

Secure Wireless Communication for Military and Tactical IoT Networks

N Thejasree

1 Introduction

The evolution of warfare is becoming more dependent on innovations in wireless communication technologies and interconnected intelligent systems. Warfare today is largely a facilitative action for military operations, which rely on wireless communication technologies like Tactical Internet of Things (IoT). Tactical IoT is a collection of devices like sensors, unmanned aerial vehicles, ground robots, wearable devices for soldiers, mobile command centers, and edge devices. Today, warfare involves a digital evolution of the defense infrastructure, which is a highly interconnected ecosystem where information dominance is critical for strategic dominance. As opposed to traditional warfare environments, which were based on a centralized command hierarchy and hardwired communication infrastructure, today's warfare infrastructure is characterized by distribution, dynamism, and data. At the heart of this change is the tactical IoT-based networks, which provide the communications backbone for these changes, with emphasis on the safe exchange of data between the air, land, sea, cyber, and space domains. The use of heterogeneous devices has introduced unprecedented flexibility to warfare systems, which has, in turn, increased the risk of cyber attacks. Unlike the commercial IoT systems, the military and tactical IoT systems function within a hostile and dynamic environment. Wireless communication is more prone to interception, jamming, spoofing, and denial of service. Furthermore, the military environment also adds the issues of mobility, limited connectivity, environmental factors, node capture, and energy limitations. The communication channels are also affected by electronic warfare and environmental interference. Consequently, wireless communication security is no longer a choice but a requirement. Without a secure communication mechanism, leakage of intelligence, compromise of operations, failed missions, and strategic disadvantages may occur. Thus, tactical IoT networks require a robust and multi-layered security mechanism, ensuring the continuity of operations despite potential adversaries' efforts. This paper will provide an exhaustive study on the various mechanisms in wireless communications designed to ensure the security of wireless communications in military and tactical IoT networks.

This paper will integrate various models like the architectural model, the security framework, the threat analysis, performance considerations, and future research directions in one single platform on secure wireless communications in tactical IoT networks. Warfare today looks nothing like it did before, thanks to fast-moving progress in wireless tech and smart linked-up systems. Not separate anymore, military teams now work as one through live data sharing, where timing shapes outcomes. A web of connected gear - drones, sensors, soldiers' wearables, robots, control hubs, and watchers - forms what is known as tactical IoT, tying everything into a single flow of signals. This shift turns scattered efforts into synchronized actions, guided constantly by fresh incoming details. Out on today's front lines, knowing what's happening often matters just as much as sheer power. Getting data quickly - then using it fast - can mean better choices under pressure. Thanks to smart battlefield links, units stay aware through a blend of inputs from ground, sky, and sea. Warnings pop up sooner, movements sync without delay, robots follow paths - all fed by shared signals. But every new link added sharpens risk along with reach. Signals float through air, so anyone nearby might catch them. Wired setups hide data inside cables, but radio waves spread out where enemies can grab hold. Devices on the move use smart gadgets that talk without wires, yet foes may drown those talks with noise or fake messages. Some attackers sneak in, twist information, or team up to hit both digital and physical parts at once. Since gear shifts position constantly during operations, connections form and break all the time - opening more gaps for trouble. Out in the wild, military IoT gear keeps working even when everything goes sideways. Though cut off from cities, these tools survive deserts, mountains, or war-torn areas with almost nothing to lean on. Power runs low, processing muscle is weak, and signals drop - making security tough to maintain. So protection can't weigh much, needs to shift on its own, and operate beyond a central hub. Clouds and steady links? They're nice for everyday tech - but out there, that kind of trust gets broken fast. New tech like smart systems, local processing, and self-operating tools brings more moving parts into play. Because they speed up choices and improve how things run, yet open more doors for threats. To keep messages safe across tightly linked networks demands attention beyond just locks and keys - think verified gadgets, trusted paths, unbroken data, real-time oversight, plus safeguards built right into hardware. Not one fix covers it all when connections multiply. One way to start is by looking at how wireless signals stay protected when used in battlefield-connected devices. Because setups differ, each design must handle threats while keeping data flowing under tough conditions. Some systems rely on layered defenses, others build trust through verified access points across moving units. A different angle shows that real missions shape what security actually works during fast-changing operations. Even small flaws can ripple outward when machines make split-second decisions without human checks. Looking ahead, new methods may shift control closer to where actions happen instead of central hubs. The last point stands clear: protection

isn't just about code - it shapes whether orders succeed or fail when surroundings turn unpredictable.

2 Background and Conceptual Foundations

Secure tactical communication systems rely on wireless networking paradigms like Wireless Sensor Networks, Mobile Ad Hoc Networks, Delay Tolerant Networks, and cognitive radio networks. The networks identified above are preferably self-organizing, adaptive, self-managing, autonomous, and infrastructural independent, making these types of wireless networking paradigms quite appropriate for the battlefield environment.

Wireless sensor networks enable the monitoring of the surrounding environment as well as the collection of intelligence. MANETs allow the mobile nodes of a network to use other nodes in the network to form communication paths between each other without any fixed infrastructure. Cognitive radio technology includes spectrum awareness, allowing it to avoid interference and jamming. These combined technologies form the conceptual backbone for tactical IoT networks.

A tactical IoT network can also be abstracted as a time-varying graph:

$$G(t) = (V(t), E(t))$$

where $V(t)$ represents nodes with active states, and $E(t)$ denotes communication links at any given time t . Owing to various effects like mobility, interference, and environment, communication links fluctuate dynamically, impacting routing stability as well as security. The reliability of the links is continuously monitored. It should be ensured that a robust tactical system, even under partial compromise or spectrum warfare conditions, sustains operational continuity. This demands that security can no longer be treated as an add-on layer, but rather must be integrated inherently within the design of a network.

Out in the field, military IoT setups depend on core network ideas refined through years of real use and study. To build reliable wireless links for chaotic situations, you need to grasp those basics first. Fixed hubs aren't part of the picture - instead, devices move freely, connect loosely, driven by immediate objectives. Because operations shift constantly, security models must adapt just as fast. What works in stable conditions falls apart here, so designs start from a different mindset altogether. Right in the middle of tactical IoT setups sit wireless sensors alongside mobile ad hoc nets. Spreading out over large stretches of land, those sensors gather information piece by piece, useful when watching nature shifts, spotting dangers, or keeping eyes on war zones. Instead of fixed hubs, mobile ad hoc systems link gadgets on the fly, building paths as they go. Each device pitches in, passing messages along so the whole group stays connected, shaping its own structure as needed. Even though that adaptability fits well with combat needs, shifting

layouts plus thin control layers open up risks too. Close to where data begins, processing happens faster. Not waiting for faraway centers cuts delays when quick choices matter. Information gets handled nearby instead of traveling long distances. Between devices and central systems sit extra points that sort details ahead of time. Those spots work together without constant links backward. Security stays tight even with parts spread out differently. Coordination across levels keeps everything running smoothly. Radio smarts and smart talking sit at the core just as much. Out in the field, airwaves often teem with noise or get jammed on purpose. Because of that, gear needs to spot open channels, dodge signal clashes, move around problems - on its own, mid-mission. Jumping wisely makes links hold up better, though staying safe means locking down how those choices are made so enemies can't steer them wrong. Secret messages stay safe when shared carefully in high-pressure moments. What matters most? Only the right people see them. A message sent must arrive unchanged, every single time. Even if systems are under pressure, they still need to work without fail. When systems face attack, staying operational matters just as much as performance. Even if parts fail, the network must keep running somehow. That is what surviving really means here. Bouncing back fast comes into play once things go wrong. Adapting on the fly makes a difference when interruptions hit hard. What keeps some systems running smoothly? It's how they handle trust. Networks without a central control need gadgets to judge who they're connecting to. Before passing private data, each device checks if others are dependable. This check happens by watching actions over time, looking at past exchanges, and confirming valid access proofs. When these evaluations work well, sketchy participants struggle to mess up paths or leak lies. A solid approach quietly blocks bad actors from gaining influence. Out in the field, gear from different times and makers has to work together. That reality pushes how we think about tactical IoT setups. Instead of chaos, common rules for talking and staying safe make things line up properly. Where networks meet, secure gateways step in like referees. They check IDs, lock down data, keep mismatches from causing failures. Protection stays strong even when devices do not speak the same language. When it comes to tactical IoT, people and how they work matter just as much as the tech itself. Civilian setups often focus on making life easier or saving time. Military systems? Their main job is keeping missions alive no matter what. Tough terrain, sudden moves, little access to repair help - security can't ignore those realities. Protection has to fit within limits that most networks never face. What holds it all together shapes how safety works in military radio links and field IoT setups. Built on that foundation sit defense layers, smart rules for data flow, things staying connected under stress.

2.1 Threat Model and Adversarial Capabilities

Military IoT networks are vulnerable in different layers: physical, network, and application layers. The adversary may possess advanced electronic warfare capabilities, cyber intrusion tools, and AI-driven attack systems. Threat categories include:

- Passive eavesdropping on wireless channels
- Active packet injection and replay attacks
- Spectrum jamming and denial-of-service
- Node capture and hardware tampering
- Routing manipulation (blackhole, wormhole, Sybil attacks)
- Machine learning-based traffic analysis
- GPS spoofing and time synchronization attacks

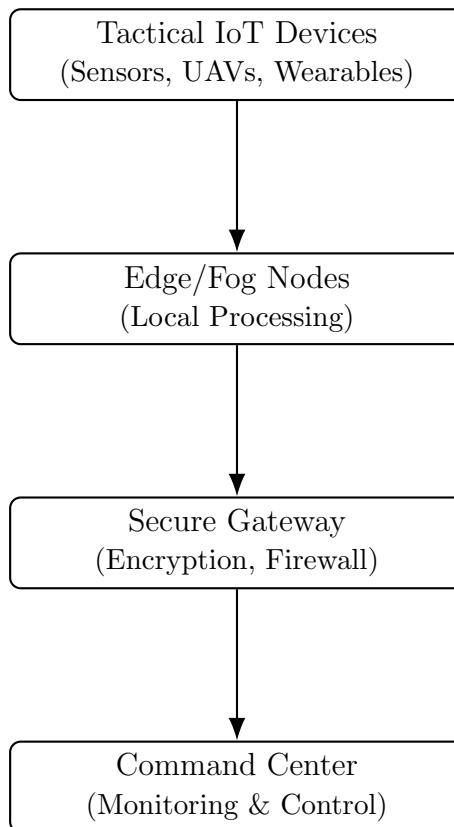


Figure 1: Secure Communication Architecture for Tactical IoT Networks

Starting strong means knowing what could go wrong. Spotting key equipment comes before anything else when setting up smart device networks. Once those are clear, weak spots need a close look - what might fail, how badly. Picture each break-in method,

Table 1: Security Mechanisms in Military and Tactical IoT Networks

Layer	Security Mechanism	Purpose
Physical Layer	Frequency Hopping	Anti-jamming and interception resistance
Physical Layer	Spread Spectrum	Signal confidentiality and robustness
Network Layer	Secure Routing Protocols	Protection against routing attacks
Network Layer	Trust Management Systems	Malicious node detection
Transport Layer	End-to-End Encryption	Data confidentiality and integrity
Application Layer	Authentication Schemes	Identity verification and access control
Cross-Layer	Intrusion Detection Systems	Anomaly and attack detection

then weigh the damage it could cause. Frameworks for judging risks shift focus toward what keeps operations alive. Protection steps get lined up by importance, nothing more. Stopping threats means using steps before trouble happens along with plans for after. Strong login checks, hidden message routes, plus tight rules about who can see what help block break-ins early. The goal here is making it harder for hackers to win. If something slips through, actions shift toward limiting damage and getting things back. Once a breach shows up, cutting off infected parts fast matters most. Bringing safe connections online again becomes the next move. Testing with red teams gives clear hints about weak spots in systems. Because flaws get found on purpose, defenders learn where shields need fixing - before attackers show up. When checks happen often, safety stays close behind new threats. Even with progress, most ideas still live inside computer tests or lab conditions. When actual combat zones enter the picture, things like shifting weather, movement challenges, and mission demands strain current systems. Because of this, testing in real situations must keep going if theory is ever to meet reality on the ground.

2.2 Wireless Sensor and Ad Hoc Network Foundations

The backbone of tactical IoT systems consists of Wireless Sensor Networks (WSNs) and Mobile Ad Hoc Networks (MANETs). Both types of networks operate without fixed infrastructure, allowing for self-organizing communication nodes, dynamic routing, and cooperative communication capabilities. As a result, they have a decentralized structure, which provides flexibility but leaves room for attacks like Routing Attacks and Compromise.

2.3 Security Principles and Threat Models

The basic security requirements, which include aspects of confidentiality, integrity, availability, authentication, and non-repudiation, serve as the guidelines for military communication systems. Due to the nature of a tactical environment, there is a need to consider advanced threat possibilities, which include aspects such as jamming, spoofing, eavesdropping, denial of service, Sybil attacks, and advanced persistent threats. A good

understanding of these aspects is required so as to offer positive.

2.4 Architectural Paradigms in Tactical IoT

Current tactical IoT architectures incorporate new trends in IoT solutions, including edge computing and zero trust. These new trends distinguish themselves from traditional architectures that implement a centralized cloud-based environment and foster the reduction of latency. In addition, security integration across layers is now possible. Out in the field, tough gear matters more than perfect blueprints. When setting up radio links for defense work, surprises pop up fast - planning needs room to shift. Testing happens nonstop, not just once. Equipment gets baked by sun, choked with sand, shaken hard, soaked through - all while staying online. Even under that kind of pressure, encryption can't slip. Protection runs deep, built into how things operate, not layered on top. Out in the field, how things move affects how safely messages travel. When IoT gear hits the ground fast, it has to work right away without waiting. Because of that, getting systems secure from the start needs speed plus accuracy. If setup drags on, operations stall - mistakes creep in more easily too. Just knowing the tools matters as much as using them right. When people work with battlefield-connected devices, they need clear rules for safe messaging along with practical steps that actually fit their tasks. A high-end defense setup might still fail if settings go wrong or someone makes a slip. Staying sharp through regular practice plus designs that feel natural cuts down on mistakes before they happen. How long gadgets stay online affects how they're managed over time. Even after years of use, these tools still need fresh software and fixes for weak spots. Updates pushed from afar keep them safe without hauling hardware back in person. Yet every change sent remotely has to resist tampering by outsiders.

3 Core Concepts and Approaches

Security in military wireless networks begins where standard encryption ends. When chaos strikes on the battlefield, protection can't live just in code. Layers matter - each part of the system holds a role. Trust isn't built through secrecy alone. Operation must persist, even when signals flicker. Resilience shapes how messages travel. Data stays safe not by chance, yet through design woven deep. Reliability becomes visible when everything else fails. Mission success depends on connections that adapt. Right where signals meet air, keeping them safe starts with shielding at the physical level. Because radio waves travel openly, anyone nearby might catch them or scramble them. Jumping between channels fast, along with smearing data across broad frequencies, blocks snooping attempts pretty well. Instead of staying on one frequency, systems shift rapidly - this confuses anyone trying to lock on. Focus matters too: shaping the signal like

a spotlight aims it only where needed. Looking at military tactical IoT networks beside everyday commercial ones shows how each shapes its tech around very different needs. Though they both connect many gadgets through wireless links, what they aim to do - also how they stay safe - splits sharply. Devices in regular consumer setups usually help people by automating tasks, cutting effort, or saving time inside predictable places like offices, factories, or houses. But gear used in battlefield-connected systems must work under fire, handle sudden changes, survive jamming attempts, while staying reliable when lives depend on it. What sets them apart most is how strong and complex the dangers can be. While everyday internet-connected devices deal with hackers trying to sneak in, steal information, or cut off services, those attacks usually aren't backed by entire governments. Military setups face something sharper - attacks that blend digital strikes with physical disruption, jamming signals on purpose, or eavesdropping through clever tech tricks. Because of this, armed forces need tougher locks on their data, stricter ways to verify users, gear built to survive harsh conditions, and systems always watching for new threats before they strike. Behind every message sent, there's a layer of defense ready to respond. That way, less spills out into surrounding areas, leaving fewer chances for outsiders to overhear. Out in the open, away from cables and anchors, moving data safely becomes critical when devices shift constantly. Fixed setups do not face what military-grade IoT faces - nodes on the move, reshaping connections every few minutes. Because positions reset so often, bad actors find more openings to twist how traffic flows. One way around this? Watch each device like a cautious neighbor, tracking who behaves well over time, then picking those paths first. Another angle: send pieces of information through separate lanes at once, avoiding all-eggs-in-one-basket risks without shouting about redundancy. Safety grows quietly when options multiply behind the scenes. Even though cryptography is essential for safe messaging, using it on small field gadgets means working within tight limits. Instead of heavy methods, lighter encryption cuts down processing work while saving battery power. Only trusted gear gets into the network because strong checks stop fake or outsider connections. Rather than one main control point, spreading out how keys are handled avoids weak spots and fits better with scattered missions. A fresh line of protection shows up through monitoring tools. Because they watch how data moves and what systems do, odd actions stand out more easily. These signs often point to something harmful happening behind the scenes. With machine learning stepping in, small shifts in usual flow become easier to catch. Once these smart alerts trigger, responses kick off without waiting. That speed helps shut down affected parts fast. Then paths across the network shift on their own. Work keeps going even when pieces fail. The whole setup runs smoother because each piece reacts before damage spreads. Security for battlefield IoT leans on flexibility, multiple safeguards, smart tech that acts fast. Mix in hardware-level shields, self-adjusting data paths, lean encryption, round-the-clock watch - military comms gain strength against today's shifting warzone

threats. A single idea stands out when thinking about safety in systems: stacking barriers like layers. When safeguards exist across different stages of how devices talk, problems in one area won't bring everything down. If someone tries to eavesdrop or cause noise, the first level can make it harder - right where signals travel through air or wires. Further up, decisions about which path data takes stay protected by checks built into connections. Closer to users, rules decide who gets in and what each machine is allowed to do. Because defenses repeat themselves in smart ways, breaking through becomes much tougher even if one part fails. Change readiness matters just as much. When threats shift fast, tactical networks need ways to keep up. So security settings in communications adapt on the fly, driven by what happens at that moment. Detection of odd traffic or disruptions might trigger tighter logins, block questionable devices, or reroute signals through safer lanes. Reacting as events unfold cuts risk while keeping missions running, even when humans aren't watching every second. Out in the field, one thing becomes clear - central systems might vanish without warning. When that happens, gadgets can't wait around for permission to act. Instead, they check identities on their own, talking directly to stay linked. Trust builds between them through shared rules, not top-down orders. If contact with headquarters drops, operations keep moving because power spreads across units. Survival gets easier when no single node holds everything together. A single trusted ID per gadget keeps things locked down tight. When machines talk on a battlefield mesh, proof of who they really are stops fakes from sneaking in. Hard checks at entry points make certain only approved units join the flow. Who gets to see or send what rides on clear rules set ahead of time. Lockstep verification cuts down rogue actors before they trigger chain reactions inside. Even when parts break, staying connected matters just as much. When main pathways stop working, tactical networks lean on spare links and different relay points. Should one gadget get taken out, the system finds another way using reliable backups. Traffic shifts without waiting, keeping messages moving. Functionality holds up, because the design expects pieces to fail. Watching things closely while staying alert makes these main methods stronger. Because unusual signs might point to threats, tools check how data moves and how gadgets act. Once odd behavior shows up, automatic reactions step in by cutting off impacted parts or starting protective steps. Small weak spots stay small when they get caught early through constant watchfulness. What makes these networks stand out? Old gear works alongside new tech through smart connections. Security stays strong because trusted gateways manage data flow between them. Different teams operate together even when using separate tools. Sensitive details remain protected during shared missions. Over time, how well a system handles repairs matters just as much as its initial setup. When dangers change, so should the tools fighting them. Updates pushed from afar keep operations running while improving protection. Adjustments to rules and background software happen smoothly when design allows it. Staying ahead means building something ready for what comes next. Longevity hides in small upgrades,

not big launches. When it comes to secure wireless links in military and tactical IoT setups, defense happens in layers. One key is shifting quickly when threats appear. Systems often operate without a central hub, relying instead on distributed control. Trust hinges on precise identification of every device involved. Even under pressure, operations must keep moving - resilience shapes design choices. Watching traffic nonstop helps catch anomalies early. Equipment from different sources still needs to work together smoothly. Future changes stay manageable because flexibility builds into the foundation. Each piece supports the whole, making field communications tough enough for real combat scenarios.

4 Comparative Discussion

As one creates contrasts between the commercial IoT systems and the military tactical IoT network, different reasons establish the differences between the two, hence making their structure different from one another. These fundamental requirements of the structure of the system for the commercial systems are scalability, cost-effectiveness, convenience, and energy utilization. Except in those areas, attention is majorly put on the security of the system, especially with the mechanisms that are usually adopted by the IoT system in protecting the data of the consumers to ensure no unauthorized access. In the case of military systems, the context of application is an area where all forms of communication are likely to be attacked. Another major difference is observed in terms of architecture design. For instance, civilian IoT networks are often cloud-based, whereby the data from everything is channeled through a central hub for easier management. While this is easy, it exposes the network to a single point of failure together with a potential increase in latency. When it comes to a tactical network, architectural design becomes a major factor because it adopts a decentralized network design. In the case of IoT networks, especially within a commercial setting, it is often true that networks are implemented within moderately stable environments such as smart homes, industries, or even within infrastructure located within a city and others, among them. In contrast to that, within a military environment, it is apparent that the networks ought to be dynamic; particularly because these types of networks shall be consistently involving very dynamic nodes such as soldiers, vehicles, UAVs, maritime, among others. In addition, the degree of threat and adversary will also produce a line of demarcation between these two domains; while IoT domain for civilians will require protecting against cybercriminals and privacy aggressors, the tactical domain will require protecting against, for example, state adversaries who will also be better equipped as far as jamming gears are concerned. For instance, it is deemed extremely key to understand that IoT security solutions used in military domains will require more encryption and faster signal compared to those used for civilians. From the discussion above, it can be concluded that IoT security solutions used for civilians will not work for military IoT networks. What happens in the field

goes beyond wires and signals. Decisions about who knows what tie directly into laws that guide how armies act worldwide. Hiding critical details cannot come at the cost of mismanaging data. How messages travel matters just as much as what they say. Secrets need safeguards, yet those guards must follow clear moral lines. Firm links between teams let choices unfold together, fast moves follow - that pushes missions forward. Yet too much control in one place, or leaning hard on machines, risks collapse once tech stumbles. So plans take shape best when backup paths and staying strong under stress guide how messages flow. Working across borders brings tricky questions about who gets what data. To team up smoothly, allies need systems that are both safe and adaptable, built on clear rules.

5 Practical Insights and Use Cases

Unmanned systems, which include UAV swarm technology, can also be another major application area for these technologies, which require timely and seamless communication. Similarly, for these automated systems, which can include autonomous ground technology, it is important to include robust wireless network technology to enable these systems to avoid being hijacked or taken control of by unauthorized users. For autonomous systems using swarm technology, it is also important to consider robust cryptographic solutions to enable these systems to ensure the integrity of the system even when they are compromised. Additionally, for UAVs, which can be greatly impacted by other systems using the same spectrum, lightweight cryptography solutions are critical. The wearable soldier systems enable health status monitoring, positioning, and communication. Secure methods of communication are required for the safe and effective transmission of health status, position coordinates, and military strategy. The system used should enable the verification of the source of the information and also be effective enough for use. The smart military bases and camps use secure IoT systems for military base security, management of military personnel, surveillance cameras, and tracking of military supplies. The use of intrusion detection systems and communication systems in both wearable soldier systems and smart military bases and camps enable effective security against cyber attacks and physical interference. Lately, protecting wireless signals in battlefield gadgets and smart devices matters more - defense setups now link up heavily, sharing tons of live data. At first, studies zeroed in on coded messages and safe radio waves to keep secrets locked down. When sensor webs and roaming device clusters evolved though, new paths opened - decentralized shields popped up, routes started relying on verified nodes, shared ID checks spread across systems without a central hub. Some studies look at safe ways to route information in fast-changing conditions. Instead of trusting every part equally, they focus on reducing damage when parts fail unexpectedly. Different projects examine tools that spot intrusions during field operations, relying heavily on quick recognition of risks.

Because threats emerge suddenly, these tools watch how devices act, noticing odd shifts in normal messaging styles. When signals face disruption, staying connected becomes a challenge. Though jamming attempts grow more common, new methods help maintain links. Where enemies target frequencies, systems now shift on their own. Instead of sticking to one band, they move around smartly. Some radios sense open channels, then adjust without delay. Even under pressure, transmission stays strong. These changes make interruptions less effective. Lately, focus moved to blending artificial intelligence with tactical communication safety. Some suggest using machine learning to spot faint irregularities, foresee threats, then trigger automatic defenses. Still, experts point out dangers like tampering by attackers - raising demand for solid, dependable AI methods models. Even with progress, most ideas still live inside labs or computer tests. Out there where fighting happens, things shift fast - weather changes, movement gets messy, missions evolve. That throws off current systems, no matter how smart they look on paper. So work has to keep going, tested outside, where real conditions push every part to its edge. Finally, the actual application of the solutions also underscores the significance of scalability and, above all, interoperability. As portrayed, higher command systems often require both legacy-based comm systems and latest IoT systems to communicate effectively. The lessons learned from the application of these solutions underscore the significance of scalable security systems with rapid upgradability, remote patch, and adaptability, among other qualities. Consequently, wireless security for military applications, in summary, calls for a balance between strength, flexibility, and performance for maximum support of military missions. Out in the field, wireless signals carry vital updates where military gear links through toughened networks. When eyes on the ground need to report motion or shifts in terrain, tiny detectors spread wide send back live details. Instead of sitting still, these tools keep feeding fresh readings straight to central teams who act on what they receive. So long as messages stay locked down, outsiders can't peek, twist, or exploit what flows between nodes. With every signal verified and shielded, patrols gain sharper awareness during watch tasks and early warnings take clearer shape. Drones, robots, and underwater craft often depend on stable connections to move, work together, or follow orders. When groups operate as a team, smooth data exchange keeps them aligned and effective. Without strong encryption, signals might be hijacked, faked, or disrupted - putting tasks at risk. It's not just messages that need shielding; actual vehicle control hangs in the balance. Safety and performance hinge on trustworthy links between units. Missions fail if outsiders seize command channels. Protection means more than secrecy - it means staying in charge. Soldiers today wear gear that shows why strong IoT links matter in combat zones. Health signs, whereabouts, and mission updates flow from tools strapped on service members. Because of these feeds, leaders grasp events faster - also act sooner during sudden shifts in warzone activity. Yet sending body metrics and GPS spots opens risks around exposure and hacking threats. Strong logins and scrambled signals

guard such details, letting only approved users reach them at critical moments. Keeping communications safe matters just as much on smart military sites as it does at temporary field locations. Surveillance cameras connected through modern networks work alongside entry checkpoints, border alarms, and supply monitors - each part relies on the others. When these tools link up, they help guard the site while keeping tasks running smoothly. Threats might come online or from someone nearby trying to interfere. Protection comes from locked-down connection points, constant oversight, and strict rules about who can reach what. Safety holds when defenses block outsiders and watch those already inside too. In military settings, reliable IoT links help manage gear, transport, and materials on the move. Because updates happen instantly, teams adjust faster and distribute assets more wisely. Yet when signals get intercepted, enemies might track where forces go or block essential deliveries. That means every system must guard data from start to finish, limit who sees what, and work smoothly within current command setups. Real situations show one thing clearly: encrypted wireless networks aren't just theory - they shape whether missions succeed or fail.

6 Challenges and Open Issues

Although there have been rapid developments in secure communication systems, it is still challenging for military and tactical IoT systems to achieve higher operational potential. One of the major challenges faced is how to achieve adequate security enforcement with stricter resource constraints. IoT devices like sensors, wearables, and unmanned systems, while deployed in the field, normally run with limited resources. The use of robust security mechanisms like encryption, continuous authentication, intrusion detection, etc., often causes computational overheads, making IoT devices consume more power. The other important challenge can be viewed from the perspective of a dynamic and hostile environment. Generally, topology fluctuates following node mobility, as well as interference, which renders the problem of secure routing and key management a challenge. Next, promoting and maintaining trust relationships and ensuring the continuity of a secure session over an ever-changing topology is a challenge yet to be solved. Similarly, spectrum jamming, spoofing, and interference injection, which form a part of electronic warfare against wireless networks, remain dynamic and a challenge, requiring an intelligent and adaptive form of anti-jamming to handle a hostile environment. Another major challenge would come from the level of interoperability and heterogeneity. Tactical IoT networks will typically incorporate legacy systems, satellite systems, mobile command units, and other new and emerging communication systems. Hence, it would be important to ensure seamless and secure communication across all these disjointed systems without adding any new vulnerabilities. With the advent of new elements of AI systems for anomaly detection and autonomous decision-making, several other challenges to security would

come from adversarial machine learning, data poisoning, and model evasion attacks. In addition to this, AI security is still an emerging area of research. Finally, the advent of quantum computing poses an irresolvable threat to many of the cryptographic systems used today. The transition to quantum-resistant cryptography, balancing requirements for low latency and negligible computational processing with the demands of applications like UAV swarm control and remote robotic operation, remains a major hurdle. Overcoming these challenges entails the development of adaptable cross-layer security models that can grow with the technology and the sophistication of our adversaries. Out in the field, keeping wireless signals safe within military IoT setups gets tricky fast - battle conditions change everything. What stands out? The need to lock things down tightly while still meeting tight mission limits. Gadgets like sensor nodes, body-worn tech, and drones usually run on weak processors, tiny storage, and small batteries. Heavy-duty protections - think encryption, identity checks, constant watch routines - they eat up computing power and drain energy quick. Making sure safety stays solid without slowing gear down or killing it early - that's what engineers wrestle with every day. Shifting patterns make tactical networks tough to manage. Not like stable setups, warzone IoT gear moves a lot - topologies shift often, links drop now and then. Devices appear or vanish mid-operation: motion, weather, harm can all pull them offline. Keeping paths secure, connections trusted, timing aligned gets messy when everything keeps changing. Building methods that adjust fast to these shifts - without losing protection or adding delay - is still something researchers haven't fully solved. Another area of open questions is related to interoperability and system diversity. Tactical IoT networks are typically composed of devices from different manufacturers, legacy communication systems, satellite communication, and newly developed systems. The challenge of ensuring secure communication between systems with different capabilities is a complex one. It is difficult to achieve seamless interoperability without compromising security. There may be security vulnerabilities that can be exploited by attackers due to system diversity. Finally, the pace of development of emerging technologies is also bringing new uncertainties. The growing role of artificial intelligence in tactical communication networks is improving detection and automation capabilities, but it is also providing new avenues for adversarial machine learning attacks. On the other hand, the growing role of quantum computing is threatening the long-term sustainability of many conventional cryptographic algorithms. The challenge of moving to quantum-safe algorithms without sacrificing efficiency is a difficult one. The solution to these open problems will require ongoing research and collaboration. Looking at military tactical IoT networks beside everyday commercial ones shows how each shapes its tech around very different needs. Though they both connect many gadgets through wireless links, what they aim to do - also how they stay safe - splits sharply. Devices in regular consumer setups usually help people by automating tasks, cutting effort, or saving time inside predictable places like offices, factories, or houses.

But gear used in battlefield-connected systems must work under fire, handle sudden changes, survive jamming attempts, while staying reliable when lives depend on it. What sets them apart most is how strong and complex the dangers can be. While everyday internet-connected devices deal with hackers trying to sneak in, steal information, or cut off services, those attacks usually aren't backed by entire governments. Military setups face something sharper - attacks that blend digital strikes with physical disruption, jamming signals on purpose, or eavesdropping through clever tech tricks. Because of this, armed forces need tougher locks on their data, stricter ways to verify users, gear built to survive harsh conditions, and systems always watching for new threats before they strike. Behind every message sent, there's a layer of defense ready to respond. How buildings inside machines are set up matters too when you look close. Instead of spreading tasks out, most business IoT systems store information, handle computing, and manage protection through one main cloud hub. Easier to grow and fix, sure - yet if that central spot breaks, everything can halt. Military-style setups go another way entirely, scattering functions across many nodes so the system keeps running even under stress. When connections to central control fail, systems rely on edge computing so decisions happen locally instead. That setup changes the way security rules get applied in practice. When it comes to movement and surroundings, the gap between commercial and military IoT grows clear. Devices used outside defense usually stay put, working in calm places where nothing much happens around them. Troops on foot, drones in flight, armored trucks pushing through mud - these keep moving fast across rough lands, battered by snow, sand, or rain. Each shift in position shakes up how signals travel, breaking links without warning. Because connections come and go unpredictably, paths for data must reshape themselves constantly. Security setups locked in place might work fine at a warehouse but fail when units scatter under fire. Out in the field, how well things work ties closely to what risks get allowed. While everyday tech leans toward saving money and smoothing out how people interact with devices, it might let some safety gaps slide if it means easier access or lower prices. On the other hand, battlefield-connected gear puts completing the task first, ahead of nearly everything. When signals drop even a little during fights, outcomes can turn badly fast. Because of that, backup systems, automatic fallbacks, and multiple overlapping shields show up far more often when building military-grade links. One thing stands clear when comparing these settings - how they handle working together shifts dramatically. Commercial setups chase smooth links inside everyday tech environments, whereas defense grids tie together old equipment, cross-domain tools, plus connections across allied forces worldwide. Getting varied groups spread far apart to exchange data safely means tight user limits, agreed-upon encrypted methods, and adaptable rules on who sees what. It's obvious looking at both sides - the safeguards built for household gadgets fall short in battlefield networks unless heavily reworked. What plays out operationally, the dangers faced, along with design limitations push military needs into a

tougher category altogether - one demanding something sturdier, less breakable, entirely separate in mindset.

7 Future Directions

Hence, the direction that the future of robust wireless communications will take in military and tactical IoT networks will revolve around intelligent, adaptive, and autonomous security infrastructures. This follows the fact that security solutions in military contexts will move from the traditional data-centric paradigm of warfare to data-centric, security solutions. In effect, autonomous and dynamically adaptive security infrastructures will substitute the traditional security infrastructures. A new frontier in the realm of secure IoT communications will revolve around the development of cognitive security infrastructures. Post-quantum cryptography is another area of research significance. As quantum computing innovations threaten to undermine traditional public-key infrastructures, tactical networking infrastructures must adapt to new generations of cryptography that can support long-term security guarantees. Post-quantum cryptography solutions, which might incorporate lattice-based cryptography, Hash-based cryptography, or code-based cryptography, will be required to support edge environments with low latency. Artificial intelligence, when referred to as broadly as machine learning, among other terms, has considerable potential that is significant for tactical communication systems that can influence the character of next-generation communication systems. For instance, it can engage different capabilities such as predictive anomaly detection, self-healing and cumulative capabilities, or automatic containment of intrusions. For instance, it can disconnect illegal nodes in networks without human supervision. There are distributed learning paradigms, such as federated learning, which can assist these systems in allowing different nodes to work cooperatively to develop threat intelligence providers without raising any data privacy concerns, as well as without incurring any major costs. With regard to the formulation of opportunities for developing the role of emerging technologies applied to communication, which will impact the tactical role of IoT, it is asserted that the emerging technologies include communication technologies, which will be incorporated into 6G technology, satellite-integrated technologies, and SDNs, which will eventually improve the communication security process within the system. Furthermore, zero trust architectures will be a vital element in the validation of communication within IoT systems, irrespective of the location in terms of the communication architecture. Tomorrow's battlefields might reshape how we lock down connected gear, simply because tech keeps shifting. Intelligence built into machines could demand tighter data handoffs, step by step. When devices link more deeply, keeping them honest and reliable may grow tangled without clear paths forward. New tools like shared digital ledgers, stronger hardware shields, and smart network splits could reshape how field strategies are built. They open paths to safer

teamwork and better use of supplies. Even so, opponents keep upgrading their ways to disrupt and take advantage. Success over time in tactical IoT protection hinges on steady invention, teamwork across fields, yet constant refinement through cycles. Frameworks for safety need adaptability built in, ways to update easily, while reacting quickly when missions shift. Wireless security progress drives how well tomorrow's military networks withstand threats, even as challenges grow more complex.

8 Conclusion

These days, safe radio links are essential for military gadgets tied into digital networks. When fighting shifts to rely on live data and linked gear, staying connected keeps missions running smoothly. Devices like drones, body sensors, cameras, robots, and control centers talk to one another through battlefield internet setups. Because they share information instantly, teams see threats faster, react together, sometimes even act without waiting. Yet every link added to boost speed can open doors hackers might slip through if left unchecked. One thing stands out from this research: locking down communications in battlefield IoT settings does not come from one tool alone. Layered defenses spread across hardware, data flow, and software layers make real security possible. Signals at the physical level resist eavesdropping and interference more easily when built with certain methods. On top of that, smart path selection and trust checks guard how information hops between nodes. Devices must prove identity before joining any operations - this gate keeps imposters out. Watchful background systems spot odd behavior early, stopping small glitches from snowballing into chaos. What stands out most is how crucial it is to stay flexible. When movement, weather, or enemy actions shift without warning, situations transform fast. Because of this, defenses need to move at the same pace - changing instantly as threats grow or missions evolve. If a system cannot bend under pressure, new tactics will simply bypass it. Protection that learns from surroundings, shifts settings on its own, adjusts rules based on context keeps operations running. Without these responsive layers, even strong barriers fail when faced with surprise. Down the road, strong wireless links in battlefield IoT systems keep changing along with new tech. With better comms protocols, spread-out data processing, and trust rooted in shared control comes a shift in military networks. Even so, attackers won't stand still - new tricks to break or misuse systems will emerge. Because of this, steady progress, tough evaluations, and staying ahead on safety checks stay critical. Mission success ties directly to how well tactical IoT links are shielded. When signals stay protected, leaders get correct data, self-operating tools work without hiccups, also troops keep contact with backup networks. If the wireless base fails, top-tier gear might still fall short. Because of this reality, shielding messages cannot play a minor role - it has to weave through each phase of building and rolling out systems. When it comes to military and tactical IoT networks, keeping wireless

links safe isn't just about one fix - it ties together tech choices, how teams operate, and bigger strategic goals. Layered defenses, flexible protections, strong recovery abilities, smooth system connections, along with smart oversight, help create comms infrastructure tough enough for today's battlefield conditions. Progress won't stop there - ongoing study, new approaches, plus real-world testing play key roles in maintaining trustworthy, ready-to-use network performance amid growing threats and chaos. Radio links that stay safe shape today's battlefield tech. When machines watch, move, or share live updates - connections do more than carry signals. Outcomes shift based on whether messages arrive intact. Missions stall if signals get hijacked or scrambled mid-air. Hidden risks rise when gear talks without guardrails. Trust grows only when tampering fails. Strength hides in silent safeguards built into every pulse sent. Keeping control means blocking ears before they listen. One thing stands clear across this work: safety in battlefield IoT isn't about single shields standing alone. Layered defenses, woven together, do more - linking hardware links, trusted pathways, identity checks, live oversight. Each part feeds the next, building strength that shifts when chaos hits. Protection lives inside the design now, tucked into signals and rules soldiers follow daily. Tougher networks emerge - not because they block everything, but because they bend without breaking. Hidden guards run constant drills, spotting danger before it spreads too far. One thing stands clear - staying flexible matters more than ever. Where movement never stops, where threats hide in doubt, operations keep shifting unpredictably. When links break or signals fade, systems still need to find ways through chaos while holding their course. Backup paths form naturally. Control spreads out, avoiding single points of failure. Smart reactions kick in before danger takes hold. Through pressure, these layers help missions stay on track. Out in the open, talk shifts toward how fresh tech trends are quietly steering the path of battlefield messaging. Because of progress in machine learning systems alongside spread-out data networks, plus newer radio wave formats, spotting threats gets sharper while teamwork improves. Still, fitting these pieces together demands care so defenses grow stronger instead of tangled. Each step forward needs checking, rechecking, then adjusting when blind spots pop up from tomorrow's tools arriving today. When you look at military and tactical IoT networks, keeping wireless links safe isn't just about tech - it ties into how forces operate and plan. Strong encryption alone won't cut it; systems must shift quickly, work together across platforms, bounce back when hit, plus stay ahead of evolving risks. Though battlefields grow more digital by the day, one thing stays clear: reliable, shielded comms are non-negotiable for armed forces everywhere.

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15]

References

- [1] Salih Mousay Abraheem, Muftah Emtir Ali, and Reda Muftah Abuali. Emerging trends in quantum sensors: Applications in defense and communication. *Middle East Journal of Pure and Applied Sciences (MEJPAS)*, pages 19–37, 2025.
- [2] Deafallah Alsadie. Cybersecurity and artificial intelligence in unmanned aerial vehicles: Emerging challenges and advanced countermeasures. *IET Information Security*, 2025(1):2046868, 2025.
- [3] Victor Monzon Baeza, RaÃel Parada, Laura Concha Salor, and Carlos Monzo. Ai-driven tactical communications and networking for defense: A survey and emerging trends. *arXiv preprint arXiv:2504.05071*, 2025.
- [4] Bruno Branco, JosÃ Silvestre Serra Silva, and Miguel Correia. Cyber attacks on commercial drones: A review. *IEEE Access*, 13:9566–9577, 2025.
- [5] Rajni Idiwali and Monika Mathur. Wearable antennas for next-generation wireless communication: A comprehensive review. *environments*, 6:7.
- [6] Charalampos Katsis, Imtiaz Karim, and Elisa Bertino. Zero-trust strategies for o-ran cellular networks: Principles, challenges and research directions. *arXiv preprint arXiv:2511.18568*, 2025.
- [7] Rachel Kufakunesu, Herman Myburgh, and Allan De Freitas. The internet of battle things: a survey on communication challenges and recent solutions. *Discover Internet of Things*, 5(1):3, 2025.
- [8] Sudesh Kumar, Anshuman Tiwari, Yogesh Ahirwar, Gaurav Kumar, and Muhammad Yeasir Arafat. The rise of uav-based smart surveillance: A systematic review of trends and technologies. *IEEE Access*, 2025.
- [9] Chang Lu and He-Jing Huang. Performance and development trends of ultrasound diagnostic systems in military settings: a review. *The Ultrasound Journal*, 17(1):54, 2025.
- [10] Richa Priyadarshani, Yalçin Ata, Mohamed-Slim Alouini, et al. Jamming intrusions in extreme bandwidth communication: A comprehensive overview. *IEEE Open Journal of the Communications Society*, 2025.
- [11] Paulo HL Rettore, Jannis Mast, Thorsten Aurisch, Aline Carneiro Viana, Peter Sevenich, and Bruno P Santos. Military iot from management to perception: Challenges and opportunities across layers. *IEEE Internet of Things Magazine*, 8(2):25–31, 2025.

- [12] Branislav Todorović, Zoran Vasić, Andrija Ostojić, Saša Sretenov, Aleksandar Kopta, Aleksandar Lazović, Lazar Paunović, Veljko ilas, Miloš Delić, and Mirko Delić. Command and control information systems for military applications. *Vo-jnotehnički glasnik/Military Technical Courier*, 73(4):1510–1530, 2025.
- [13] Tong Wu, Xueguang Zhou, and Wei Fu. Security issues in software-defined radio: a review. *Cybersecurity*, 9(1):19, 2026.
- [14] Haowen Yang, Yuan Liu, Xuran Li, Zhiquan Bai, Liang Yang, Gaofeng Pan, and Hongwu Liu. Physical layer security and covert communication in uav-isac networks: A comprehensive survey. *Journal of King Saud University Computer and Information Sciences*, 37(10):312, 2025.
- [15] Aaron Yu, Iuliia Kolotylo, Hashim A Hashim, and Abdelrahman EE Eltoukhy. Electronic warfare cyberattacks, countermeasures and modern defensive strategies of uav avionics: A survey. *IEEE Access*, 2025.