EUROPEAN OPEN SCIENCE SPACE

Section: Information Technology, Cyber Security and Computer Engineering

THE U.S. ARMY'S ROLE IN ADVANCING MOBILE MESH NETWORKS: HISTORICAL EVOLUTION, TECHNOLOGICAL TRANSFORMATION, AND PRACTICAL APPLICATIONS

Vertebnyi Maksym
Master's degree
Shapovalova Olena
PhD, Assoc. Prof.
Educational and Scientific Institute of Information Technologies
Department of Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics, Ukraine

Abstract

Mobile mesh networks have emerged as a transformative innovation, revolutionizing communication in environments characterized by limited infrastructure. The U.S. Army has played a pivotal role in advancing this technology, leveraging it for tactical operations while fostering its adoption in civilian contexts. This study delves into the historical trajectory, technological evolution, military and civilian utilizations, and security vulnerabilities associated with mobile mesh networks.

Keywords: Mesh networks, MANET, ATAK, U.S. Army, cybersecurity, IoT, mobile communications

Historical Context and Contributions of the U.S. Army

The U.S. Army's pursuit of robust and adaptive communication systems, particularly for scenarios where conventional infrastructure was infeasible, catalyzed the exploration of distributed networking technologies. In the 1970s, the Defense Advanced Research Projects Agency (DARPA) initiated research into Mobile Ad Hoc Networks (MANETs), which enabled devices to establish dynamic, decentralized connections without reliance on centralized nodes. This innovation became critical for ensuring real-time communication under unpredictable conditions [2].

Programs such as the Global Mobile Information Systems (GloMo) and Wireless Network After Next (WNaN) epitomized advancements in dynamic data exchange and network resilience. Another landmark initiative, the Combat Service Support Automated Information Systems Interface (CAISI), facilitated the development of one of the largest tactical mesh networks globally, comprising over 40,000 devices. These initiatives underscored the indispensable role of mobile mesh networks in modern military operations, particularly under high-stakes scenarios [1].

Military Applications and Tactical Innovations

Mobile mesh networks have been integral to enhancing operational effectiveness in military contexts. Integration with reconnaissance systems, such as Unmanned Aerial Vehicles (UAVs), has amplified situational awareness by enabling seamless communication among ground forces, aerial assets, and command units. The Android Tactical Assault Kit (ATAK), leveraging mesh connectivity, exemplifies such advancements, fostering synchronized operations in dynamic combat zones [1].

Moreover, telemedicine applications have enabled field units to transmit critical medical data to remote specialists, facilitating timely, life-saving interventions. Temporary, self-dissolving "short-lived nodes" represent another innovative deployment, wherein ephemeral networks enable secure and rapid data transfer before adversarial detection becomes feasible. This adaptability underscores the strategic value of mesh technologies in contested environments [2].

Transitioning to Civilian Domains

The robustness and self-organizing attributes of military-grade mesh networks have rendered them invaluable in civilian sectors. Urban planners have adopted these networks to enable smart city infrastructure, integrating Internet of Things (IoT) devices for traffic management and public safety. For instance, San Jose leveraged mesh networks to optimize its urban transportation systems and bolster emergency response capabilities [4].

In disaster response scenarios, mesh networks have proven indispensable by maintaining connectivity when conventional networks failed. Technologies such as goTenna have empowered rescue teams to coordinate effectively under adverse conditions. Furthermore, the proliferation of consumer-level mesh systems, including those developed by Google and Eero, highlights the growing mainstream adoption of this technology to ensure consistent connectivity across residential and commercial environments [8].

Comparative Analysis of Mesh Networks: Historical and Technological Advancements

Table 1 - Comparison of major mesh network technologies, focusing on their historical context, technological capabilities, and encryption improvements [1-3]

Network System	Era	Applications	Encryption
MANET (DARPA)	1970s	Military communications	Basic encryption
GloMo	1990s	Dynamic data exchange	Enhanced cryptographic protocols
WNaN	2000s	Resilient tactical networks	Real-time encryption algorithms
CAISI	Early 2010s	Logistics and medical data transfer	WPA2 with secure keys
ATAK	Late 2010s	Battlefield situational awareness	AES-256 encryption
Smart City Networks	2020s	Urban management and IoT connectivity	WPA3 and secure tunnels

*data generated by the author [1]

These systems underscore a progressive enhancement in mesh network capabilities, reflecting the U.S. Army's focus on integrating cutting-edge encryption methods to protect sensitive data (table 1).

Challenges and Security Implications

Despite their numerous advantages, the decentralized architecture of mesh networks introduces significant cybersecurity vulnerabilities. Key threats include man-in-the-middle attacks, where malicious actors intercept and manipulate communications between nodes, and Sybil attacks, wherein adversaries use falsified identities to disrupt network integrity. This vulnerability has become evident in examples such as the Evil Twin attack, where malicious nodes masqueraded as legitimate access points [9]. Examples such as the 2016 Mirai Botnet attack highlight the exploitation of IoT devices in mesh configurations, resulting in large-scale distributed denial-of-service (DDoS) incidents [7].

Emerging attack vectors, including device spoofing, further underscore the necessity for advanced security measures. For example, injecting false data into vehicular communication systems can induce traffic disruptions, while similar tactics against smart grids compromise infrastructure reliability.

Future Directions and Technological Innovations

To address the vulnerabilities inherent in mesh networks, researchers are increasingly focusing on enhanced cryptographic protocols and real-time monitoring systems. Automated intrusion detection mechanisms and advancements in quantum communication hold promise for achieving unbreakable encryption, ensuring data authenticity and resilience against sophisticated attacks [5].

The sustained efforts of military institutions in refining mesh network technologies underscore their strategic importance. As these innovations permeate civilian domains, challenges such as energy efficiency, interoperability standards, and privacy concerns must be addressed. The evolution of mesh networks continues to redefine global connectivity, bridging gaps between military exigencies and civilian necessities.

Conclusion

The development of mobile mesh networks represents a cornerstone in the evolution of communication technologies, with the U.S. Army at the forefront of this paradigm shift. From enabling secure military operations to enhancing disaster response and urban management, mesh networks demonstrate unparalleled versatility. However, addressing their inherent vulnerabilities is imperative for unlocking their full potential and ensuring their sustainable integration into broader technological ecosystems [3-6].

References

1. Naval Postgraduate School. (2020). Networks that don't exist expand the boundaries of battlefield communication. Naval Postgraduate School. Retrieved from https://nps.edu
2. Smith, J. (2022). Military tactics and the future of mobile communications. All About Circuits. Retrieved from https://www.allaboutcircuits.com

3. U.S. Army Public Relations. (2021). The integrated tactical network: Transforming battlefield communications. Army University Press. Retrieved from https://www.armyupress.army.mil
4. FedTech Magazine. (2021). How mesh networks extend military communication. FedTech Magazine. Retrieved from https://fedtechmagazine.com
5. DARPA. (2018). Wireless networks after next: Enhancing battlefield communication. Defense Advanced Research Projects Agency. Retrieved from https://www.darpa.mil
6. Inovasense. (2023). IoT security: 15 types of attacks with real-world examples. Inovasense. Retrieved from https://www.inovasense.com
7. Kanpur IIT. (2023). Wireless network hacking: Identifying and exploiting vulnerabilities in wireless networks. E&ICT Academy. Retrieved from https://eicta.iitk.ac.in
8. IFSEC Global. (2018). How mesh networks can isolate cyber breaches in smart cities and critical infrastructure. IFSEC Global. Retrieved from https://www.ifsecglobal.com
9. AUT Repository. (2016). Evaluation of network attacks in wireless mesh networks. AUT Open Repository. Retrieved from https://openrepository.aut.ac.nz

APPLICATION OF MACHINE LEARNING METHODS FOR ANALYSIS NETWORK TRAFFIC STRUCTURES

Ostrovska Kateryna
Ph.D., associate professor, associate professor
Bak Dmitry
master's degree, specialty "Computer science"
Department of Information Technologies and Systems
Ukrainian State University of Science and Technology

In the modern world, the Internet plays an important role in the lives of people and organizations. It allows you to exchange information, conduct business, learn and have fun. However, with the increase in the number of users and the volume of transmitted data, there is a need to analyze and optimize Internet traffic. In this context, machine learning becomes an important tool for traffic analysis and forecasting.

Neural networks are a powerful tool that is used in various fields, including computer vision, speech recognition, and natural language processing. They are able to learn on large volumes of data and will reveal complex patterns that may not be obvious to a person. Machine learning also allows you to create algorithms that help self-learning and adapt to new data, which makes them especially useful for network traffic analysis.