Secure 5G-Assisted UAV Access Scheme in IoBT for Region Demarcation and Surveillance Operations

Deepti Saraswat, Pronaya Bhattacharya, Arunendra Singh, Ashwin Verma, Sudeep Tanwar, and Neeraj Kumar,

Abstract

This article proposes a generic scheme that integrates blockchain (BC) and unmanned aerial vehicles (UAVs) through a fifth-generation (5G) Tactile Internet (TI) service to leverage responsive and secure communications in the Internet-of-Battlefield-Things (IoBT)-based ecosystems. UAVs are deployed with camera sensors to monitor and transfer ultra-high resolution (UHR) images and real-time live video feeds of region demarcation and surveillance to ground control stations (GCS). Currently, UAVs operate through Long-Term Evolution-Advanced (LTE-A) services and face bottlenecks in terms of bandwidth and end latency for live feeds. As the feed is sent through open channels, it is vulnerable to security attacks by an adversary. The proposed scheme addresses the dual issues of responsive network orchestration, and induces trust, immutability, and transparency in shared data among UAVs and GCSs via BC as a key solution. Through a case study, the scheme is compared to baseline LTE services. In the simulation, transactions through BC achieve 31.85 percent improvement over cloud-based GCS, an average frame loss of 18.42 percent in 5G-TI compared to 94.07 percent in 4G-LTE-A channel, and processing latency of 0.1061 s in 5G-TI, compared to 2.2133 s in 4G-LTE, which indicates the viability of the proposed scheme.

Introduction

Military forces in any country play a vital role in protecting the nation's boundaries and protecting the integrity of the citizens in case of external threats and attacks. The U.S. Department of Defence (DoD) proposed the integration of the Internet of Things (IoT) in military setups to extend its supremacy over other competitors. IoT in military ecosystems is often referred to as the Internet of Battlefield Things (IoBT). IoBT connects heterogeneous and scattered sensors, robots, machines, networks, persons, and data, and collectively processes the battlefield conditions [1]. However, the deployment of equipped sensors in warfare and on troops can be tricky in adverse geographical locations, high terrain, and extreme weather conditions. In such conditions, allocating troops or war-equipped ammunition would involve a huge risk of life and demand large logistics and supply chain formations.

To tackle the above limitations, unmanned aerial vehicles (UAVs) are a suitable choice as they simplify and expedite logistics support, and can operate in adverse conditions with minimal human intervention [2]. UAVs are heavily employed for surveillance, boundary demarcations, maps, remote sensing, search and rescue operations, disaster control, and infotainment. In a similar direction, UAVs can simplify and automate region surveillance and demarcation operations. UAV surveillance requires continuous monitoring of boundaries against possible trespassing by neighboring country troops, civilians, and illegal trafficking and smuggling of goods. Similarly, UAV involves aerial region demarcation that involves the classification of areas or plots surrounded by coastlines, streams, and land regions. Due to diverse geographical terrains, demarcation of boundaries is difficult, as it involves accurate estimation and analysis of spatial data points, and delineates false boundary regions [3]. The problem leads to incorrect boundary estimations with wrong maps that cause rifts among neighboring nations. Table 1 shows a summary of the classification of UAVs based on their categories.

To address the issues of continuous UAV region surveillance and accurate spatial demarcations, strong communication infrastructure is required. Currently, UAVs communicate with ground control stations (GCSs) through fourth generation (4G)-based Long-Term Evolution (LTE), or LTE-Advanced (LTE-A), or global positioning system (GPS)-assisted satellites. For accurate spatial analysis, the captured ultra-high-resolution (UHD) images and video feeds must be transferred to GCS in near real time to avoid buffering latency and storage of packets in frame buffers. The current 4G-LTE/LTE-A and GPS communication networks are not mature enough to avoid buffering and glitches due to higher processing and transmission delays of bulk feed. Moreover, UAV communication networks (UAVCNs) suffer from potential issues of consistent bandwidth, diffraction, line-of-sight (LoS) interference, limited UAV mobility, and intermittent disconnections. Thus, in the case of peak data traffic, UAVs cannot communicate effectively with GCS in near real time.

Thus, to address the above limitations and allow real-time connectivity of UAVs with GCS, the best fit is to deploy fifth-generation (5G) communication

Deepti Saraswat, Pronaya Bhattacharya, Ashwin Verma, and Sudeep Tanwar (corresponding author) are with Nirma University, India; Arunendra Singh is with Pranveer Singh Institute of Technology, India; Neeraj Kumar is with Thapar Institute of Engineering and T echnology, India, and also with the University of Petroleum and Energy Studies, India.

Digital Object Identifier:
10.1109/MCOMSTD.0001.2100057

2471-2825/22/$25.00 © 2022 IEEE

UAV category	UAV sub-category	Weight (kg)	Range (km)	Altitude (m)
Tactical	Nano	0.025	< 1	100
	Micro	< 5	< 10	250
	Mini	< 20 (150)	< 30	150–300
	Close range (CR)	25–150	10–30	3000
Short-range flights	Short range (SR)	50–250	30-80	3000
Medium-range flights	Medium range (MR)	150–500	80–200	5000
	Medium-range endurance (MRE)	500–1500	200–500	8000
	Low altitude deep penetration (LADP)	250–2500	250–300	50–9000
Long-range flights	Low altitude long endurance (LALE)	150–250	500–800	3000
	Medium altitude long endurance (MALE)	1000–1500	500–800	14,000
Strategic	High altitude long endurance (HALE)	2500–5000	> 2000	20,000
Special applications	Unmanned combat aerial vehicle (UCAV)	10000	1500 (approx.)	10,000
	Lethal (LETH)	250	300	4000
	Decoy (DEC)	250	0–500	5000
	Stratospheric (STRATO)	To be defined	> 2000	20,000–30,000
	Exostratospheric (EXO)	To be defined	Not below 2000	> 30,000
	Space	To be defined		To be defined

TABLE 1. Classification of UAVs.

Security, confidentiality, and trust among decentralized UAV communication are critical to IoBT operational success. As IoBT data is highly confidential and requires a high degree of integrity, permissioned blockchain is a preferred choice for secure and trusted UAV communication.

services. In IoBT ecosystems, near-responsive decisions are required in case of boundary intrusions. Thus, Tactile Internet (TI)-based UAV communication offers flexibility, high precision, extremely low latency (< 1 ms), accurate LoS, and ultra-high reliability (99.99999 percent). Moreover, 5G-TI offers flexibility in network services, virtualization of resources, and better and swift adaptation to difficult terrains to support the IoBT requirements. 5G supports higher spatial resolution, which accounts for accurate geometrical analysis and precise map generations for surveillance and demarcation operations. However, UAVs communicate with GCSs and peer UAVs through public networks; thus, the exchanged data is at risk against security and privacy attacks by malicious intruders. A malicious attacker might inject false propagation updates to malicious UAVs, that compromise the communication links to GCSs and peer UAVs in UAVCNs. This results in incorrect paths, energy drains, accidents, and incorrect UAV sightings [4].

Thus, security, confidentiality, and trust among decentralized UAV communication are critical to IoBT operational success. As IoBT data is highly confidential and requires a high degree of integrity, permissioned blockchain (BC) is a preferred choice for secure and trusted UAV communication [5]. BC can mitigate critical attack vectors in UAV communication such as impersonation, side-channel, channel hijacking, and distributed denial of service (DDoS) attacks. In BC, all the UAV access events about flight setup, path control, and the route can be verified and recorded through a suitable consensus mechanism before final commitment to the chain [6]. As a result, the data can be protected from unauthorized access by an institution or an agency. 5G-TI assisted warfare UAV swarms might contain malicious UAVs that can steal confidential information, which is mitigated through BC as it does not allow unverified oral updates to be forwarded.

Motivation

The motivation of the proposed scheme is as follows.

- In traditional IoBT setups, UAVs communicate through LTE networks, and store data over cloud-based GCS servers. Thus, end-user communication suffers from high latency, jitter, frequent disconnection, security, and privacy concerns through assisted attacks on GCSs by adversaries. Thus, in the proposed scheme, we include 5G-TI network service to allow effective UAV-to-UAV, and GCS communication in near real time.
- IoBT setups require resilient UAVCNs, and thus UAV swarms are a viable choice. Thus, in the proposed architecture, we assume the UAV swarm network is controlled through a swarm controller in the proximity of the 5G-TI controller. The swarm controller is responsible for supporting UAV in-flight route setups, region demarcation and surveillance map points, and path coordinate setups. Through 5G-TI service, it supports computational edge-based offloading schemes that can provision the UAV swarms as per IoBT network orchestration.
- However, message updates may be intercepted, and thus an adversary can inject false updates in the network. Thus, to mitigate the critical attack vectors in IoBT setups, we envision a BC-based UAV scheme, with UAV swarm path, location, and coordinate setups stored as meta-information in transactional

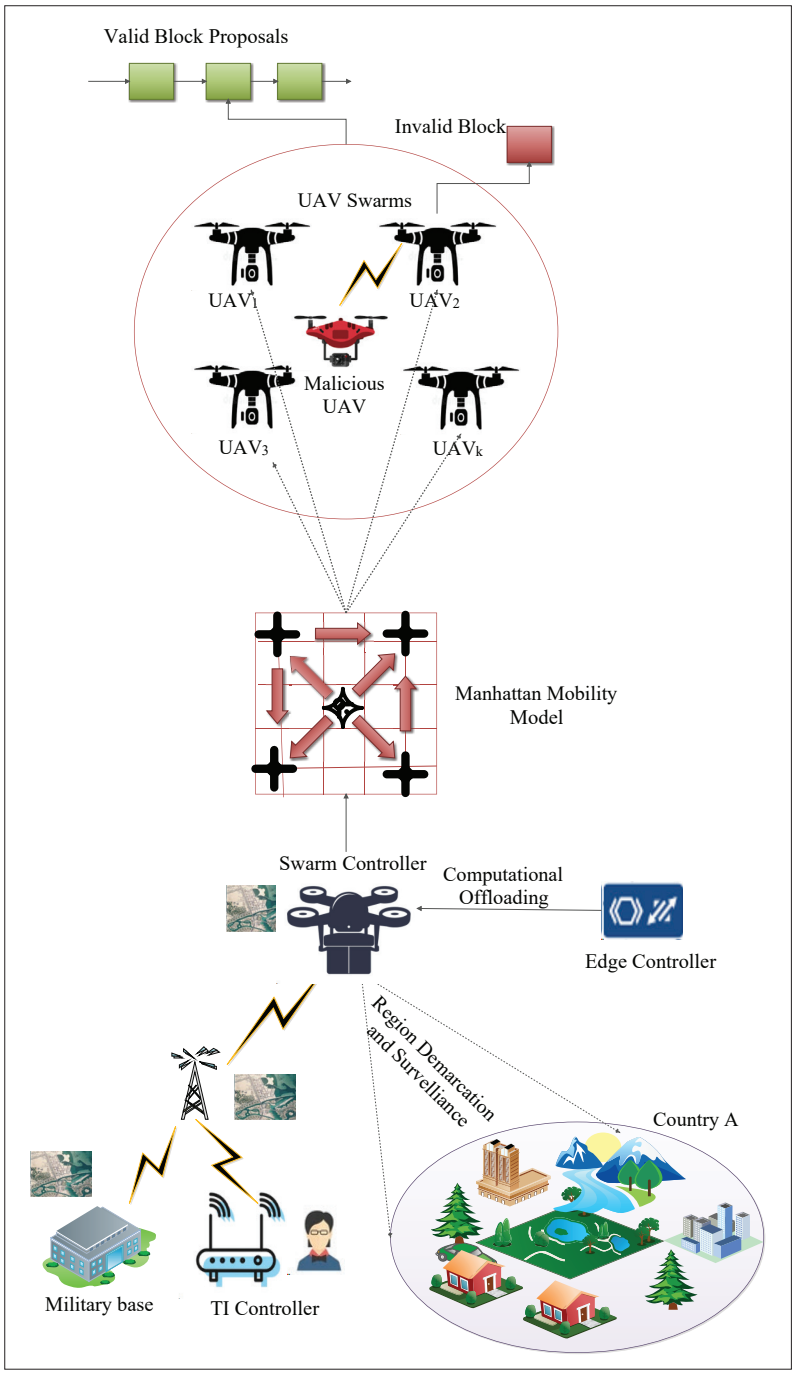

FIGURE 1. A view of the secured 5G-TI envisioned mobility model in IoBT ecosystems.

ledgers. To assist with a high volume of video feed storage, distributed offline storage is necessary, and thus interplanetary file systems (IPFSs) are a viable choice. In IPFS, only authorized personnel can access the stored data through a generated IPFS key, and hashed key references are stored in the main BC ledger. This improves the scalability of chain operations as transaction size is smaller, and more transactions fit into a single block.

Research Contributions

The research contributions of the article are:

- We propose a layered architecture that integrates BC and 5G-TI-assisted UAVs in IoBT ecosystems. We assume inter-country communication for region demarcation and surveillance setups, assisted through UAV swarms and a hyperledger fabric network.
- In the proposed architecture, we assume a Manhattan mobility model for UAVs, controlled through the UAV swarm controller. We propose an edge-based computational offloading scheme to the swarm controller, which enables low latency in communication for UAV flight setups, and accurate and precise measurement of region demarcation and surveillance operations. The records are stored in IPFS and are verified through BC-assisted transactional ledgers.
- The performance of the proposed architecture is compared to the baseline 4G/LTE scheme, and cloud GCS servers, highlighting the scheme viability over parameters like processing latency, frame loss, and throughput computation.

Article Layout

The structure of this article is as follows. We present the IoBT key technical drivers. We present the proposed scheme that comprises military surveillance, and UAV and BC layer. We present a case study that presents a comparative analysis of traditional IoBT deployments with the proposed scheme. We discuss the open issues and future research scope, and finally present the concluding remarks and future scope.

IoBT: Key Technical Drivers

This section describes the key concepts and technical aspects of IoBT-driven technologies. The section discusses the background of 5G-TI assisted UAVs, UAV mobility and offloading models, and BC deployments in IoBT ecosystems.

UAV Mobility Model and Edge-Based Offloading in IoBT Ecosystems

In IoBT ecosystems, UAV-assisted military operations support smart-sensor-driven warfare, rescue, and responsive communication setups between military bases. Military drones are classified based on flying mechanisms viz. multi-rotor drones, fixed-wing drones, and hybrid-wing drones [7]. IoBT encompasses sensor-driven warfare, with real-time connectivity with ships, UAVs, battle tanks, and soldiers (equipped with warfare and healthcare-assisted sensors to measure weapon health, heart rate, gait, and facial characteristics through combat suits, and armory) into a connected and ubiquitous network. Thus, IoBT supports many covert military operations such as persistent close air support, precision strikes, precision shelling, aerial surveillance/reconnaissance, unmanned airstrikes, UAV hijacking, evading radar detection, footage interception, and targeted assassination. However, we have restricted our discussion toward UAV surveillance and region demarcation operations.

In UAV communication, we assume a UAV swarm network, where the UAV motion patterns determine the UAV mobility. Figure 1 presents a high-level view of secured 5G-TI envisioned mobility model in IoBT ecosystems. 5G-TI ensures ultra-low latency in the communication of the UAV swarm controller node with the GCS and the TI-controller. A UAV controller node is stationed strategically

to capture UHD images and videos of surveillance and region demarcation regions, to form the aerial maps, with assisted intelligent models for object detection and recognition, for possible trespassers and intrusions by enemy regions. To support the computation-intensive streaming tasks, we assume a 5G-assisted edge offloading model, where the UAV controller delegates the offloading task to the edge node. The offloading request bits are placed on the TI-uplink channel, and result bits are sent through the downlink channel [8]. To assist the offloading, we assume the controller node to be stationary. Through the edge offloading mechanism, the video feeds are then streamed to the TI controller connected to a GCS in wired mode. Based on captured data, the UAV controller is instructed by the GCS to form a UAV mobility map pattern, and guide local UAVs for IoBT surveillance.

As a leader, the controller node forms a motion and guided pattern, and communicates the initial location coordinates, directions, and initial swarm movement speed. We assume a Manhattan grid mobility model (MGMM) to assist the directional movements. In MGMM, the UAV node movements are mapped to random directional numbers so that mobility patterns are not intercepted by an adversary node [9]. Once the map pattern is decided, the controller node stores the pattern in the IPFS node, and transactional meta-data is published in the BC network. From IPFS, only registered UAVs can access the map data, and align themselves accordingly. As the message is stored in BC, all UAVs have trust, and any malicious UAV communication update is marked as an invalid block. Only captured data from authorized UAVs are verified and then added as transactional ledgers.

5G-TI-Based UAV Communications

The IEEE Standard Working Group adopted IEEE 1918.1, or TI, as the working standard that leverages human-to-machine interactions with negligible interaction latency. This has pushed the boundaries of remote physical interactions [10]. It allows haptic interactions and kinesthetic components through wireless communication boundaries, at a strict round-trip time (RTT) latency of < 1 ms at high availability of 99.99999 percent, with failure rates as low as 10^{-7}. Ultra-low latency emulates a local operating experience for remote operations. Every TI-frame is bounded by 33 μs delay for decoding and detection at sending and receiving transmitters. Current LTE systems are not mature enough to handle TI requirements, with a user-experienced data rate of 1 Gb/s and a frame duration of 70 μs. TI requires the support of 5G-massive multiple-input multiple-output (m-MIMO) channels to allow parallel carrier aggregation and reduce the noise outage probability of non-TI channels. Due to responsive and short RTT delays, 5G-assisted TI UAVs are suitable in IoBT to leverage precise military setups to process UHD frames with precise boundary demarcation and surveillance operations. 5G-TI channels support UAV swarms for accurate flight control and route information, even in the case of intermittent connection setups.

Blockchain for IoBT Applications

BC is a decentralized ledger that records transactions as immutable ledgers and stores them in blocks, linked through a hashed chain of ledgers [11]. Thus, BC preserves auditability and chronology in transactions that support the wide array of IoBT applications. BC derives data from weapon systems, commands, and controls, sensor grids, aircraft, and network channels, and maintains trust and sustainability among military stakeholders, even in hostile conditions. BC ledgers mitigate malicious UAV interference and prevent a wide array of malicious attacks like side-channel, UAV impersonation, DDoS, and routing (blackhole and wormhole) attacks in the UAVCN. In IoBT, energy-efficient consensus mechanisms like proof of authority, leased proof of stake, and IOTA is suitable over private or consortium chain structures. Figure 1 presents a possible integration scenario of BC and 5G-TI-assisted UAVs for secured data access and responsive communication in IoBT setups.

Integration of IoBT Technical Drivers

As discussed in the aforementioned discussions, 5G-TI supports real-time latency in communication between UAV swarms and GCSs, which assists IoBT operations [12]. Through the mobility model, the UAV swarm controller can communicate with peer UAVs in its range and is supported through edge offloading to satisfy a large number of requests. Thus, the proposed scheme addresses the gaps in earlier approaches through a responsive and resilient edge offloading network. This supports key operational tasks like unified path planning, barrier avoidance, and route formation. To envision trust and immutability, we present verified transactional BC-ledgers, The records are stored in IPFS and accessed by a GCS through GCS private key. The data communicated over open channels are encrypted and signed by GCS, and encrypted with a UAV public key. Thus, the integration supports secure and trusted region demarcation and surveillance setups.

The Proposed Scheme

In this section, we present the layered architecture of the proposed ecosystem for the BC-envisioned 5G-TI-assisted UAV access scheme in IoBT setups, specifically for region demarcation, and surveillance operations. Figure 2 presents the details as a two-layered scheme, namely, the military surveillance layer and the UAV and BC layer.

Military Surveillance Layer

In this layer, we assume IoBT operations between two countries, M_A and M_B. In both M_A and M_B, we consider entities denoted as $E = \{E_{MP}, E_D, E_{PO}\}$, where E_{MP} represents military personnel, E_D represents diplomats, and E_{PO} presents peace organizations. To ensure IoBT operations, such as region demarcation of common boundaries of M_A and M_B, and surveillance operations at demarcated zones, we consider UAV swarms S_A and S_B for M_A, and M_B, respectively. Both S_A, and S_B are also responsible for boundary demarcations. For M_A, the land, air, and water boundary zones, are represented as $\{A_L\ A_A, A_W\}$, and similarly, $\{B_L\ B_A, B_W\}$ for M_B.

The captured surveillance and region demarcation data is denoted as D_S, and D_{RD}, and is stored by S_A and S_B, respectively. In D_S, we store $\{L_P, M_{UAV}, V_{MI}, V_C, T, V_{per}\}$, where L_P denotes the latitude and longitude information of the surveillance area, M_{UAV} denotes the swarm of monitoring UAVs, V_{MI} denotes the UHD video meta-informa-

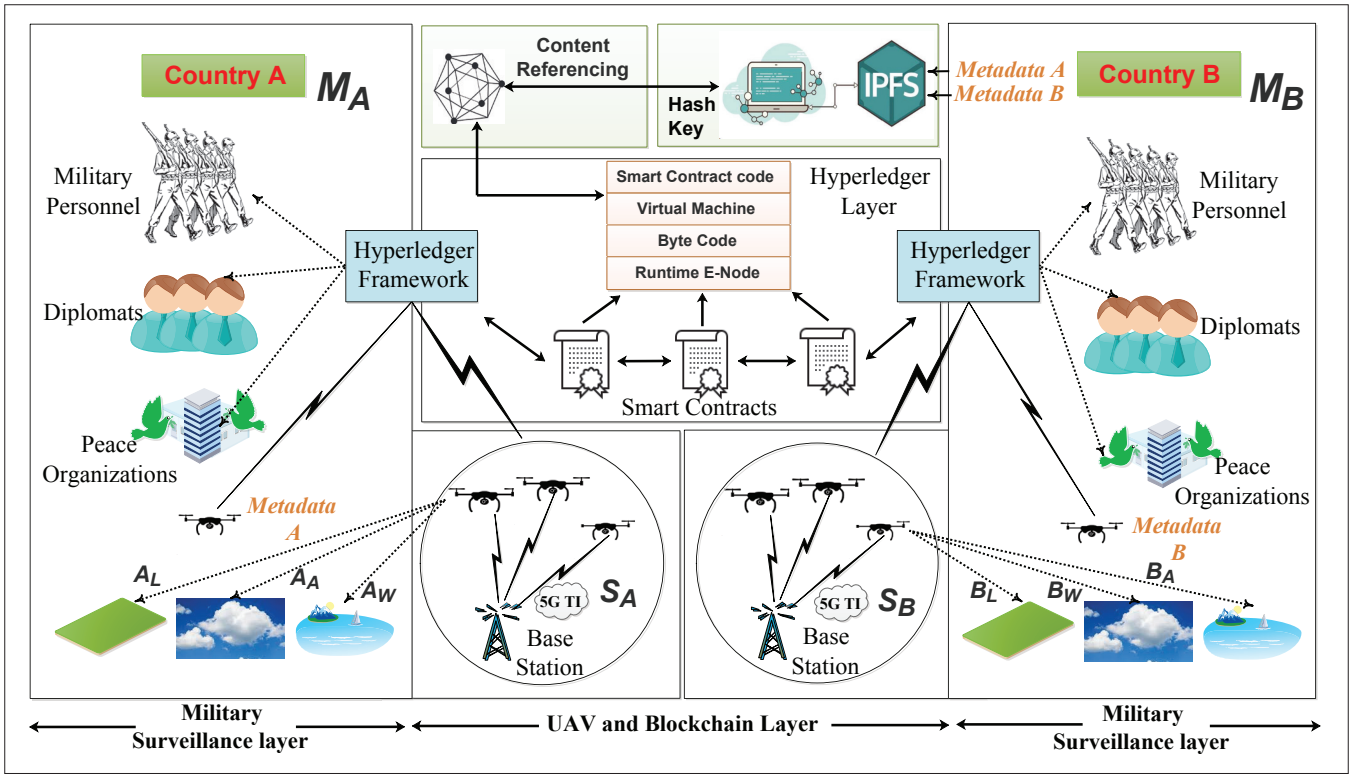

FIGURE 2. The proposed reference architecture for region demarcation and military surveillance in IoBT ecosystems.

tion, V_C, denotes the video content, T denotes the video capture timestamps, and V_{per} denotes the video capture period. For D_{RD}, we store $\{T_{DB}, L_{DB}, L_D, I_{DB}, V_{DB}, T\}$. T_{DB} denotes the demarcation type (land, air, or underwater), L_{DB} denotes the latitude and longitude information of the demarcation boundary, L_D denotes the demarcation length (in square kilometers), and I_{DB} and V_{DB} denotes the UHD images and videos, respectively, of demarcated zones. The records stored by S_A and S_B are accessed by $E = \{E_{MP}, E_D, E_{PO}\}$ through stored keys in the IPFS ledger. For both V_C and V_{DB}, real-time and responsive live streaming is critical so that unidentified intruders or objects are restricted from entering the surveillance and demarcated regions.

UAV and Blockchain Layer

In this layer, we propose the UAV and BC layers. The details of each sublayer are presented as follows.

5G-TI-assisted UAVs: Based on captured D_S and D_{RD}, UAVs S_A and S_B initialize the coverage areas (drone cells), represented as CA_A, and CA_B, respectively. UAVs are equipped with camera, position, and altitude measurement sensors. For both CA_A, and CA_B, at the GCS, two entities, GCS_{man} and S_{con}, are proposed to monitor virtualized management services. S_{con} is the UAV swarm controller, whereas GCS_{man} sets up the UAV flight control parameters and UAV stabilization parameters. At GCS_{man}, based on coverage drone cells CA_A and CA_B, TI service is set up to manage UAV setup $S_{UAV} = \{\theta_{SA}, \theta_{SB}, V_{SA}, V_{SB}\}$, where θ_{SA} and θ_{SB} represent the UAV altitude Euler angles, and V_{SA} and V_{SB} represent the driving velocity of the UAV in the coverage range. S_{UAV} sets up S_{con}, which initiates UAV mobility, to set and position all UAVs to start the journey with initial Euler angles, and also decides the horizontal speed and angular momentum of UAVs, denoted as β_V and ω_V respectively. In each drone cell, $\forall\ CA_X : CA_X = \{CA_A, CA_B\}$, and a swarm leader selection algorithm is set up to manage route and cooperative path [13]. Once all UAVs are stationed over a surveillance range $\mathbb{R}_s$, mobility position is secured via MGMM. We position the UAVs in an $n \times n$ grid G. We assume the initial position of any UAV_k in G to be (x_k, y_k). To determine the next move, we have four coordinate possibilities in the grid, namely $\{(x_{k-1}, y_k), (x_k, y_{k-1}), (x_{k-1}, y_{k-1})$, and $(x_{k+1}, y_{k+1})\}$. The selection patterns depend on the joint decision $\forall$ UAV_k in CA_X, and the grid mobility stabilizes after a few iterations. With TI service, the UAV swarm selection is completed in 1/8 ms, and oral propagation messages are delivered in 1/50 ms [13].

Once UAVs are stationed, they start the capture process of real-time images and video feeds to be streamed at the GCS node. To support the operations, we assume that S_{con} is assisted through a 5G-task offloading process by a local edge node, denoted by L_{ed}. S_{con} creates a task $T_k = \{T_s, C_s, t_u^{max}\}$, where T_s denotes the task size, C_s denotes the required number of CPU instruction cycles of L_{ed}, and t_u^{max} denotes the permissible latency. An offloading request T_k^{eq} is placed by S_{con} to L_{ed}, which offloads T_k bits to the edge server through the uplink 5G-TI channel. L_{ed} sends $l_k T_k$ bits back to S_{con} through the downlink TI, with constraint $l_k < 1$. Ideally, edge computing time t_{off}^k by L_{ed} is computed as $l_k T_k / P_k^i$ where P_k^i is the local computing capability of ith processor at L_{ed}. The edge offload response time T_{off}^{res} is $\omega^c l_k T_k (f_c^2)$, where ω_c is the computing power, and f_c is the computing chip latency. During flight setups, S_A and S_B capture images and real-time videos to be streamed at the GCS. For the same, in each drone cell C_X, UAVs position themselves strategically to capture live V_C, V_{DB},, and V_I, which

support region surveillance and boundary demarcations. For captured images and videos, to locate and track intruders, object detection algorithms are set up. For still images, faster region convolutional neural networks (RCNNs) are a preferred choice due to customization in the training and detection model. The task is critical in the case of A_W zones, and thus gamma correction is essential for images, denoted as $V_I = A$. V_C^{γ}. For $\gamma < 1$, the object detected parts are highlighted, and the rest of the image is suppressed. Normally, a value of $\gamma = 0.6$ is considered suitable for maximum object detection accuracy. For video object detection, you-only-look-once (YOLOv3) with a single-shot detector (SSD) is a preferred choice, due to low localization losses. Based on default box and ground truth box values, confidence value *C* is captured for object detection.

BC and Hyperledger-Driven Contracts: At the UAV layer, UAVs S_A and S_B capture D_S and D_{RD}. The captured data is then encrypted and signed using the GCS key. The data is then stored in IPFS, and every $E = \{E_{MP}, E_D, E_{PO}\}$ can access the data through its respective $IPFS_{key}$. Each record *R* stored in IPFS is searched through index-key value. For the index, the records are pointed by a hashed form of *R*, and the reference is stored in the main BC ledger. Storage of *R* is added to BC as a transactional ledger, and as the data is referenced securely, it evades security attack vectors like fake certificate generation, timestamp attacks, man-in-the-middle, and denial-of-service floods. For international treaty setups among *E*, smart contracts (chain åcodes) are initiated in hyperledger fabric (HF) and executed as secured docker containers. Both M_A and M_B acts as hyperledger client nodes, denoted as $HF(Cln) = \{M_A, M_B\}$, and initiate a common proposal (transaction) $P = \{A, SL\}$, where *A* denotes the asset, and *S*L denotes the shared ledger state. *P* is sent to the chain-code stub interface through an application programming interface (API) call. A hyperledger channel *C*(*HF*) is initialized by HF, and *P* is forwarded to endorsing peer E_p. E_p verifies client signatures, simulates the HF transaction in container C(P), and sends the endorser signature $E_p(Sig)$ to HF ordering service O_q. O_q commits transactions for client HF(Cln). Post transaction, *SL* is updated to state *COMMIT*, and contract is executed successfully.

Performance Evaluation: A Case Study

In this section, we test the viability of the proposed scheme against traditional approaches.

Tuning Parameters

To ensure uniformity in simulation, we have assumed a distributed homogeneous workbench, and the experiments are carried out on Intel®Core™ i7-960X at 3.2 GHz, with 8 GB RAM. For BC node setups, we considered *Hyperledger Besu*, designed for permissioned networks. We consider a total of 150 submitted assets and monitor the transaction rate. Data storage is supported through IPFS storage, and for mining purposes, a Nvidia RTX 1650 graphics processing unit is considered, connected to 1 GbE ethernet switch. Table 2 presents the details of the tuning parameters in the design.

Parameters	Values
Communication protocol	IEEE 1918.1 BS evolved nodeB (eNB) (UAV-UAV-GCS), LTE eNB (UAV-UAV-GCS)
Number of GCSs	2
UAV coverage area	1830 × 1830 m
UAV swarm	15
UAV placement	Random
UAV height	13,200 ft
UAV payload	8 kg
Hyperledger assets	150
UAV operational velocity	63 mph
Transmission packet length	512 bytes
Transmission power	100 mW (UAV-UAV)

Table 2. Tuning parameters for UAV-UAV-GCS communication.

Traditional LTE-Based Cloud Service Setups

In traditional surveillance applications, UAV S_A and S_B are positioned with camera, GPS, and measurement sensors. They are controlled through cloud-based GCS services for semi-autonomous control. UAVs are present with communication interfaces, UAV-GCS, and UAV-UAV communication over 4G-LTE/LTE-A channels. The UAV interfaces send/receive telemetry data, including GPS information, $\{\beta_v, \omega_v, \theta_{SA}, \theta_{SB}\}$. Each UAV in S_{con} is initialized with initial coordinate positions, and the transaction information is stored in cloud-based infrastructures. Figure 3 presents the schematics of the traditional ecosystem. UAVs collect UHD images from common orthogonal frequency-division multiplexing (OFDM) channels, which operate at 1 Gb/s with GCS. The captured UHD images and live feeds are compressed and then transmitted to GCS through standard lossless compression techniques.

Efficiency of the Proposed Scheme

In this section, we evaluate the performance of the proposed scheme against the traditional ecosystem. We consider two experimental benchmarks:

- UAV-to-UAV via GCS (cloud servers), represented as UAV-UAV-GCS (without BC).
- UAV-to-UAV via GCS (with BC), represented as UAV-UAV-GCS (with BC). The performance is analyzed over 5G-TI channels.

We present the potential benefits of BC adoption in transaction verification in the network. Figure 4a presents the details. Based on simulation parameters defined in Table 2, verified transaction rate is defined as V_X/V_{TC}, where V_X is the authenticated and timestamped GCS data from $\{V_C, V_{DB}\}$, and V_{TC} is the total data. We consider that 150 transactions are captured. Initially, with few messages, all transactions are verified via GCS, but as transactions increase, due to high cloud server latency, packets are delayed or time out [14]. For example, the success rate of UAV-UAV-GCS control for 100 messages is 48.12 percent for UAV-UAV-GCS (without BC), compared to 63.45 percent for UAV-UAV-GCS (with

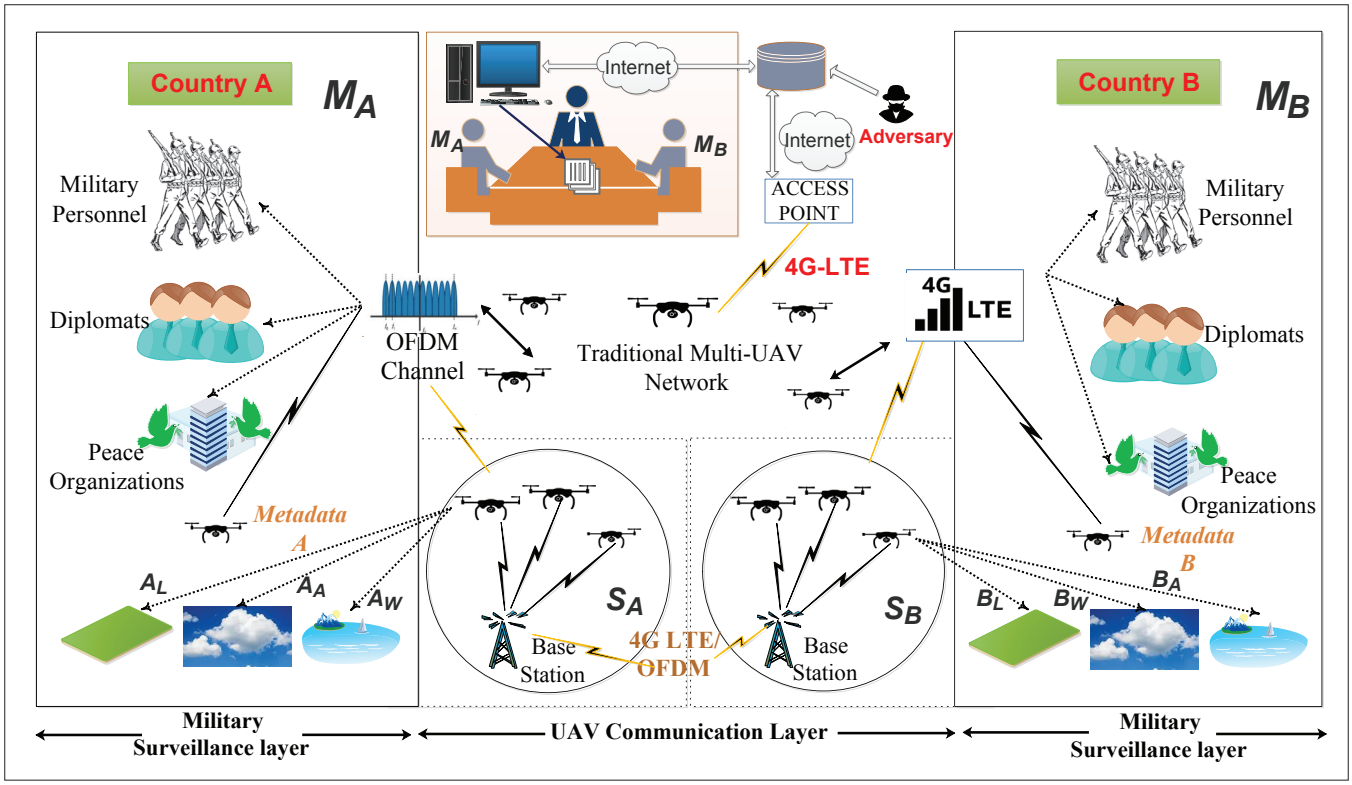

FIGURE 3. Case study: traditional UAV military surveillance through cloud-based GCS.

BC), which shows ≈31.85 percent improvement. This indicates that BC ensures higher transaction validity for open compromised channels, and thus ensures the integrity of the critical IoBT data. As the 5G-TI channel is considered, due to low latency, the transaction validity is maintained for high-traffic and dense regions.

Next, we investigate the performance of 5G-TI channels against the standard baseline 4G-LTE/LTE-A network for parameters percentage of frame loss and frame processing latency. In traditional schemes, 4G-LTE/LTE-A channels multiplexed with OFDM can provide a maximum throughput of 1 Gb/s. Compared to this, the 5G-TI channel supports a data rate of 20 Gb/s [15]. The captured D_{RD} consists of I_{DB}, which are 4K UHD images of resolution 4096 × 2160 pixels. We consider a monochrome (8 bits) single-color image, compressed with lossy compression technique, with a compression factor of 0.75 for demonstration purposes. Figure 4b presents the details. To process 600 I_{DB} compressed frames, 4G-LTE channel requires ≈10.61 s, whereas 5G-TI channel requires ≈0.53 s. Thus, for the RTT measure, 4G-LTE requires 21.22 s, and 5G-TI takes 1.06 s. As IoBT operations require real-time telemetry support, the network has to maintain consistent low RTT <1 ms. To maintain the RTT measure, 96.86 percent of total frames are lost, while the loss in the 5G-TI channel is 37.20 percent. The average loss in 4G-LTE is ≈94.07 percent of total frames, while in 5G-TI, the average loss is ≈18.42 percent. Thus, 5G-TI-assisted UAVs can consistently deliver more precise and accurate D_S and D_{RD} data at the designated latency.

Finally, we present the impact of processing latency on 5G-TI channels compared to the conventional 4G-LTE channel. Figure 4c presents the simulation details. In IoBT, real-time surveillance is critical. For the same, in the case of 40 fps, the processing latency of the 4G-LTE channel is 2.2133 s, compared to 0.1061 s in the 5G-TI channel. The average processing latency of the 4G-LTE channel is ≈1.85 s, compared to 0.092 s in 5G-TI channels. Due to the low processing latency of TI channels, precise D_{RD} is possible over a UAV drone cell.

Open Issues and Future Research

This section discusses the research challenges of integrating BC and 5G-TI in UAVs for IoBT ecosystems.

Network Connectivity

Due to high UAV mobility, UAVs suffer through intermittent and irregular connectivity. The issue is more intensified in extreme climatic regions, where the wireless connectivity service drops from 5G to baseline 4G or lower networks. Due to this, data transmission is interrupted, which might result in delays in UAV communications, thereby affecting the responsive and mission-critical IoBT applications.

Synchronization and Energy Management

In multi-UAV systems, due to the dynamic nature of the communication network, frequent hand-offs between drone cells and UAVs are forwarded to BS results in packet drops, and affect the overall stability of the multi-UAV communication. In such scenarios, a soft hand-off state is preferred, but the same might result in disconnected data offloading. Proper mechanisms are required as the issue is more problematic due to varying topology and dynamic connection links.

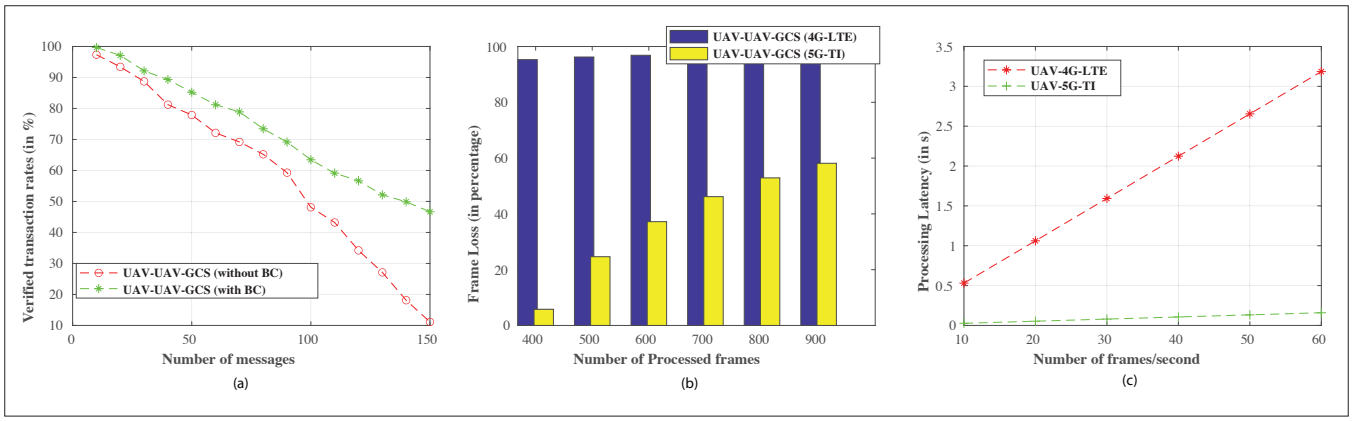

FIGURE 4. Performance evaluation: comparative analysis of 5G-TI and BC-assisted UAV communication against traditional (cloud/base station) approaches: a) reduction in unverified transactions via BC; b) pixel loss vs. number of frames; c) transmission time vs. frame rate.

Swarm Leader Election

In a UAVCN, the swarm leader is selected with high computational power, as it has to support multi-relay dissemination. Thus, proper energy harvesting between UAVs for energy exchange is required for longer network lifetime and prolonged service period of UAVs during mission-critical surveillance operations.

Channel Access

Due to thre common channel, effective medium access and the collision avoidance strategies are required to reduce the probability of packet drops. In wireless channels, due to high error rates, signal interference, path reflection, and diffraction result in intersymbol interference and wireless spread. To address the limitations, non-orthogonal multiple access (NOMA) strategies are a preferred choice, as compared to orthogonal access, NOMA provides higher spectral efficiency for multiple UAVs simultaneously. NOMA utilizes the same frequency for all UAVs and also addresses the limitations of noise interference in neighboring channels through successive interference cancellation (SIC) techniques.

Restricted Zones

In restricted flying zones, only authorized UAVs are allowed to operate. Thus, responsive identity authentication of UAVs is critical. If restricted zones are in dense areas, effective load balancing of a BS is required. For the same reason, the BS needs to deploy micro and sectorized cells to address the traffic requirements in a better manner.

Data Privacy

Any authorized stakeholders can access the IPFS ledger through a secure IPFS key. However, an adversary might propose an informed attack to know the IPFS content hash and access the stored data sequence. Based on data sequences, meta-content in an on-chain ledger might be traced as the IPFS hash acts as an external reference to main ledgers.Currently, to address the issue, no-inbuilt solutions are provided by IPFS, and the issue is addressed through the inclusion of cryptographic primitives, which protects the user data through private membership of the IPFS ledger. This adds a burden on the overall architecture, which limits the scalability of the operations.

Energy Efficiency vs. Communication Latency Trade-off

Due to small cell 5G femtocells, a large number of BSs are required to communicate with UAVs through short-range communication. This results in increased overhead on wireless channels, and subsequently affects the energy consumption of the BS. Thus, BS communication with UAVs is affected, and the communication latency increases. The control protocols employ dynamic scheduling operations with UAVs, which are resource-intensive. Thus, reduction of latency requires high resources at the BS, and an optimal fit of energy vs. communication is required to maintain consistent service availability for a longer duration.

Conclusion

The article proposes guidelines for a BC-leveraged 5G-assisted UAV access scheme in IoBT for region demarcation and surveillance operations. In IoBT ecosystems, real-time and responsive military setups are critical to support connected and networked infrastructures. Through 5G-TI. UAVs are powered to process UHD images and videos at ultra-low latency and constant availability. However, as the data is communicated through open untrusted channels, BC preserves trust and confidentiality of sensitive military data to be accessed and shared between IoBT stakeholders. BC-assisted UAVs can communicate with GCS securely with low attack vector probability. A reference scheme is proposed for consortium BC, and hyperledger-driven chain codes are presented as part of the scheme that ensures automated transactions among neighboring countries. The scheme is validated through a comparative analysis with conventional cloud-based GCS support, and baseline OFDM multiplexed 4G-LTE/LTE-A channels for comparative evaluation against the proposed 5G-TI channel. The results demonstrate the efficacy of the scheme, which supports the IoBT surveillance and demarcation operations. Finally, open issues and possible research directions are presented.

As part of the future scope of the proposed work, the authors would like to investigate NOMA-based multiple-UAV access that improves the reliability in TI channels through SIC. In a given spatial range, power allocation in NOMA UAVs ensures data secrecy, user fairness, and higher spectral efficiency, which ensures higher throughput in IoBT ecosystems.

References

[1] W. Lang *et al.*, "Iobtchain: An Integration Framework of Internet of Battlefield Things (IoBT) and Blockchain," *2020 IEEE 4th Info. Technology, Networking, Electronic and Automation Control Conf.*, Chongqing, China, vol. 1, 2020, pp. 607–11.

[2] J. Grzybowski, K. Latos, and R. Czyba, "Low-Cost Autonomous Uavbased Solutions to Package Delivery Logistics," *Advanced, Contemporary Control*, A. Bartoszewicz, J. Kabzinski, and J. Kacprzyk, Eds., Springer, 2020, pp. 500–507.

[3] D. Bhattacharya *et al.*, "Idea: IoT-Based Autonomous Aerial Demarcation and Path Planning for Precision Agriculture with UAVs," *ACM Trans. Internet of Things*, vol. 1, June 2020.

[4] A. Shafique, A. Mehmood, and M. Elhadef, "Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles," *IEEE Access*, vol. 9, 2021, pp. 46,927–48.

[5] J. Wang *et al.*, "Lightweight Blockchain Assisted Secure Routing of Swarm UAS Networking," *Computer Commun.*, vol. 165, 2021, pp. 131–40.

[6] A. Singh *et al.*, "Sidechain Technologies in Blockchain Networks: An Examination and State-of-the-Art Review," *J. Network and Computer Applications*, vol. 149, 2020, p. 102,471.

[7] H. Hassani, A. Mansouri, and A. Ahaitouf, "Mechanical Modeling, Control and Simulation of a Quadrotor UAV," *Proc. 2nd Int'l. Conf. Electronic Engineering and Renewable Energy Systems*, B. Hajji *et al.*, Eds., Singapore, Springer, 2021, pp. 441–49.

[8] H. Guo and J. Liu, "UAV-Enhanced Intelligent Offloading for Internet of Things at the Edge," *IEEE Trans. Industrial Informatics*, vol. 16, no. 4, 2020, pp. 2737–46.

[9] K. Kabilan *et al.*, "Performance Analysis of IoT Protocol under Different Mobility Models," *Computers & Electrical Engineering*, vol. 72, 2018, pp. 154–68.

[10] O. Holland *et al.*, "The IEEE 1918.1 'Tactile Internet' Standards Working Group and Its Standards," *Proc. IEEE*, vol. 107, no. 2, 2019, pp. 256–79.

[11] T. Gayvoronskaya and C. Meinel, *Technical Basics for a Better Understanding of Blockchain Technology*, Springer, 2021, pp. 15–33.

[12] R. Gupta *et al.*, "Vahak: A Blockchain-Based Outdoor Delivery Scheme Using UAV for Healthcare 4.0 Services," *IEEE INFOCOM Wksps. 2020*, Toronto, ON, Canada, 2020, pp. 255–60.

[13] F. D'Ursol *et al.*, "The Tactile Internet for the Flight Control of UAV Flocks," *2018 4th IEEE Conf. Network Softwarization and Wksps.*, Montreal, QC, Canada, 2018, pp. 470–75.

[14] M. Aloqaily *et al.*, "Design Guidelines for Blockchain-Assisted 5G-UAV Networks," *IEEE Network*, vol. 35, no. 1, Jan./Feb. 2021, pp. 64–71.

[15] M. Simsek *et al.*, "Chapter 15 — Tactile Internet Standards of the IEEE p1918.1 Working Group," *Tactile Internet*, F. H. Fitzek *et al.*, Eds.), Academic Press, 2021, pp. 351–74.

Biographies

Deepti Saraswat (deepti.saraswat@nirmauni.ac.in) is an assistant professor in the Computer Science and Engineering Department at Nirma University, Ahmedabad, India. She is pursuing a Ph.D. at Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar, India. Her research interests include data security and privacy, blockchain technology, optimization techniques, and IoT.

Pronaya Bhattacharya (pronoya.bhattacharya@nirmauni.ac.in) is an assistant professor at Nirma University. He has authored/co-authored more than 50 publications including SCI Indexed journals and IEEE ComSoc sponsored international conferences. His research interests include blockchain technology, edge computing, and software-defined networking.

Arunendra Singh (arun.sachan@gmail.com) is presently working as an associate professor in the Department of Information Technology at Pranveer Singh Institute of Technology, Kanpur. He has authored/co-authored more than 12 publications in Web of Science and Scopus. His areas of interest include network security, optical communications, computer networks, machine learning, IoT, and GIS.

Ashwin Verma (ashwin.verma@nirmauni.ac.in) is an assistant professor in the Computer Science and Engineering Department at Nirma University. He is pursuing a Ph.D. at Amity University, Jaipur, Rajasthan, India. He has authored/co-authored seven publications in leading journals and conferences. His research interest includes network security, communications, and federated learning.

Sudeep Tanwar (sudeep.tanwar@nirmauni.ac.in) is a full professor at Nirma University and was a visiting professor at Jan Wyzykowski University, Polkowice, Poland, and the University of Pitesti, Romania. He received his Ph.D. in computer science and engineering from Mewar University, India. His research interests include WSN, blockchain technology, fog computing, and smart grid. He has authored/coauthored more than 270 research papers in leading journals and conferences of repute and has edited/authored 13 books published in leading publication houses including IET and Springer. He is an Associate Editor of *IJCS* , *Computer Communications*, and the *Security and Privacy Journal*, Wiley.

Neeraj Kumar (neeraj.kumar@thapar.edu) is a professor at Thapar Institute of Engineering and Technology, Deemed to be University, India. He received his Ph.D. from SMVD University, India, in CSE and was a postdoctoral research fellow at Coventry University, United Kingdom. He has more than 400 research papers in leading journals and conferences of repute. He is an Associate Editor/Technical Editor of *IEEE Communications Magazine*, *IEEE Network*, *IJCS* (Wiley), *JNCA* (Elsevier), *ComCom* (Elsevier), *Security and Privacy* (Wiley), the *IEEE Systems Journal*, and *ACM Computing Surveys*.