5G Femtocell-Drone Interconnected Tactical Network: Topological Avoidance and Adaptive Architecture

Kwangmin Yoo
Department of Information Security
Sejong Univ
Seoul, South Korea
ceang14@gmail.com

Ki-Woong Park*
Department of Information Security
Sejong University,
Seoul 05006, South Korea
woongbak@sejong.ac.

Abstract Modern warfare demands tactical networks that can survive rapid Electronic Warfare adaptation. This study proposes a 5G Femtocell Drone Interconnected architecture utilizing Integrated Access and Backhaul and Network Slicing to establish self healing connectivity without wired infrastructure. The system addresses scalability and precision challenges through a Group Handover scheme and an adaptive navigation fusion of PTPsec and Visual Inertial Odometry. Furthermore, context aware Adaptive Policies are implemented to balance Zero Trust security with rapid network recovery. Simulation results confirm that this approach reduces signaling overhead by 86 percent and shortens link recovery time by 57 percent, effectively satisfying tactical requirements for survivability and cognitive superiority in GPS denied environments.

Keywords: 5G Tactical Network, Electronic Warfare (EW), Integrated Access and Backhaul, Group Handover, Zero Trust Architecture, Network Slicing

I. INTRODUCTION

The aspect of the 21st-century battlefield is rapidly shifting from traditional Conventional Warfare, which emphasized physical destructive power, to Hybrid Warfare, where information superiority and network survivability determine victory or defeat. In particular, the Ukraine-Russia war demonstrated a new form of conflict where Commercial Off-The-Shelf (COTS) technologies and military doctrines are fused, and the combination of drones (UAVs) and Electronic Warfare poses a serious challenge to existing tactical communication systems.

Past tactical communication networks relied on physical concealment or simple Frequency Hopping technologies to evade enemy detection and Jamming. However, the rapid development of Software Defined Radio (SDR) and Artificial Intelligence (AI) technologies has evolved the mode of EW attacks from 'wide-area noise jamming' to 'precision strikes and protocol analysis.' This implies that it has become impossible to overwhelm the enemy simply with signal strength, suggesting that the network itself must change into an intelligent structure that actively detects and evades threats.

Empirical data recently collected from the Ukraine battlefield quantitatively shows how fast the threat speed of modern electronic warfare is. According to Watling and Reynolds [1] of the Royal United Services Institute (RUSI), it takes an average of about 6 weeks for Russian forces to analyze and neutralize the Ukrainian military's new communication frequency patterns and drone control protocols.

This '6-week' period holds the following critical strategic implications for tactical communication designers:

- **Effective Life of Encryption and Patterns**: Deployed communication protocols or frequency hopping patterns are highly likely to be fully identified and neutralized by the enemy 1.5 months after deployment.
- **Need for Adaptation**: Communication equipment relying on fixed hardware wiring or unchangeable firmware cannot survive in the modern battlefield. A software-centric network structure capable of evolving and transforming faster than the enemy's learning speed is essential.
- **Shift in Avoidance Strategy**: The enemy performs 'Intelligent EW' that goes beyond simply disrupting signals to learning and exploiting signal characteristics. Therefore, a 'Resistance' strategy trying to overcome jamming output with stronger output is disadvantageous in terms of energy efficiency, forcing a shift to a 'Topological Avoidance' strategy that physically bypasses or neutralizes the jammer's effective range itself.

The FPAC architecture proposed in this study starts from this background. The core objective is to establish an 'Electromagnetic Sanctuary' utilizing terrain features through low-power 5G femtocells densely deployed on the ground, and to secure survivability

* Corresponding author

from the enemy's wide-area jamming threats by having drone swarms fly inside this safe corridor.

The strategic value of FPAC goes beyond simply maintaining communication connections; it lies in drastically increasing the decision-making speed of friendly forces. This is directly linked to military strategist John Boyd's OODA (Observe, Orient, Decide, Act) loop theory. In his briefing [2], Boyd emphasized that the core of the OODA loop lies in the 'Orient' phase.

The Orient phase is a cognitive process of judging the situation by synthesizing genetic heritage, cultural traditions, and 'new information.' In the modern battlefield, especially the Intelligent Battlefield where AI is introduced, the 'Orient' phase corresponds to the learning and inference process of AI models. If battlefield video and sensor data collected by drones (Observe) are contaminated by the enemy's spoofing or jamming during transmission, the AI's situation judgment (Orient) will commit fatal errors, leading to wrong decisions (Decide) and actions (Act). Therefore, the jam-free high-bandwidth connection provided by FPAC functions as a 'Field AI Training Ground' that allows friendly AI to learn the enemy's EW patterns in real-time and establish countermeasures based on pure, uncontaminated data. This is an essential infrastructure that enables friendly forces to rotate the OODA loop faster than the enemy, thereby securing 'Cognitive Superiority.'

II. Core Design and Technical Analysis of 5G Femtocell-Drone Interconnected Architecture

The feasibility of FPAC depends on optimizing commercial 5G technologies to meet tactical requirements. Reflecting the constraints of 3GPP standards and commercial hardware, this section analyzes the architecture's core elements: IAB, Network Slicing, and SWaP-C optimization.

A. Integrated Access and Backhaul Based Self-Healing Network

One of the biggest vulnerabilities of tactical networks is the absence or potential destruction of wired backhaul. While general commercial 5G networks have fiber optic cables connected to base stations, such infrastructure cannot be expected at the Tactical Edge. Therefore, wireless backhaul technology is essential, and for this, this architecture adopts the IAB technology standardized in 3GPP Release 16 [3].

The IAB architecture defined in the relevant standard [3] shares the 5G NR(New Radio) air interface for both user equipment (UE) access and backhaul links between base stations. IAB nodes consist of two main logical functions:

- IAB-MT (Mobile Termination): A terminal function that maintains the backhaul link by connecting to an upper Parent Node.
- IAB-DU (Distributed Unit): A base station function that provides wireless access to lower Child Nodes or general UEs.

This structure allows for rapid expansion of network coverage through multi-hop relays without physical cable installation.

The core of tactical survivability lies in IAB's Topology Adaptation function. If a specific IAB node is destroyed or a link is blocked due to enemy shelling or concentrated jamming, the MT of the lower IAB node detects this and re-establishes the path by selecting a pre-defined backup path or an adjacent node with the highest RSRP as an 'Alternative Parent Node.' This process is performed locally with minimal intervention from the central core network, granting the network a 'Self-Healing' capability. This structurally resolves the Single Point of Failure (SPOF) problem of existing centralized fixed networks and guarantees robust connectivity in a Mesh form.

B. Traffic Isolation and QoS Assurance through Network Slicing

Drone swarms simultaneously generate large-capacity data, such as high-resolution reconnaissance video, and ultra-low latency control data for drone control and flight synchronization. If these two traffics compete in the same Queue, control signals may be delayed during a surge in video data, causing drones to crash. To prevent this, Network Slicing technology defined in the technical standard [4] is applied.

Network slicing partitions a single physical network into multiple logical virtual networks (Slices) to allocate resources optimized for each service.

- eMBB (enhanced Mobile Broadband) Slice: For reconnaissance video and high-capacity sensor data transmission. High bandwidth is guaranteed, but sensitivity to latency is set relatively low. 5QI (5G QoS Identifier) values of 6~9 are mainly used.
- URLLC (Ultra-Reliable Low Latency Communications) Slice: For Command and Control (C2) and Precision Time Protocol (PTP) transmission. Bandwidth is small, but packet loss rate (10^{-5} or less) and latency (1ms or less) are minimized to guarantee survivability. 5QI values of 80~85 are allocated.

The NSSF (Network Slice Selection Function) classifies and isolates packets into appropriate slices according to traffic characteristics (S-NSSAI). Through this, even in situations where the network is congested due to video data, control signals, which are mission-critical traffic, are guaranteed independent resources and can be transmitted safely.

III. Security Framework: Zero Trust and Firmware Resiliency

Femtocells and drones deployed deep in enemy territory are constantly exposed to the risk of physical capture and seizure. Therefore, existing security models relying on physical perimeter defense are invalid, and a security architecture that excludes implicit trust in the internal network is required.

NIST standards [5] present the Zero Trust principle that "all communication must be secured regardless of network location" and "access to resources must be granted on a per-session basis." This means that authentication and integrity checks must be performed continuously every time a femtocell connects to the 5G core network and every time a new data flow is created.

Physically captured femtocells can have their firmware tampered with by attackers and used as backdoors. To defend against this, NIST's Firmware Resiliency Guidelines [6] are applied. This standard defines three core capabilities:

- Protection: Firmware code and critical data must be protected from unauthorized changes. For this, hardware write-protection and digital signature verification are essential.
- Detection: Firmware tampering or malicious code injection must be immediately detectable during the boot phase. This is implemented through a HROT such as TPM (Trusted Platform Module) 2.0. The system measures the binary hash value of each stage during boot, stores it in the PCR (Platform Configuration Register), and a remote attestation server verifies it.
- Recovery: If tampering is detected, the system must automatically rollback to a secure Golden Image stored in an isolated area to restore function. Initiatives such as Microsoft's [7] support a hardware ecosystem complying with these regulations.

Malone et al. [8] warned through their research that attackers could seize control of femtocells or operate fake base stations (Rogue Femtocells) to lure user terminals and eavesdrop. This suggests that femtocells with physical access can turn into insider threats. In response, FPAC introduces RF Fingerprinting technology proposed by Reus-Muns et al. [9] in addition to 5G AKA (Authentication and Key Agreement) mutual authentication. This technology analyzes the minute physical signal characteristics (I/Q imbalance, DC offset, etc.) unique to base station hardware (power amplifiers, DACs, etc.) using deep learning models. Research results show that cloned base stations can be identified with 99.86% accuracy, enabling the construction of a multi-layered defense system that determines whether hardware itself is forged even in situations where encryption keys are stolen.

IV. High-Precision Navigation (PNT) Strategy in GPS-Denied Environments

In tactical environments, GPS/GNSS are assets most likely to be neutralized first by jamming. 5G networks provide OTDOA (Observed Time Difference of Arrival) positioning using the signal arrival time difference between base stations as an alternative, but this presupposes precise time synchronization between base stations.

A. PTP Vulnerabilities and Time Delay Attacks

Generally used IEEE 1588 PTP aims for synchronization in nanoseconds, but security vulnerabilities exist. Finkenzeller et al. [10] proved that attackers can insert artificial delays (Delay Attack) into network paths to distort PTP time calculations. Since the speed of radio waves is about $3 \cdot 10^8$ m/s, a time error of just 1 microsecond (1 μs) results in a position error of 300m. An error of 300m is an unacceptable figure for tactical navigation or precision strikes.

B. PTPsec and Cyclic Path Asymmetry Analysis

As a countermeasure, this architecture applies PTPsec [10]. This technique uses Cyclic Path Asymmetry Analysis. By utilizing the redundant paths provided by the IAB mesh network, PTP packets are circulated in multiple paths, such as clockwise and counter-clockwise, and the Round Trip Time (RTT) of each path is compared and analyzed. If an attacker injects a delay into a specific link, the symmetry between paths is broken, and the system immediately detects this and excludes contaminated PTP data.

C. Adaptive Time-Fusion and VIO (Ride-Through)

When the network is unstable or temporary jitter occurs due to consensus algorithms, PTP data becomes unreliable. At this time, the system must immediately switch to Visual-Inertial Odometry sensors to maintain navigation.A benchmark study by Kim et al. [11] quantitatively verified the performance of commercial

VIO algorithms (e.g., Apple ARKit, Google ARCore, etc.). Experimental results showed that the latest VIO systems exhibit a very low position drift rate of 0.02m per second. This means that even if PTP connection is lost for 10 seconds, position error can be suppressed within 0.2m (0.02 $m/s \cdot 10s$) using VIO alone.

In this study, a Kalman Filter-based adaptive fusion engine was designed based on this. This engine provides 'Ride-Through' capability that guarantees continuity of navigation by allocating Measurement Update weights entirely to VIO at the moment PTP reliability drops (e.g., during GHO consensus, upon attack detection).

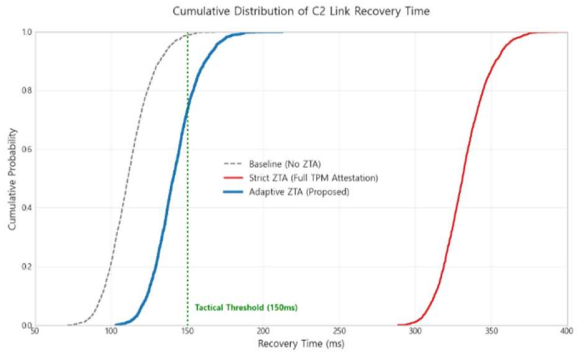

Fig. 1. Navigation Position Error Accumulation during Handover

V. CONCLUSION

This report proposed and verified the 5G femtocell-based FPAC architecture to respond to the '6-week learning cycle' threat of modern electronic warfare. Backhaul survivability and traffic isolation were implemented through 3GPP IAB and Network Slicing, and SWaP-C constraints were overcome through a layered structure based on actual hardware specifications. In particular, this study quantitatively proved that conflicting goals of security vs. survivability and scalability vs. precision can be resolved through 'Adaptive Policies.' Simulation results based on prior research data from Belding-Royer [12], Weinhold [13], Ongaro [14], Finkenzeller [10], Kim [11], etc., show that FPAC possesses engineering feasibility for actual deployment beyond simple concept proposals.

ACKNOWLEDGEMENT

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Ministry of Science and ICT (Project No. Project No.2022-11220701, 40%; RS-2022-00165794, 10%; RS-2024-00438551, 30%), and the Ministry of Science and ICT grant through the Information Technology Research Center (ITRC) Program (Project No. RS-2023-00228996, 20%)

References

[1] J. Watling and N. Reynolds, "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine," RUSI Special Report, May 2023.

[2] J. R. Boyd, "The Essence of Winning and Losing," Unpublished briefing, Jan. 1996.

[3] 3GPP, "Study on Integrated Access and Backhaul (IAB) for NR," Technical Report TR 38.874, Release 16.

[4] 3GPP, "System Architecture for the 5G System," Technical Specification TS 23.501, Release 16/17.

[5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, Aug. 2020.

[6] A. Regenscheid, "Platform Firmware Resiliency Guidelines," NIST Special Publication 800-193, May 2018.

[7] Microsoft Research, "Cyber-Resilient Platform Program," [Online]. Available: *https://www.microsoft.com/en-us/research/project/cyber-resilient-platform-program/*

[8] D. Malone, D. F. Kavanagh, and N. R. Murphy, "Rogue femtocell owners: How Mallory can monitor my devices," in Proceedings of IEEE INFOCOM, Turin, Italy, 2013, pp. 3387-3392.

[9] G. Reus-Muns, D. Jaisinghani, K. Sankhe, and K. R. Chowdhury, "Trust in 5G Open RANs through Machine Learning: RF Fingerprinting on the POWDER PAWR Platform," in IEEE Global Communications Conference (GLOBECOM), Taipei, Taiwan, 2020.

[10] A. Finkenzeller, O. Butowski, E. Regnath, M. Hamad, and S. Steinhorst, "PTPsec: Securing the Precision Time Protocol Against Time Delay Attacks Using Cyclic Path Asymmetry Analysis," in IEEE INFOCOM 2024 - IEEE Conference on Computer Communications, Vancouver, BC, Canada, 2024.

[11] P. Kim, J. Kim, M. Song, Y. Lee, M. Jung, and H.-G. Kim, "A Benchmark Comparison of Four Off-the-Shelf Proprietary Visual–Inertial Odometry Systems," Sensors, vol. 22, no. 24, p. 9873, 2022

[12] .E. M. Belding-Royer, "AODV Implementation Design and Performance Evaluation," International Journal of Wireless and Mobile Computing, 2005.

[13] C. Weinhold et al., "Separate but Together: Integrating Remote Attestation into TLS," in 2020 USENIX Annual Technical Conference (USENIX ATC '20), 2020.

[14] D. Ongaro and J. Ousterhout, "In Search of an Understandable Consensus Algorithm," in 2014 USENIX Annual Technical Conference (USENIX ATC '14), Philadelphia, PA, 2014, pp. 305–319.