks adjustment to time-varying attributes, such as a device's remaining battery and application switching. When a device's battery runs low, the security scheme configuration is preferred to have lower complexity for less energy consumption. Considering these two challenges, the selection and configuration of security schemes in the 6G network need to be customized in an adaptive and dynamic manner for various scenarios. Meanwhile, energy efficiency becomes an increasingly critical issue in 6G security. Devices and base stations may have limited power supply to support the implementation of security schemes due

Digital Object Identifier:
10.1109/MCOMSTD.101.2000090

*Shuaiqi Shen, Chong Yu, and Kuan Zhang are with University of Nebraska, Lincoln; Jianbing Ni is with Queen's University; Song Ci is with Tsinghua University.*


2471-2825/21/$25.00 © 2021 IEEE

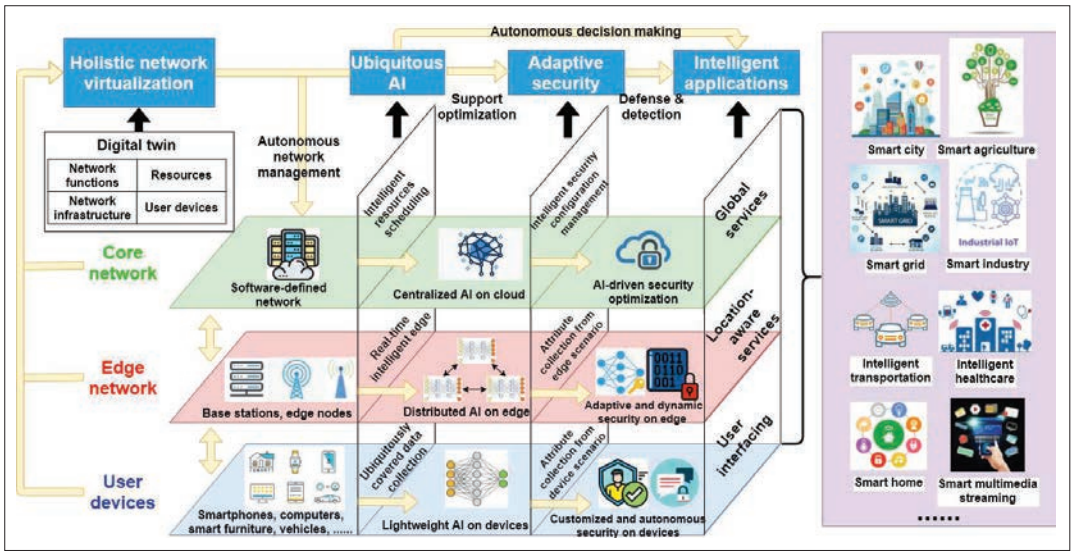


**FIGURE 1.** Proposed AI-empowered architecture of the 6G network.

to their hardware capabilities and physical locations. The high energy consumption also raises the operating cost as a critical obstacle for the future commercialization of the 6G network [4]. The complexity of 6G security solutions should be adjusted for diverse scenarios in response to the heterogeneous network and dynamic operating conditions. Therefore, 6G security should be customized from an energy efficiency perspective while guaranteeing the desired security strength.

In this article, we explore adaptive and dynamic security in the 6G network from an energy efficiency perspective to balance security-energy trade-off in various scenarios. Specifically, we first investigate an AI-empowered architecture of the 6G network and identify promising intelligent applications. Second, we discuss the challenges to optimize the security strategy by identifying emerging security threats and issues when balancing security-energy trade-off from the aspects of heterogeneity, dynamics, and modeling complexity. Then we propose an optimization framework for 6G security that integrates non-additive measure-based attribute selection and complex function approximation for model training. The proposed framework provides adaptive and dynamic security solutions for various scenarios to reduce energy consumption while guaranteeing the desired security strength. Finally, we discuss several open issues about 6G security optimization from the energy efficiency perspective.

The remainder of this article is organized as follows. The following section proposes 6G architecture, promising applications, and key visions. Challenges in 6G security are discussed following that. Then we propose the optimization framework for 6G security. Open research issues are discussed. Finally, the article is concluded.

## Overview of 6G Architecture and Visions

### Architecture for 6G

We present an AI-empowered architecture for the 6G network as illustrated in Fig. 1. Compared to 5G architecture, the 6G network is expected to ubiquitously utilize AI techniques to support intelligent services throughout the core network, edge network, and user devices:

- The core network consists of software defined networking for intelligent resource scheduling and security configuration management. Accurate simulation can be performed on virtualized network infrastructure to collect operating data and identify proper network management strategies. Learning from the simulation data, AI in the core network realizes autonomous network management. Centralized AI is also utilized to make decisions for global services by aggregating model training parameters and data transmitted from the edge network.
- AI can be distributed from the centralized cloud to the edge of a 6G network, such as base stations, for intelligent edge computing, mobility, and handover management, resource orchestration, and task scheduling. To address the insufficiency of data and user privacy issues for edge-assisted AI, federated learning can be employed on edge nodes to collaboratively train distributed AI models for the same problem by aggregating model parameters on the core network. The AI-assisted edge network provides intelligent services with lower latency and location awareness due to the proximity to user devices.
- Billions of heterogeneous user devices are connected to a 6G network, such as smartphones, sensors, and vehicles with different levels of capabilities in computation, storage, and energy. The collected data and user requests are transmitted to base stations on the edge network. Supported by lightweight AI embedded on user devices, intelligent services can be carried out in a more accurate, real-time, and robust manner than in 5G networks.

Based on the AI-empowered architecture, emerging intelligent services can be realized in the 6G network, benefiting daily life, industry production, and city governance. For instance, the

Accurate simulation can be performed on virtualized network infrastructure to collect operating data and identify proper network management strategies. Learning from the simulation data, AI in the core network realizes autonomous network management. Centralized AI is also utilized to make decisions for global services by aggregating model training parameters and data transmitted from the edge network.

Many conventional threats in 6G can be traced back to previous generations, such as DDoS, malware injection, and side channel attack. Meanwhile, the ubiquity of AI increases vulnerabilities of the 6G network to novel threats that target AI availability and integrity.

*Internet of Vehicles* benefits from the broad coverage of 6G that enables seamless connectivity for vehicles, aircraft, and ships to achieve traffic safety and travel efficiency. Although intelligent transportation has been preliminarily realized by 5G networks, the 6G network tends to expand the dimension of vehicle connectivity from ground into space, airborne, and underwater areas [5]. Empowered by blockchain-based techniques, information exchange and data processing among connected vehicles can achieve better decentralization, security, transparency, immutability, and automation properties [6]. The Internet of Vehicles is expected to integrate autonomous driving techniques in the next decade, allowing transportation to be independent of user intervention, so new lifestyles such as mobile working and mobile entertainment become feasible. Furthermore, smart industry can be realized by the digital twin technology emerging in 6G, which creates a virtualized copy of the physical manufacturing environment in cyber space. The digital twin of a factory's production chain includes virtualized workers, machines, raw materials, and the entire life cycle of the product. Based on the historical production data, smart industry performs real-time monitoring and optimization of production policy so that all entities on the production chain can coordinate with the highest efficiency [7]. In addition, more public services for smart city can be realized with the ubiquitous intelligence in the 6G network. With billions of intelligent devices covering space, airborne, ground, and ocean areas, public services can overcome geographic obstacles to achieve balanced distribution of public resources, such as remote medical treatment and remote education [8]. To realize the investigated AI-empowered architecture and promising intelligent applications, the 6G network should be more than just a faster version of 5G, and some revolutionary advancements are expected as visions for 6G.

### Key Visions

**Ubiquitous AI:** In the 6G network, intelligence is expected to be decentralized and distributed to the edge (e.g., base stations) and user devices, due to the availability of big data and great promotion in computing capability [1]. With the development of the Internet of Things (IoT), 5G networks connect numerous smart devices to enhance the quality of human-to-human and human-to-things communications, allowing information to be accessed and shared anywhere and any time. Based on the ubiquity of information, the 6G network intends to achieve ubiquity of intelligence to realize a plethora of intelligent applications and autonomous network management by making decisions with reduced human intervention [9]. Ubiquitous AI is necessary because most scenarios of 6G are diverse and dynamic, requiring customized pattern learning and low latency to provide fast responses. For example, to realize fully autonomous driving, each vehicle needs to learn its own driving pattern according to vehicle status and user preferences, and make real-time driving decisions in response to complex traffic environments. Conventional AI centralized in the cloud can no longer fulfill the demands of 6G services. Decentralized AI techniques, especially edge-assisted intelligence, are expected to play an essential role in the 6G network. Federated learning can be adopted to enhance edge intelligence to address the unbalanced distribution of training data. The local AI models in edge nodes can be trained collaboratively through federated learning to achieve global knowledge discovery.

**Holistic Network Virtualization:** Based on ubiquitous deployment of AI, 6G network management is expected to achieve more intelligent task scheduling and resource orchestration than previous generations. In 5G, the virtualization technique optimizes resource allocation by implementing functions such as load balancing, routing, and security solutions as software instances running on virtual machines. The 6G network is intended to expand the scope of virtualization and softwarization to cover the network infrastructure, user devices, and network resources to realize holistic network virtualization (HNV), in which digital replicas of user devices and base stations are created to represent the corresponding hardware. HNV enables powerful simulation of the entire network infrastructure and numerous user devices to evaluate different network management and resource orchestration strategies. Learning from the accurate and comprehensive data provided by the HNV simulation, ubiquitous AI in 6G can determine network management strategies automatically. Then HNV synchronizes different configurations for network infrastructure and user devices to the physical entities to optimize network performance, such as latency and energy efficiency. Therefore, HNV is considered as a significant vision of 6G for autonomous network management.

## Challenges in 6G Security

Besides the aforementioned visions, adaptive security is also an essential expectation for the 6G network. Although many security vulnerabilities have been addressed in 5G, such as illegal interception of communication channels, compromised access points, privacy leakage, and identity forgery, 6G security encounters new challenges. First, due to the network softwarization and intelligentization, novel threats emerge in 6G that target the AI training process. More powerful security solutions are necessary to handle the emerging AI related threats, such as backdoor embedding and training data poisoning in federated learning [10]. Second, 5G networks lack a universal standard to optimize security strategy in various scenarios to fulfill diverse security demands while reducing corresponding overheads. For instance, when a device's remaining battery runs low, the complexity of employed security schemes should be adjusted for longer operating time of the device. With the increasing heterogeneity, dynamics, and complexity of the 6G network, security should be adaptively customizable for different services, energy conditions, and other time-varying attributes. In this section, we first identify emerging threats in 6G network and then discuss the security issues from an energy efficiency perspective.

### Emerging Threats

Many conventional threats in 6G can be traced back to previous generations, such as distributed denial of service (DDoS), malware injection, and

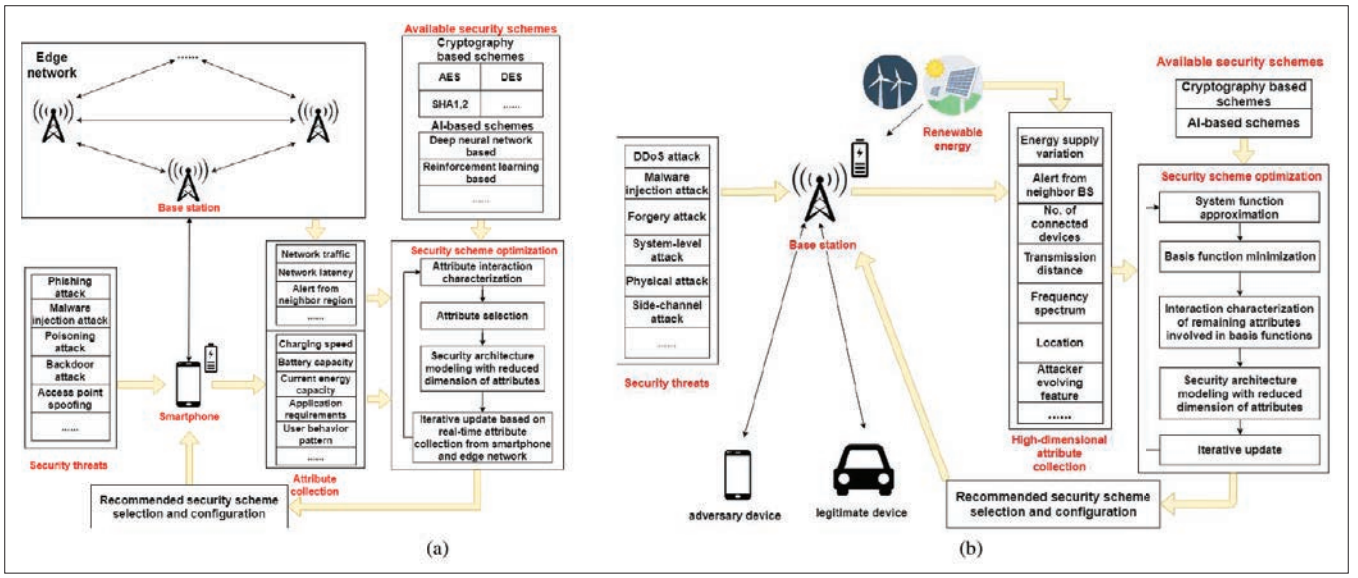


**FIGURE 2.** Scenarios of adaptive and dynamic security optimization for: a) user device; b) base station.

side channel attack. Meanwhile, the ubiquity of AI increases vulnerabilities of the 6G network to novel threats that target AI availability and integrity [11].

Threats on AI Availability: These impede users from using intelligent services and autonomous network management by attacking the availability of intelligence distributed in the edge network and user devices. The AI training processes in the edge nodes and devices are compromised so that no reasonable decisions can be made by deep learning models. For example, a poisoning attack injects falsified data into a user's model training pool to shift a model's decision boundary, causing unreasonable decisions or inaccurate prediction. The injected data is elaborately forged according to the data distribution of the targeted service, so even a minor portion of injection may poison the whole training dataset and cause substantial accuracy drop. As the deep learning model cannot function normally, the AI availability is damaged by attackers.

Threats on AI Integrity: These do not damage AI availability but leave the compromised AI functioning as normal. Instead of injecting falsified training data, the attackers embed backdoor signals into the model without user awareness. By including the backdoor trigger in the input, such as a certain string in file or pixel pattern in image, attackers can leverage the compromised model to provide desired classification or detection outcomes regardless of the actual input data. Compared to 5G, the 6G network is expected to be more vulnerable to backdoor-driven attacks due to the popularity of advanced AI techniques, such as transfer learning and federated learning. For example, transfer learning facilitates users solving their own problems with limited dataset, as users utilize a pre-trained model generated from a relevant problem to refine their own models. If the pre-trained model provided by the third party is inserted through a back door, the entire learning process can be compromised.

When launching an AI-related attack, such as a data poisoning attack or adversarial learning, the attackers first obtain access to the training dataset of AI systems. Many applications collect training data from public users to improve their deep learning models, such as spam email filters. These applications have high vulnerability to AI-related attacks since they can hardly verify the reliability of users' inputs. Once gaining access to the training dataset, attackers have multiple means to compromise the generated AI model from normal functioning. Data poisoning and backdoor installation, as discussed previously, are two common ways to manipulate a trained classifier to provide a false outcome by tampering with its decision boundary. For example, in autonomous driving, vehicles need to recognize stop signs via roadside images by learning from the common patterns of stop sign images in a training dataset. If attackers inject a large volume of stop sign images into the training dataset and label them as green traffic lights, the vehicle classifier may associate the patterns of stop signs with green lights, so it continues driving at the intersection. To this end, AI-related attacks can cause severe damage to user safety and property due to the ubiquity of AI applications in the 6G network. To address the conventional and merging AI-related threats, adequate security should be guaranteed across billions of connected devices and millions of base stations, where the high energy consumption becomes a major obstacle.

## Security Issues from the Energy Perspective

Compared to previous generations, the requirement for energy efficiency takes higher priority in the 6G network to accommodate the sheer volume of limited-power devices and power supply variation from renewable energy. We present two cases of smartphone and base station in Fig. 2 as examples to illustrate the optimization of 6G security strategy to balance the trade-off between security and energy consumption.

Trade-off between Security and Energy Consumption: Users can balance security-energy trade-off by selecting various security schemes and customizing their configurations according to different device capabilities, energy condi-

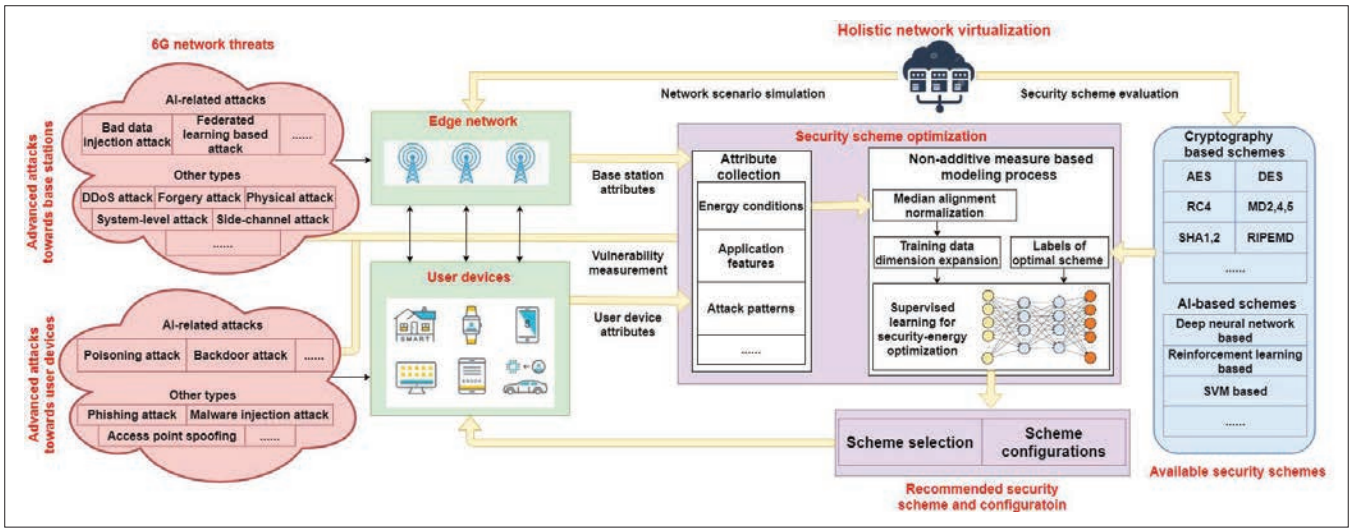


**FIGURE 3.** Proposed optimization framework for security scheme configuration with balanced security-energy trade-off.

tions, attack vulnerabilities, services, and other attributes. In this article, we discuss two major categories of existing security schemes: cryptography-based schemes and AI-based schemes. The first category applies cryptographic keys for security defense tasks, including data encryption, authentication, and digital signatures. By selecting different algorithms, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest Cipher 4 (RC4), and Secure Hash Algorithms (SHA), and adjusting their key lengths, users can adapt the security strength and energy consumption for various scenarios. Schemes of the second category are empowered by AI to detect malicious behaviors, attacker intrusion, and abnormal system status. Different AI techniques, such as deep neural network (DNN), reinforcement learning (RL), and support vector machine (SVM), are utilized to develop existing security schemes. These AI-driven schemes usually consume large amounts of computing resources and energy from the underlying hardware. Since embedded devices and micro edge nodes are widely deployed in the 6G network with diverse properties and resource constraints, the configurations of AI-driven schemes should also be customizable. For example, various configurations need to be determined during model training, such as model structure, training algorithm, and terminating conditions, to find the best possible trade-off between security strength and energy consumption.

Balancing Security-Energy Trade-off: Obtaining the optimal security-energy trade-off in 6G can be much more challenging than in 5G due to the substantially increased heterogeneity, dynamics, and modeling complexity.

*Heterogeneity:* As the 6G network connects a huge volume of devices and base stations with diverse capabilities and working conditions, the one-size-fits-all strategy of 5G is no longer suitable for 6G security. Heterogeneity should be fully considered to determine the optimal security scheme with energy efficiency. The 6G network contains heterogeneous service features, hardware capabilities, communication conditions, power supply, and attack types, leading to highly diverse security demands and energy availability. The balancing of security-energy trade-off should be adaptive to the heterogeneous 6G network.

*Dynamics:* The time-varying nature of the 6G network brings more difficulties to security-energy trade-off balancing due to the variations in security demands and energy availability. Network status variations, such as substantial changes in transmission traffic or latency, and attacking alerts raised by neighbor base stations or devices, may occur from time to time. The power supply condition is also time-varying: for devices such as smartphones, battery can have low capacity, so powerful security schemes may be restricted for longer operating time; for base stations, renewable energy such as wind and solar power also have supply fluctuation. Thus, the selection and configuration of security schemes should be updated iteratively to address the dynamics in the 6G network.

*Modeling Complexity:* A large number of attributes, as presented in Fig. 2, can be derived from the aspects of service features, hardware capabilities, network operating conditions, energy status, and attack vulnerabilities. Modeling the relation between numerous attributes and desired security strategy can be quite complex in balancing the security-energy trade-off. The modeling process for security optimization should be lightweight so that the additional overhead does not counteract the advantages in energy efficiency achieved by the proposed framework for 6G security. Therefore, reducing modeling complexity is a critical challenge for 6G security optimization.

To address these challenges in balancing security-energy trade-off, we propose a dynamic and lightweight optimization framework for adaptive security in the 6G network.

## Optimization Framework for Security-Energy Trade-off

### Overview of the Proposed Framework

The proposed optimization framework has three design principles. First, the generated optimization model should be adaptive to various scenarios in edge network and user devices to

| Collected attributes | Value |
|---|---|
| Application | Online banking |
| AI utilization | Biometric identification |
| Battery capacity | 6400 mAh |
| Remaining capacity (%) | 80% |
| Charging speed | 65 W |
| Charged or not | No |
| No. of threads | 6 |
| Location | Urban |
| Attack type | DDoS |
| No. of neighbor attack detections | 3 |
| Network latency | 700 ms |
| Network traffic | 1000 Mb/s |
| … | … |
| **Security strategy** | **Configuration** |
| Cryptography-based scheme | AES |
| Cryptographic key length | 1024 bits |
| … | … |

**TABLE 1.** Example of collected attributes and security strategy applied as training data in the optimization framework.

customize a security scheme for a specific base station or device from the energy efficiency perspective. Second, the framework should address the dynamics of the 6G network by iteratively updating the optimization model and providing real-time recommendations for security scheme selection and configuration. Third, the framework should be lightweight so that it does not cause excessive overhead and energy consumption to 6G security. The overview of the proposed framework is presented in Fig. 3. Attributes are collected from the edge network, user devices, and security threats to indicate network conditions, device/base station status, energy status, and other information. HNV can provide sufficient training data to the proposed framework through accurate simulation of various network scenarios. By proactively introducing attacks to the simulated network, different security schemes and their configurations can be evaluated in metrics such as encryption strength, detection rate, and energy consumption. Then an optimal security scheme can be determined to balance security-energy trade-off given the pre-determined user demands on energy efficiency. For instance, a user can require CPU usage of a security scheme to be less than a percentage if remaining energy capacity is between *b* and *c* percentage so that user demands can be formulated as piece-wise functions. Table 1 shows an example of a training sample including the collected attributes and corresponding security strategies that are derived from network simulation for the subsequent modeling process.

Empowered by AI, the proposed framework involves all the related attributes as training data

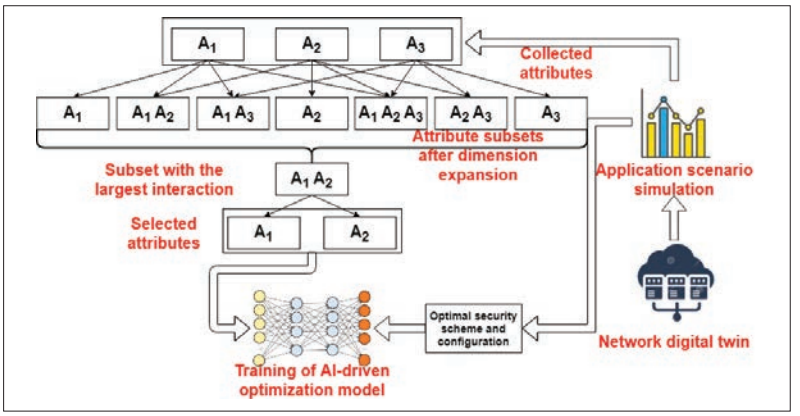


**FIGURE 4.** Non-additive measure-based modeling process for the optimization model.

and learn their relations with recommended scheme selection and configurations, leading to high modeling complexity. Since 6G security optimization aims to achieve energy-efficient security, the additional energy consumption caused by the modeling process needs to be restricted. A non-additive measure-based modeling approach is proposed to reduce the computational complexity while guaranteeing the accuracy of the generated optimization model. By characterizing the interactions among attributes on determining the optimization outcome, the proposed modeling approach selects significant attributes for subsequent supervised learning to generate the optimization model. More details on the non-additive measure-based modeling and attribute selection can be found in our prior work [12]. As illustrated in Fig. 4, attributes collected from the simulation are expanded into the power set of the original attribute set. The interaction of each attribute subset is measured to indicate the aggregated impacts of subset elements on optimization outcomes. The larger interaction implies a greater contribution made by the subset to security-energy trade-off balancing. Only attributes belonging to the subset with the largest interaction are selected for AI-driven optimization model training so that the model complexity can be substantially reduced. After generating the optimization model with the training data provided by HNV-based simulation, the proposed framework iteratively provides real-time recommendation of security scheme selection and configuration. To this end, different devices and base stations in the 6G network can customize their security schemes to reach optimal security-energy trade-off according to users' demands.

## Security Optimization in Various Scenarios

The AI-empowered optimization framework models the relation between collected attributes and recommended selection and configurations for security schemes. The security-energy trade-offs for various scenarios are balanced in an adaptive and dynamic manner. For instance, the hardware capabilities in computation and communication may also affect security optimization, since the additional overhead and latency caused by the security scheme should be constrained. Various power supply types, such as wired charging, wire-

By minimizing the number of basis functions for approximation, the attributes involved in the remaining basis functions can be selected for the first round. Then the modeling approach processes the attributes with reduced dimension with interaction characterization to select attributes for the second round. The optimization model is updated iteratively to provide the optimal security scheme solution to the base station in real time.

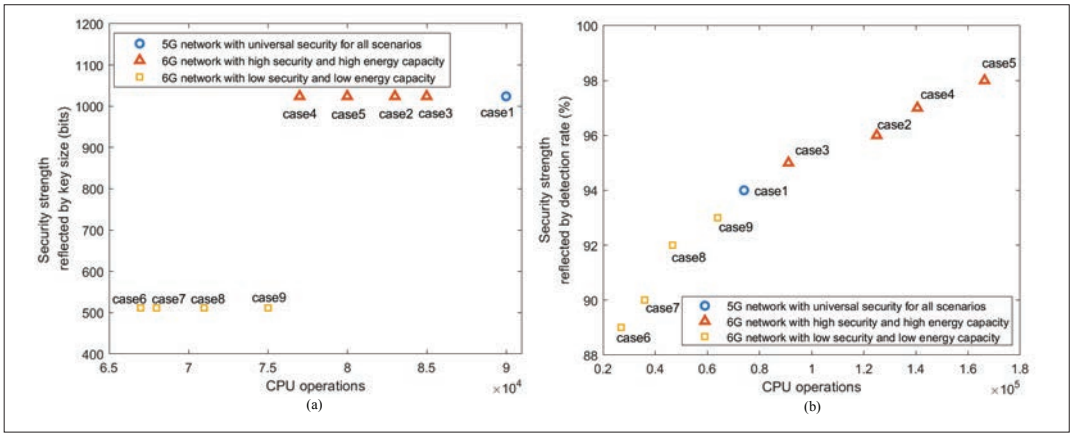


**FIGURE 5.** Simulation results of security-energy trade-off balancing in various scenarios for different intelligent services and energy capacities in 5G and 6G networks for: a) cryptography-based scheme; b) AI-driven scheme. The 9 cases represent: (1) 5G network; (2) smartphone for online banking; (3) smartphone with high battery capacity; (4) base station for online banking; (5) base station with high battery capacity; (6) smartphone for video streaming; (7) smartphone with low battery capacity; (8) base station for video streaming; (9) base station with low battery capacity.

less charging, and renewable energy, provide different energy capacities and charging speeds for user devices and base stations. Under different energy conditions, the complexity of security schemes should be customized adaptively. The vulnerability to different attacks can affect security scheme optimization due to heterogeneity in attack characteristics. Recognizing a compromised edge node requires more complex AI-driven schemes than detecting DDoS attacks. In addition, not only the 6G network but also attackers are empowered by AI techniques to evolve themselves by learning from previous malicious activities. Security schemes should be continuously improved against the evolving attackers, changing the trade-off between security strength and energy consumption.

To illustrate the proposed framework in detail, we present two cases of smartphone and base station. In Fig. 2a, the smartphone collects attributes from security threats, energy condition, device status, service features, and information from base stations in neighboring regions. The attributes are transmitted to the proposed optimization framework and selected based on attribute interaction characterization to reduce model training complexity. The solution is selected from available security schemes and configured to achieve optimal security-energy trade-off for the smartphone. For instance, when the smartphone has high energy capacity, the length of cryptographic key for data encryption can be long (e.g., 1024-bit) for high encryption strength. When energy capacity becomes low, the key length may be shortened (e.g., 512-bit) as a compromise for lower computational overhead and longer operating time. In Fig. 2b, the case switches to a base station, which has more adequate power supply and higher priority for security than a smartphone, and it may select a more sophisticated scheme and complex configuration. Security schemes on base stations are optimized with different sets of attributes, including services, attack vulnerabilities, hardware capabilities, user demands, network environments, and other time-varying attributes. Since base stations utilize renewable energy as partial power source, the variation in renewable energy supply is also involved as a significant indicator for energy condition. Moreover, additional attributes, such as attacking alert from neighbor nodes, metrics on network communication, and status of connected devices, may also impact security-energy trade-off. In this case, the attribute collection for base station tends to be higher-dimensional than user devices. To facilitate interaction characterization with a large number of attributes, function approximation is integrated with the proposed modeling approach. By formulating the optimal solution of security schemes as a function of attributes, we approximate the complex relation into a series of simpler Fourier basis functions. By minimizing the number of basis functions for approximation, the attributes involved in the remaining basis functions can be selected for the first round. Then the modeling approach processes the attributes with reduced dimension with interaction characterization to select attributes for the second round. The optimization model is updated iteratively to provide an optimal security scheme solution to the base station in real time.

## Simulation Results

We conduct extensive simulations on security scheme optimization to validate the effectiveness of our proposed framework for balancing the security-energy trade-off in the scenarios of *smartphone* and *base station*, respectively. In both scenarios, security strength and energy consumption are compared with and without the proposed optimization framework under various services and energy conditions. The applied services include *online banking* and *video streaming*, representing different demands on security strength. The battery conditions include cases of *high* and *low* capacity. Both the *cryptography-based scheme* [13] and *AI-driven scheme* [14] are evaluated in the simulation. We use key size to reflect the strength of cryptography-based schemes and detection rate to evaluate the performance of AI-driven schemes. The energy consumption is estimated with the number of CPU operations

required by the security scheme. As shown in Fig. 5a, the energy consumption and security strength of the cryptography-based scheme are presented as coordinates and can be clustered into groups 1, 2, and 3, shown as circles, triangles, and squares, respectively. Group 2 represents the cases with high security demands and high energy capacity in the 6G network. The corresponding schemes of group 2 utilize longer keys and consume more CPU operations than group 3, as group 3 has low security demands and low energy capacities. In comparison, group 1 represents the 5G security and has no other points for different cases due to its universal configurations. Since we utilize key size as the metric of security strength for cryptography-based schemes, the selected key sizes are 1024-bit and 512-bit in the simulation results. To this end, the 5G security scheme has the highest energy consumption in all cases, even though the security demands and energy capacities are low. Similarly, as shown in Fig. 5b, the coordinates of security scheme metrics in different cases can also be clustered into the same three groups as in Fig. 5a. As detection rate is used as the metric of security strength for AI-driven schemes, the increment of security strength is more obvious in Fig. 5b than in Fig. 5a. Higher CPU operations lead to better security strength, which can be adjusted for 6G security schemes according to different security demands and energy capacities. The group for 5G security is in the middle with only one point, since it adopts only one universal configuration. The simulation results validate that for both smartphones and base stations, and both categories of security schemes, the proposed framework can customize 6G network security to balance the security-energy trade-off. Compared to 5G security, which applies universal configurations for all scenarios, 6G security is adaptive to different services and energy conditions. Therefore, the proposed framework can effectively optimize security in the 6G network from an energy efficiency perspective.

## Open Issues for 6G Security

As the 6G network is still in its infancy, many open issues remain to be resolved in the future research for 6G security:

- First, a promising direction is to optimize security strategy with the awareness of the holistic network situation. In the proposed framework, security is customized based on operating data collected from devices and neighbor edge nodes. In the future, the situation awareness can be expanded to a holistic network so that security-related information can be shared among devices and base stations throughout the network infrastructure to predict, analyze, and respond to attacks in a real-time and cooperative manner. A global platform needs to be established for information sharing among various devices and edge nodes. More subsequent concerns will emerge: what information should be shared and analyzed to reduce transmission overhead and learning complexity, and how to protect user privacy during information sharing.
- Second, the attack vulnerabilities in the 6G network should be quantitatively measured so that the demands for security strength can be determined more accurately for optimizing security strategy. The evolution and variation of attacks should also be considered, since attackers may be empowered by AI to learn from the previous activities to bypass the detection of current security solutions. The vulnerability assessment for false data injection attack has been explored in 6G-enabled smart grid based on deep learning techniques [15]. In the future, more research efforts are needed to establish a universal standard of vulnerability measurement for various attacks to different devices, edge nodes, and services.
- Finally, the relation between security schemes and energy consumption needs to be further investigated. Currently, the energy consumption of security schemes are estimated through CPU usage information. In the future, the estimation should be extended from system level to physical level so that energy status can be collected from hardware directly. By monitoring the actual energy capacity changes, we may infer the corresponding operations executed by security schemes, such as homomorphic encryption and secure multi-party computation. If a more accurate and direct security-energy relation can be established, we may obtain a deeper insight on 6G security from the energy efficiency perspective.

The relation between security schemes and energy consumption needs to be further investigated. Currently, the energy consumption of security schemes is estimated through CPU usage information. In the future, the estimation should be extended from system level to physical level so that energy status can be collected from hardware directly.

## Conclusion

In this article, we have explored adaptive and dynamic security in the 6G network from an energy efficiency perspective. We have first investigated an AI-empowered 6G architecture with promising applications and visions. Then we have discussed emerging security threats for 6G and the challenges in optimizing security strategy from the aspects of heterogeneity, dynamics, and modeling complexity. In addition, we have proposed an optimization framework to address the identified challenges. The proposed framework optimizes security scheme selection and configurations to balance the security-energy trade-off in various scenarios. Finally, open issues for 6G security have been discussed.

### Acknowledgments

This work is partly supported by the S&T Major Project of Inner Mongolia Autonomous Region under grant number 2020ZD0018 and by the State Key Laboratory for Safety Control and Simulation of Power Systems and Large Power Generation Equipment under grant number SKLD20Z02.

### References

[1] M. Giordani *et al.*, "Toward 6G Networks: Use Cases and Technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, Mar. 2020, pp. 55–61.
[2] K. Letaief *et al.*, "The Roadmap to 6G: AI Empowered Wireless Networks," *IEEE Commun. Mag.*, vol. 57, no. 8, Aug. 2019, pp. 84–90.
[3] Z. Zhang *et al.*, "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," *IEEE Vehic. Technology Mag.*, vol. 14, no. 3, 2019, pp. 28–41.
[4] I. Ahmad *et al.*, "Overview of 5G sEcurity Challenges and Solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, Jan. 2018, pp. 36–43.
[5] S. Shen *et al.*, "Security in Edge-Assisted Internet of Things: Challenges and Solutions," *Science China Info. Sciences*, vol. 63, no. 12, 2020, pp. 1–14.

[6] A. Al-Dulaimi and X. Lin, "Reshaping Autonomous Driving for the 6G Era," *IEEE Commun. Standards Mag.*, vol. 4, no. 1, Jan. 2020.
[7] M. Mollah *et al.*, "Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey," *IEEE Internet of Things J.*, vol. 8, no. 6, 2020, pp. 4157–85.
[8] Q. Bi, "Ten Trends in the Cellular Industry and an Outlook on 6G," *IEEE Commun. Mag.*, vol. 57, no. 12, Dec. 2019, pp. 31–36.
[9] F. Tariq *et al.*, "A Speculative Study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, Aug. 2020, pp. 118–25.
[10] J. Zhang *et al.*, "PoisonGAN: Generative Poisoning Attacks Against Federated Learning in Edge Computing Systems," *IEEE Internet of Things J.*, vol. 8, no. 5, 2020, pp. 3310–22.
[11] N. Kato *et al.*, "Ten Challenges in Advancing Machine Learning Technologies Toward 6G," *IEEE Wireless Commun.*, vol. 27, no. 3, June 2020, pp. 96–103.
[12] S. Shen *et al.*, "Toward Fast and Accurate SOH Prediction for Lithium-Ion Batteries," *IEEE Trans. Energy Conversion*, vol. 36, no. 3, Sept. 2021, pp. 2036–46.
[13] K. Zhang *et al.*, "Security and Privacy for Mobile Healthcare Networks: From a Quality of Protection Perspective," *IEEE Wireless Commun.*, vol. 22, no. 4, Aug. 2015, pp. 104–12.
[14] N. Mowla *et al.*, "AFRL: Adaptive Federated Reinforcement Learning for Intelligent Jamming Defense in FANET," *J. Commun. Networks*, vol. 22, no. 3, 2020, pp. 244–58.
[15] M. Tariq *et al.*, "Vulnerability Assessment of 6G-Enabled Smart Grid Cyber-Physical Systems," *IEEE Internet of Things J.*, vol. 8, no. 7, 2020, pp. 5468–75.

## Biographies

Shuaiqi Shen [STM'21] (sshen@huskers.unl.edu) received his B.Sc. degree in electronic and information engineering from Hong Kong Polytechnic University in 2016. He obtained his M.Phil. degree in system engineering and engineering management from the Chinese University of Hong Kong in 2018. Currently, he is working toward a Ph.D. degree at the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln. His research interests include energy-efficient distributed learning, edge intelligence, and cyber security.

Chong Yu [STM'21] (cyu6@huskers.unl.edu) received her B.Sc. degree in communication engineering and M.Sc. degree in communication and information system from Northeastern University, Shenyang, China, in 2015 and 2017, respectively. She is working toward a Ph.D. degree in the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln. Her research interests include the Intelligent Internet of Things, cybersecurity, intelligent vehicle, cloud/edge computing, and machine learning.

Kuan Zhang [S'13-M'17] (kuan.zhang@unl.edu) is an assistant professor in the Department of Electrical and Computer Engineering at the University of Nebraska–Lincoln In 2016, He received his Ph.D. degree from the University of Waterloo, Canada, in electrical and computer engineering. He has published over 100 papers in journals and conferences. He was the recipient of Best Paper Award in IEEE WCNC 2013, Securecomm 2016, and IEE ICC 2020. His research interests include cyber security, big data, and cloud/edge computing.

Jianbing Ni [M'18] (jianbing.ni@queensu.ca) is currently an assistant professor with the Department of Electrical and Computer Engineering, Queen's University, Kingston, Canada. He received his Ph.D. degree in electrical and computer engineering from the University of Waterloo in 2018. His research interests are applied cryptography and network security, with current focus on edge computing, mobile crowdsensing, the Internet of Things, and blockchain technology.

Song Ci [SM] (sci@tsinghua.edu.cn) received his Ph.D. degree from the Department of Electrical Engineering, University of Nebraska-Lincoln. His current research interests include large-scale dynamic complex system modeling and optimization as well as its applications in the areas of the Internet and Energy Internet, especially in energy digitization and digital battery energy storage.