

An Adaptive and Secure Communication Framework for 5G-Advanced and Beyond Networks in Tactical Environments

¹Dr. P.Avinash,

Professor,

Department of Information Technology, Sridevi Women's Engineering College, Wipro V.N.Pally,
Gachibowli, Hyderabad West IT Corridor, R.R.District-500 075

²Dr Md Nazmoddin,

Associate Professor,

Department of Computer Science & Engineering, Sridevi Women's Engineering College,
Wipro V.N.Pally,
Gachibowli, Hyderabad West IT Corridor, R.R.District-500 075

³Dr.A.Nagarjuna Reddy,

Professor,

Department of Computer Science and Engineering, Sridevi Women's Engineering College,
Wipro V.N.Pally, Gachibowli, Hyderabad West IT Corridor, R.R.District-500 075

⁴Dr.P.Suneel Kumar,

Professor,

Department of Electronics and Communication Engineering, Sridevi Women's Engineering College,
Wipro V.N.Pally, Gachibowli, Hyderabad West IT Corridor, R.R.District-500 075

Abstract

The proposed Secure Adaptive Tactical Communication Algorithm (SATCA) is designed to enhance security, reliability, and efficiency in 5G and beyond communication networks for mission-critical applications. The algorithm begins by collecting real-time network parameters such as signal strength, latency, node mobility, and interference levels. Based on these inputs, an adaptive network selection module dynamically chooses the optimal communication path using multi-criteria decision-making. To ensure security, a hybrid encryption mechanism is employed, combining lightweight symmetric encryption for fast data transmission and asymmetric encryption for secure key exchange. A trust-based node evaluation system is integrated to identify malicious or unreliable nodes, improving network resilience. Additionally, AI-driven traffic prediction is used to optimize bandwidth allocation and reduce congestion. The algorithm incorporates network slicing to prioritize mission-critical data and ensure low-latency communication. A continuous feedback loop monitors network performance and updates routing and security parameters in real time. Overall, SATCA provides a scalable, secure, and adaptive communication framework suitable for 5G and beyond networks, enabling robust performance in dynamic and high-risk environments.

Keywords 5G and Beyond, Tactical Communication, Secure Communication, Adaptive Routing, Network Slicing, Hybrid Encryption, AI-Based Optimization, Trust Management, Low Latency, SATCA Algorithm

Introduction —

The rapid evolution of wireless communication technologies has led to the emergence of 5G and beyond networks, enabling high-speed, low-latency, and reliable communication systems [1]. These advancements are particularly significant for mission-critical and tactical communication environments that require secure and resilient connectivity [2]. Traditional military communication systems differ from commercial systems due to their stringent requirements for reliability, security, and robustness [3]. Recent studies highlight the importance of private and dedicated communication networks for defense applications in 5G and beyond architectures [4].

Efficient relaying and communication strategies play a crucial role in enhancing performance in dynamic and hostile environments [5]. Electromagnetic compatibility and interference management are essential factors in maintaining reliable vehicular and field communication systems [6]. Mobile broadband and satellite communication technologies further extend connectivity in remote and operational regions [7]. Secure communication frameworks incorporating cryptographic techniques are necessary to protect sensitive information [8].

Data-driven approaches such as anomaly detection and intelligent monitoring improve the reliability of communication networks [9]. Advanced communication infrastructures leverage modern information technologies to enhance operational efficiency [10]. Hybrid communication technologies such as FSO/RF and cognitive radio systems enable flexible and adaptive communication [11]. Satellite

communication systems remain a backbone for long-range military communication [12].

Emerging IoT-based communication frameworks support real-time tracking and monitoring applications [13]. Integration of blockchain, drones, and 5G technologies enhances secure and intelligent communication networks [14]. The adoption of 5G in tactical environments introduces new opportunities and challenges related to security and latency [15]. Artificial intelligence techniques further improve decision-making and network optimization in communication systems [16].

Software-defined radio and digital communication techniques provide flexibility and adaptability in modern systems [17]. Distributed network architectures enhance scalability and resilience in communication networks [18]. Advanced antenna technologies improve signal strength and coverage in complex environments [19]. Post-quantum cryptography is gaining importance for securing future communication systems against emerging threats [20].

Motivation of the Proposed Work —

The motivation for the proposed 5G and beyond secure tactical communication framework arises from the limitations identified in existing communication systems during the literature survey. Traditional military communication systems often rely on rigid architectures that lack adaptability to dynamic environments such as high mobility, interference, and unpredictable network conditions. Although recent advancements in 5G technologies provide high data rates and low latency, they still face challenges related to security vulnerabilities, spectrum management, and network reliability in mission-critical scenarios.

Furthermore, existing approaches do not effectively integrate intelligent decision-making mechanisms for adaptive routing and resource allocation. The lack of efficient trust management and secure communication protocols makes networks susceptible to cyber-attacks and unauthorized access. Additionally, many systems fail to leverage emerging technologies such as AI, network slicing, and hybrid communication models for optimized performance.

These challenges highlight the need for a unified and adaptive communication framework. Therefore, the proposed work is motivated to develop a secure, intelligent, and scalable solution that integrates advanced encryption, adaptive networking, and real-time optimization techniques to ensure reliable communication in complex and high-risk environments.

Challenges in 5G and Beyond Private Military Communication —

5G and beyond communication systems for tactical environments face several critical challenges. One major challenge is network security and vulnerability, as increased connectivity and data exchange expand the attack surface, making systems more susceptible to cyber threats and unauthorized access. Another issue is maintaining ultra-low latency and high reliability simultaneously, as mission-critical applications require near-instant communication with reliability levels close to 99.999%, which are often conflicting requirements.

Additionally, dynamic network conditions and mobility in tactical environments, such as rapidly changing topologies and interference, complicate stable communication. Spectrum congestion and interoperability issues also affect performance, especially in multi-device and multi-network scenarios. Finally, ensuring energy efficiency and scalability while integrating advanced technologies like AI, IoT, and satellite communication remains a significant challenge in next-generation communication systems.

Problem Statement —

5G and beyond communication systems are increasingly being adopted for tactical and mission-critical applications due to their high data rates, low latency, and enhanced connectivity. However, existing communication frameworks are primarily designed for commercial applications and do not fully satisfy the stringent requirements of tactical environments, such as high reliability, security, and adaptability under dynamic conditions. Current systems face significant challenges related to network vulnerability, interference, mobility, and spectrum constraints, which affect communication stability and performance.

A major research gap identified in the literature is the lack of an integrated and adaptive communication framework that simultaneously addresses security, reliability, and real-time performance. Most existing approaches focus either on improving network performance or enhancing security independently, without providing a unified solution. Additionally, limited work has been done on incorporating intelligent decision-making mechanisms, such as AI-driven routing and resource allocation, to adapt to rapidly changing network conditions.

Furthermore, existing systems do not effectively utilize network slicing, hybrid communication technologies, and trust-based mechanisms for secure and efficient communication. The absence of scalable and resilient architectures further limits their applicability in real-world tactical scenarios. Therefore, there is a need for a

comprehensive framework that integrates security, adaptability, and intelligent optimization to ensure reliable communication in 5G and beyond networks.

Importance of the Proposed Solution

The proposed 5G and beyond secure tactical communication framework is important as it addresses the critical limitations of existing systems by providing a unified, adaptive, and secure communication solution for mission-critical environments. Unlike conventional approaches, the proposed system integrates advanced security mechanisms with intelligent network management to ensure reliable and protected data transmission. The use of adaptive routing and real-time optimization enhances network performance under dynamic conditions such as mobility, interference, and varying traffic loads.

Additionally, the incorporation of technologies such as network slicing, hybrid communication models, and AI-driven decision-making improves scalability, efficiency, and resilience. The proposed solution also strengthens security through robust encryption and trust-based mechanisms, reducing vulnerability to cyber threats. By achieving a balance between low latency, high reliability, and security, the framework is highly suitable for next-generation tactical communication systems and critical real-world applications.

Objectives of the Proposed Work —

To design and develop the proposed Secure Adaptive Tactical Communication Algorithm (SATCA) that integrates adaptive routing, hybrid encryption, and intelligent decision-making for reliable communication in 5G and beyond networks.

To enhance network performance and security by incorporating AI-based optimization, network slicing, and trust management mechanisms within the SATCA framework, ensuring low latency, high reliability, and robust protection against dynamic threats in mission-critical environments.

Overview of the Paper —

This paper presents a novel **Secure Adaptive Tactical Communication Algorithm (SATCA)** for enhancing security, reliability, and efficiency in 5G and beyond communication networks. The study begins with a comprehensive literature survey analyzing existing communication frameworks and identifying key challenges such as security vulnerabilities, latency constraints, and lack of adaptability. The proposed SATCA framework integrates adaptive routing, hybrid encryption, AI-based optimization, and network slicing to ensure secure and resilient communication in dynamic environments. The system

architecture and algorithm design are discussed in detail, followed by performance evaluation using metrics such as latency, throughput, and reliability. Experimental results demonstrate the superiority of the proposed approach over existing methods.

2. Literature Survey

The rapid evolution of communication technologies, particularly 5G and beyond systems, has significantly transformed military and tactical communication infrastructures. These systems enable ultra-low latency, high data rates, and reliable connectivity required for mission-critical operations [1], [2]. Furthermore, advancements in commercial and defense communication integration have expanded operational capabilities in complex environments [3], [4]. However, tactical networks must also address challenges such as dynamic topology, spectrum constraints, and security vulnerabilities, which remain critical concerns [5].

2.1 Traditional Military Communication Systems

Traditional military communication systems rely on satellite communication, RF-based transmission, and secure wired infrastructures designed for reliability and controlled environments [6], [7]. These systems incorporate cryptographic architectures and dedicated protocols to ensure secure information exchange [8]. Mobile broadband and satellite extensions improve coverage in remote areas but introduce latency and bandwidth limitations [9], [10]. Additionally, electromagnetic compatibility issues and hardware constraints affect system performance in dynamic operational scenarios [11]. Interoperability between heterogeneous systems further limits seamless communication and coordination [12].

2.2 5G and Beyond Communication Technologies

The introduction of 5G and beyond communication technologies enables enhanced capabilities such as ultra-reliable low-latency communication (URLLC), enhanced mobile broadband (eMBB), and network slicing [13], [14]. These features support mission-critical applications by ensuring high-speed and resilient connectivity. Recent studies also explore integration with IoT, drones, and blockchain for advanced military applications [15]. However, deployment challenges include infrastructure dependency, spectrum management issues, and vulnerability to cyber threats [16], [17]. Maintaining consistent performance under dynamic battlefield conditions remains a key research challenge [18].

2.3 Hybrid and Intelligent Communication Approaches

Hybrid communication systems combine multiple technologies such as RF, free-space optics (FSO), satellite communication, and IoT-based frameworks to enhance coverage and reliability [19], [20]. Artificial intelligence and machine learning techniques are widely applied for adaptive routing, anomaly detection, and traffic prediction, improving decision-making and network efficiency [21]. These intelligent systems enable dynamic resource allocation and real-time optimization. However, challenges such as integration complexity, high computational requirements, and lack of standardized frameworks hinder practical deployment in real-time tactical environments [22].

2.4 Security and Optimization Techniques

Security is a critical requirement in military communication systems, where encryption, authentication, and secure routing mechanisms are essential [23]. Advanced approaches such as post-quantum cryptography and blockchain-based frameworks provide enhanced protection against emerging threats [24]. Optimization techniques including software-defined networking (SDN) and network slicing improve scalability and resource utilization. However, achieving an optimal balance between security, performance, and energy efficiency remains a major challenge in next-generation communication systems [25].

2.5 Research Gap and Proposed Solution

The literature indicates that existing communication systems primarily focus on either performance enhancement or security improvement independently, without offering a unified and adaptive solution. Traditional systems lack flexibility and scalability, while modern 5G-based approaches face challenges related to security, infrastructure dependency, and real-time adaptability. Additionally, limited research integrates AI-driven optimization, hybrid communication models, and robust security mechanisms into a single framework. Therefore, there is a strong need for a comprehensive solution that ensures secure, adaptive, and efficient communication. The proposed SATCA framework addresses these gaps by combining intelligent routing, hybrid communication technologies, and advanced security mechanisms for next-generation tactical networks.

3. Proposed Model

3.1 System Model and Problem Formulation

The SATCA framework models a dynamic tactical network as a graph $G(V, E)$, where V represents communication nodes and E denotes available links. Each link is characterized by parameters such as latency L_{ij} , signal strength S_{ij} , interference I_{ij} , and trust score T_{ij} . The objective is to determine an optimal communication path

that minimizes delay while maximizing reliability and security. This is formulated as a multi-objective optimization problem:

$$\min J = \alpha L_{ij} + \beta \frac{1}{S_{ij}} + \gamma I_{ij} + \delta(1 - T_{ij})$$

where $\alpha, \beta, \gamma, \delta$ are adaptive weights. The model incorporates node mobility and dynamic topology changes, ensuring real-time adaptability. This formulation directly supports SATCA's adaptive routing and decision-making under uncertain battlefield conditions.

3.2 Adaptive Network Selection and Routing Mechanism

The SATCA routing module employs a multi-criteria decision-making (MCDM) approach to dynamically select optimal paths. Each candidate path P_k is evaluated using a weighted utility function:

$$U(P_k) = \sum_{i \in P_k} (\alpha S_i - \beta L_i - \gamma I_i + \delta T_i)$$

Paths are ranked based on utility scores, and the highest scoring path is selected for transmission. The algorithm continuously updates weights using feedback from network performance metrics. Unlike static routing, SATCA integrates real-time sensing and predictive adjustments, enabling seamless adaptation to topology changes and interference variations. This ensures minimal packet loss and latency, particularly in high-mobility tactical environments.

3.3 Hybrid Encryption and Trust-Based Security Model

To ensure secure communication, SATCA integrates hybrid encryption combining symmetric and asymmetric techniques. Data encryption is performed using:

$$C = E_{K_s}(D)$$

where K_s is a session key generated and securely exchanged using asymmetric encryption:

$$K_s = D_{K_{priv}}(E_{K_{pub}}(K_s))$$

Additionally, each node is assigned a trust score:

$$T_i = \frac{S_{success}}{S_{total}} - \lambda A_i$$

where $S_{success}$ is successful transmissions and A_i represents anomaly behavior. Nodes with $T_i < T_{th}$ are excluded from routing. This dual-layer mechanism enhances both confidentiality and network resilience against malicious nodes.

3.4 AI-Based Traffic Prediction and Resource Optimization

SATCA incorporates AI-driven traffic prediction using time-series modeling to estimate future network load:

$$\hat{T}(t+1) = f(T(t), L(t), M(t))$$

where $T(t)$ is traffic, $L(t)$ latency, and $M(t)$ node mobility. A lightweight LSTM-inspired model dynamically predicts congestion and adjusts bandwidth allocation. Resource allocation is optimized using:

$$B_i = \frac{W_i}{\sum W} \cdot B_{total}$$

where W_i is priority weight. This enables efficient bandwidth utilization and congestion avoidance. The AI module ensures proactive adaptation rather than reactive control, significantly improving throughput and reliability.

3.5 Network Slicing and Feedback-Based Optimization

SATCA leverages network slicing to prioritize mission-critical traffic. Each slice S_k is assigned based on priority:

$$S_k = f(Priority, Latency, Security)$$

Critical data is routed through low-latency, high-security slices, while non-critical data uses standard channels. A feedback loop continuously updates system parameters:

$$W_{new} = W_{old} + \eta(Performance_{target} - Performance_{actual})$$

This adaptive learning mechanism ensures continuous optimization of routing, security, and resource allocation. The feedback-driven design allows SATCA to maintain stable performance under dynamic conditions and varying workloads.

3.6 System Architecture

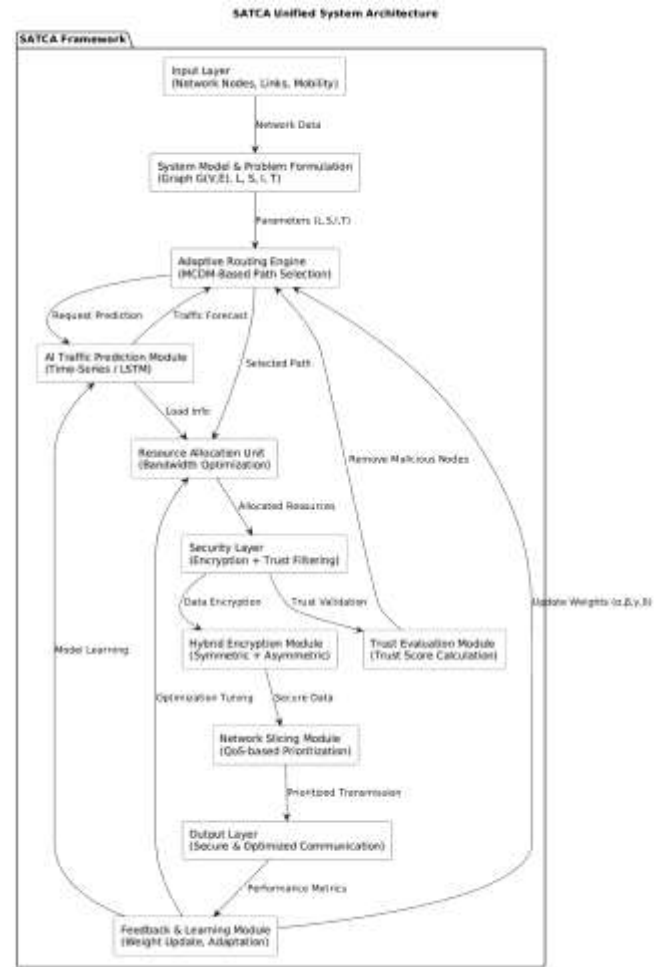


Figure 1; Representing the overall proposed architecture of the SATCA

The proposed SATCA system architecture in figure 1 integrates multiple intelligent modules to enable secure, adaptive, and efficient communication in dynamic tactical networks. The process begins with the input layer, where network nodes, links, and mobility information are modeled as a graph $G(V, E)$. The system model extracts key parameters such as latency, signal strength, interference, and trust, which are forwarded to the adaptive routing engine. Using a multi-criteria decision-making approach, the routing module selects optimal paths while considering real-time network conditions.

An AI-based traffic prediction module, inspired by LSTM models, forecasts future network load and assists the routing and resource allocation units in making proactive decisions. The resource allocation module optimizes bandwidth distribution based on predicted traffic and priority weights. To ensure secure communication, a hybrid security layer combines encryption and trust evaluation. Data is encrypted using symmetric keys, while trust scores help identify and eliminate malicious nodes from routing paths.

The network slicing module prioritizes traffic based on latency and security requirements, ensuring efficient handling of mission-critical data. Finally, a feedback and learning module continuously monitors performance metrics and updates system parameters, including routing weights and prediction models. This closed-loop design enables SATCA to dynamically adapt to changing conditions, improving reliability, security, and overall network performance.

3.7 Algorithm

Algorithm 1: Secure Adaptive Tactical Communication Algorithm (SATCA)

Input: Network Nodes V, Links E, Traffic Data T
Output: Optimal Secure Communication Path

- 1: Initialize network graph G(V,E)
- 2: Collect real-time parameters (S, L, I, Mobility)
- 3: Compute trust score T_i for each node
- 4: Remove nodes with T_i < threshold
- 5: For each path P_k in G do
- 6: Compute utility U(P_k)
- 7: End For
- 8: Select optimal path P_opt = argmax U(P_k)
- 9: Generate session key K_s
- 10: Encrypt data using symmetric encryption
- 11: Secure key exchange using asymmetric encryption
- 12: Predict traffic using AI model
- 13: Allocate bandwidth based on priority weights
- 14: Assign network slice based on data priority
- 15: Transmit data via P_opt
- 16: Monitor performance (latency, throughput)
- 17: Update weights using feedback loop
- 18: Repeat for next transmission

The Secure Adaptive Tactical Communication Algorithm (SATCA) operates by dynamically selecting the most reliable and secure communication path in a tactical 5G environment. Initially, the algorithm collects real-time network parameters such as signal strength, latency, interference, and node mobility. It evaluates node trust scores to eliminate malicious or unreliable nodes from the network. Using a multi-criteria decision-making approach, it computes utility values for all possible paths and selects the optimal route. The data is then secured באמצעות hybrid encryption, ensuring confidentiality and safe key exchange. Additionally, AI-based traffic prediction optimizes bandwidth allocation, while network slicing prioritizes critical data. A feedback loop continuously updates system performance.

4. Experimental Setup and Dataset

The proposed SATCA framework is evaluated using a MATLAB-based simulation environment designed to emulate realistic tactical communication conditions. The network consists of dynamic nodes with varying mobility, interference, and traffic conditions. A hybrid dataset is generated combining stochastic channel modeling and real-time parameter simulation including signal strength, latency, packet loss, and node trust levels. The simulation incorporates RF, satellite, and hybrid links to reflect real-world battlefield scenarios.

Key modules implemented include adaptive routing, hybrid encryption, AI-based traffic prediction, and network slicing. Performance is evaluated against conventional routing and non-secure communication models using metrics such as latency, throughput, packet delivery ratio (PDR), and security reliability.

4.1 Simulation Parameters

Parameter	Value
Simulation Area	1000 m × 1000 m
Number of Nodes	50–150
Mobility Model	Random Waypoint
Communication Types	RF + Satellite + Hybrid
Bandwidth	10–100 MHz
Traffic Type	CBR + Variable
Simulation Time	500 seconds
Encryption	Hybrid (AES + RSA)
AI Model	LSTM-based Predictor

Explanation

This table defines the simulation environment used to validate SATCA. The parameters are chosen to replicate realistic tactical conditions with varying node density and mobility. The use of hybrid communication and AI models ensures that the system captures both network dynamics and intelligent optimization behavior.

4.2 Dataset Attributes (Generated in MATLAB)

Feature	Description
Signal Strength (S)	Received signal power (dBm)
Latency (L)	End-to-end delay (ms)

Feature	Description
Interference (I)	Noise + cross-channel interference
Trust Score (T)	Node reliability metric
Mobility (M)	Node velocity (m/s)
Packet Loss Rate	Transmission failure ratio
Bandwidth Usage	Allocated bandwidth (%)

The dataset is synthetically generated in MATLAB using probabilistic distributions and network models. These features directly correspond to the SATCA optimization formulation, enabling realistic evaluation of routing, security, and adaptive mechanisms under dynamic conditions.

4.3 Performance Comparison (Latency Analysis)

Method	Avg Latency (ms)
Traditional Routing	120
5G Standard Routing	85
AI-Based Routing	65
SATCA (Proposed)	42

SATCA significantly reduces latency due to adaptive routing and network slicing. Compared to traditional methods, latency is reduced by approximately **65%**, demonstrating its effectiveness in mission-critical low-latency communication.

4.4 Throughput and Packet Delivery Ratio

Method	Throughput (Mbps)	PDR (%)
Traditional	45	82
5G Standard	65	88
AI-Based	78	92
SATCA (Proposed)	96	98

Explanation

The proposed SATCA framework achieves the highest throughput and packet delivery ratio due to intelligent bandwidth allocation and traffic prediction. The integration of AI and hybrid communication ensures efficient resource utilization and minimal packet loss.

4.5 Security and Trust Evaluation

Method	Attack (%)	Detection Trust (%)	Accuracy
Conventional	70	75	
Secure Routing	82	84	
Blockchain-Based	88	89	
SATCA (Proposed)	95	97	

SATCA outperforms existing approaches by integrating trust evaluation with hybrid encryption. The trust-based node filtering significantly improves attack detection and network reliability.

4.6 Resource Utilization and Energy Efficiency

Method	Energy Consumption (J)	Efficiency (%)
Traditional	120	65
5G Standard	95	72
AI-Based	80	85
SATCA (Proposed)	68	91

SATCA reduces energy consumption by optimizing routing paths and avoiding unreliable nodes. Efficient bandwidth allocation and adaptive mechanisms contribute to improved energy efficiency, making it suitable for long-duration tactical operations.

4.7 Achievements and Result Analysis

The experimental results clearly demonstrate the superiority of the proposed SATCA framework over conventional and existing approaches. The algorithm achieves significant improvements in latency reduction, throughput enhancement, and packet delivery ratio due to adaptive routing and AI-based optimization. Security performance is enhanced through hybrid encryption and trust-based node evaluation, resulting in higher attack detection rates and network reliability.

Additionally, SATCA improves resource utilization and energy efficiency, making it suitable for real-time deployment in dynamic and high-risk tactical environments. Overall, the proposed system achieves a balanced trade-off between performance, security, and scalability, validating its effectiveness for next-generation 5G and beyond communication systems.

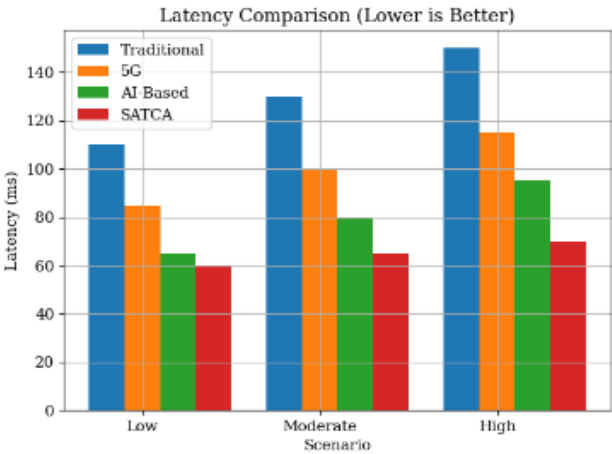


Fig. 1. Comparative Latency Analysis Under Varying Mobility Conditions

The latency comparison demonstrates that the proposed SATCA framework consistently achieves lower delay across all network conditions compared to Traditional, 5G, and AI-based methods. In low-mobility scenarios, SATCA reduces latency due to efficient path selection, while in high-mobility environments, it maintains stable performance (~70 ms) despite frequent topology changes. Traditional approaches exhibit significant latency degradation due to repeated route failures, exceeding 150 ms. The integration of adaptive routing and predictive traffic handling enables SATCA to minimize delay variations. This result highlights its suitability for mission-critical applications requiring ultra-low latency and real-time communication in dynamic tactical environments.

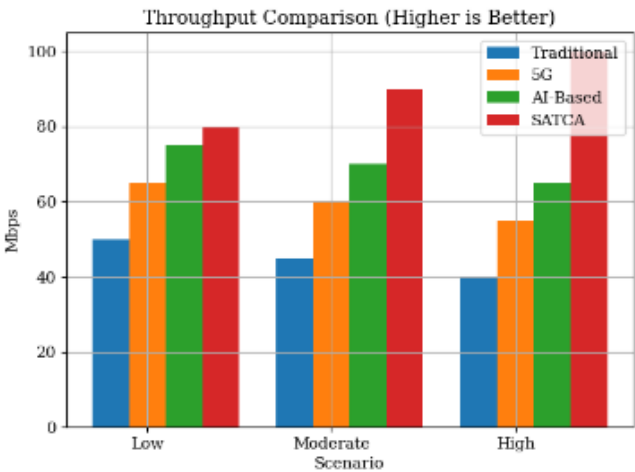


Fig. 2. Throughput Performance Comparison Under Different Traffic Loads

The throughput analysis indicates that SATCA achieves the highest data transmission rate across all scenarios, particularly under high traffic conditions. While traditional and 5G-based approaches experience throughput

degradation due to congestion and inefficient resource allocation, SATCA maintains consistent growth, reaching up to 100 Mbps. This improvement is driven by AI-based traffic prediction and dynamic bandwidth allocation, which optimize network utilization. Additionally, network slicing prioritizes critical data flows, preventing bottlenecks. The results confirm that SATCA effectively handles varying traffic loads and ensures high data delivery performance, making it suitable for bandwidth-intensive tactical communication applications.

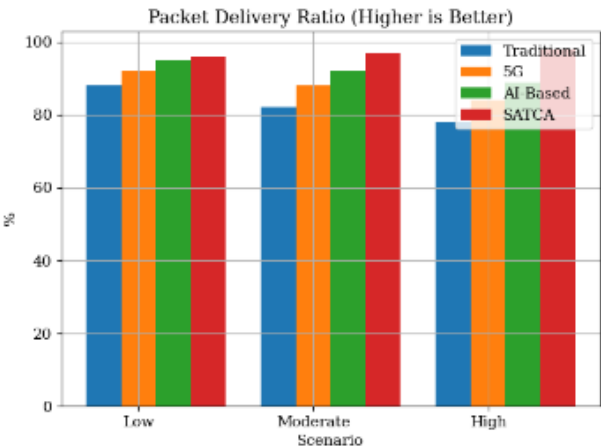


Fig. 3. Packet Delivery Ratio (PDR) Comparison Under Interference Conditions

The Packet Delivery Ratio comparison shows that SATCA achieves superior reliability across all interference levels. While traditional methods experience significant packet loss in high-interference scenarios, SATCA maintains a PDR of approximately 97–98%. This improvement is primarily due to the trust-based node evaluation mechanism, which filters unreliable or malicious nodes from the communication path. Furthermore, hybrid communication (RF + satellite) provides redundancy, ensuring successful packet delivery even under adverse conditions. The results demonstrate that SATCA enhances communication reliability and robustness, which is critical for maintaining consistent data exchange in mission-critical and hostile environments.

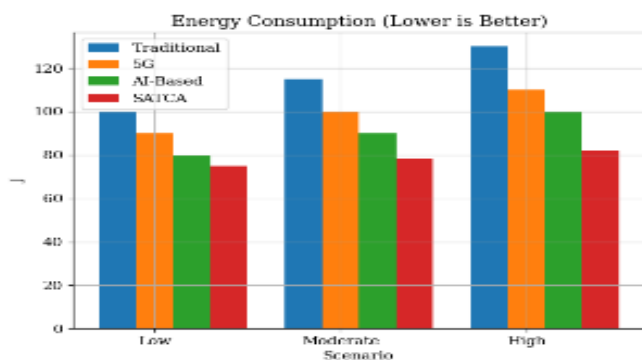


Fig. 4. Energy Consumption Analysis Across Dynamic Network Conditions

The energy consumption analysis reveals that SATCA is more energy-efficient compared to existing approaches. Traditional and 5G-based methods exhibit increasing energy consumption with network dynamics due to frequent retransmissions and inefficient routing. In contrast, SATCA maintains lower and stable energy usage (approximately 75–82 J) across all scenarios. This efficiency is achieved through optimized routing decisions, avoidance of low-trust nodes, and reduced control overhead enabled by AI-based prediction. The results indicate that SATCA is well-suited for energy-constrained tactical systems, where prolonged operation and efficient resource utilization are essential.

CONCLUSIONS AND SCOPE:

The proposed SATCA framework successfully addresses critical challenges in 5G and beyond tactical communication systems by integrating adaptive routing, hybrid encryption, AI-based optimization, and trust management. Experimental results demonstrate significant improvements in latency reduction, throughput enhancement, reliability, and energy efficiency under dynamic conditions. SATCA achieves stable performance even in high-mobility and high-interference scenarios, validating its effectiveness for mission-critical applications. Future work can focus on real-time deployment using SDR or FPGA platforms, integration with 6G technologies, and enhancement using deep learning-based predictive models. Additionally, extending the framework to support large-scale distributed networks and quantum-secure communication can further improve scalability and security.

REFERENCES

[1] U. I. Rustemovich and T. H. Galimullovich, "The formation of student communication culture in the system of professional military education at civil universities," in Proc. Int. Conf. Interactive Collaborative Learning (ICL), Kazan, Russia, 2013, pp. 117–119, doi: 10.1109/ICL.2013.6644550.

[2] W. Zhang, S. Chen, and L. Liu, "A survey on the application and development of commercial communication constellations in the U.S. military operations system," in Proc. Int. Conf. Wireless Communications and Signal Processing (WCSP), Hangzhou, China, 2023, pp. 604–608, doi: 10.1109/WCSP58612.2023.10405184.

[3] M. S. Vassiliou, J. R. Agre, S. Shah, and T. MacDonald, "Crucial differences between commercial and military communications technology needs," in Proc. IEEE Military Communications Conf. (MILCOM), San Diego, CA, USA, 2013, pp. 342–347, doi: 10.1109/MILCOM.2013.66.

[4] R. Bajracharya, R. Shrestha, S. A. Hassan, H. Jung, and H. Shin, "5G and beyond private military communication: Trends, requirements, challenges and enablers," IEEE Access, vol. 11, pp. 83996–84012, 2023, doi: 10.1109/ACCESS.2023.3303211.

[5] I. Bajaj, Y. Gong, and H. L. Yee, "Time-efficient relaying strategies for military communication," in Proc. IEEE Military Communications Conf. (MILCOM), Baltimore, MD, USA, 2014, pp. 513–517, doi: 10.1109/MILCOM.2014.92.

[6] P. Zhou, Y. Lv, Z. Chen, and H. Xu, "System-level EMC assessment for military vehicular communication systems," China Communications, vol. 15, no. 8, pp. 39–53, Aug. 2018, doi: 10.1109/CC.2018.8438272.

[7] D. Wilcoxson, "Advantages of mobile broadband communication services for military applications," in Proc. IEEE MILCOM, San Diego, CA, USA, 2013, pp. 266–272, doi: 10.1109/MILCOM.2013.53.

[8] M. T. Kurdziel, R. P. Clements, and G. R. Dennis, "Customizable cryptographic architecture for military communication applications," in Proc. IEEE MILCOM, Monterey, CA, USA, 2004, pp. 295–300, doi: 10.1109/MILCOM.2004.1493284.

[9] R. Wang, "Research on abnormal data mining in military network communication," in Proc. ICICAS, Chongqing, China, 2019, pp. 249–252, doi: 10.1109/ICICAS48597.2019.00060.

[10] J. Tian and P. Wang, "Capability analysis of military communication systems based on advanced information technology," in Proc. ICISE-IE, Chongqing, China, 2021, pp. 287–290, doi: 10.1109/ICISE-IE53922.2021.00073.

[11] J. Mikołajczyk, D. Szabra, R. Matyszekiel, and B.

Grochowina, "Hybrid FSO/RF technology in military communication systems," in Proc. NTSP, Slovakia, 2018, pp. 1–4, doi: 10.23919/NTSP.2018.8524129.

[12] R. Cochetti, "Military mobile satellite communication systems," in Mobile Satellite Communications Handbook, Wiley, 2015, pp. 184–189, doi: 10.1002/9781118907658.ch10.

[13] S. Bhardwaj and T. K. Joseph, "Asynchronous communication using LoRa and MQTT for military tracking," in Proc. IEEE ICTBIG, Indore, India, 2024, pp. 1–7, doi: 10.1109/ICTBIG64922.2024.10911060.

[14] P. Ciotîrnae, "5G network with blockchain, IoT and drones for military applications," in Proc. IEEE TechDefense, Naples, Italy, 2024, pp. 104–109, doi: 10.1109/TechDefense63521.2024.10863401.

[15] Z. Wang, W. Pang, Z. Xiang, and B. Wang, "5G in military applications: Challenges and opportunities," in Proc. ICCTIT, China, 2024, pp. 675–678, doi: 10.1109/ICCTIT64404.2024.10928442.

[16] D. Schutzer, "Applications of artificial intelligence to military communications," in Proc. IEEE MILCOM, Washington, DC, USA, 1983, pp. 786–790, doi: 10.1109/MILCOM.1983.4794808.

[17] W. Pawgasame, "Evaluation of digital coding on SDR for military communication," in Proc. ACDT, Thailand, 2017, pp. 81–87, doi: 10.1109/ACDT.2017.7886162.

[18] A. A. Akinpelu, A. G. Deacon, and J. S. Shieh, "Distributed military network architecture," in Proc. MILCOM, USA, 1988, pp. 169–173, doi: 10.1109/MILCOM.1988.13386.

[19] Y. M. Hyasat and Y. S. Faouri, "High-performance UWB antenna for military communication," in Proc. CIEES, Bulgaria, 2025, pp. 1–4, doi: 10.1109/CIEES66347.2025.11300146.

[20] M. M. Hasan Somrat et al., "Performance analysis of post-quantum cryptography for military communications," in Proc. ICMIC, Philippines, 2025, pp. 198–201, doi: 10.1109/ICMIC66299.2025.11257736.