Discover Internet of Things

Review

The internet of battle things: a survey on communication challenges and recent solutions

Rachel Kufakunesu[1] · **Herman Myburgh**[1] · **Allan De Freitas**[1]

Received: 29 August 2024 / Accepted: 1 January 2025
Published online: 10 January 2025

Abstract
The use of Internet of Things (IoT) technology in military settings has introduced the notion of "Internet of Battle Things" (IoBT), transforming modern warfare by interconnecting various equipment and systems essential for battlefield operations. This connectivity facilitates real-time communication, data sharing, and collaboration among military assets, enhancing situational awareness, decision-making processes, and overall operational effectiveness. The domain for IoBT encompasses a broad range of military assets, from drones and ground vehicles to soldier-worn wearables, sensors, and munitions. These assets are capable of collecting and transmitting critical information from the battlefield, including location data, status updates, environmental conditions, and the movements of adversaries. IoBT networks depend on robust communication networks, secure data transmission protocols, advanced data analytics for processing vast datasets, and seamless integration with command-and-control infrastructures. However, IoBT devices and systems function in dynamic and challenging battlefield conditions which present unique communication challenges. This study aims to review research efforts that provide current state-of-the-art solutions, their limitations, and emerging technologies. We classify these challenges into interoperability, power and energy management, security, and network resilience, while also discussing future research directions to improve communication in IoBT networks.

Article Highlights

1. IoBT enhances military operations through real-time data sharing and decision-making.
2. Communication challenges arise from interoperability, power, and security constraints.
3. Emerging solutions focus on improving network resilience, energy efficiency, and secure data exchange.

Keywords Communication · Energy-efficiency · Interoperability · Internet of battle things · Military · Network security

Herman Myburgh and Allan De Freitas contributed equally to this work.

✉ Rachel Kufakunesu, rachel.kufakunesu@tuks.co.za; Herman Myburgh, herman.myburgh@up.ac.za; Allan De Freitas, allan.defreitas@up.ac.za | [1]Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Cnr Lynnwood and Roper Street, Pretoria 0028, South Africa.

1 Introduction

Integrating advanced technologies in modern warfare has transformed traditional battlefields into dynamic and interconnected ecosystems called the Internet of Battle Things (IoBT) [1]. IoBT signifies a significant change in military operations as it harnesses the capabilities of interconnected devices, sensors, and communication systems, enhancing situational awareness, decision-making processes, and overall operational performance [2]. The landscape of IoBT is a multi-domain environment consisting of land, air, sea, space, and cyberspace, where boundaries are often blurred and integrated. The core of IoBT involves the smooth integration of different military assets, like unmanned aerial vehicles (UAVs), ground vehicles, soldier-worn wearables, sensors, and munitions, all equipped with Internet of Things (IoT) capabilities [3].

Although IoBT provides vast prospects for transforming military operations with its potential for real-time data analytics, enhanced situational awareness, and streamlined logistics, it also poses unique challenges that must be carefully navigated regarding energy usage and sustainability, cyber security threats, and interoperability issues. Several IoBT devices and systems operate in resource-constrained environments, depending on battery power, and are frequently deployed off-grid for extended periods. Optimizing communication strategies improves energy efficiency, an essential consideration for ensuring prolonged operational endurance and mission success in military settings [4–6].

This review article explores communication challenges in IoBT, intending to produce a thorough overview of current research, methodology, technologies, and future directions in this emerging field. By examining the fundamental principles, challenges, and novel solutions related to IoBT, we highlight the significance of network efficiency in communication in military operations and point out potential areas for further research and development. Safety, reliability, and predictability of IoT behavior are important for military operations, hence analyzing the state of affairs. The topic of IoBT remains veiled in secrecy and government-imposed limitations, effectively removing it from the public domain. This brings its own challenge of information void. We summarise our key contributions in this review article as follows: i) An overview of the IoBT; ii) a review of the existing communication challenges in IoBT; iii) an evaluation of the schemes that address the communication challenges; iv) a consideration of the strengths and shortcomings of the propositioned algorithms; and v) the identification of areas of further research and potential future directions.

The rest of the paper is structured as follows: Sect. 2 provides a framework to guide readers through the research. Section 3 presents a technological overview of IoBT, and Sect. 4 outlines the IoBT architecture. Section 5 provides insights into the communication challenges in this domain. Section 6 compares and discusses the existing strategies. Section 7 identifies the research gaps and future direction, and Sect. 8 concludes the paper.

2 Methodology

The methodology used to identify and select the communication challenges discussed in this paper follows a systematic literature review approach. The selection of the relevant literature for analysis in this article was based on a keyword search, namely,"Internet of Battle Things", "The Internet of Battlefield Things", "The Internet of Military Things", "Military Internet of Things" and "Defence Internet of Things". The search included all these words as the terms were used interchangeably in literature but referred to the same technology. The scope of the review was initially based on preliminary research in IoBT literature and identifying key challenge areas. The focus was on communication challenges encountered within the Internet of Battle Things environment, including interoperability, power and energy management, security, and network resilience. This methodology involved the following steps:

1. Research questions: We aimed to address the following research questions
   - What are the most critical communication challenges faced in IoBT environments?
   - How do existing research efforts propose to overcome these challenges?
   - What are the emerging trends and future directions in this domain?
2. Keyword search: A comprehensive keyword-based search was conducted to identify relevant literature. Keywords such as "IoBT communication challenges," "IoBT interoperability, "Energy efficiency in IoBT," "IoBT security," and "IoBT

network resilience" were used to search major academic databases like IEEE Xplore, ACM Digital Library, Springer, Web of Science, and Scopus, as well as works cited by other articles. A further search was done on the communication challenges for all the synonyms mentioned. This ensured a thorough coverage of recent developments.

3. Inclusion and exclusion criteria: To filter the identified papers, specific inclusions were applied as follows:
   - Papers directly addressing communication challenges within IoBT or military IoT.
   - Studies focusing on interoperability, power and energy management, network resilience, and security challenges.
   - Research published in peer-reviewed journals or conference proceedings within the last decade. The exclusion criteria were applied to:
   - Papers primarily focusing on non-military IoT applications or general IoT without addressing battlefield-specific conditions.
   - Studies that do not propose solutions or lack technical insights relevant to IoBT.
4. Classification of challenges: Once the relevant papers were identified, the communication challenges were classified into four primary categories based on the frequency of occurrence and emphasis in the literature:
   - Interoperability: The ability to ensure seamless communication among diverse IoBT devices and systems.
   - Power and Energy Management: Optimizing energy consumption to extend operational lifetimes of devices in battlefield conditions.
   - Network resilience: Ensuring reliable communication in dynamic and hostile environments, including disruptions or jamming.
   - Security: Addressing vulnerabilities such as cyberattacks, data integrity, and secure transmission in military contexts.
5. Literature review and analysis: The identified literature was analyzed to provide a comprehensive overview of the communication challenges, existing solutions, and their effectiveness. We evaluated the methodologies, technologies, and algorithms proposed in each study, noting their strengths, limitations, and applicability in the IoBT context.

3 Technological overview

In this section, we present an overview of the fundamental components and principles of IoBT, laying the groundwork for the subsequent discussion on communication challenges in IoBT. IoBT represents a transformative approach to military operations, integrating interconnected devices, sensors, and communication networks on the battlefield. At its core, IoBT harnesses IoT principles to enable seamless communication, data exchange, and collaboration among various military assets, ranging from unmanned vehicles to soldier-worn wearables and battlefield sensors. Understanding the fundamentals of IoBT is essential for appreciating its role in modern military operations and addressing the unique challenges associated with its deployment. By harnessing interconnected devices, communication networks, and advanced analytics, IoBT offers unique capabilities for enhancing situational awareness, decision-making, and operational effectiveness on the battlefield [7].

3.1 Internet of battle things synonyms

In September 2015, a report of the Center for Strategic and International Studies (CSIS) Strategic Technologies Program entitled "Leveraging the Internet of Things for a More Efficient and Effective Military" [7], the terminology "Military Internet of Things" (MIoT) is utilized. This term refers to the military deployment of IoT-related technologies in the military system, as found in literature as early as 2012 [8]. Kott et al. [1] constructed the expression "The Internet of Battle Things," referring to the intelligent end nodes interconnected in the world of the military. Over time, other terms like "The Internet of Military Things" (IoMT) [9], "The Internet of Battlefield Things" [10, 11], and "Defence Internet of Things" [12] have been used throughout the literature to describe the telecommunication network of smart devices incorporated by IoT paradigm for military objectives. We found a significant semantic overlap between these terms, implying that they are essentially interchangeable due to their common underlying meanings.

3.2 Fundamentals of IoBT

As early as 1999, network-centric warfare was outlined to enhance information sharing and collaboration [13, 14]. The authors presented a model incorporating three segments: the physical segment, which encompasses events and processes; the information segment, which involves data transmission and storage; and the cognitive segment, which focuses on data processing and analysis. These three spheres of network-centric warfare strongly correspond to the contemporary concept of the Internet of Things, integrating sensors and embedded devices, internet connectivity, database technology, and software analytics. Network-centric warfare applied IoT technology to military operations before the emergence of the IoT concept [15]. The military primarily focused on utilizing IoT-related technology in Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR), and fire-control systems. The prevailing perspective was that the primary function of sensors and networks was as instruments for collecting and exchanging data on the battlefield, ultimately enhancing the command and control of military assets [3, 7]. IoBT should not be perceived as a standalone system but instead as a combination of interconnected technologies and end devices that are widely connected, intelligent, and frequently dynamically combined to achieve desired outcomes in cyber and physical environments.

IoT influenced the idea of IoBT, which included a variety of intelligent devices and sensors deployed on the battlefield. A key distinction of IoBT is that it is goal-driven; the objective is not to ensure equity for all devices but to effectively accomplish the military mission. A "thing" in the IoT context refers to any physical object integrated into the internet that can collect, process, and transmit data in real-time [16, 17]. These devices have varying intelligence, capacities, and limitations regarding energy, power, computation, and communication resources. In IoBT, these devices include UAVs, autonomous ground vehicles, wearable sensors for soldiers, environmental sensors, surveillance cameras, robots, and fire-and-forget missiles, among other examples. The IoBT system must be functional, supporting mission goals, creating situational awareness, engendering trust, understanding the commander's intent, calculating prudent risk and exercising disciplined initiative [18]. IoBT increases efficiency, effectiveness, and cost savings in the military. The ability to support heterogeneous "things", scalability, and robustness are essential for IoBT to fulfill the battlefield environment's Quality of Service (QoS) prescriptions.

C4ISR is a military term for the systems and processes used by military commanders to gain a comprehensive understanding of the battlefield, make informed decisions, and communicate effectively with their forces. Making decisions, planning, and directing operations are all important aspects of a commander's authority over his or her assigned forces to complete missions. The forces' regulation, direction, or command is important, encompassing monitoring, coordinating, and adjusting operations to achieve the objectives. Communication includes transmitting information and orders between commanders, units, and platforms using various technologies such as radios, satellites, and data networks. The computers support military operations for data processing, storage, and analysis. Given the many important tasks of intelligent systems, they become attractive targets for adversaries due to their extensive attack surface. There is increased vulnerability to attacks on their information, information processing, communications, and potential physical threats or capture. Security is of utmost importance in the design and operation of IoBT systems [19].

IoBT depends on robust communication networks to provide connectivity and data exchange among the deployed assets in the network. These deployments can include wireless technologies like Wi-Fi, Bluetooth, and cellular connectivity, along with specialized military-grade communication protocols explicitly designed for battlefield environments [20]. The systems integrate data from multiple sources, such as sensors, combat attire, weaponry, surveillance systems, and intelligence feeds, to provide commanders with comprehensive situational awareness and practical insights. Limitations exist in the IoMT environment regarding power, storage, and bandwidth. The absence of permanent infrastructure may impose constraints on computer and communications capabilities. The data gathered via IoBT can originate from various sources with varying levels of trustworthiness. These sources can range from dependable and accurately calibrated sensors controlled by trusted entities to devices, human sources whose allegiances are uncertain, and even sources that potential adversaries own. Limitations may arise regarding interoperability between these heterogeneous components, leading to a decrease in the functionality of the network [7]. The command and control systems must have the capability to support the proliferation of these smart devices [21]. The increase in diversity and interconnectedness of networked devices that sense and relay real-time data to military bases poses significant challenges for military defense and national security systems. Advanced analytics methodologies, such as machine learning and artificial intelligence, can handle substantial data and derive pertinent actionable insights in real time [22].

IoBT is a rapidly advancing domain that utilizes various technologies to interconnect battlefield devices and systems. This system facilitates real-time data exchange, enhances situational awareness, and optimizes decision-making processes in military operations. By integrating advanced communication protocols, sensor technologies, and data analytic technologies, IoBT has the potential to transform the field of military operations.

3.2.1 Communication protocols

Communication protocols are vital in ensuring secure, resilient, and efficient data exchange in battlefield environments. Selecting the optimal communication protocol for IoBT depends on factors like the range, bandwidth, power constraints, latency, scalability, security needs, and environmental challenges of the battlefield. Given that power consumption is a critical consideration in IoBT, low-power wireless technologies are preferred. These technologies can be broadly categorized into two primary groups, namely, Low Power Wide Area Networking (LPWAN), offering extended coverage of up to several kilometres and Wireless Personal Area Networking (WPAN), with a range typically reaching up to 200 ms. LPWAN technologies, such as 6LoWPAN, LoRaWAN, Sigfox, NB-IoT, and Wi-Fi, are characterized by relatively limited data rates [23–25]. WPAN technologies, including Zigbee and Bluetooth, Z-Wave, provide data rates of up to 250 kbps and 3 Mbit/s, respectively [26]. Ad-hoc networks form self-configuring networks on the battlefield without fixed infrastructure, such as mobile ad-hoc and vehicular ad-hoc networks, providing dynamic, decentralized communication between mobile entities. Tactical Edge Networks utilize 5 G and LTE technologies for high-speed, low-latency communication [27, 28], while software-defined networking and network function virtualization enable flexible and scalable network management. Delay-Tolerant Networks ensure communication in disrupted environments by enabling store-and-forward mechanisms [29–31]. In areas where ground-based communication is challenging, IoBT can use satellite communication protocols for long-distance communication between different parts of the battlefield and central command [28, 32, 33]. Routing Protocol for Low-Power and Lossy Networks (RPL)is designed for low-power and lossy networks, making it particularly suitable for IoBT applications where devices often operate under resource constraints. RPL operates under the assumption that the network contains a sink node with greater computing ability and energy resources than the rest of the nodes in the network [34]. Secure communication protocols, including encryption and blockchain, protect sensitive battlefield data from interception and tampering, maintaining operational security in hostile environments. Message Query Telemetry Transport (MQTT) is a lightweight messaging protocol that supports effective communication between diverse systems, enhancing interoperability-a critical requirement in battlefield operations [35, 36]. Its efficiency in dynamic environments aligns well with the needs of IoBT.These protocols collectively enhance the connectivity and robustness of IoBT systems, supporting mission-critical operations.

3.2.2 Sensor technologies

Sensor technologies are the backbone for gathering and transmitting real-time data to enhance situational awareness, improve decision-making, and support autonomous systems on the battlefield. These sensors are designed to operate in harsh environments, provide reliable data, and enable rapid response. These include environmental monitoring sensors which measure atmospheric conditions and inform troops about weather changes that could impact operations or equipment. Barometric pressure sensors are useful for tracking altitude and atmospheric pressure changes, which may affect air-based or high-altitude operations. Gas sensors help detect hazardous gases (e.g., chemical weapons, smoke) in the battlefield environment, alerting troops to possible dangers [37]. Positioning and navigation sensors provide real-time location data for soldiers, vehicles, drones, and other battlefield assets, aiding in navigation, coordination, and tracking of personnel or equipment. Magnetometers provide heading data for navigation and can help in detecting metallic objects, like weapons or vehicles, hidden underground. Health monitoring sensors to track vital signs in real-time to ensure soldiers maintain optimal performance [38]. Acoustic or seismic sensors are used for detecting movement or disturbances. Imaging sensors, such as infrared, Light Detection and Ranging, and hyperspectral cameras, provide enhanced visibility and object detection, while RF and electromagnetic sensors monitor communication signals and detect jamming threats. Specialized Chemical, Biological, Radiological, Nuclear, and Explosives Sensors detect chemical, biological, radiological, and explosive hazards, crucial for battlefield safety. There are energy-harvesting sensors that capture energy from environmental sources (e.g., solar, thermal, kinetic) to power other devices on the battlefield, enhancing the autonomy of IoBT devices [39, 40]. These diverse sensors, integrated into secure networks, support real-time data collection, enabling rapid decision-making and resilient battlefield operations.

3.2.3 Data analytics

Data analytics technologies in IoBT enable real-time decision-making and enhance operational efficiency by processing vast amounts of battlefield data. They serve as the analytical backbone of IoBT, transforming raw data collected from sensors into actionable insights. The integration of advanced analytics is essential for effective decision-making in complex battlefield environments. IoBT environments generate large volumes of heterogeneous data from multiple sensors, vehicles, drones, and personnel. Big data technologies such as Apache Hadoop and Spark enable the aggregation, storage, and processing of this data at scale, allowing commanders to draw insights from diverse battlefield inputs. Machine learning models analyze historical and real-time data to predict battlefield outcomes, such as enemy movement patterns, equipment failures, and health status of soldiers [41]. These models utilize techniques such as deep learning and neural networks for complex, pattern-based analysis. Artificial Intelligence systems are integrated into autonomous battlefield robots, drones, and vehicles, using data to make operational decisions. For instance, reinforcement learning algorithms allow systems to dynamically adapt to new threats or changing conditions in the field. Edge and fog computing ensure low-latency analytics at the tactical edge, and reduce bandwidth constraints. Edge AI enables the processing of critical data on the device, reducing latency and bandwidth consumption by only sending essential data back to the command center. Multisensor data fusion integrates heterogeneous sensor inputs, and geospatial analytics processes spatial data for trajectory prediction and battlefield mapping. Kalman filters, Bayesian networks, and fuzzy logic are commonly used techniques to fuse these disparate data streams, providing a coherent, comprehensive understanding of battlefield scenarios [42]. Cybersecurity analytics monitor for threats, ensuring data integrity, while simulation tools like digital twins optimize asset deployment. These technologies are crucial for creating responsive, intelligent systems that adapt to dynamic battlefield environments.

3.3 Applications of IoBT

Due to escalating military operations, the integration of IoT in the military and defense sectors has become imperative [43]. By incorporating IoT technology into current military and defense infrastructures, IoBT enhances operational efficiency and effectiveness, substantially decreasing casualties and equipment losses during wartime. Examples of the integration of IoT into various operations are military combat, enemy base surveillance, search and rescue missions, equipment tracking, battlefield communication, and environmental monitoring. During peacetime, IoBT is utilized for military training, weapon, vehicle, or system maintenance optimization [44]. Command-and-control (C2) infrastructure supports IoBT operations by enabling commanders to oversee and coordinate military operations across the battlefield. This infrastructure includes centralized command centers, tactical operation centers, and distributed C2 nodes equipped with communication, computing, and visualization capabilities [45]. IoBT environment is very dynamic because of end device mobility, bandwidth and topology changes, and possible jamming attacks, thus requiring robust end-to-end communication strategies. However, the fast-paced evolution of technology necessitates that defense and security systems constantly adapt and employ cutting-edge solutions to enhance their capabilities and responsiveness.

3.3.1 Intelligence gathering

Intelligence gathering entails collecting, analyzing, and disseminating information about the enemy, terrain, and other relevant factors to support decision-making, including signals intelligence, human intelligence, and imagery intelligence. Having a deep understanding of intelligence is crucial for successfully executing military operations. The systematic observation and evaluation of enemy activities, terrain, and other factors to gather information for military planning and operations is essential. This can involve ground patrols, UAVs, and other reconnaissance assets. Integrating various sensors, cameras, microphones, and a computing system allows IoBT to analyze data patterns more efficiently and accurately than a human analyst. IoBT can significantly reduce the time required to generate actionable intelligence [46, 47].

3.3.2 Logistics and maintenance

IoBT sensors can monitor the location, condition, and movement of supplies and equipment, enabling more efficient logistics and supply chain management. Ensuring the regular upkeep of military vehicles and the effective movement of ammunition and troops is essential for the success of military operations. IoT technology enables tracking supplies from their origin to their destination on the battlefield through interconnected sensors and advanced data analysis.

Integrating sensors into military vehicles facilitates monitoring their location, fuel consumption, extent of damage, engine condition, and other vital indicators. Implementing intelligent tracking systems for defense and military transportation allows military fleets to detect discrepancies and take appropriate actions promptly. This enables them to decrease transit expenses and minimize human labor. Furthermore, sensors can monitor and trace weaponry, ammunition, and unmanned equipment. Incorporating sensors into guns can enhance soldiers' awareness of when to reload. Unmanned equipment can be tracked and monitored on hostile territory for espionage and reconnaissance purposes. Examples are condition-based maintenance, real-time fleet management, and inventory management [48, 49].

3.3.3 Environmental monitoring

The surveillance monitors and observes the battlefield and other areas of interest using various sensors, platforms, and techniques, including aerial reconnaissance, ground-based sensors, and satellite imagery. IoBT technology allows military forces to effectively monitor the battleground using UAVs fitted with advanced cameras and sensors. These drones are capable of capturing real-time images, tracking the terrain, locating potential threats, and transmitting instantaneous data to the command centre. Using this data, officers can closely monitor the battlefield and make well-informed decisions promptly [50].

3.3.4 Augmented reality remote training

Models are generated using historical field data, and a training simulation environment is subsequently established. The soldiers are equipped with virtual or augmented reality gear, which is then transferred to the simulated environment for evaluation. This includes assessing accuracy, emotional response, movement speed, and other relevant parameters. Practising in a controlled environment allows soldiers to improve their goals and precision without risking physical harm, effectively preparing them for actual combat. Mistakes can occur during training, and repeating those mistakes during a fight could have long-lasting consequences [51]. Flight simulators are available for pilots to practice and gain practical experience using a simulator before flying an actual aircraft. Pilots are required to perform various manoeuvres to elude enemy pursuit or tracking missiles. Preparing for such situations can incur significant costs and even result in fatalities. Simulation is the preferred method for training pilots in such scenarios [52–54]. Mixed reality is a cutting-edge immersive technology also used in IoBT, that combines virtual reality with augmented reality to create immersive environments where the physical and digital worlds blend [55].

3.3.5 Connected soldiers

Knowing the health status of a soldier is essential in the military. Sensors are integrated into the combat suits, helmets, weapons systems, and other gear that troops use to gather a wide range of biometrics, including iris scans, facial recognition, fingerprints, heart rate monitoring, gestures, and facial expressions. The connected soldier uses military gear that enables real-time health monitoring and improves communication and situational awareness for the soldier [56–59]. Doctors can receive real-time updates on changing medical conditions, enabling them to proactively prepare medical supplements or equipment according to the patient's needs or, in adverse situations, can be removed from the field.

3.3.6 Data processing and analysis

The data sent by IoBT end nodes in the network needs processing and analysis to aid decision-making. There are multiple perspectives to consider when identifying the conceptual and physical framework of data management for IoT. Several data formats can be transmitted in IoBT, such as raw data, anonymized data, model parameters, mildly encrypted data, or data that is homomorphically encrypted. The basic concept of data management in IoBT comprises four modules: data collection, data transmission, data administration, and data processing [60]. Given the constantly evolving and challenging threat landscapes in which IoBT devices are deployed, determining the appropriate data to share is difficult. The technology must provide intelligent systems capable of conducting analytics and interpreting data streams from heterogeneous devices. Language and Artificial Intelligence can produce accurate decisions [61, 62].

3.4 Examples of IoBT systems

We look at some notable existing IoBT systems, along with a comparison of their effectiveness based on real-time communication, security, scalability, and energy efficiency. The U.S. Army initiated Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA) to research and develop the integration of autonomous systems, sensors, and AI into battlefield operations. This initiative focuses on embedding intelligence into everyday battlefield objects (e.g., vehicles, drones, soldier wearables) to create a network of autonomous agents that share data in real-time. Its key features are AI-driven decision-making for real-time data analysis, integration of wearable sensors for soldiers to monitor health and combat conditions and swarm robotics for autonomous UAV and unmanned ground Vehicle coordination [17, 63]. IoBT-CRA system has AI-based data analytics to ensure rapid information processing and sharing. It has secure communication protocols and encryption to protect sensitive military data. The energy efficiency is moderate, as many devices (e.g., wearables) are battery-operated and require optimized protocols for longevity. It is scalable with autonomous agents communicating over various network layers.

Edge-Directed Cyber Technologies for Reliable Mission Communication is a Defense Advanced Research Projects Agency (DARPA) project that focuses on developing cyber technologies to maintain secure, reliable communication in contested battlefield environments. Edge computing is a core feature, allowing for decentralized data processing closer to the battlefield. The system uses decentralized edge computing nodes for local data processing, machine learning algorithms to predict network failures and reroute communication accordingly, and secure, adaptive, and self-healing networks to counter cyber threats [64]. The system exhibits highly effective real-time communication due to local data processing at the network edge, which minimizes latency. It has robust security features using AI-based cyber defense systems that dynamically protect data from cyberattacks. It has high scalability since edge computing reduces the need for centralized processing, improving responsiveness across larger areas. Energy Efficiency is moderate, as edge nodes are resource-intensive, though they reduce the load on central servers.

A wearable military system, Broadsword Spine, provides soldiers with enhanced communication and power management capabilities. It integrates wearable electronics into the soldier's uniform to create a mobile hub for data exchange between soldiers and command centers. This system uses an E-textile fabric embedded with communication and power management tools. It provides connectivity and sensor data integration with Wireless power distribution to soldiers' wearable devices [65]. Real-time communication is moderate, relying on existing communication infrastructure, but it offers soldiers enhanced mobility and ease of use. Security is high, as it employs military-grade encryption. Scalability is moderate, designed for platoon-level or company-level deployment rather than larger networks. Energy Efficiency is high, with wireless power management reducing the need for frequent battery changes in wearables.

These core technological components and functionalities essential to IoBT employ a structural framework that supports these technologies on the battlefield. The IoBT architecture provides this framework for integrating various devices and communication protocols, ensuring efficient and secure operations. The layered architecture highlights how each layer addresses the unique challenges of military environments while supporting the dynamic demands of battlefield communication.

4 The architecture of IoBT

In traditional networking, the Open System Interconnection (OSI) reference model establishes the protocol for transmitting and receiving data inside a network. This concept breaks down data transmission into seven distinct layers. Every layer is responsible for executing distinct duties related to transmitting and receiving data. For a communication to reach its destination, it must traverse through all of the layers [66]. IoT technology has modified the OSI model to form an architecture ranging from three to five layers depending on the technology or application [8, 67–69]. A literature study revealed that there is currently no universally accepted and proven architecture for IoT [70–72]. The three-layer structure comprises the perception, network, and application layers and provides the base of the other two architectures [73, 74]. The four-layer architecture includes a support layer between the network and application layers to enable cloud computing technologies [75]. The five-layer design consists of the middleware layer above the network layer and a business layer above the application layer [76, 77]. IoBT poses various challenges because of its

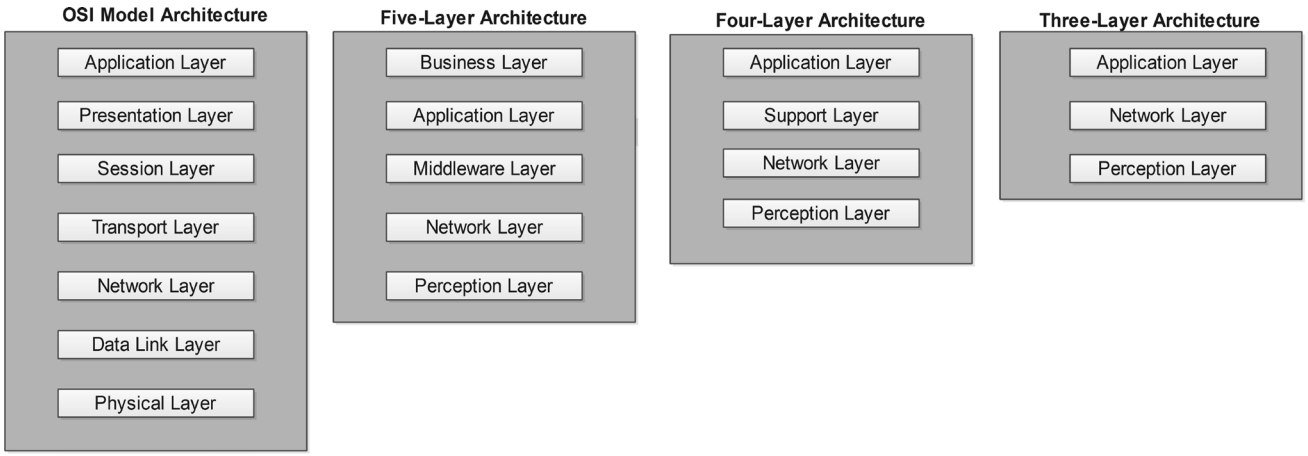

Fig. 1 A comparison of the OSI model and IoBT architectures

demanding operational environment, as military applications require robust, secure, and real-time data collection and dissemination. The five-layer architecture can be adopted for IoBT systems to address these needs, building upon the core functionalities of the traditional three-layer IoT architecture. The infrastructure of the IoBT network closely resembles IoT environment, with minor variations in the types of devices and communication methods used. Figure 1 shows the relationship between the OSI model and IoBT architectures.

4.1 The perception layer

The perception layer represents the OSI model's physical layer, which contains devices that sense and collect data in the surrounding environment. This layer identifies the devices connected to the network and collects information from these devices. Sensors and actuators are integrated into military weaponry and personnel to enhance their integration into an IoT-oriented infrastructure. These devices are connected to the network layer through wireless communication protocols. This layer gathers data and converts it to digital signals. The acquisition and processing of data in IoBT must be resilient to communication disruptions and malignant sensory inputs. Algorithms that can decipher the quality of information from noise and misrepresentation are necessary for robust information [10].

There is a strong need for tactical computer resources, networking-capable sensors, unmanned systems, and wearable gadgets to better understand the complex and competitive military environment. These technologies help facilitate faster and more informed decision-making by the military personnel involved. By utilizing collaborative sensing of the environment and advanced communication technologies, battlefield IoT nodes actively share mission-specific information. Therefore, this perception layer consists of all the military assets that work together in the physical warfare arena to sense and monitor enemy activity. The effectiveness of the mission relies not only on environmental sensing but also on monitoring troop movement, inventory management, and health checkups of individual soldiers. By utilizing this type of information, timely and essential support can be coordinated, thereby potentially minimizing the likelihood of mission failure [66].

Military equipment and soldiers are equipped with diverse sensors and actuators capable of measuring location, speed, health, brightness, temperature, pressure, electrochemical properties, and electro-mechanical properties. Not all network-capable elements on the battlefield adhere to a uniform communication protocol. Various media and protocols, including WiFi, Infrared, Bluetooth, Near-Field Communication (NFC), X10, cellular networks, and ZigBee, are employed to distribute the detected data among one another. Therefore, achieving operational efficiency in IoBT network relies heavily on addressing the key interoperability and protocol standardization difficulties in this layer. Security is also a challenge to implement in the perception layer. Because the sensors have constrained resources, their storage capacity and computational power are limited. This restricts security mechanisms that can be put in place to safeguard devices vulnerable to attacks like denial of service and interferences on this layer. Node authentication and data encryption are essential for a robust and secure implementation. Authentication is essential for preventing unauthorized access to nodes, while data encryption is necessary to ensure confidentiality. Subsequently, the limitations imposed by memory become relevant, resulting in the potential adoption of lightweight cryptographic algorithms in the context of IoBT [78].

4.2 The network layer

The network layer, sometimes called the transmission layer, is the communication layer that facilitates the transfer of data from the end devices in the IoT network via the gateway to the network server or cloud infrastructure. After the initial data processing, such as data aggregation and compression, data frames are routed to their destination. The network layer establishes a link between the perception and middleware layers using various wireless technologies [79]. In a battlefield scenario, the lack of connectivity to cellular networks or base stations for the entire operation could be challenging; therefore, device-to-device communication is incorporated so the devices can exchange information. Weak connections and a volatile nature characterize the networks established on the battlefield, indicating that the network structure may not be able to support long-term usage. Military missions usually involve a high level of dynamism where battlefield equipment and soldiers constantly change positions. The network that is created will have both spatial and temporal variations in its topology. Additionally, the energy depletion on the end devices could potentially disrupt the network, so network entities need to adjust their transmission parameters to ensure uninterrupted network connectivity.

4.3 The support layer

The support layer sometimes called the middleware or processing layer, acts as an intermediary between the network and application layers. The core function of the support layer is to cleanse, filter, and potentially transform the raw data received from the network layer. Techniques like outlier detection and data validation can be employed to ensure data integrity and eliminate noise from sensor readings. Data from various sensors can be fused to create a more comprehensive picture of the battlefield environment. The support layer also provides security in the architecture of IoBT. It has two responsibilities, to confirm that the authentic users send information and to protect from threats. This layer processes the data and provides partial security, ensuring data transmission is secure and dependable [80, 81]. The middleware layer provides a range of advanced features, including storage, computation, processing, and action-taking capabilities. It efficiently stores and retrieves data based on device address and name, ensuring accurate delivery to the intended device. This layer connects applications, data, and users. It can make informed decisions by analyzing data collected from sensors. The middleware layer is significant for enabling interoperability between various platforms of connected devices through Application Programming Interfaces. This layer is important in facilitating data management and is sometimes referred to as a Service platform or Enabler [82–84]. The middleware layer provides a level of abstraction for the programmers, allowing them to conceal the hardware details and provide a more simplified and user-friendly experience. This improves the interoperability of smart devices and simplifies the process of offering various types of services [85]. Resource-constrained devices at the perception layer can benefit from offloading some pre-processing tasks to more powerful edge servers within the support layer.

4.4 The application layer

The application layer generates reports and analyses for end users to interact with the system and access specific services. This layer is responsible for interpreting data using advanced algorithms or analytical instruments and presenting the information in an easily understandable manner. The features in the Application Layer are customized to suit the specific objectives of each IoT environment. These features may encompass sending notifications to users, integrating data with external systems, initiating automation based on data analysis, or presenting visualizations to enhance comprehension of accumulated information. Hence, this layer functions as the focal point where technology and usability intersect, guaranteeing that the IoT system is effective and prioritizes the needs of the user [86]. The application layer comprises various applications in war missions, including management and surveillance. This layer is responsible for managing the functions of these applications using a single, unified application while ensuring that their efficiency remains unaffected. Hypertext Transfer Protocol (HTTP) is the foundation of the application layer on the Internet. Nevertheless, HTTP may not be ideal for resource-constrained environments like the battlefield due to its verbose nature, resulting in significant parsing overhead. Several alternative protocols have been created for IoBT environments, including Constrained Application Protocol and Message Queue Telemetry Transport.

The application layer leverages the processed data from the support layer to deliver mission-critical functionalities. In IoBT, this layer provides real-time situational awareness platforms that provide a consolidated view of the battlefield,

integrating data from various IoBT sensors with friendly troop locations and enemy activity. Threat detection and analysis provides advanced algorithms to analyze sensor data to identify potential threats, classify enemy targets, and predict enemy movement patterns. Finally, automated command and control systems integrate IoBT data with C2 systems to enable semi-autonomous or autonomous weapon platforms or provide real-time decision support for commanders.

4.5 The business layer

The business layer presents business applications to end users. This layer oversees the management of the IoT system as a whole. Planning based on data obtained from the lower layers helps create various business models, graphs, flow charts, and specifications for direct application management [87]. These tasks are dependent on the data received from the Application layer. It encompasses the design, analysis, implementation, evaluation, monitoring, and development of elements relevant to IoT systems. The Business layer facilitates decision-making processes through the utilization of Big Data analysis. Furthermore, this layer evaluates the output of each layer by comparing it to the desired output to improve services and safeguard users' privacy. The business layer encompasses functionalities like secure data monetization, where strategies for anonymized data sharing or selective access to specific data streams for authorized partners can be

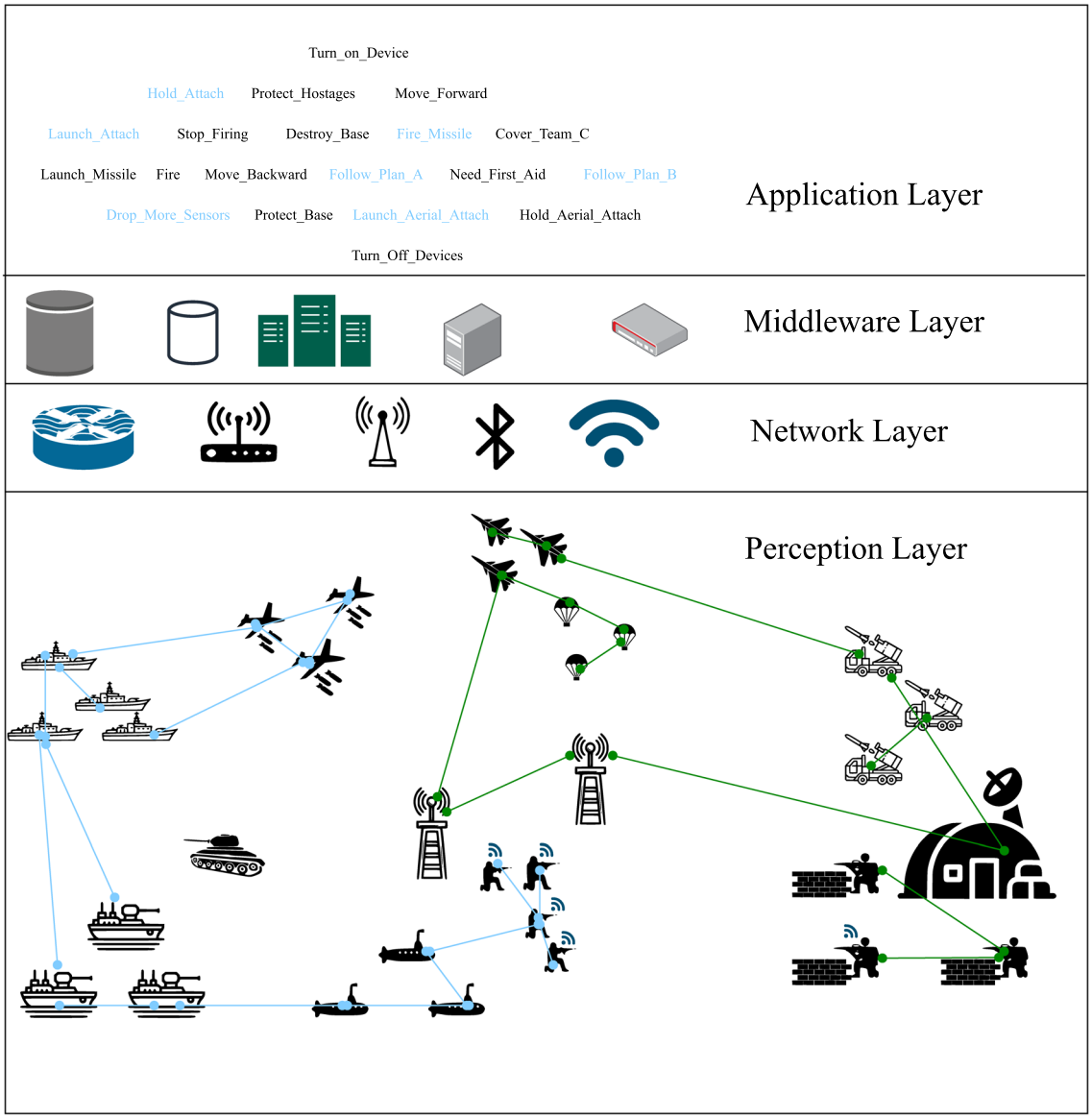

Fig. 2 Layers of IoBT architecture: adapted from [88]

established. Device lifecycle management is ensured in this layer by the efficient provisioning, deployment, maintenance, and disposal of IoBT devices throughout their operational life. Service-level agreements performance metrics, data security guarantees, and service uptime expectations for IoBT deployments would be determined in the business layer.

Each layer plays a specific role in ensuring seamless data collection, processing, and utilization, ultimately contributing to enhanced battlefield awareness and improved decision-making capabilities. Figure 2 depicts the layered architecture of IoBT.

5 Communication challenges in IoBT

Communication in the Internet of Battlefield Things is necessary for enabling the interconnectedness of the various devices, systems, and personnel deployed in military environments. IoBT relies on various communication technologies to ensure seamless connectivity and information exchange among deployed assets. IoBT networks consist of heterogeneous devices with different communication standards and capabilities, which presents a unique and complex environment for communication that demands robust and secure solutions to overcome inherent challenges. Ensuring seamless interoperability between these diverse systems requires efficient routing protocols and data translation mechanisms that can manage bandwidth, latency, and data format variations. Effective communication strategies enhance information sharing and improve situational awareness, command and control capabilities, and mission effectiveness on the battlefield. IoBT networks must scale to accommodate thousands of interconnected devices, leading to challenges in bandwidth management and network congestion. Dense device deployment can overload communication channels, resulting in packet loss, increased latency, and degraded network performance. Low latency is critical, especially for real-time control of UAVs, weapon systems, and soldier health monitoring. Delays in data transmission can hinder decision-making and mission execution, making minimising latency across the network essential. Most battlefield devices, especially wearables and sensors, rely on battery power, and frequent recharging is not feasible in combat situations. Thus, energy-efficient communication protocols are essential to extend the operational lifetime of IoBT devices without compromising performance. IoBT communications are vulnerable to a variety of cyber threats, including jamming, eavesdropping, and data manipulation. Ensuring secure communication while maintaining high performance is a complex challenge. Additionally, battlefield networks must be resilient to physical damage and cyber-attacks, ensuring continuous operation even under adverse conditions.

The successful deployment of IoBT systems revolves around addressing the major challenge of energy consumption in resource-constrained military environments, the interoperability challenges between different devices, systems, and networks, network security against cyber threats, spectrum management, and fusing data from various sources to meet the unique requirements of modern military operations [89–91]. In a military setting, operations are usually in hostile territories and involve constant movement, which means that military communications networks experience disruption, intermittent connectivity, limited bandwidth, and dynamic configuration. Cloud resources may experience interruptions, sporadic availability, or be non-existent.

The communication challenges faced in the IoBT environment are multifaceted and require innovative solutions to ensure operational efficiency and security. Researchers are actively exploring various technologies and strategies to address these challenges, including blockchain, Attribute-Based Encryption, AI/ML, deception-based methods, robust encryption protocols, collaborative object labelling, secure and reconfigurable network design, and vehicle-assisted communication schemes. The successful implementation of these solutions will be crucial for developing and deploying IoBT systems, enabling the seamless integration of interconnected devices and autonomous systems in modern warfare. Scholarly literature has explored various approaches to tackle these challenges, proposing various strategies. In this section, we review the proposed solutions to address these complexities posed by the emergence of the Internet of Defence Things.

5.1 Interoperability

Interoperability is essential in IoBT to facilitate seamless communication and collaboration among diversified components and systems deployed by different military branches or allied forces. Standardized protocols and interfaces enable interoperable communication and data exchange, allowing disparate IoBT assets to work together effectively toward common mission objectives. The extensive and advanced capacities of IoMT to sense and act intelligently make artificial intelligence and autonomy crucial components of military strategies. Emerging operational concepts, including

multi-domain operations, prioritize encompassing several operational domains, including cyber, sea, air, space, and land. IoBTs are intricate networks of interconnected systems that can provide widespread machine intelligence, processing power, and sensing abilities. They may also interact with physical spaces through cyber interfaces, significantly transforming the modern battlefield [63, 92–96].

The IoBT-MAX testbed was suggested in [97] to collect data from multiple sensors and test different IoBT technologies in real time. It can be used to research and develop technologies like distributed classification and detection, distributed multi-object tracking, data compression, communication-efficient inference, and scheduling. The data collection experimentation has yielded over 10 gigabytes of multi-modal sensing and tracking data. The authors in [98] explore the evaluation of node trustworthiness in IoBT and present a decentralized trust management framework empowered by blockchain technology. The system model has been carefully designed to include two types of IoBT nodes: the IoBT edge nodes and the portable ping-pong stations. The network's IoBT edge nodes generate trust values by interacting through mutual information. The portable ping-pong station determines the overall trustworthiness of the IoBT edge node by accessing the local trust value stored within the jurisdiction and applying a trust value transfer formula. Meanwhile, a cutting-edge consensus protocol has been developed specifically for IoBT. The new protocol encourages blockchain nodes to actively uphold the correct trust levels of nodes on the blockchain. The portable ping-pong station utilizes a cutting-edge consensus algorithm to keep the global trust values of IoBT edge nodes up to date on the blockchain. The simulation scenarios are carefully crafted and a multitude of simulations are executed. However, the simulation results show that the proposed scheme can quickly find malicious nodes. This makes it much less likely that attacks will succeed, and in the end, it ensures safe and reliable operation in IoBT. A novel protocol known as "Secure 5 G-Assisted UAV Access Scheme" is proposed in [99] which integrates 5 G Tactile Internet with blockchain to enhance communication and security for UAV operations in IoBT ecosystems. The scheme addresses the limitations of traditional 4 G LTE-A networks, such as high latency, bandwidth constraints, and vulnerability to security attacks. Simulation results show a significant improvement in terms of latency, frame loss, and overall performance compared to LTE-A networks, making the scheme suitable for mission-critical IoBT applications. The use of edge computing for task offloading and blockchain for decentralized data management ensures that the system can scale and adapt to large networks of UAVs, even in heterogeneous and intermittent network conditions. The work in [100] proposes a novel scheme for designing secure and reconfigurable networks for critical information dissemination in IoBT. The approach utilises stochastic geometry and mathematical epidemiology to analyze the communication of mission-critical data among different types of network devices. This allows for the design of cost-effective and resilient networks in dynamic battlefield environments.

5.2 Power and energy management

In the context of IoT, minimizing energy through resource efficiency has shown to be effective. Therefore, it is reasonable to anticipate increased success when implementing cost-reduction mechanisms to manage IoT devices in a military environment [101]. IoBT devices and systems operate in dynamic and often hostile battlefield conditions, where access to traditional power sources may be limited or unreliable [44, 102]. Energy efficiency remains a critical challenge for IoBT, as many devices operate in remote, power-constrained environments where recharging or replacing batteries is infeasible. As a result, optimizing energy consumption is important to ensure prolonged operational endurance and mission effectiveness in IoBT deployments. IoBT can also be vulnerable to electromagnetic and directed-energy attacks, disrupting communication, collaboration, and access to processing power and information sources [103]. Environmental factors, such as temperature extremes, humidity, and terrain, can impact the energy efficiency and performance of IoBT devices. Extreme temperatures can affect battery performance and lifespan, while rugged terrain may impose additional energy requirements on ground-based vehicles and sensors. Designing robust and resilient IoBT systems capable of operating in diverse environmental conditions is essential for ensuring mission success.

The work in [7] studies the deficiencies in existing IoT component systems utilized by the military and identifies the obstacles that hinder the implementation of IoT technology. Several key challenges contribute to the energy consumption issues faced by IoBT systems. Many IoBT devices, including UAVs, ground sensors, and soldier-worn wearables, rely on battery power for operation. These batteries must provide sufficient energy to support continuous operation over extended periods, often in harsh environmental conditions. However, the limited energy storage capacity of the batteries and the finite lifespan of rechargeable batteries pose significant challenges to maintaining operational readiness in IoBT networks. IoBT deployments frequently occur in off-grid or remote locations where access to traditional power infrastructure is limited or nonexistent. Subsequently, the devices must rely on self-contained power sources, such as batteries, solar panels, or fuel cells, to sustain their energy needs [104–106].

Managing power consumption and optimizing energy usage is critical to ensuring mission continuity and operational effectiveness in battlefield environments. Specific techniques have been developed to address energy consumption while ensuring the reliability and resilience of communication. Several key techniques to enhance energy efficiency in IoBT are provided as follows:

- **Energy harvesting and solar power**: Utilizing ambient energy sources like solar, thermal, or kinetic energy to power IoBT devices reduces reliance on batteries. Recent studies have explored solar-powered energy management for portable devices. Kunatsa et al. [107] presented an optimal power flow management modelling and optimization approach for solar-powered soldier-level portable electronic devices. In their work, the proposed solution ensures that the supply of solar-powered portable electronic devices for soldiers remains uninterrupted and adequately met, regardless of the specific prevailing limitations. The authors explore a nonlinear optimization approach to manage power flows for soldier-level portable electronic devices powered by solar photovoltaic systems. The study uses MATLAB's OPTI Toolbox with the SCIP solver to ensure optimal power distribution between solar PV systems, primary batteries, and individual PED batteries to meet energy demands under varying shading and solar irradiance conditions. The approach minimizes the disparity between power supply and portable electronic device demands while considering constraints such as battery capacity, charging efficiency, and operational requirements. Specific IoBT applications, such as real-time video streaming, sensor data collection, and analytics, can be computationally intensive and energy-demanding. Balancing the need for timely data transmission and processing with energy efficiency considerations poses a significant challenge for IoBT designers and operators. Xie et al. [108] proposed an energy harvesting technique called "Minimal Retention Energy Harvesting", a technique designed to optimize energy efficiency in IoT edge computing devices, improving the energy efficiency and energy harvesting of edge computing end nodes. Energy-sufficient edge nodes are utilized to offload and exchange duties by employing a predictive estimation of energy distribution. Predictive learning is employed to identify instances of offloading and exchanging to validate computations utilizing available energy. This learning framework predicts energy needs and facilitates computation offloading and energy swapping among neighboring nodes. This allocation and distribution reduces the premature energy depletion of the peripheral nodes, thereby enhancing their energy harvesting. Simulations validate the method's effectiveness against existing models, demonstrating reduced energy usage, improved service response, and enhanced energy harvesting. The approach contributes to a faster task processing rate, optimising responses and improving the edge nodes' longevity. It minimizes the latency, energy consumption, and offloading ratio for various tasks and edge nodes.
- **Data compression and intelligent sampling**: Efficient data compression techniques, adaptive data sampling strategies, and intelligent task scheduling algorithms are essential for minimizing energy consumption without compromising mission-critical functionalities. These strategies reduce the volume of transmitted data. Compressing or aggregating data before transmission decreases the frequency and amount of data sent, conserving energy. Intelligent sampling further minimizes data collection activities based on real-time mission requirements, ensuring only necessary data is collected and transmitted [109, 110]. The work in [111] addresses the challenge of high energy consumption and transmission latency in IoT systems by integrating a fast, error-bounded lossy data compression technique with edge computing. The adapted SZ algorithm compresses multivariate time-series data efficiently. The approach supports dynamic data handling while maintaining low computational overhead, suitable for resource-constrained IoBT devices. Data is reconstructed and processed at edge nodes using supervised machine learning models. The results showed that data size was reduced up to 103 times, extending device battery life by 27%. Despite compression, stress classification accuracy remained high, demonstrating the technique's ability to preserve critical information. This solution addresses IoT systems' latency, bandwidth, and energy constraints while enabling real-time analytics at the edge. The approach supports dynamic data handling while maintaining low computational overhead, which is suitable for resource-constrained IoT devices. In [112] the authors introduce the Compression-Based Data Reduction (CBDR) technique to address energy consumption and data volume issues in IoT sensor networks. The CBDR framework combines lossy SAX quantization, which reduces dynamic range and increases redundancy in patterns, with lossless LZW compression, further reducing data size. The authors also propose Dynamic Transmission CBDR which adds a mechanism to dynamically decide whether to transmit full data or send notifications based on data correlation, further reducing unnecessary transmissions. The results show reduced data transmission and energy consumption while maintaining data accuracy, achieving high compression ratios (above 95%) and significant energy savings (up to 78%).

- **Energy-aware routing and protocol optimization**: Cross-layer design approaches allow interaction between different network layers to optimize energy consumption, packet delivery, and network lifetime. By coordinating the data link and network layers, energy-aware routing protocols can balance load distribution and minimize energy usage, particularly in multi-hop scenarios where data transmission can be energy-intensive. A few authors have explored strategies to minimize energy consumption while maintaining reliable communication and data exchange in IoBT deployments. The authors in [113] developed a routing protocol for military applications to address power efficiency, delay reduction, and load balancing in MANETs using a cross-layer approach for routing protocol optimization. The cross-layer design approach involves interaction between the data link layer and the network layer to optimize power consumption, delay, packet delivery ratio, and network lifetime. The protocol includes an optimized service layer that ensures correct delivery of data, bounded delay, minimum guaranteed bandwidth, and maximum guaranteed jitter. It employs an optimized channel access technique to improve the performance metrics. Simulation results show that the proposed protocol performs better in power consumption, delay, packet delivery ratio, and network lifetime than similar protocols based on cross-layer design approaches. Tortonesi et al. [20] highlighted the need for resource-efficient middleware solutions in the military network that filter, prioritize, and intelligently deliver intent-driven and context-sensitive decision support. They demonstrate how middleware solutions, especially for those used in tactical settings, might offer features that help lessen some of the drawbacks associated with IoT-enabled military applications. The work done in [114] proposes two application models, "the sequential module" and the "master-worker module," to process data collected by the end devices within the IoMT network. The work explores energy-efficient strategies for managing IoT devices in military environments using fog computing. They incorporate IoT-Fog architecture to create an energy-aware environment. The objective is to minimize energy consumption in the IoMT by exploiting fog computing to process data closer to devices rather than relying on centralized cloud systems. The authors present a comprehensive analysis of energy consumption and strategies for its reduction. The Sequential Module processes data in a linear flow, where each module processes and forwards the output to the next module. The Master-Worker Module employs a central "master" module that assigns tasks to "worker" modules and consolidates their results. The Master-Worker Module. The "Master-worker module" performed better, demonstrating better energy efficiency, lower delay, and higher network utilization than the Sequential Module resulting from the engagement of fewer nodes during data processing. Software algorithms play an important role in optimizing energy efficiency in IoBT communication. Research in this area encompasses the development of adaptive data transmission protocols, dynamic power management algorithms, and energy-aware routing protocols tailored for IoBT deployments. Techniques such as duty cycling, packet aggregation, and sleep mode operation aim to reduce idle energy consumption and minimize overhead associated with wireless communication. Furthermore, machine learning and optimization algorithms are employed to dynamically adjust communication parameters based on network conditions and device constraints. The authors in [115] propose IoBT-OS, an operating system for the Internet of Battlefield Things that aims to optimize decision latency, improve decision accuracy, and reduce corresponding resource demands on computational and network components. It addresses critical challenges in modern battlefield environments, such as reducing latency, improving decision accuracy, and ensuring computational efficiency under resource-constrained and adversarial conditions. This work focuses on optimizing the efficiency and efficacy of the sensor-to-decision loop and offers an architecture to accomplish the optimization goals. The IoBT-OS architecture has four modules: (i) an edge AI efficiency library that optimizes machine learning models to operate efficiently at the tactical edge using methods like neural network compression (DeepIoT), confidence estimation (RDeepSense), and compressive offloading to manage bandwidth limitations. (ii) mission-informed real-time data management algorithms that implement data prioritization and scheduling algorithms to focus computational resources on critical tasks and reduce processing latency. (iii) digital twin support that maintains a virtual replica of the battlefield system for global optimization, anomaly detection, and root cause analysis, synchronizing real-time system state data under bandwidth constraints, and iv) offline training support which provides tools like self-supervised contrastive learning to train models using minimal labeled data and builds latency models to predict computational performance accurately. By pushing computations closer to the edge, the system minimizes latency and dependency on centralized resources, critical for dynamic battlefield scenarios. The approach combines neural network compression, real-time scheduling, and data prioritization for high performance in resource-constrained settings. The protocol results showed reduced latency and an improved inference quality of a small sensing-to-decision loop.

5.3 Network security

Security is critical in IoBT to safeguard classified military information and prevent unauthorized access or tampering. Encryption, authentication, and other cryptographic techniques are employed to secure communication channels and data transmissions between battlefield assets, ensuring the confidentiality, integrity, and authenticity of information exchanges [116–118]. Adversaries may physically tamper with IoBT devices, altering their functionality or introducing malicious components. If an IoBT device is lost, stolen, or captured by the enemy, sensitive data can be compromised. Communication vulnerabilities such as eavesdropping, jamming, and spoofing disrupt IoBT operations and can lead to unauthorized access or misinformation. The work in [45] explores a secure network approach to accomplish C2 agility in an IoBT heterogeneous environment by integrating the application and network with a multi-layer, defense-in-depth cyber security strategy at the hardware, network, and application levels. The research delves into the complexities of establishing secure C2 capabilities in the IoBT environment. It supports the implementation of a comprehensive cyber security framework that covers hardware, network, and application layers to guarantee the safe and efficient sharing of information. The proposed framework utilizes the software-defined networking paradigm to coordinate network services, incorporating data from information-centric networks and delay-tolerant networks that focus on semantics-oriented information. Preliminary simulation results showcased a notable enhancement in network metrics and resilience against cyber-attacks, highlighting the potential effectiveness of the suggested approach.

The authors in [119] propose a stochastic geometry-based model to characterize the connectivity of IoBT networks regarding the degree distribution of the devices. They formulate a tractable optimization problem that can assist commanders in cost-effectively planning the network and reconfiguring it according to the changing mission requirements. The authors develop a specialized framework for information dissemination over IoBT networks that utilizes the connectivity structure in the multilayer heterogeneous network by using existing works in epidemiology. The authors in [120] introduce a novel design that combines a classical cryptographic algorithm with a quantum secret-sharing algorithm to bolster the security of the MIoT network. This design involves multiple layers of security protocols addressing various security requirements, including authentication, authenticity, undeniability, data integrity, confidentiality, freshness, anonymity, and unrelatedness. The presented scheme is highly secure and provides protection against a wide range of attacks, and is evaluated through theoretical analysis. It outperforms previous works regarding efficiency and effectiveness in resilience against various types of cyberattacks. In [121], the authors present a scheme that utilizes deception to strengthen the security of location information for IoBT nodes. A new encryption method and dummy identities and packets are suggested. The authors created a mathematical model to assess the effectiveness of the proposed scheme. The model considers factors such as safety time, probability of failure, and probability of correctly identifying the real packet. The results clearly show the proposed method's effectiveness in minimizing the chances of accurately determining the actual location of the communicating entities. They employ NetLogo simulations to validate the mathematical models. The authors in [122] studied the resilience of IoBT. The initial focus was on addressing the security needs of the IoBT network, so they developed a directed network model and a method for measuring connectivity. After careful analysis, they successfully developed an advanced attack strategy optimization model and were able to determine the worst-case attacks by solving the model. By utilizing the network model, they conducted an analysis on the resilience of the IoBT network when subjected to the most effective attack strategy. Utilizing their developed network model, the authors conducted an analysis on the robustness of the IoBT network when subjected to the most effective assault technique. This analysis yielded valuable insights that can be used to design protection strategies that effectively safeguard the security and dependability of the IoBT network, even in the face of adversarial actions. The results show that the adversary will change the attack mode according to the parameter settings of attack resources and network communication link density. To enhance the network's robustness, the defense strategy needs to be adjusted in time to deal with this change.

An approach for enhancing border security using Tiny Machine Learning (TinyML) integrated with IoBT technology is developed in [123]. The authors address sensor hacking issues that compromise traditional sensor-based systems. Specifically, TinyML models are deployed on microcontrollers to detect abnormal movements along border fences, distinguishing between natural causes (e.g., wind) and potential threats (e.g., intrusion attempts). Using Edge Impulse, the authors trained a TinyML model on accelerometer data, deployed it on an Arduino Nano 33 BLE Sense, and subjected it to electromagnetic pulse (EMP) attacks. Compared to a standard sensor system (MPU6050 sensor with Arduino Nano), TinyML-based systems could detect things correctly even when the sensors were hacked, while the

standard system gave erroneous readings. Integrating TinyML in IoBT for border security offers a practical application of machine learning in resource-limited environments. The approach demonstrates robustness against EMP-based sensor attacks, showing TinyML's potential in critical, high-risk applications. The authors in [124] present a novel system for identifying injured soldiers in battlefield environments using UAVs integrated with deep learning models and blockchain technology. In this system, UAVs employ deep learning to analyze visual data, while smartwatches on soldiers collect and transmit heart rate data. The use of blockchain ensures secure data access and prevents unauthorized access. If an injured soldier is identified by the UAV's deep learning model, this identification is confirmed by the smartwatch's heart rate data, which is relayed via the UAV to an edge computing server. The edge computing server performs further analysis and sends the results to command authorities. The combination of blockchain for secure access control and UAVs for data collection addresses battlefield security and privacy concerns. By using both deep learning image recognition and heart rate data from a smartwatch, the system reduces the likelihood of false positives in injury identification. Butun and Mahgoub [125] developed a technique that examines a security strategy designed to protect the location privacy of military personnel in IoBT environments. The authors propose "Expandable Mix-Zones," a technique to obscure precise location data through a system of concentric privacy zones. These zones provide varying levels of protection (high, medium, and low) by using pseudonym exchanges and obfuscating location data to create uncertainty for adversaries. Simulated in Python with a Random Walk Model, the study quantifies the effectiveness of these zones by measuring location estimation error within and outside the mix-zones. The findings suggest that mix-zones reduce adversaries' accuracy in tracking soldiers, especially within the innermost zones. A Trust-Based Support Vector Regression (TSVR) Security Mechanism to enhance the security of IoBT by mitigating black hole attacks is developed in [126]. Black hole attacks disrupt communication by advertising false routing paths and dropping data packets. The TSVR model calculates trust values for IoBT devices using metrics like packet delivery ratio, end-to-end delay, energy consumption, goodness, and closeness. It employs Support Vector Regression to classify nodes as malicious or trusted and predict their future behavior. The mechanism integrates with the Routing Protocol for Low-Power and Lossy Networks to optimize secure routing. Simulations demonstrate that TSVR improves metrics such as packet delivery ratio, average delay, and detection accuracy compared to existing models.

5.4 Cyber security

Research works on IoBT security challenges [127] cover a large area, and it is changing every day, with new loopholes being exposed regularly. Cyber attacks, such as malware-distributed denial-of-service attacks and zero-day exploits, can significantly decrease the QoS of a network. Most works analyze software operations to detect malware and exploit vulnerabilities in generic IoT devices deployed in military scenarios [128]. However, only a few deal with spectrum sensing data falsification attack detection in IoBT cognitive radio to improve network performance, [129] propose a resource allocation algorithm that optimizes user access control using RF fingerprinting due to small-scaled available signal samples and optimization of network performance. Drones can be regarded as an evolutionary development in cyberwarfare rather than a revolutionary one. The authors in [130] study the implementation of on-demand multi-access edge computing enabled UAVs and suggest a method called bender decomposition to tackle the cyber security challenge. In [131], the work focused on modelling threats on IoBT by formulating the problem as a learning of a graph to extract high-level IoBT context information. They presented a novel approach that utilizes n-grams and incorporates a random walk strategy. This research investigated the efficacy of employing cyber deception as a defensive measure against an adversary's actions. They demonstrated that having incomplete information can enable an adversary to gather significant insights across the entire network. Various types of attacks, such as ACK attacks, eavesdropping attacks, middleman attacks, message manipulation attacks, traffic analysis attacks, message forgery attacks, and identity disclosure attacks, have been considered. The work in [132] introduces SpecForce, a framework that combines behavior fingerprinting and machine learning and deep learning techniques to effectively detect a wide range of cyber-attacks targeting IoBT spectrum sensors, including jamming, spoofing, and eavesdropping. SpecForce has been deployed in a highly advanced battlefield scenario of 25 IoBT spectrum sensors powered by Raspberry Pi. In this situation, an analysis has been conducted on the cyber security threats that impact the spectrum sensors of IoBT. The focus was on identifying attacks related to identity, malware, and SSDF that exploit these threats. The detection results achieved by SpecForce for each attack family impacting IoBT spectrum sensors show that the approach can significantly improve the security of IoBT systems.

5.5 Data management

The heterogeneity of end devices in IoBT generates multi-modal data while using different computing devices, which leads to diverse processing capabilities in the network. This data needs to be properly managed. There is an increasing demand for software-based solutions to maintain confidentiality, which necessitates the use of computationally intensive resources. However, these resources are limited in the context of IoBT [133–135]. The work in [133] proposes a blockchain technology that employs "sharding" to manage data and communication of unmanned vehicles efficiently. The integration of software-defined networking further aids in managing the complex and dynamic networking requirements of the battlefield. The architecture is designed to ensure secure communication among UVs, even under the high mobility and limited power conditions typical of battlefield environments. SDN allows for better visibility and management of the network, ensuring persistent connectivity. In [136] the authors use machine learning to develop a target system model for information fusion from multiple IoBT sources. They also deal with message integrity and authenticity by introducing the JointField blockchain, effectively minimizing threats from malicious adversaries. The authors in [134] introduce a novel approach that combines Named Data Networking (NDN) and blockchain technology to enhance the resilience and security of IoBT. NDN is highlighted for its ability to simplify data transmission in IoBT environments by focusing on data rather than device-specific connections. Blockchain technology is introduced to ensure data integrity, immutability, and trust within the network. This approach allows nodes to efficiently store and distribute the most critical data within the network. It involves implementing a unique network sharding technique known as the Interest Groups. Using this approach, nodes with a higher degree of similarity in the data they store are grouped in the same Interest Group. Segmenting the network in this manner guarantees that the network is not overwhelmed by redundant Interest Packets. Additionally, the article presents a unique consensus process known as the Proof of Common Interest. Based on the evaluation results, the network segmentation leads to improved packet transfers and reduced packet floods.

The work in [137] presents a blockchain-assisted content sharing scheme called MR-Block for mixed reality applications, focusing on multi-user data sharing. Before accessing the system, every entity goes through a registration process. Before transmitting data, a set of rules and regulations are established within a smart contract. Validation is conducted within the smart contract to ensure that only authorized users can access the data. A controlled environment is established to conduct these experiments. The work in [135] proposed Modified Elliptic Curve Cryptography, a scheme to secure communication in UAV networks. The scheme safeguards the sensitive nature of the data being transmitted and the potential for unauthorized access or cyberattacks. The suggested approach utilizes a certificate authority to associate UAVs' unique identity number information with elliptic curve cryptography keys. The protocol recognizes and rejects unauthorized UAVs from joining the network by analyzing their periodic messages and the coordinate information received from neighboring UAVs. Different machine learning classifiers are evaluated in [136] to determine the best-suited classifier for securely sharing data in IoBT environments. The study examined their accuracy, precision, recall, F1-score, and computation time under various scenarios and attack models. They introduce the JointField blockchain network for joint and allied force data sharing, an adaptive classifier that could effectively balance the need for security and efficiency in battlefield communications.

6 Comparison and discussion

In this paper, we performed a comprehensive analysis of solutions developed to optimize communication capabilities in IoBT systems. The proposed techniques to deal with specific challenges such as power management [5, 20, 107, 108, 113, 114], network security [45, 119–123, 126], cyber security [91, 124, 125, 129–132], data management [136, 137], and interoperability [97–99, 115]. Our analysis distinguishes the approaches employed and highlights the challenges and performance in the studies considered. Table 1 shows a summary of the comparison of the reviewed literature. The literature analysis shows that existing techniques and algorithms improve the communication performance of IoBT albeit with some drawbacks.

The strength of the method used in [107] is that it ensures the necessary supply of solar-powered portable electronic devices for soldiers remains uninterrupted and adequately met, regardless of the specific prevailing constraints. The article considers various factors such as solar PV modelling, battery modelling, objective function, and constraints

Table 1 Comparison of the reviewed literature

Refs.	Contribution	Approach	Strengths	Drawbacks
[106]	Energy harvesting technique	Predictive estimation	Dynamic optimisation, improves energy efficiency	Scalability issues, assumes relatively stable harvesting rates
[110]	Energy efficiency	SDN controller architecture	Optimized resource management, scalable	Introduction of latency, data privacy issues
[107]	Power-efficient routing protocol	Algorithm design, performance evaluation	Ensures uninterrupted solar power	Does not consider the sizes of the solar photovoltaic generator
[108]	Energy-aware application models	System modelling, and experimentation	Improves the energy efficiency and energy harvesting of edge computing devices	Only the edge nodes are optimized
[45]	C2 agility in IoBT heterogeneous environment	Network Function Virtualization	Real-time monitoring and network reconfiguration	Scalability, energy consumption
[114]	Secure network strategy	Multi-layer cyber security mechanism	Reduction in energy consumption	Only focused on the logical components of the application modules
[116]	Network connectivity optimization	Intelligent task scheduling	Improved bandwidth efficiency and reduced network congestion	Reliance on edge computing for real-time processing
[117]	Cryptographic scheme	Multi-layered security approach	Balances security, power and computational efficiency	Scalability challenges
[129]	Resource allocation	RF fingerprint identification	Low computational overhead	Vulnerability to environmental factors
[120]	Resilience of IoBT network	Quantum cryptography	Ensures the security of key exchanges	Limited practical implementation details
[121]	Deception encryption scheme	Security encryption	Introduces ambiguity into the location information	False positives and collateral effects
[123]	Novel security mechanism	A trust-based approach and machine learning	Resilience to sensor hacking, energy efficiency	Reliance on user cooperation, scalability
[124]	Deep learning security model	Blockchain integration	Robust system design, scalable and adaptive	UAV battery dependency, smartwatch reliance
[125]	Novel security mechanism	A trust-based approach and machine learning	Flexible and adaptive design	Reliance on user cooperation, scalability
[126]	Deception technique	Random walk model integration	Comprehensive trust evaluation, effective black hole attack mitigation	Limited attack scope, dependency on trust calculation
[137]	Content-sharing mechanism	Smart contracts to automate access control	Data integrity and tamper resistance	Latency concerns, inherent delays
[132]	Securing IoBT-based spectrum sensors	SpecForce framework	Comprehensive security for spectrum sensors	Computational overhead
[133]	Sharding-enabled blockchain with SDN	Communication optimization	Efficient resource allocation, low latency	Centralized control risks in SDN
[115]	IoBT-OS protocol	Efficiency optimization for the sensor-to-decision loop	Distributed processing, communication efficiency	Dependence on communication infrastructure
[135]	Secure, reliable, and efficient data dissemination	Named data networking	Improves the resilience of IoBT networks	Increased energy consumption
[97]	IoBT-MAX testbed	Multimodal Sensor Integration protocol optimization	Interoperability testbed	Scalability and security concerns
[100]	Secure and reconfigurable network design	Game theory optimization	Adaptability, energy efficiency	Scalability challenges

to develop a comprehensive optimization model. The drawback of this approach is that it does not consider the sizes of the solar photovoltaic generator and batteries in relation to the overall weight to be carried by the soldier. The work does not compare the proposed approach with existing or alternative methods for optimal power flow management. In [108], the approach improves the energy efficiency and energy harvesting of edge computing devices, thereby enhancing the edge nodes' lifetime. The drawback is that only the edge nodes are optimized. The authors did not mention real-world validation or experiments to validate the proposed methods. It would be valuable to have experimental results or case studies to demonstrate the approach's effectiveness in practical scenarios. The cross-layer approach employed in [113] has the strength that it allows interaction between TCP/IP layer to improve energy conservation in military applications where nodes have limited battery power. By incorporating a cross-layer design approach, the protocol enables efficient communication and coordination between the data link layer and the network layer, leading to improved throughput, packet delivery ratio, and network lifetime performance. The drawback is that the work does not explicitly discuss the scalability of the proposed protocol, particularly in large-scale networks, where the number of nodes and network complexity can significantly impact performance. The strength of the master-worker module in [114] lies in the considerable savings achieved in energy consumption, making it effective in handling smart devices. The drawback is that the paper only focused on the logical components of the application modules. The authors do not provide specific details about the experimental setup, such as the number of devices used, the specific metrics measured, and the specific scenarios tested. The paper could benefit from a more detailed discussion on the practical implementation of the proposed modules, including deployment strategies.

The work in [45] highlights significant network resilience and performance improvements. The drawback is that it lacks explicit details regarding the routing techniques employed and the specific performance metrics used for evaluation. This gap hinders a comprehensive understanding of the proposed solution's quantitative impact. Additional investigation into the routing algorithms and performance indicators would be necessary to determine the practical viability and usefulness of the proposed framework. The strength of the approach proposed in [119] is that it is robust and cost-effective. The drawback is that the proposed scheme needs verification in a heterogeneous environment. The strength of the work in [120] represents a cutting-edge approach using quantum cryptography to secure IoBT.The overall robustness of this approach is enhanced by the multi-layered security design, which provides multiple points of defense. The drawback of this approach could be scalability challenges across the different IoT networks, particularly in resource-constrained environments, because of its complexity. Further exploration is required for its practical application. The study in [121] proposed a deception-based scheme using a novel encryption technique, along with dummy IDs and fake packets, to strengthen the security of location information for IoBT nodes. The strength of the proposed method is its highly effective ability to minimize the chances of accurately determining the actual location of the communicating devices. The drawback is that the approach considered one-hop communication between the gateway and IoBT entities and did not consider multi-hop communication. The strength of the approach proposed in [122] is that they used theoretical analysis and an actual military organization to verify their model. The drawback of this approach is that they only considered attacks against edges and used homogenous devices; therefore, they only considered homogenous multi-layer networks. Considering heterogeneous devices would be a more realistic reflection of the characteristics of IoBT. Trust-based Support Vector Regressive Security Mechanism [126] is a machine learning-based approach to enhance security in IoBT environments. The TSVR model mitigates black hole attacks by computing trust values for IoBT devices using metrics like packet delivery ratio, end-to-end delay, energy consumption, goodness, and closeness. The approach combines direct trust (based on first-hand data) and indirect trust (recommendations from neighboring nodes).Simulations show significant performance improvements. The strength of this approach is in its effective black hole attack mitigation. TSVR demonstrates high detection accuracy in identifying malicious nodes, protecting network integrity. By incorporating multiple metrics, the model evaluates node behavior more accurately than single-metric approaches. Machine learning enhances predictive capabilities, enabling proactive measures against potential threats. However, the model's effectiveness is solely assessed through simulations under controlled environments, limiting its validation under real-world IoBT conditions. Although optimized, the computational requirements for trust evaluation and SVR may still impact energy-constrained IoBT devices. Addressing its scalability, energy demands, and broader attack resilience could further enhance its applicability in real-world battlefield scenarios. The proposed Expandable Mix-Zones in [125] offer a promising solution to enhance location privacy in IoBT deployments, combining deception strategies with dynamic privacy levels. The concept of expandable mix-zones tailored for battlefield environments is innovative, addressing specific military needs for location privacy. The tiered privacy structure allows real-time adaptability to threat levels, which is practical for dynamic combat environments. Its drawback lies in that the success of the mix-zone strategy depends on all users' active participation in pseudonym exchanges, risking the system's integrity if individuals do not comply.

Sophisticated adversaries could infer positions by analyzing entry and exit points or movement patterns near mix-zones. As IoBT networks grow, managing and expanding mix-zones dynamically might introduce logistical and computational challenges. Integrating TinyML with IoBT to enhance border security and mitigate vulnerabilities in conventional sensor systems, especially against Electromagnetic Pulse (EMP)-based sensor hacking is developed in [123]. The approach aims to distinguish natural fence movements caused by environmental factors from deliberate intrusions using TinyML-powered microcontrollers. The system was tested for its ability to detect such intrusions with high accuracy and was evaluated for resilience against EMP attacks. TinyML-based systems showed robustness against EMP interference, highlighting their potential for secure applications.The study achieved 95.4% accuracy in detecting intrusions, with 99.29% accuracy during controlled tests. The methodology is adaptable to different types of fences and field conditions, making it versatile.TinyML's low resource consumption makes it suitable for continuous deployment in remote, power-constrained environments.One of the drawbacks of this model is limited testing.The experiments primarily focused on mid-range EMP attacks and basic intrusion scenarios. Broader testing under varied battlefield conditions (e.g., extreme weather or complex intrusions) could strengthen the findings.

SpecForce [132] has strength in that it addresses a variety of threats, making it a robust solution for securing IoT spectrum sensors. The strength of this scheme lies in the inclusion of anomaly detection, which enhances its ability to identify and respond to new or unforeseen threats. The drawback of SpecForce is its complexity. The scheme may require significant computational resources, which could be a challenge in resource-constrained battlefield environments. The scheme's scalability in larger, more complex IoBT systems is not fully addressed, which could be a limitation as the number of connected devices increases. The sharding technique employed in [133] allows for scalability. The system can handle many end devices and transactions efficiently, which is important for fast-paced and data-heavy operations in military settings. Sharding further enhances security by limiting the exposure of each shard to potential attacks, while the integration of SDN improves overall network efficiency. Although the system is designed to minimize latency, the time-sensitive nature of military operations means that even slight delays in transaction validation could have serious consequences. Implementing a sharding-enabled blockchain combined with SDN in a battlefield environment adds significant complexity to the system, which could pose challenges in deployment and maintenance. The Interest Group protocol proposed in [134] supports data confidentiality and access control through name-based access control, which addresses a vital requirement in military communication. The NDN segment focuses on data rather than connections, thus reducing the complexity of maintaining consistent communication channels in dynamic and mobile environments like battlefields. The drawback of this protocol is that blockchain can introduce computational overhead, which may not be suitable for resource-constrained IoT devices commonly used in battlefield environments.

The IoBT-OS protocol proposed in [115]reduces decision latency and improves accuracy contributing to better decision-making. It is relevant for military applications where timely and accurate decisions are critical. The drawback of the protocol is the trade-off between balancing resource optimization with decision quality which can be challenging.Despite the promising performance demonstrated by the proposed blockchain-empowered framework for decentralized trust management in IoBT, some limitations still need to be addressed in future work. The proposed protocol in [98] exploits the EigenTrust algorithm to aggregate the global trust of IoBT nodes. The validity of EigenTrust is based on the assumption that computed global trusts will not change frequently over time, allowing its computation to converge among all participating nodes after several iterations. However, this assumption may not hold when IoBT nodes maliciously change their behaviours over time, leading to difficulties in dealing with time-varying reputations. The proposal uses the proof-of-trust consensus protocol to synchronize the blockchain. Although this design integrates trust management with the consensus process to form a decentralized framework, solving the hash puzzle will require significant computational power. A scheme that improves constraints such as high latency, bandwidth and attack vulnerability was developed in [99]. They proposed a layered architecture combining 5 G and blockchain for UAV-based IoBT to provide ultra-low latency, reliable communication, and precise surveillance. The strength of this scheme is that the performance evaluation showcases improvements in latency (from seconds to milliseconds), frame loss, and data throughput, illustrating the effectiveness of the proposed scheme. Using edge computing for task offloading and blockchain for decentralized data management ensures that the system can scale and adapt to large networks of UAVs, even in heterogeneous and intermittent network conditions. Incorporating a "permissioned" blockchain mitigates various security threats (e.g., DDoS attacks, data manipulation, UAV impersonation), ensuring high data integrity and trust in IoBT networks. However, the drawbacks of the scheme are that the authors acknowledge intermittent disconnections but need to address network resilience strategies beyond blockchain. In situations where 5 G coverage is poor or absent (e.g., remote, hostile terrains), the performance of the proposed scheme might degrade. The reliance on edge-based offloading raises concerns about resource availability in remote locations. If edge nodes are not adequately deployed or suffer failures, the system could

experience delays or interruptions in real-time data processing. The work discusses the use of blockchain for security. Still, it does not adequately address the overhead and potential latency introduced by blockchain consensus mechanisms, especially in high-speed military operations where every millisecond counts. The scheme in [100] combines multiple disciplines (stochastic geometry and mathematical epidemiology) to provide a holistic approach to network design. The reconfigurable nature of the network allows it to adapt to changing battlefield conditions and threats, ensuring continued operation. The scheme incorporates security measures to protect critical information from adversaries, enhancing the reliability of the network. The drawback is that the approach is relatively complex, which may pose challenges for implementation and maintenance and relies on certain assumptions about the battlefield environment and network parameters. If these assumptions are not met, the effectiveness of the network may be compromised. The study in [124] proposes an advanced system integrating UAVs, deep learning, and blockchain to enhance soldier injury detection on the battlefield. The system utilizes UAVs for aerial reconnaissance and smartwatches for real-time health monitoring (e.g., heart rate). A lightweight deep learning model processes video data to detect injured soldiers, while heart rate analysis confirms injuries. Blockchain-based Access Control Lists ensure secure data handling, preventing unauthorized access. The UAVs capture images and collect heart rate data from smartwatches. Data is transmitted to edge computing servers for analysis. Blockchain-based access control list verifies device and user access rights. A custom 16-layer CNN deep learning model with convolutional filters extracts features for injury detection. The model utilizes Public Key Infrastructure and blockchain for secure data transmission and storage. The study evaluates its approach through simulations, demonstrating improved accuracy and system performance. The strength of this approach is that it has a robust system design with a two-step verification (deep learning model + smartwatch data) which enhances reliability in injury detection. It is scalable and adaptive to various battlefield scenarios and IoBT deployments. The drawback of this approach is its dependency on UAV battery. Despite improvements, UAV operations remain limited by battery capacity and flight duration. Injury detection relies on soldiers wearing functioning smartwatches, which may not always be feasible. The key research papers discussed in this section are summarized in Table 1

7 Research gaps and future direction

The research shows that while some progress has been made in addressing communication challenges within the Internet of Battlefield Things, several research gaps persist, paving the way for future investigations and advancements. Research gaps and future work that were identified in the literature reviewed are as follows:

7.1 Integration of emerging technologies

While AI algorithms and edge computing platforms have demonstrated significant potential for optimizing decision-making processes and reducing latency in IoBT deployments, their seamless integration into communication infrastructures remains relatively under-explored. Future research could explore novel approaches for incorporating AI-driven decision support systems and edge computing capabilities into IoBT adaptive communication models tailored for resource-constrained, decentralized environments typical of IoBT. Research should investigate:

- AI-driven adaptive data filtering at the edge to prioritize critical information, minimizing unnecessary data transmission and reducing communication overhead. Real-time dynamic AI algorithms that can adapt to fluctuating battlefield conditions, such as network congestion, device failures, and hostile interference.
- Exploration of lightweight AI models to enable fast inference on low-power edge devices, reducing reliance on cloud-based processing.
- A hierarchical data management system that includes efficient caching strategies for battlefield data, with dynamic policies on data freshness, retention, and security, ensuring critical decisions are made based on up-to-date information. This system should also automate decision-making on data re-computation based on network load and resource availability.

7.2 Robust and adaptive communication protocols

Existing protocols for IoBT have provided useful insights into energy-efficient communication, but they often lack the flexibility to cope with rapidly changing and hostile battlefield conditions. Future research should focus on the design

and validation of robust, context-aware communication protocols that dynamically adjust based on real-time network conditions, adversarial threats, and device constraints. Key research directions include:

- Development of self-healing protocols capable of dynamically re-routing communication pathways in response to network failures or jamming attempts.
- Protocol optimization frameworks that allow for adaptive modification of communication parameters (e.g., bandwidth allocation, transmission power, frequency hopping) in real time based on evolving network conditions.
- Integration of reinforcement learning algorithms to optimize protocol performance by continuously learning from the battlefield environment and adjusting strategies to maximize both communication reliability and energy efficiency.

7.3 Security and resilience of IoBT communication systems

Although encryption and cryptographic methods have been implemented to secure IoBT networks, emerging cyber threats like advanced persistent threats (APTs) and zero-day exploits demand more proactive and intelligent security frameworks. Future research should focus on developing real-time, AI-powered defense mechanisms to detect, prevent, and mitigate these evolving threats, enhancing both the security and resilience of battlefield communication systems. Research should focus on:

- Design of autonomous, AI-based intrusion detection systems that can identify suspicious behavior and anomalies in network traffic patterns, enabling real-time mitigation of threats.
- Implementation of zero-trust architecture principles in IoBT communication, ensuring that every communication link and device is authenticated, regardless of its origin, with continuous monitoring for integrity violations.
- Resilient encryption schemes that can withstand partial network failures and cyber-attacks, ensuring communication security even in disrupted environments.
- Development of dynamic key management protocols to ensure secure key exchange and encryption in rapidly changing, hostile environments, minimizing the risk of compromised communication.

7.4 Interdisciplinary research

Effective IoBT deployment requires not just technological advances but also seamless integration into operational military environments. While there has been considerable progress in communication technologies, there remains a gap in aligning these innovations with real-world military doctrine, operational tactics, and organizational structures. Future research could include:

- Collaborative interdisciplinary projects involving communication engineers, military strategists, and defense policymakers to design communication solutions that are both technologically advanced and tactically relevant.
- Field experiments and simulations to validate the effectiveness of new communication technologies under simulated military conditions, ensuring they are operationally feasible.
- Development of mission-specific communication frameworks, where researchers work alongside military commanders to design communication architectures that align with specific tactical objectives and combat scenarios.
- Human factors research to assess the usability and reliability of communication systems under high-stress, fast-paced military operations, ensuring that the technologies developed can be seamlessly integrated into decision-making processes on the battlefield.

8 Conclusion

IoBT represents a transformative approach to modern military operations, using interconnected devices, sensors, and communication networks to enhance situational awareness, decision-making, and operational effectiveness on the battlefield. Emerging solutions such as AI-driven decision support systems, edge computing, and adaptive communication protocols show great promise in addressing these challenges. However, substantial gaps remain in the integration of these technologies into robust, real-world IoBT communication architectures. More specifically, the lack of protocols

capable of adapting to dynamic battlefield conditions and the limited exploration of proactive cybersecurity measures for evolving threats like advanced persistent threats (APTs) and zero-day exploits continue to present significant barriers.

Future research must focus on interdisciplinary approaches that blend cutting-edge communication technologies with operational military strategies to ensure their relevance and effectiveness in mission-critical scenarios. Furthermore, advancements in AI and machine learning, coupled with enhanced security frameworks, are pivotal to ensuring the future viability and success of IoBT deployments.

In conclusion, while the current body of work has made notable strides in addressing communication challenges within IoBT, there remains a clear need for more targeted research efforts. These should aim to develop resilient, adaptive, and secure communication infrastructures that can thrive in the complex, contested environments characteristic of modern warfare. Addressing these gaps will be key to unlocking the full potential of IoBT and ensuring its effective integration into future battlefield operations.

Acknowledgements The research was sponsored by the ARO and was accomplished under Grant Number: W911NF-22-1-0006. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of ARO or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

Author contributions Conceptualization, R.K., H.C.M and A.D.; methodology, R.K., H.C.M and A.D.; investigation, R.K.; resources, H.C.M; writing—original draft preparation, R.K.; writing, review and editing, R.K., H.C.M and A.D.

Data availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

1. Kott A, Swami A, West BJ. The internet of battle things. Computer. 2016;49(12):70–5.
2. Kott A, Alberts DS, Wang C. Will cybersecurity dictate the outcome of future wars? Computer. 2015;48(12):98–101.
3. Zhu J, McClave E, Pham Q, Polineni S, Reinhart S, Sheatsley R, Toth A. A vision toward an internet of battlefield things (IoBT): autonomous classifying sensor network. US Army Research Laboratory, 2018.
4. Fraga-Lamas P, Fernández-Caramés TM, Suárez-Albela M, Castedo L, González-López M. A review on internet of things for defense and public safety. Sensors. 2016;16(10):1644.
5. Wigness M, Abdelzaher T, Russell S, Swami A. Internet of battlefield things: challenges, opportunities, and emerging directions. IoT Defense Nat Secur. 2022;48(12):5–22.
6. Hossein Motlagh N, Mohammadrezaei M, Hunt J, Zakeri B. Internet of things (IoT) and the energy sector. Energies. 2020;13(2):494.
7. Zheng DE, Carter WA. Leveraging the internet of things for a more efficient and effective military. Rowman & Littlefield, 2015.
8. Yushi L, Fei J, Hui Y. Study on application modes of military internet of things (MIOT). In: 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), 2012;3:630–634. IEEE.
9. Zieliński Z, Fongen A, Fuchs CJ, Furtak J, Niewiadomska-Szynkiewicz E. IST-ET-076 on internet of military things—framework for the application of internet of things in the military domain. Report: NATO IST Panel; 2015.
10. Abdelzaher T, Ayanian N, Basar T, Diggavi S, Diesner J, Ganesan D, Govindan R, Jha S, Lepoint T, Marlin B, et al. Toward an internet of battlefield things: a resilience perspective. Computer. 2018;51(11):24–36.
11. Azmoodeh A, Dehghantanha A, Choo K-KR. Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning. IEEE Trans Sustain Comput. 2018;4(1):88–95.
12. Montiel-Sánchez I. Defence internet of things. Eur Defence Agency. 2017;14:15–6.
13. Alberts DS, Garstka J, Stein FP, et al. Network centric warfare: developing and leveraging information superiority. DC: National Defense University Press Washington; 1999.
14. Alberts DS, Garstka JJ, Hayes RE, Signori DA. et al. Understanding information age warfare. CCRP Publication Series Washington, DC, 2001;8.

15. Nie J-G, Li D-S, Han Y-Y. Implementation environment of net-centric warfare based on internet of things. Fire Control Command Control. 2012;37(9):14–7.
16. Russell S, Abdelzaher T. The internet of battlefield things: the next generation of command, control, communications and intelligence (C3I) Decision-making. In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). IEEE, 2018;737–742.
17. Wigness M. Devcom ARL program announcement for the internet of battlefield things (IoBT). https://arl.devcom.army.mil/cras/iobt-cra/. Accessed 29 Mar 2024.
18. Rahmah U, Mustapa M, Samad PI, Budiarti NAE. Internet of things (IoT) in defense and security systems: a literature review. Int J Sci Eng Sci. 2023;7(5):115–8.
19. Wigness M, Abdelzaher T, Russell S, Swami A. Internet of battlefield things: challenges, opportunities, and emerging directions. IoT for Defense and National Security. 2022;5–22.
20. Tortonesi M, Morelli A, Govoni M, Michaelis J, Suri N, Stefanelli C, Russell S. Leveraging internet of things within the military network environment—challenges and solutions. In: IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE. 2016;2016:111–6.
21. Heidari A, Jabraeil Jamali MA. Internet of things intrusion detection systems: a comprehensive review and future directions. Clust Comput. 2023;26(6):3753–80.
22. Joshi S, Thakar A, Patel C. Applications of machine learning and deep learning in securing internet of battlefield things: a futuristic perspective. In: 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2023;333–338.
23. Michaelis J, Morelli A, Hernandez L, James D, Freeman J, Suri N. LoRaWAN testing for military communications in urban environments. In: IEEE 7th World Forum on Internet of Things (WF-IoT). IEEE. 2021;2021:885–90.
24. Chilamkurthy NS, Pandey OJ, Ghosh A, Cenkeramaddi LR, Dai H-N. Low-power wide-area networks: a broad overview of its different aspects. IEEE Access. 2022;10:81–959.
25. Sun Z, Yang H, Liu K, Yin Z, Li Z, Xu W. Recent advances in LoRa: a comprehensive survey. ACM Trans Sensor Netw. 2022;18(4):1–44.
26. Tlili S, Mnasri S, Val T. The internet of things enabling communication technologies, applications and challenges: a survey. Int J Wireless Mobile Comput. 2022;23(1):9–21.
27. Sharma SK, Wang X. Toward massive machine type communications in ultra-dense cellular iot networks: current issues and machine learning-assisted solutions. IEEE Commun Surv Tutorials. 2020;22(1):426–71.
28. Jiménez-Fernández S, Salcedo-Sanz S. Examining 5G Technology-Based Applications for Military Communications. In: Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT &SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers, vol. 13785. Springer Nature, 2023;449.
29. Fall K. A delay-tolerant network architecture for challenged internets. In: Proceedings of the 2003 conference on applications, technologies, architectures, and protocols for computer communications.2003;27–34.
30. Barz C, Cramer E, Fronteddu R, Hauge M, Marcus K, Nilsson J, Poltronieri F, Tortonesi M, Suri N, Zaccarini M. Enabling Adaptive Communications at the Tactical Edge. In: MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM). IEEE, 2022;1038–1044.
31. Zacarias I, Gaspary LP, Kohl A, Fernandes RQ, Stocchero JM, de Freitas EP. Combining software-defined and delay-tolerant approaches in last-mile tactical edge networking. IEEE Commun Mag. 2017;55(10):22–9.
32. Qu Z, Zhang G, Cao H, Xie J. Leo satellite constellation for internet of things. IEEE Access. 2017;5:18–401.
33. Qu G, He C, Chen Q, Meng W. Tactical data-oriented decentralized communication scheme in vehicle-assisted networks: challenges and solutions. IEEE Commun Mag. 2023;62(1):56–61.
34. Kannimuthu P, Thangamuthu J. Decision tree trust (DTTrust)-based authentication mechanism to secure RPL routing protocol on internet of battlefield things (IoBT). Int J Bus Data Commun Netw (IJBDCN). 2021;17(1):1–23.
35. Saputro N, Tonyali S, Aydeger A, Akkaya K, Rahman MA, Uluagac S. A review of moving target defense mechanisms for internet of things applications. Model Design Secure Internet Things. 2020;563–614.
36. Lysogor I, Voskov L, Rolich A, Efremov S. Study of data transfer in a heterogeneous LoRa-satellite network for the internet of remote things. Sensors. 2019;19(15):3384.
37. Sokolović VS, Marković GB. Internet of things in military applications. Vojnotehnički glasnik. 2023;71(4):1148–71.
38. Bandopadhaya S, Dey R, Suhag A. Integrated healthcare monitoring solutions for soldier using the internet of things with distributed computing. Sustain Comput Inf Syst. 2020;26: 100378.
39. Chaari MZ, Al-Rahimi R, Aghzout O. High power wireless power transfer for the future of the battlefield challenges. Secur Defence Quart. 2022;40(4):9–26. 10.35467/sdq/152548.
40. Li C, Fu Y, Liu Z, Liu X-Y, Wu W, Xiong L. spectrum trading for energy-harvesting-enabled internet of things in harsh environments. IEEE Access. 2018;6:16–726.
41. Varghese V, Desai SS, Nene MJ. Decision making in the battlefield-of-things. Wireless Pers Commun. 2019;106:423–38.
42. Paul S, Silaghi M, Këpuska V, Alghanmi A, Liu S. Mobile Fog AI for internet of battlefield things (IoBT). In: The International FLAIRS Conference Proceedings. 2024;37.
43. Malone D. Integration of the internet of things into the operations of the US Army. Master's thesis, Utica College, 2020.
44. Burmaoglu S, Saritas O, Yalcin H. Defense 4.0: Internet of Things in Military. Emerg Technol Econ Dev.2019;303–320.
45. Stocchero J.M, Silva CA, de Souza Silva L, Lawisch MA, dos Anjos JCS, de Freitas EP. Secure command and control for internet of battle things using novel network paradigms. IEEE Commun Magaz. 2022.
46. Herman ME. Military applications for the internet of things. Ph.D. dissertation, Utica College, 2019.
47. Kott A. Challenges and characteristics of intelligent autonomy for internet of battle things in highly adversarial environments. arXiv preprint arXiv:1803.11256, 2018.
48. Stanley-Lockman Z. Revisiting the revolution in military logistics: technological enablers twenty years on. In: Disruptive and Game Changing Technologies in Modern Warfare: Development, Use, and Proliferation, 2020;197–222.
49. Akbar RS, Kholid F, Kasiyanto K, Widiatmoko D, Achmad A. Design of fuel monitoring application for reservoir tanks in army fuel supply point on military logistics corps based on internet of things. Int J Eng Comput Sci Appl (IJECSA). 2024;3(1):19–32.

50. Suri N, Tortonesi M, Michaelis J, Budulas P, Benincasa G, Russell S, Stefanelli C, Winkler R. Analyzing the applicability of internet of things to the battlefield environment. In: 2016 International Conference on Military Communications and Information Systems (ICMCIS). IEEE, 2016;pp. 1–8.
51. Popescu F. From the IoT to the IoBT. The path to superior situational understanding. Land Forces Acad Rev. 2019;24(4):276–82.
52. Kang J-S, Lee J-J. Augmented reality and situation awareness applications for military computing. J Image Graphics. 2015;3(2):126–31.
53. Gurusubramani S, Sureshanand M, Jeganamarnath J, Sathishkumar D, Sheela A. Augmented reality in military applications. Int J Eng Adv Technol. 2019;9(1S):51–4.
54. Islam A, Masuduzzaman M, Akter A, Shin SY. MR-Block: a blockchain-assisted secure content sharing scheme for multi-user mixed-reality applications in internet of military things. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2020;407–411.
55. Llasag R, Marcillo D, Grilo C, Silva C. Human detection for search and rescue applications with UAVs and mixed reality interfaces. In: 2019 14th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2019;1–6.
56. Chaphadkar A, Ghodse S, Gone M, Khaserao Y, Kulkarni A. Real-time soldier health monitoring system using IoT. Available at SSRN 4716430, 2024.
57. Meerabi C, Navya G, Priyanka K, Priya CS. Soldier health and position tracking system. Iconic Res Eng J. 2020;3(10):116–20.
58. Sujitha V, Aishwarya B, Vigneswari P et al. IoT-based Healthcare Monitoring and Tracking System for Soldiers Using ESP32. In: 2022 6th International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2022;377–381.
59. Iyer B, Patil N. IoT enabled tracking and monitoring sensor for military applications. Int J Syst Assurance Eng Manage. 2018;9(6):1294–301.
60. Vongsingthong S, Smanchat S. A review of data management in internet of things. Asia-Pacific J Sci Technol. 2015;20(2):215–40.
61. Jalaian B, Russell S. Uncertainty quantification in internet of battlefield things. In: Artificial intelligence for the internet of everything. Amsterdam: Elsevier; 2019. p. 19–45.
62. Ehala J, Kaugerand J, Pahtma R, Astapov S, Riid A, Tomson T, Preden J-S, Motus L. Situation awareness via internet of things and in-network data processing. Int J Distrib Sens Netw. 2017;13(1):1550147716686578.
63. Russell S, Abdelzaher T, Suri N. Multi-domain effects and the internet of battlefield things. In: MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM). IEEE, 2019;724–730.
64. D. A. R. P. A. (DARPA) Edge-directed cyber technologies for reliable mission communication. Accessed October 2024, at https://www.darpa.mil/archive/our-research.
65. Systems B. BROADSWORD SPINE Soldier System. Accessed October 2024, at https://newatlas.com/bae-systems-broadsword-spine/44342/.
66. Tosh DK, Shetty S, Foytik P, Njilla L, Kamhoua CA. Blockchain-empowered secure internet-of-battlefield things (IoBT) architecture. In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). IEEE, 2018;593–598.
67. Sethi P, Sarangi S. R. Internet of things: architectures, protocols, and applications. J Electr Comput Eng. 2017.
68. Crawford A. Study report on iot reference architectures/frameworks. ISO, Report, 2014. https://silo.tips/download/study-report-on-iot-reference-architectures-frameworks.
69. Burhan M, Rehman RA, Khan B, Kim B-S. IoT elements, layered architectures and security issues: a comprehensive survey. Sensors. 2018;18(9):2796.
70. Jabraeil Jamali MA, Bahrami B, Heidari A, Allahverdizadeh P, Norouzi F, Jabraeil Jamali MA, Bahrami B, Heidari A, Allahverdizadeh P, Norouzi F. IoT architecture. Towards the Internet of Things: Architectures, Security, and Applications, 2020;9–31.
71. Benotmane M, Elhari K, Kabbaj A. Survey of IoT reference architectures and models and IoT initiatives. In: Proceedings of the Future Technologies Conference (FTC) 2021, vol. 1. Springer, 2022;294–320.
72. Wu M, Lu T-J, Ling F-Y, Sun J, Du H-Y. Research on the architecture of internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010;5: V5–484 IEEE.
73. Aslan FY, Aslan B. Comparison of IoT protocols with OSI and TCP/IP architecture. Int J Eng Res Dev. 2023;15(1):333–43.
74. Gazis V, Sasloglou K, Frangiadakis N, Kikiras P, Merentitis A, Mathioudakis K, Mazarakis G. Architectural blueprints of a unified sensing platform for the internet of things. In: 2013 22nd International Conference on Computer Communication and Networks (ICCCN). IEEE, 2013;1–5.
75. Ray PP. Towards an internet of things based architectural framework for defence. In: 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE, 2015;411–416.
76. Weber RH. Internet of things-need for a new legal environment? Comput Law Secur Rev. 2009;25(6):522–7.
77. Khan R, Khan SU, Zaheer R, Khan S. Future internet: the internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology. IEEE, 2012;257–260.
78. Adat V, Gupta BB. Security in internet of things: issues, challenges, taxonomy, and architecture. Telecommun Syst. 2018;67:423–41.
79. Herrero R. Ultrasonic physical layers as building blocks of IoT stacks. Internet Things. 2022;18: 100489.
80. Gupta BB, Quamara M. An overview of internet of things (IoT): architectural aspects, challenges, and protocols. Concurr Comput Pract Exp. 2020;32(21): e4946.
81. Pan J, McElhannon J. Future edge cloud and edge computing for internet of things applications. IEEE Internet Things J. 2017;5(1):439–49.
82. Fremantle P. et al. A reference architecture for the internet of things. WSO2 White paper, 2015;02–04.
83. da Cruz MA, Rodrigues JJP, Al-Muhtadi J, Korotaev VV, de Albuquerque VHC. A reference model for internet of things middleware. IEEE Internet Things J. 2018;5(2):871–83.
84. Rondon LP, Babun L, Aris A, Akkaya K, Uluagac AS. Survey on enterprise internet-of-things systems (E-IoT): a security perspective. Ad Hoc Netw. 2022;125: 102728.
85. Bandyopadhyay S, Sengupta M, Maiti S, Dutta S. Role of middleware for internet of things: a study. Int J Comput Sci Eng Surv. 2011;2(3):94–105.
86. Wu M, Lu T-J, Ling F-Y, Sun J, Du H-Y. Research on the architecture of internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010;5: V5–484. IEEE.

87. Bouaouad A.-E, Cherradi A, Assoul S, Souissi N. The key layers of iot architecture. In: 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech). IEEE, 2020;1–4.
88. Shah IA, Mehmood A, Khan AN, Elhadef M, Khan AuR. Heucrip: a malware detection approach for internet of battlefield things. Clust Comput. 2023;26(2):977–92.
89. Kim D, Solomon MG. Fundamentals of information systems security. Jones & Bartlett Publishers, 2010.
90. Jalaian B, Suri N, et al. Investigating LoRa for the internet of battlefield things: a cyber perspective. In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). IEEE, 2018; 749–756.
91. Sarjito A, Lelyana N. Enhancing battlefield awareness: integration of IoMT sensors and networks in national defense systems. Jurnal Ilmu Sosial dan Humaniora. 2024;3(1):41–60.
92. Rana B, Singh Y. Internet of things and UAV: an interoperability perspective. In: Unmanned aerial vehicles for internet of things (IoT) concepts, techniques, and applications, 2021;105–127.
93. Ahmad A, Cuomo S, Wu W, Jeon G. Intelligent algorithms and standards for interoperability in internet of things. 2019;1187–1191.
94. Pradhan M, Manso M, Michaelis JR. Concepts and directions for future IoT and C2 interoperability. In: MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM). IEEE, 2021;231–236.
95. Poltronieri F, Sadler L, Benincasa G, Gregory T, Harrell JM, Metu S, Moulton C. Enabling efficient and interoperable control of IoBT devices in a multi-force environment. In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). IEEE, 2018;757–762.
96. Ang KL-M, Seng JKP. Application specific internet of things (ASIoTs): taxonomy, applications, use case and future directions. IEEE Access. 2019;7:56–590.
97. Marlin BM, Suri N, Fang S, Srivastiva MB, Samplawski C, Wang Z, Wigness M. IoBT-MAX: a multimodal analytics experimentation testbed for IoBT research. In: MILCOM 2023-2023 IEEE Military Communications Conference (MILCOM). IEEE, 2023;127–132.
98. Wang H, Wang T, Shi L, Liu N, Zhang S. A blockchain-empowered framework for decentralized trust management in internet of battlefield things. Comput Netw. 2023;237: 110048.
99. Saraswat D, Bhattacharya P, Singh A, Verma A, Tanwar S, Kumar N. Secure 5G-assisted UAV Access scheme in IoBT for region demarcation and surveillance operations. IEEE Commun Standards Magaz. 2022;6(1):58–66.
100. Farooq MJ, Zhu Q. Secure and reconfigurable network design for critical information dissemination in the internet of battlefield things (IoBT). In: 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt). IEEE. 2017;2017:1–8.
101. Mariani J, Williams B, Loubert B. Continuing the march: the past, present, and future of the IoT in the Military. The Internet of Things in Defense. Technical Report: Tech. Rep; 2015.
102. Yu C, Shen S, Yang H, Zhang K, Zhao H. Leveraging energy, latency, and robustness for routing path selection in internet of battlefield things. IEEE Internet Things J. 2021;9(14):12–613.
103. Samaras C, Nuttall WJ, Bazilian M. Energy and the military: convergence of security, economic, and environmental decision-making. Energ Strat Rev. 2019;26: 100409.
104. Liang Q, Durrani TS, Gu X, Koh J, Li Y, Wang X. Guest editorial special issue on spectrum and energy efficient communications for internet of things. IEEE Internet Things J. 2019;6(4):5948–53.
105. Hasan BT, Badran AI. A study on energy management for low-power IoT devices. In: Sharma K, Sharma R, Jeon G, Polkowski Z, editors. Singapore: Springer Nature Singapore, 2023.
106. Lin H, Chen Z, Wang L. Offloading for edge computing in low power wide area networks with energy harvesting. IEEE Access. 2019;7:78–929.
107. Kunatsa T, Myburgh HC, De Freitas A. Optimal power flow management for a solar PV-powered soldier-level pico-grid. Energies. 2024;17(2):459.
108. Xie Z, Poovendran P, Premalatha R. Retention-based energy harvesting technique for efficient internet of things aided edge devices. Sustain Energy Technol Assess. 2021;47: 101424.
109. Said O, Tolba A. A reliable and scalable internet of military things architecture. Comput Mater Continua. 2021;67(3).
110. Yazdinejad A, Parizi RM, Dehghantanha A, Zhang Q, Choo K-KR. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Trans Serv Comput. 2020;13(4):625–38.
111. Azar J, Makhoul A, Barhamgi M, Couturier R. An energy efficient IoT data compression approach for edge machine learning. Futur Gener Comput Syst. 2019;96:168–75.
112. Abdulzahra SA, Al-Qurabat AKM, Idrees AK. Compression-based data reduction technique for IoT sensor networks. Baghdad Sci J. 2021;18(1):0184–0184.
113. Rath M, Pattanayak BK, Pati B. Energy efficient MANET protocol using cross-layer design for military applications. Def Sci J. 2016;66(2):146–50.
114. Bichi BY, Islam SU, Kademi AM, Ahmad I. An energy-aware application module for the fog-based internet of military things. Discov Internet Things. 2022;2(1):4.
115. Liu D, Abdelzaher T, Wang T, Hu Y, Li J, Liu S, Caesar M, Kalasapura D, Bhattacharyya J, Srour N. et al. IoBT-OS: optimizing the sensing-to-decision loop for the internet of battlefield things. In: 2022 International Conference on Computer Communications and Networks (ICCCN). IEEE, 2022;1–10.
116. Wrona K. Securing the internet of things a military perspective. In: IEEE 2nd World Forum on Internet of Things (WF-IoT). IEEE. 2015;2015:502–7.
117. Jung S-H, An J-C, Park J-Y, Shin Y-T, Kim J-B. An empirical study of the military IoT security priorities. Int J Secur Appl. 2016;10(8):13–22.
118. Tóth A. Internet of things vulnerabilities in military environments. Vojenské rozhledy. 2021;30(3):45–58.
119. Farooq MJ, Zhu Q. On the secure and reconfigurable multi-layer network design for critical information dissemination in the internet of battlefield things (IoBT). IEEE Trans Wireless Commun. 2018;17(4):2618–32.
120. Doustimotlagh S. A new mechanism for enhancing the security of military internet of things by using quantum and classic cryptography. Electron Cyber Defense. 2021;9(2):29–49.
121. Alkanjr B, Mahgoub I. A novel deception-based scheme to secure the location information for IoBT entities. IEEE Access. 2023;11:15–554.

122. Feng Y, Li M, Zeng C, Liu H. Robustness of internet of battlefield things (IoBT): a directed network perspective. Entropy. 2020;22(10):1166.
123. Singh RK, Mishra S. TinyML meets IoBT against sensor hacking. In: The Network and Distributed System Security (NDSS) Symposium, Workshop on Security and Privacy in Standardized IoT (SDIoTSec), 2024:1–9.
124. Masuduzzaman M, Rahim T, Islam A, Shin SY. UAV-employed intelligent approach to identify injured soldier on blockchain-integrated internet of battlefield things. IEEE Trans Netw Serv Manage. 2024.
125. Butun I, Mahgoub I. Expandable mix-zones as a deception technique for providing location privacy on internet-of-battlefield things (IoBT) deployments. IEEE Access. 2024.
126. Rutravigneshwaran P, Anitha G, Prathapchandran K. Trust-based support vector regressive (TSVR) security mechanism to identify malicious nodes in the internet of battlefield things (IoBT). Int J Syst Assur Eng Manage. 2024;15(1):287–99.
127. Alam S, Siddiqui ST, Ahmad A, Ahmad R, Shuaib M. Internet of things (IoT) enabling technologies, requirements, and security challenges. In: Advances in Data and Information Sciences: Proceedings of ICDIS 2019. Springer, 2020;119–126.
128. Malik MI, McAteer IN, Hannay P, Ibrahim A, Baig Z, Zheng G. Cyber security for network of things (NoTs) in military systems: challenges and countermeasures. In: Security Analytics for the Internet of Everything. CRC Press, 2020;231–249.
129. Lin D, Wu W. Rf fingerprint-identification-based reliable resource allocation in an internet of battle things. IEEE Internet Things J. 2022;9(21):21–120.
130. Hassan SS, Park YM, Hong CS. On-demand MEC empowered UAV deployment for 6G time-sensitive maritime internet of things. In: 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE. 2021;2021:386–9.
131. Park J, Mohaisen A, Kamhoua CA, Weisman M.J, Leslie NO, Njilla L. Cyber deception in the internet of battlefield things: techniques, instances, and assessments. In: Information Security Applications: 20th International Conference, WISA. Jeju Island, South Korea, August 21–24, 2019, Revised Selected Papers 20. Springer. 2019;2020:299–312.
132. Sánchez PMS, Celdrán AH, Bovet G, Pérez GM, Stiller B. Specforce: a framework to secure IoT spectrum sensors in the internet of battlefield things. IEEE Commun Magaz. 2022.
133. Ghimire B, Rawat DB, Liu C, Li J. Sharding-enabled blockchain for software-defined internet of unmanned vehicles in the battlefield. IEEE Netw. 2021;35(1):101–7.
134. Doku R, Rawat DB, Garuba M, Njilla L. Fusion of named data networking and blockchain for resilient internet-of-battlefield-things. In: IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). IEEE. 2020;2020:1–6.
135. Safavat S, Rawat DB. Securing unmanned aerial vehicular networks using modified elliptic curve cryptography. In: MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM). IEEE, 2021; 999–1004.
136. Karim H, Rawat DB. Evaluating machine learning classifiers for data sharing in internet of battlefield things. In: IEEE Symposium Series on Computational Intelligence (SSCI). IEEE. 2021;2021:01–7.
137. Islam A, Masuduzzaman M, Akter A, Shin SY. MR-Block: a blockchain-assisted secure content sharing scheme for multi-user mixed-reality applications in internet of military things. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2020; 407–411.