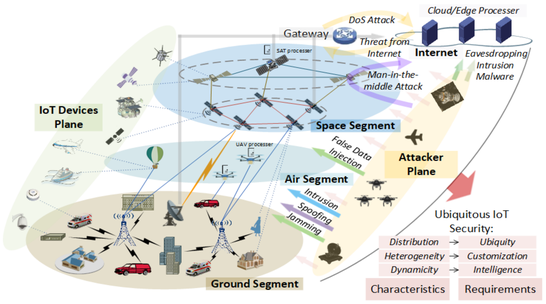
TOWARDS HIGH-SECURITY UBIQUITOUS IOT NETWORKS USING AI

Neng Ye[⋆] *Bichen Kang*[⋆] *Bin Qi*[†] *Xiangyuan Bu*[†] *Jianping An*[⋆]

[⋆] School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing
[†]School of Information and Electronics, Beijing Institute of Technology, Beijing

Introduction



An illustration of ubiquitous IoT networks and its security threats.

The on-going paradigm shift knocking on the door of future wireless communication system is ubiquitous Internet of Things (IoT), and the maturity of which will be hindered by the challenges related to security:

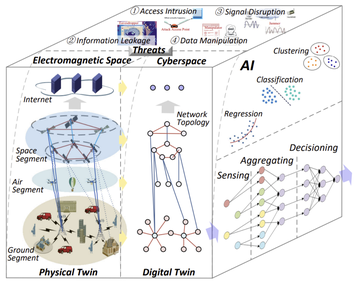
- **Open propagation environments:** The space-ground and air-ground propagation links in ubiquitous IoT have the characteristics of openness and broadcasting [2], which make the data transmissions easier to be exposed to threats such as jamming and eavesdropping.
- **Large channel dynamics:** Large dynamic propagation channels and large round-trip delay caused by ubiquitous connectivity limit the secrecy related signaling interactions between the end devices and the network side [5].
- **Diversified IoT services:** The heterogeneousness of ubiquitous IoT requires a multiplicity of access control and a interoperability of network segments [1], which cause IoT networks increasingly vulnerable.
- **Low-capability IoT devices:** The devices served by ubiquitous IoT are deployed in remote areas and cannot be recollected or recharged, which restricts the deployment of conventional security protocol [4,6].

Vulnerabilities for Ubiquitous IOT

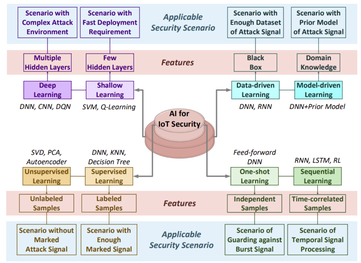
- **Access Intrusion:** Due to the wide spreading devices and the heterogeneous data types, the intrusion to the access links is a critical vulnerability to ubiquitous IoT. Denial of service (DoS) attack is typical on the network infrastructure, where the perpetrator seeks to make intensive access requests to exhaust the network resources.
- **Information Leakage:** The openness of wireless propagation links make it impressionable to information capture attacks [3]. The man-in-the-middle attacker intercepts communication links between two legitimate devices to steal data, and the spoofing attacker impersonates a legitimate device to initiate attacks against gateway, eavesdrop data, spread malware or bypass access control.
- **Signal Disruption:** The signal disruption attack targets to damage the signals conveyed by ubiquitous IoT network, usually performed by viciously adding a strong interfering signal on the transmission links. Typical measures of signal disruption include jamming and DoS attack [4]. The large propagation distance in space-ground links has weaken the signal strength, which makes the disruption much easier than that in the conventional communication networks [2].
- **Data Manipulation:** Data manipulation is a category of attacks that manipulate the electromagnetic signal or digital data so as to falsify the final processing results, including man-in-the-middle attack, spoofing attack and Sybil attack [5]. The Sybil attacker aims to ruin the reputation system of the IoT network by fabricating massive pseudonymous identities.

AI Paradigm for Safeguarding Security

- **Shallow vs Deep Learning:** Shallow learning normally holds higher data processing speed, while deep learning with strong self-learning ability can extract the in-depth features of the attack signals.
- **Supervised vs Unsupervised Learning:** The common supervised learning methods include Bayesian classification, KNN, SVM, DT, and DNN. Single-value decomposition (SVD), PCA, clustering and deep autoencoder (DAE) are commonly used unsupervised learning methods.
- **Data-Driven vs Model-Driven Learning:** When precise knowledge of attack signals is lacking, data-driven methods can be exploited to accurate models. When the prior structure of the attack signal is evident, model-driven methods are suitable.
- **One-Shot vs Sequential Learning:** One-shot learning is appropriate to deal with burst attack signal. Sequential learning is suitable when there exists relationship between the attack signals in a time series.



3D illustration of security challenges and AI solutions



Technical features and applicable security scenarios

Cyberspace Security Via AI

The cyberspace is the virtual space formed by digital mappings of IoT devices and data, and the security can be improved by deploying sophisticated AI methods on the upper layers, which will be introduced in this part. At a glance, we also summarize the AI-based security measures in Table.

A summary of potential AI methods for cyberspace space security

Contents		Security Techniques	Potential AI Methods
Cyberspace Security	Reactive Approaches	Authentication	SVM, DNN, Q-learning, DQN
		DoS Attack Detection	SVM, DNN, Q-Learning
		Malware Attack Detection	Q-learning, DT, KNN
		Anti-Eavesdropping	Q-learning, Non-parametric Bayesian
	Proactive Approaches	Access Control	DNN, RL, Multi-task Learning
		Security Protocol	LSTM
		Encryption	Cycle-GAN

Electromagnetic Space Security Via AI

The electromagnetic space security, also known as physical layer security (PLS), exploits the specificities of physical signals or channels for attack detection and secure transmission. As summarized in Table, this article studies the AI-enhanced electromagnetic space security measures.

A summary of potential AI methods for electromagnetic space security

Contents		Security Techniques	Potential AI Methods
Electromagnetic Space Security	Reactive Approaches	Intrusion Detection and Countermeasure	SVM, KNN, DT, DNN
		Jamming Observation and Resistance	DNN, RL
	Proactive Approaches	Secure Transmission	DNN, LSTM, Unsupervised learning
		Physical-Layer Authentication	SVM, KNN, DT, CNN
		Physical-Layer Encryption	SVM, Distributed DNN, DAE
		Covert Transmission	DNN, RL

Conclusion and Future Direction

In this article, we have considered the AI technology as the new paradigm for security enhancement, and investigated reactive and proactive AI techniques in both cyberspace and electromagnetic space. However, there are still many open challenges for ubiquitous IoT security.

- Existing AI methods normally require tedious communication interactions or extensive computation overheads. New AI methods such as meta-learning should be investigated for low-cost security.
- Existing methods isolate the security designs of physical layer and upper layers. The ability of AI in end-to-end optimization should be utilized for cross-layer design to exploit their joint benefits.
- As AI technology itself has been shown to be vulnerable to adversarial techniques in some applications, the security of AI itself in ubiquitous IoT should be further enhanced.

References

[1] J. An, K. Yang, J. Wu, N. Ye, S. Guo, and Z. Liao, "Achieving Sustainable Ultra-Dense Heterogeneous Networks for 5G," IEEE Commun. Mag., vol. 55, no. 12, pp. 84-90, Dec. 2017.

[2] T. Hong, W. Zhao, R. Liu, and M. Kadoch, "Space-AirGround IoT Network and Related Key Technologies," IEEE Wireless Commun., vol. 27, no. 2, pp. 96-104, Apr. 2020.

[3] M. Al-Hawawreh, N. Moustafa, S. Garg and M. S. Hossain, "Deep Learning-Enabled Threat Intelligence Scheme in the Internet of Things Networks," IEEE Trans. Netw. Sci. Eng., vol. 8, no. 4, pp. 2968-2981, Oct.-Dec. 2021.

[4] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," IEEE Signal Process Mag., vol. 35, no. 5, pp. 41-49, Sept. 2018.

[5] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 1686-1721, third-quarter 2020.

[6] N. Ye, X. Li, H. Yu, L. Zhao, W. Liu, and X. Hou, "DeepNOMA: A Unified Framework for NOMA Using Deep Multi-Task Learning," IEEE Trans. Wireless Commun., vol. 19, no. 4, pp. 2208-2225, Apr. 20