The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *October 22, 2025* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *January 21, 2026* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.21

Literature Survey on Warfighter Information Network-Tactical

Muhanned AL-Rawi
Bandung Institute of Technology
Indonesia
e-mail: muhrawi@yahoo.com
ORCID: 0000-0003-1407-6519

Abstract. Under the conditions of conducting combat operations, information superiority is becoming one of the key factors of operational success. Increasing requirements for the speed, security and volume of data transmission, as well as the need to integrate heterogeneous command, control, communications and intelligence (C4I) systems, necessitate the development of fundamentally new tactical networks. The article is devoted to the analysis of the Warfighter Information Network-Tactical (WIN-T), which forms the basis for the implementation of the Force XXI concept and ensures dominance in the information domain. The aim of the study is to describe the architecture, principles of operation and mechanisms for ensuring the information security of WIN-T, as well as to generalise the results of previous research in this field. A separate objective is to demonstrate the military applications of the network for enhancing mobility, survivability and the effectiveness of command and control of troops. The study is based on a system analysis of open architectural specifications of WIN-T, including its division into the upper and lower levels of the Tactical Internet. Network topologies (LAN-A, LAN-B, WAN) are considered using switches, routers, ATM and HSMUX technologies, as well as radio communication systems (NTDR, SINCGARS, EPLRS). To ensure security, the concept of "defence-in-depth" is applied. The methodology also includes a literature review analysing QoS solutions, cryptographic methods, cognitive radio systems and Deep Reinforcement Learning technologies. The article provides a detailed description of the WIN-T architecture, which integrates the US Army Battle Command System (ABCS) and ensures connectivity from brigade level down to individual vehicles. It is shown that WIN-T establishes a unified IP-based transport network (Everything over IP), combining satellite communications (Ku/Ka bands), radio relay links and fibre-optic channels. Measurement-Based Admission Control (MBAC) mechanisms are implemented to prioritise traffic (voice, video, data). In the security domain, a multi-layered intrusion detection and response system is employed. A separate result is the presentation of the Named Data Networking (NDN) concept as an alternative to traditional IP-based networks for improving efficiency under complex conditions. WIN-T enables commanders to receive updated topographic maps, real-time video streams from the battlefield and intelligence data directly while on the move. The network supports the operation of critical systems such as the Advanced Field Artillery Tactical Data System (AFATDS) and the Command Post of the Future (CPOF). Field test results confirmed throughput exceeding 1 Mbps in the Ka band at movement speeds above 25 miles per hour. The proposed solutions for power optimisation and resource allocation based on Multi-Agent Deep Reinforcement Learning (MADRL) significantly enhance resistance to signal interception, which is critical for the survivability of elements on the battlefield.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Keywords: WIN-T, architecture, security, military applications.

Introduction

By offering network security and interoperability support to the army battle command system (ABCS) and its battlefield functional areas (BFAs), the WIN-T helps to improve maneuver force mobility. As operations in the present and the future place increasing demands on tactical voice, data, and multimedia signal support systems, this idea of communication services will give the warfighter a force multiplier.

In order to give warfighters the information they need to make decisions, the different information systems must be combined into a single, cohesive "system-of-systems" that supports joint operations and spans the strategic, operational, and tactical levels.

Methodological Framework

The methodological framework of this study is based on a comprehensive system analysis of the architecture, protocols, and security mechanisms of the Warfighter Information Network-Tactical (WIN-T), utilizing approaches inherent to military telecommunications engineering and network management.

First, the research is founded on a structural-functional analysis of the WIN-T architecture. It examines the integration of the Army Battle Command System (ABCS) with its key subsystems: Force XXI Battle Command Brigade (FBCB2), Army Tactical Command and Control System (ATCCS), and Global Command and Control System-Army (GCCS-A). The topology of command post networks is analyzed, particularly the division into LAN-A (intra-vehicle or edge network) and LAN-B (inter-vehicle or core network), as well as the role of the Tactical Packet Network (TPN), which consists of NC, LEN, SEN nodes and the System Control Center (SCC).

Second, the methodology includes a comparative analysis of networking technologies. The study investigates local area network implementation methods: router-based architectures, where routing decisions are made between local and remote command posts, and switch-based architectures, where switches provide local data delivery within a single segment. The application of ATM, HSMUX, HCLOS, HCTR technologies, satellite systems, and radio networks (NTDR, SINCGARS, EPLRS) for bandwidth management and quality of service is also analyzed.

Third, the defense-in-depth concept is applied to assess information security. This approach involves creating multiple sequential barriers against external and internal threats, each integrating detection, protection, and response functions. The study relies on cryptographic principles (public and secret key cryptography) as well as real-time intrusion detection methods.

Fourth, the work employs modeling and experimental verification. It mentions the use of the OPNET Modeler environment for developing and testing Quality of Service (QoS) solutions, specifically the Measurement-Based Admission Control (MBAC) algorithm, which prioritizes different traffic types (voice, video, data) based on computed end-to-end congestion levels. Additionally, field test results of SOTM terminals in Ku and Ka bands are presented, measuring throughput at the application layer.

Fifth, the article uses a literature review as a method of knowledge synthesis. Previous works are analyzed in the following areas: replacement of legacy MSE/TRI-TAC systems, WIN-T vulnerabilities and cryptographic countermeasures, QoS for encrypted tactical networks, integration of WIN-T with GIG and JTRS, application of Named Data Networking (NDN) as an alternative to IP-based networks, and the use of Multi-Agent Deep Reinforcement Learning (MADRL) for optimizing power allocation and spreading factor assignment to ensure Low Probability of Interception (LPI).

Thus, the methodological framework of this work is multi-layered and combines architectural analysis, network modeling, cryptographic methods, experimental testing, and a review of

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

contemporary research, providing a comprehensive understanding of the operation, protection, and development prospects of WIN-T.

Results and Discussion

1.1 Wit-t architecture

Through an integrated digital information network that offers automated C2 and SA information through a smooth data architecture of both planned and existing C2 systems, the ABCS assists planners and leaders at the tactical to strategic level. The Force XXI battle command-brigade (FBCB2), Army tactical command and control system (ATCCS), and global command and control system-Army (GCCS-A) are all part of the ABCS.

At each echelon, the information flow requirements dictate the physical layout of command posts, the communications equipment that supports them, and the ABCS LAN infrastructure. The basis for networking and communication in each Force XXI tactical operations center (TOC) is largely the same, despite these differences. The ATCCS, which aim to offer a collection of common services, facilitate the integration of C2 functions. A client-server architectural environment is in place to integrate and enable interactive information processing in order to fulfill this shared setting. The service is requested by the client computer and related software, and it is delivered by the server and related software. A local area network (LAN) or wide area network (WAN) is used to carry out this data information media exchange process.

Several BFACS sharing a single LAN at a CP make up an ABCS LAN. The WAN that links the different ABCS LANs throughout the battlefield is connected by the tactical packet network (TPN), also referred to as the MSE packet switch network or MPN (See Fig. 1). The system control center (SCC), small extension nodes (SEN), large extension nodes (LEN), and the node center (NC) are the main resources utilized for TPN communications. The tactical network that connects the ATCCS LANs is anchored by these resources. High speed multiplexer circuit cards (HSMUX), asynchronous transfer mode (ATM) switching, satellites, range extension terminals, near-term data radio (NTDR), high capacity line-of-sight (HCLOS) and high capacity trunk radios (HCTR), and other technologies have been introduced to help manage bandwidth and improve quality of service.

Two segments typically make up a TOC LAN, as shown in referred to as LAN-A (intra-vehicle LAN or edge component) and LAN-B (inter-vehicle LAN or core component). The FSE can extend the AFATDS workstation into the TOC SICPS using a third LAN-C. All peripherals, including workstations and printers, are connected by the LAN-A. that can be found in a single car, tent, or uniform integrated command post system. All TOC LAN-A segments can be connected to the LAN-B to enable information sharing throughout the TOC.

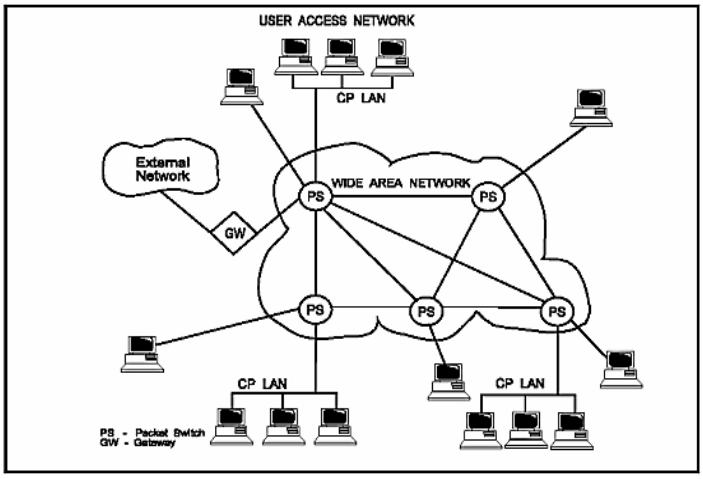


Fig. 1 Simplified TPN Architecture

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

A typical twisted pair connection, ethernet hubs, or routers/switches are used to implement the LAN-A. A router makes it easier to manage IP addresses and make decisions about internet work forwarding when LAN-A components connect to LAN-B. Additionally, this improves a LAN's effective use of its available bandwidth. Whether a message is sent to the local TOC or to another TOC is decided by a router.

Each vehicle in an ABCS BN TOC has either a standalone router or a router integrated into an Ethernet switch (a router-switch). Every vehicle at brigade and division TOCs has an Ethernet switch or router-switch. The router-switch integrates the capabilities of a switch and a router. Local forwarding decisions to LAN devices are made by Ethernet switches (see Figs. 2 and 3).

A multi-star network configuration is created by digital TOCs using at least two core routers integrated into a central ethernet switch that is connected in a star pattern to one of the core routers. Because this configuration uses less router, it simplifies the initial setup and enhances performance.

Like a LAN, a WAN is able to communicate with higher, lower, and adjacent units over a greater distance. It is a network of networks made up of several local area networks (LANs) linked to radio networks like CNR or MSE as well as to one another. Due to the limitations of a coaxial cable network, a wide area network (WAN) combines radio networks and MPNs to distribute data throughout the system as needed.

Both the physical communications network that serves as the general-purpose data backbone and the general idea of an integrated battlespace automated infrastructure are referred to as the tactical internet (TI). The "tactical internet" gets its name from its extensive and deliberate resemblance to the commercial internet.

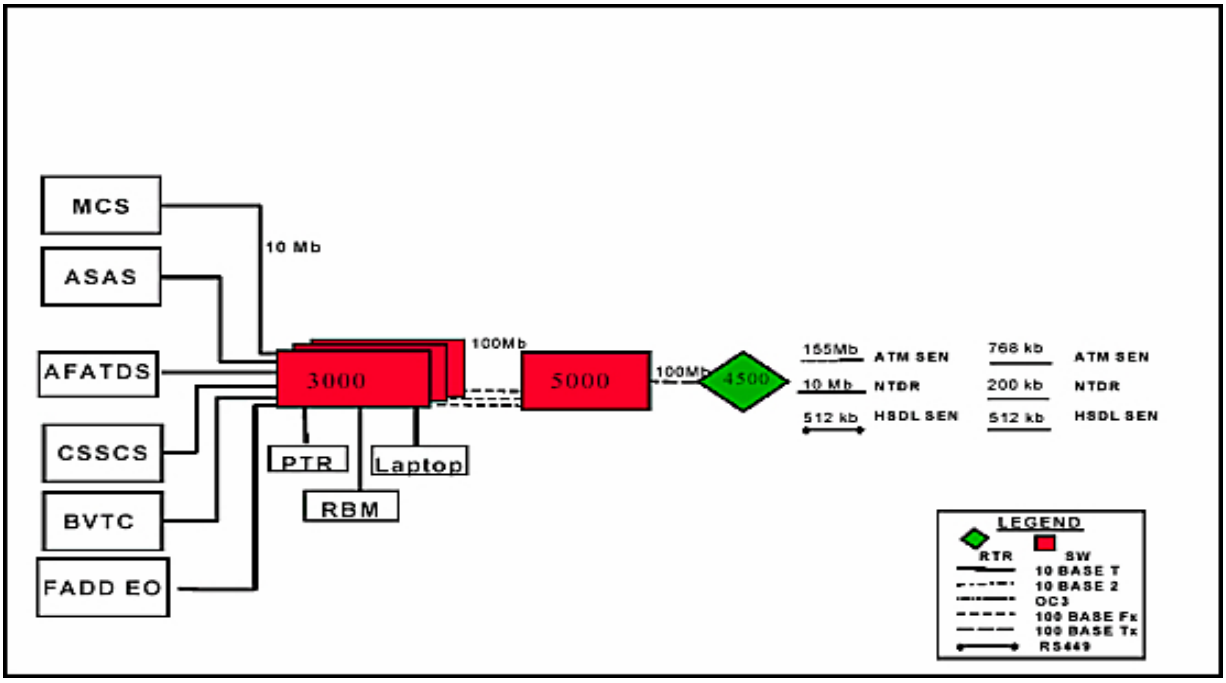


Fig. 2. Switched-based TOC Architecture

Two separate information exchange layers are formed by the TI, as shown in Fig.4 are known as the upper and lower TI. Other WIN-T systems, multi-channel satellite systems, and MSE make up the upper TI layer. For units at brigade and lower, the lower TI serves as the communications support system. It is made up of the FBCB2 computers and software, EPLRS, and SINCGARS SIP radios, which are connected via routers and both commercial and military protocols.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

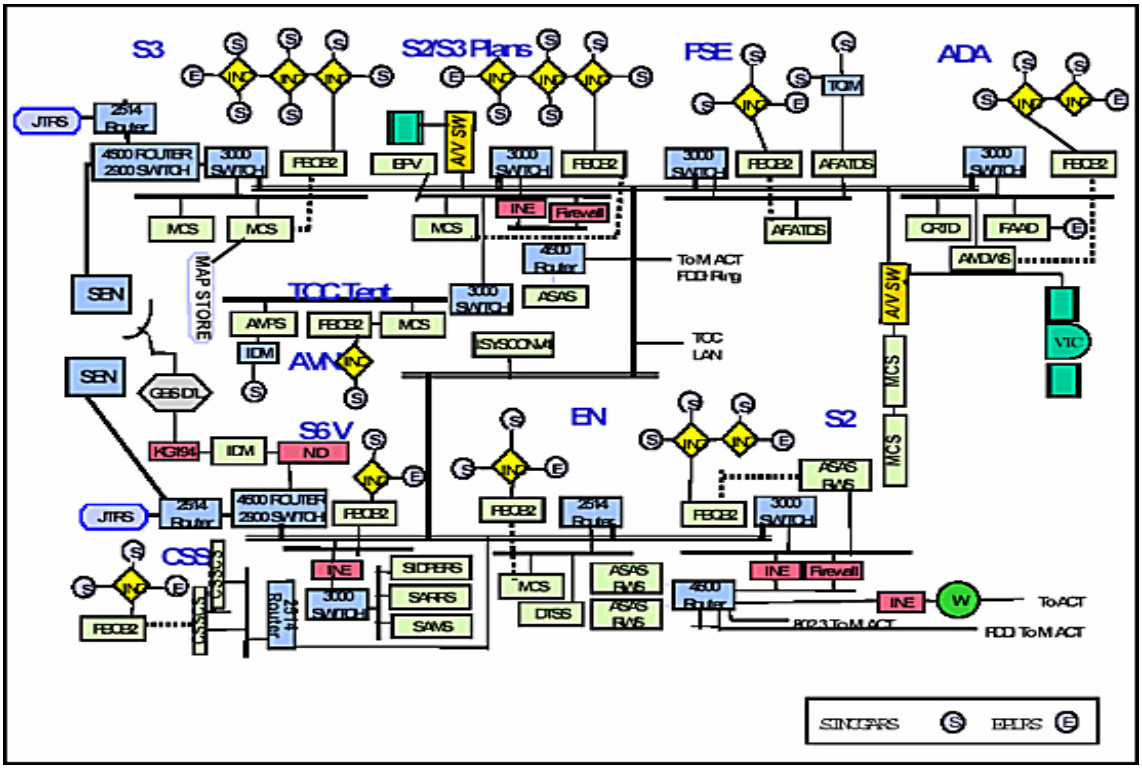


Fig. 3. Brigade TOC LAN

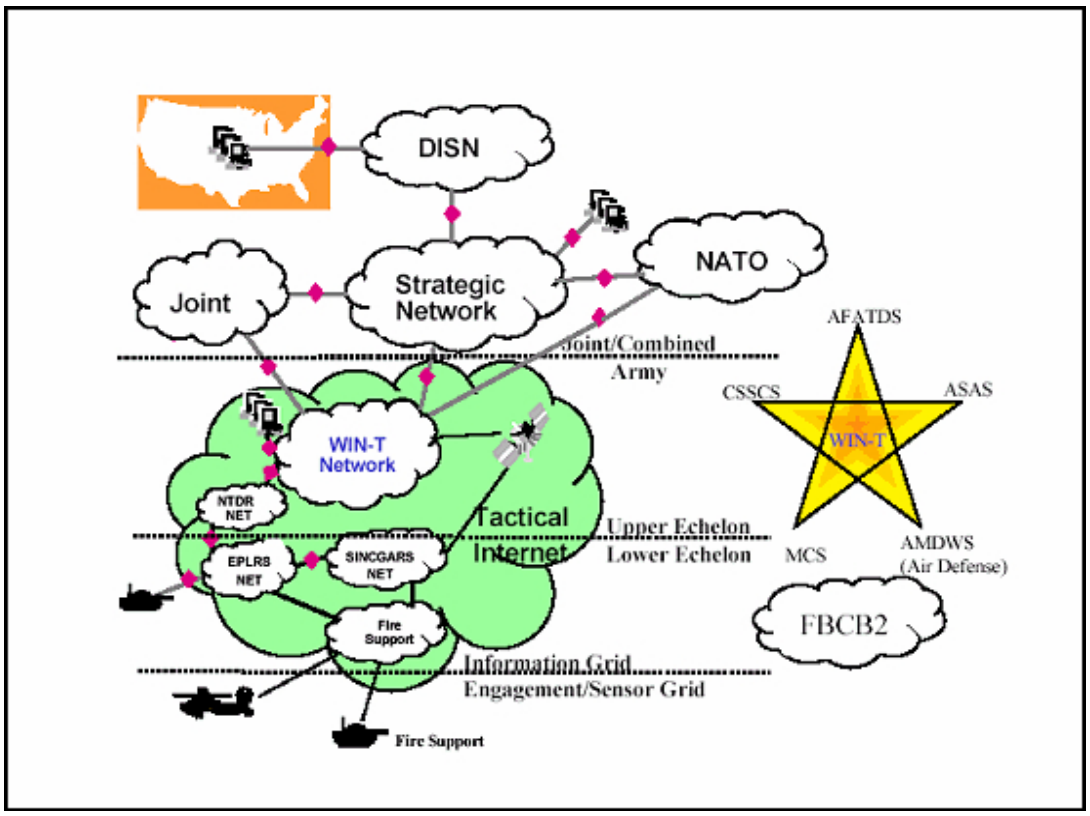


Fig. 4. WIN-T Conceptualization

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Network management and careful planning are necessary for the TI. When fully operational, the integrated system control (ISYSCON) hardware and software suite serves as the TI's management platform and interface for the FBCB2-equipped task force. The brigade task force also uses other systems, such as FBCB2, network control station-EPLRS (NCS-E), or commercial computers set up for network management, to plan and oversee the TI.

The TI contains a variety of digital systems that are intended to supply information to the commander, soldiers, and lower C2 and SA personnel from every unit in the brigade task force. The digital tools necessary for efficient C2 and battlefield SA, adapted to the operational needs and specific function of the unit's platforms, will make up each task force tier.

1.2 Information and network security

With the help of a universal TCP/IP data network, the Army's digitization efforts aim to field a variety of embedded and standalone end-user computers. That network will be made up of diverse radio networks with data capabilities (e.g. EPLRS, NTDR, MSE, SINCGARS), and wire communication links (e.g. local area networks), and a network infrastructure of specialized computers will connect and support these links (e.g. name servers, security servers, switches, and routers). The Army is unable to field a "bullet-proof" network, despite the fact that manufacturers create systems with security in mind and highly qualified personnel adhere to the proper protocols. As a result, it is essential to continue being able to perform real-time security management and intrusion detection as part of regular operations and to respond appropriately when issues arise. Real-time security management is envisioned by ABCS's information systems protection concept as an element of network and system management. Information and network security are implemented using a variety of security tools.

As shown in Fig.5, the "defense-in-depth" concept is the foundation of network protection. The defense-in-depth strategy aims to create several obstacles against an outsider, a hostile insider, etc. Every barrier integrates features for detection, protection, and response.

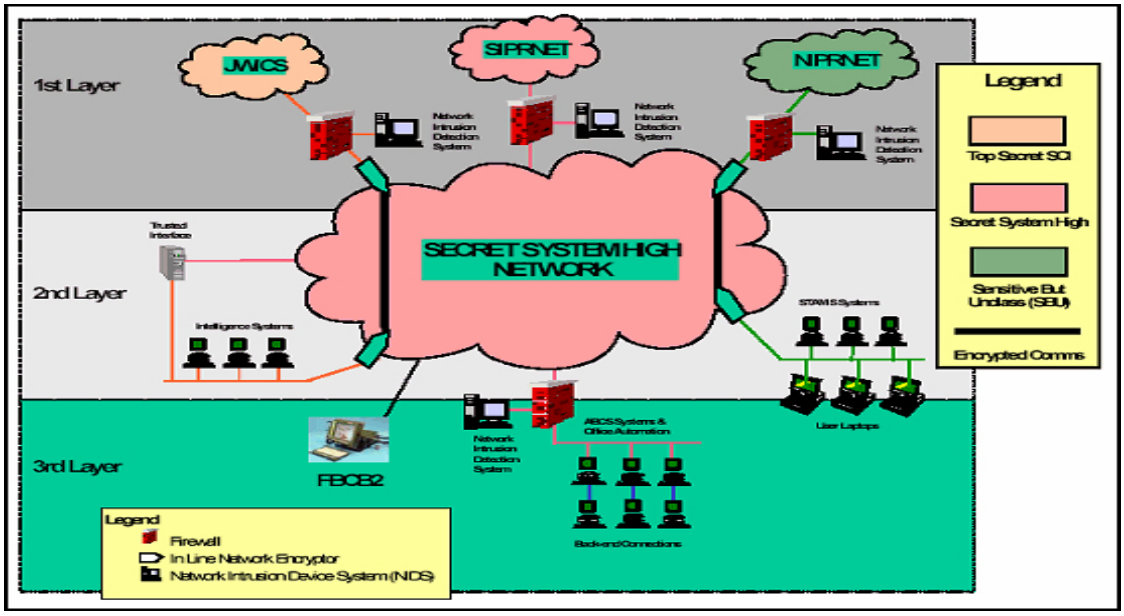


Fig. 5. Concept of Defense-in-Depth Network Protection

1.3 Military applications

The military uses of WIN-T are centered on giving the U. S. Army with a robust, mobile, and secure backbone for data, voice, and video tactical communications. It supports expeditionary

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

operations by connecting forces across long, non-linear battlefields using both line-of-sight and satellite communications, facilitating mission command for commanders from command posts to moving vehicles, and enabling real-time situational awareness through applications like live video streams and digital force maps. The following is a summary of the applications.

a) With WIN-T, commanders can view real-time topographical maps of friendly forces, access mission command applications from any location on the battlefield, and get intelligence updates to help them make prompt, well-informed decisions.

b) Voice calls, video conferences, and data transfers are all made possible by WIN-T's high-speed, high-capacity, and secure communications, which are crucial for sharing vital information and organizing operations.

c) By giving combat vehicles mobile network capabilities, WIN-T Increment 2 enables constant command and control while forces move across the battlefield.

d) Through the use of satellite and terrestrial transportation, the network provides a scalable, reliable network infrastructure that facilitates expeditionary operations and links forces in remote areas.

e) The Advanced Field Artillery Tactical Data System and Command Post of the Future are just two examples of the mission-critical systems that WIN-T supports by acting as the data pipe that gives them the connectivity they need to function properly.

f) To improve unit effectiveness and survivability, soldiers can use WIN-T to stream live video, digitally call for artillery support, and send requests for medical assistance.

2. Literature survey

The Warfighter Information Network Tactical (WIN-T), the US Army's intended replacement for the mobile subscriber equipment (MSE) and the antiquated tri-service tactical communications (TRI-TAC) system, are described in[1]. These systems are now approaching the end of their intended life cycle and are collectively referred to as the area common user system (ACUS). In place of them, WIN-T offers a cutting-edge, seamless multimedia transport system that links and supports all Army levels. It has been a mobile, secure, and resilient network with a large capacity. The current systems and how WIN-T offers an operational substitute are discussed in the paper. The cost as an independent variable (CAIV) acquisition method, which the Army has employed to acquire the new system, is also covered in the paper.

The paper in [2] looks at the different kinds of enemies, the dangers they present, and the weaknesses that the Army's Warfighter Information Network (WIN) is probably targeting. An outline of the potential applications of cryptographic techniques to address WIN vulnerabilities is given. A review of public key and secret key cryptography techniques, along with an analysis of their relative benefits and drawbacks, is included. The authors list several security-related concerns that need more thought in their conclusion.

A QoS solution for the Army's warfighter information network tactical (WIN-T) was created by general dynamics C4S in [3]. This solution is also being applied to other QoS applications in tactical networks. When using an encryption device, the encryptor prevents any information exchange between the WAN, where traffic shaping is done, and the LAN, where call admission control (CAC) decisions are made. OPNET Modeler was used to develop and test this solution. An algorithm of the measurement based admission control (MBAC) type forms the basis of this solution. Based on a calculated end-to-end congestion level, this MBAC algorithm controls the flow of diverse traffic entering a tactical wireless ad hoc network. Different types of traffic, including voice, video, and data, can have varying real-time requirements and varying levels of importance (survivability). Based on the QoS characteristics of each class of service and the state of the path to the destination node, the algorithm ranks the admission of calls or sessions (at a source node) in order of priority.

A QoS solution for tactical networks with security considerations is presented in the paper in [4]. A partitioned QoS approach is proposed since encryption stops the cipher text side and the plain text side from exchanging QoS information. The plain text side QoS solution includes

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

measurement-based admission control (MBAC), according to the authors. Based on a calculated end-to-end congestion level, MBAC uses real-time measurements to control the flow of traffic entering a tactical core network. The advantages of employing MBAC are examined in this essay, along with any potential drawbacks. The study demonstrates how a Markov chain expressing the degree of path congestion can be constructed using the measurements. A few simulation results from applying MBAC to an OPNET model of the warfighter information network-tactical (WIN-T) network are also presented in the paper.

In [5], the architecture framework that is suggested in this paper fills in the gaps in communication capacity and offers vital transport capabilities that will revolutionize battlefield communications to come. A thorough testing and evaluation process is in progress to guarantee the smooth, end-to-end integration of wireless services with the GIG resources for sending C4ISR data to the edge. Upon deployment, the WSDN will have the capability to expand DISN services to theaters with either fixed or mobile installations. The warfighter information network-tactical (WIN-T) users will have more mobility and the joint tactical radio system (JTRS) will have more interoperable capabilities.

The design, test methodology, and measured performance of the Ku- and Ka-band SOTM terminals are covered in [6]. These terminals are used to assess how the Army warfighter can be provided with dependable voice over IP (VoIP), video, and data communications while they are on the move. In order to evaluate the performance of the design in a networked and operationally relevant environment as well as the maturity of key technologies, the WIN-T DT/OT, and more especially the SOTM tests, were utilized. Antenna aperture, pedestal station keeping, and throughput performance are some of the more important design factors. The formal DT/OT testing process was successful in meeting the throughput requirement of 256 kbps at the application layer (layer 3). During SOTM testing, vehicles operating at speeds exceeding 25 mph were evaluated for throughput capability of roughly 770 kbps at Ku-band over the Americom AMC-9 satellite and Ka-band (using a satellite emulator) of 1 Mbps and higher.

According to [7], the L-3 Linkabit multi frequency-time division multiple access (MF-TDMA) demand-assigned multiple access (DAMA) Network Centric Waveform (NCW) has been chosen by the Warfighter Information Network-Tactical (WIN-T) community as the networking standard for fullmesh IP over SHF satellite communications. Large-aperture strategic terminals and small-aperture tactical/mobile terminals using satellite communications on the move (S-COTM) are just two examples of the diverse network of terminals that the NCW supports. By using an advanced network scheduler, it makes nearly optimal use of satellite and terminal resources to maximize network data throughput and terminal population. In this paper, the main characteristics of the waveform MAC and Physical Layers are described.

The study in [8] offers a methodology for evaluating and analyzing tactical communications networks to ascertain whether or not they adhere to DoD recommendations for network-centric warfare. The process is a component of the national security system (NSS) and information technology (IT) interoperability process of the Department of Defense (DoD), which is capability-focused and effects-based. The paper focuses on this process's evaluation and analysis stage. As an example, the methodology is demonstrated using the Warfighter Information Network-Tactical (WIN-T). Army tactical Global Information Grid (GIG) design, development, production, and fielding are accomplished through a single integrating net-centric framework established by the WIN-T program. In order to conduct tactical communications in a Net-Centric Environment (NCE), WIN-T had to overcome certain obstacles, which are explained and their solutions are provided. An integrated Operational, Systems, Technical, and All Views architecture that sufficiently handles all internal and external system information exchanges is said to be necessary in order to support the net-centric warfare concept. Using and updating this architecture is crucial for all stages of system development and improvement.

The paper in [9] offers a method for enabling DSA functionality on existing military radios

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

without requiring any changes to their firmware or hardware. In contrast to embedded sensors that have sophisticated feature-based sensing algorithms, application-level messaging, and a cognitive engine written in a high-level language that is located outside the radios, external sensors enable DSA functionality in radios. A network of three Warfighter Information Network-Tactical (WIN-T) Local Area Waveform (LAW) nodes in friendly and unfriendly interference was used in a real-time over-the-air demonstration for such a cognitive radio test-bed at the US Army CERDEC's Ft.Dix facility. The system, test-bed operation, and some field demonstration results are briefly described in this paper.

In [10], a plan for bringing four different networks together under the Internet Protocol (IP) umbrella is proposed. WIN-T, the Army Warfighter Information Network-Tactical area common user system, is the first network. Using the Mobile Ad Hoc Interoperability Networking Gateway (MAINGATE) system, the second network extends to the local common user system. Third is the wireless access network based on Worldwide Interoperability for Microwave Access (WiMax), and fourth is the 802.11 WiFi network. At the tactical level of the battlefield, this paper aims to present a basic wireless strategy that will establish "Everything over IEEE" ("EoIEEE") and everything over IP (EoIP) standards.

Unlike Internet Protocol (IP) network systems, Named Data Networking is a novel idea that adopts a fundamentally different approach in [11]. IP-type networks use locations, represented by IP addresses, to direct data transmission messages to their intended recipients. On the other hand, Named Data Networks (NDNs) give more attention to the data itself than to the specific locations of the data. In an NDN, the actual data being sent or requested—rather than the assumed locations of the data content—determines the forwarding decisions. To enable IP message delivery, NDNs name the data itself rather than network locations. By avoiding many of the issues and inefficiencies that plague IP networks, this novel method enables NDN nodes to more readily utilize the broadcast capabilities present in many modern networking devices. It is worthwhile to look into the advantages that NDN might be able to offer military communication systems, as many of these systems rely on IP mechanisms to provide networking functionality. Particular aspects of the NDN architecture's design offer an effective substitute for IP-based systems, especially for those functioning in challenging environments. Thus, an emulation analysis of military communication networks aided by NDN is presented in this paper. The authors also give a brief overview of the NDN architecture and how it can be integrated into different military communication networks, including the Army's Warfighter Information Network-Tactical (WIN-T) and the Navy's Automated Digital Networking System (ADNS). Initial findings indicate that applying the NDN architecture to these military communication networks results in significant performance improvements.

The study in[12] presents the theory of operation for the Warfighter Information Network-Tactical (WIN-T), the Army's future communications network. From theater-level to the commander at the company level, the WIN-T is the Army's first fully integrated data network, supporting most tactical Warfighters in the tactical theater. The future force will be widely distributed, and WIN-T will eventually provide a variety of communications tiers, such as satellite communications (SATCOM), airborne relay, and ground-based Line-Of-Sight (LOS). The WIN-T architecture was created in four stages. The Increment 2 and Increment 3 stages of the WINT program are the main topics of this study. From company level units to theater level echelon, the Army warfighter can utilize WIN-T, a common user system, which offers Everything over IP (EoIP) capabilities. With every increment, the tactical warfighter gains new capabilities and improved technologies.

Ground combat vehicles (GCVs) in Warfighter Information Network-Tactical (WIN-T) systems are autonomous and highly networked in [13,14]. In a dynamic environment, it can be difficult to safeguard numerous wireless communication links from enemy interception. GCV mobility makes it easy to breach the Low Probability of Interception (LPI) capacity, especially when using multiple interception techniques at once. The issue of maintaining LPI capability under both conventional optimization and Deep Reinforcement Learning (DRL) techniques is examined by the

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

authors in this work. In contrast to earlier research, the authors suggest an anti-interception approach that counters both correlation-based and energy-based interceptor techniques. The strategy jointly optimizes power allocation (PA) and spreading factor assignment (SA) of the WIN-T to avoid these interceptors. The authors used sophisticated techniques like decomposition and difference of convex functions (DC) to solve the problem because it is mathematically formulated as a non-convex optimization model. The authors developed a Multi-Agent Deep Reinforcement Learning (MADRL) approach to get the optimal solution almost instantly. The suggested MADRL strategy's performance is near the optimal solution, according to the numerical results, which makes it suitable for real-world systems.

Conclusion

This paper focused on warfighter information network-tactical, one of the most significant technologies in the field of military telecommunication networks. The paper described the operation of this technology and its military applications. Additionally, the paper included a brief description of some earlier technological works.

Recommendations

Based on the conducted analysis of WIN-T architecture, literature review, and identified problematic aspects (particularly regarding security, quality of service, and integration of heterogeneous networks), the following recommendations are formulated for further development, implementation, and operation of the Warfighter Information Network-Tactical.

1. Network Architecture Improvement

1.1. Fault tolerance enhancement. The current multi-star topology with core routers creates potential single points of failure. It is recommended to implement redundant core configurations (redundant core routers) with automatic failover protocols (e.g., VRRP or HSRP) at brigade and division Tactical Operations Centers (TOCs).

1.2. LAN-A/LAN-B segmentation optimization. To improve throughput, it is recommended to implement dynamic QoS marking at the LAN-A/LAN-B boundary, taking into account priorities of different traffic types (voice, video, intelligence data). This will prevent queuing at edge switches.

1.3. NDN integration. Given the promising research results of Named Data Networking (NDN) [11], it is recommended to conduct experimental implementation of NDN at the lower tactical internet (lower TI) level as an alternative or overlay to IP. This is particularly relevant for environments with limited bandwidth and frequent communication disruptions, where priority is delivery of named data (e.g., "friendly commander's position") rather than connections between specific IP addresses.

2. Information Security Assurance

2.1. Expansion of the defense-in-depth concept. It is recommended to add a separate "AI-based adaptive response" layer to the existing defense-in-depth model. Using the results from [13,14] on MADRL, it is proposed to implement machine learning agents that reconfigure in real time power allocation parameters and spreading factor assignments to counter correlation-based and energy-based interception techniques.

2.2. Elimination of the QoS gap between plaintext and ciphertext traffic. Since encryptors block information exchange between WAN and LAN [3,4], it is recommended to develop a low-overhead signaling protocol that transmits aggregated congestion metrics (e.g., delay or packet loss levels) in encrypted form. This will allow coordination of MBAC operation on both sides of the encryptor.

2.3. LPI/LPD enhancement for moving vehicles. For Ground Combat Vehicles (GCVs), it is recommended to apply a hybrid approach: combining traditional optimization methods (DC function methods and decomposition) with MADRL to ensure Low Probability of Interception (LPI) even at speeds exceeding 25 mph. This should account for the possibility of simultaneous application of multiple interception techniques.

3. Quality of Service (QoS) Management

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

3.1. MBAC adaptation to electronic warfare conditions. The Measurement-Based Admission Control (MBAC) algorithm should be supplemented with a jamming detection mechanism. In case of jamming detection, it is recommended to switch to more conservative admission thresholds and activate routing mechanisms bypassing affected areas.

3.2. Mission-based traffic prioritization. Instead of rigid service class divisions (voice, video, data), it is recommended to implement dynamic prioritization based on mission metadata (e.g., a fire support request should have higher priority than video broadcast from a general situational awareness channel).

4. Experimental Verification and Testing

4.1. Expansion of test scenarios. In addition to controlled conditions using satellite emulators [6], it is recommended to conduct WIN-T testing in more realistic conditions: with active electronic warfare jamming, multipath fading, and dynamically changing interference spectra.

4.2. MADRL field validation. Deep Reinforcement Learning algorithms [13,14] should be verified on actual WIN-T hardware using tactical radios (SINCGARS, EPLRS, NTDR) in multi-agent group configurations.

5. Integration with Joint Forces and Systems

5.1. Interoperability expansion with GIG and JTRS. It is recommended to accelerate the development of gateways for seamless data exchange between WIN-T and the Joint Tactical Radio System (JTRS), as well as with the Global Information Grid (GIG). Particular attention should be paid to ensuring operation in multinational coalition operations.

5.2. Support for expeditionary operations. To provide communications in remote areas without ground infrastructure, it is recommended to more widely use a combination of satellite channels (SOTM) and aerial relays (HALE, MALE UAVs), which will maintain communications in undeployed theaters of operations.

6. Future Research Directions

The following priority directions for further research are identified:

Development of cognitive spectrum management algorithms capable of operating within encrypted tactical networks without revealing signaling information.

Quantitative comparison of NDN and IP-based protocols in WIN-T in terms of latency, overhead, and packet loss resilience.

Investigation of defense-in-depth impact on MBAC performance and development of methods for coordinating security and QoS policies.

Creation of a realistic benchmark testbed for WIN-T testing under electronic warfare conditions with the ability to reproduce active jamming and interception scenarios.

This "Recommendations" section logically concludes the article and provides concrete steps for researchers, developers, and military professionals.

Conflict of Interest

The author declares that he has no competing interests related to the subject of the article.

References

1. Sharret, P. (1999). WIN-T—the Army's new tactical intranet. *In MILCOM 1999. IEEE Military Communications Conference Proceedings* (Vol. 2, pp. 1383–1387). IEEE. https://doi.org/10.1109/MILCOM.1999.821430
2. Jacobs, S. (1999). Tactical network security. *In MILCOM 1999. IEEE Military Communications Conference Proceedings* (Vol. 1, pp. 651–655). IEEE. https://doi.org/10.1109/MILCOM.1999.822764
3. McCann, C. J., Elmasry, G. F., Russell, B., & Welsh, B. (2004). A measurement-based approach for multilevel admission of heterogeneous traffic in wireless ad-hoc networks. *In IEEE MILCOM 2004. Military Communications Conference* (Vol. 3, pp. 1562–1565). IEEE.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

https://doi.org/10.1109/MILCOM.2004.1495171
4. Elmasry, G. F., & McCann, C. J. (2005). Partitioned QoS solution for tactical networks—addressing the impact of encryption. *In MILCOM 2005—IEEE Military Communications Conference* (Vol. 1, pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2005.1605653
5. Shah, S. A. (2005). DISN advanced wireless mobile services (DAWMS) in global net-centric environment for the warfighter. *In MILCOM 2005—IEEE Military Communications Conference* (Vol. 4, pp. 2590–2595). IEEE. https://doi.org/10.1109/MILCOM.2005.1606057
6. Wexler, R. S., Hoffmann, R., Collins, M. R., & Moran, P. (2006). Successful development and test of SATCOM On-The-Move (OTM) Ku-band Ka-band systems for the Army's Warfighter Information Network-Tactical (WIN-T). *In MILCOM 2006—IEEE Military Communications Conference* (pp. 1–7). IEEE. https://doi.org/10.1109/MILCOM.2006.302343
7. Wiss, & Gupta, R. (2007). The WIN-T MF-TDMA mesh network centric waveform. *In MILCOM 2007—IEEE Military Communications Conference* (pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2007.4454797
8. Hermelee, & Turczyn, S. (2007). Assessment and analysis of tactical communications in a net-centric environment. *In MILCOM 2007—IEEE Military Communications Conference* (pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2007.4455070
9. Mody, N., et al. (2010). On making the current military radios cognitive without hardware or firmware modifications. *In MILCOM 2010—IEEE Military Communications Conference* (pp. 2327–2332). IEEE. https://doi.org/10.1109/MILCOM.2010.5680354
10. Carlson, F. R. (2011). Strategy for tactical cellular connectivity. *Proceedings of SPIE, 8062*, 80620N. https://doi.org/10.1117/12.881205
11. Etefia, M., Gerla, M., & Zhang, L. (2012). Supporting military communications with Named Data Networking: An emulation analysis. *In MILCOM 2012—IEEE Military Communications Conference* (pp. 1–6). IEEE. https://doi.org/10.1109/MILCOM.2012.6415685
12. Ali, S. R., & Wexler, R. S. (2013). Army Warfighter Network–Tactical (WIN-T) theory of operation. *In MILCOM 2013—IEEE Military Communications Conference* (pp. 1453–1461). IEEE. https://doi.org/10.1109/MILCOM.2013.246
13. Le, V. H., Nguyen, T. T., Nguyen, K. K., & Singh, S. (2022). Joint energy and correlation based anti-intercepts for ground combat vehicles. *In MILCOM 2022—IEEE Military Communications Conference* (pp. 867–872). IEEE. https://doi.org/10.1109/MILCOM55135.2022.10017791
14. Le, V. H., Nguyen, T. T., & Nguyen, K. K. (2023). Dual wireless anti-interception for ground combat vehicles. *IEEE Transactions on Vehicular Technology, 72*(12), 16236–16248. https://doi.org/10.1109/TVT.2023.3298514

Огляд літератури щодо питань військової тактичної інформаційно-комунікаційної мережі WIN-T

Муханнад Аль-Раві
Бандунзький технологічний інститут
Індонезія
e-mail: muhrawi@yahoo.com
ORCID: 0000-0003-1407-6519

Анотація. У сучасних умовах ведення бойових дій інформаційна перевага стає одним із ключових факторів успіху операцій. Зростаючі вимоги до швидкості, безпеки та обсягів передачі даних, а також необхідність інтеграції різнорідних систем управління, зв'язку, комп'ютеризації та розвідки (C4I) вимагають створення принципово нових тактичних мереж. Стаття присвячена аналізу тактичної інформаційної мережі бійця (Warfighter Information

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Network-Tactical, WIN-T), яка є основою для реалізації концепції Force XXI та забезпечення домінування в інформаційному просторі. Метою роботи є опис архітектури, принципів функціонування та механізмів забезпечення інформаційної безпеки WIN-T, а також узагальнення результатів попередніх досліджень у цій галузі. Окремим завданням є демонстрація військових застосувань мережі для підвищення мобільності, живучості та ефективності управління військами. Дослідження базується на системному аналізі відкритих архітектурних специфікацій WIN-T, зокрема її поділу на верхній і нижній рівні тактичного інтернету (Tactical Internet). Розглядаються мережеві топології (LAN-A, LAN-B, WAN) із використанням комутаторів, маршрутизаторів, технологій ATM, HSMUX, а також засобів радіозв'язку (NTDR, SINCGARS, EPLRS). Для забезпечення безпеки застосовано концепцію «ешелонованого захисту» (defense-in-depth). Методологія також включає огляд літератури, де аналізуються рішення QoS, методи криптографії, когнітивні радіосистеми та технології Deep Reinforcement Learning. У статті детально описано архітектуру WIN-T, яка інтегрує систему управління боєм армії США (ABCS) та забезпечує зв'язок від рівня бригади до окремого транспортного засобу. Показано, що WIN-T створює єдину транспортну мережу з підтримкою IP (Everything over IP), що поєднує супутниковий зв'язок (Ku/Ka-діапазони), радіорелейні лінії та волоконно-оптичні канали. Упроваджено механізми адаптивного управління доступом на основі вимірювань (MBAC) для пріоритезації трафіку (голос, відео, дані). У сфері безпеки реалізовано багаторівневу систему виявлення вторгнень та реагування. Окремим результатом є представлення концепції Named Data Networking (NDN) як альтернативи традиційним IP-мережам для підвищення ефективності в складних умовах. WIN-T забезпечує командирів можливістю отримувати оновлені топографічні карти, відеопотоки з поля бою та дані розвідки в реальному часі безпосередньо під час руху (on-the-move). Мережа підтримує роботу критичних систем, таких як Advanced Field Artillery Tactical Data System (AFATDS) та Command Post of the Future (CPOF). Результати польових випробувань підтвердили пропускну здатність понад 1 Мбіт/с у Ka-діапазоні при швидкості руху понад 25 миль/год. Запропоновані рішення з оптимізації потужності та розподілу ресурсів на основі MADRL значно підвищують стійкість до перехоплення сигналу, що має вирішальне значення для живучості підрозділів на полі бою.

Ключові слова: WIN-T, архітектура, безпека, військові застосування.