IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 25, 2018, accepted January 2, 2019, date of current version February 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2893775

Secure and Reliable Resource Allocation and Caching in Aerial-Terrestrial Cloud Networks (ATCNs)

VISHAL SHARMA[1], (Member, IEEE), ILSUN YOU[1], (Senior Member, IEEE), JUNG TAEK SEO[1], AND MOHSEN GUIZANI[2], (Fellow, IEEE)
[1]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea
[2]Department of Computer Science and Engineering, Qatar University, Doha, Qatar

Corresponding author: Ilsun You (ilsunu@gmail.com)

This work was supported in part by the Institute for Information and Communications Technology Promotion (IITP) grant through the Korean Government (MSIT) (Rule Specification-Based Misbehavior Detection for IoT-Embedded Cyber-Physical Systems) under Grant 2017-0-00664, and in part by the Soonchunhyang University Research Fund.

ABSTRACT Aerial-terrestrial cloud networks (ATCNs), global integration of air and ground communication systems, pave a way for a large set of applications such as surveillance, on-demand transmissions, data-acquisition, and navigation. However, such networks suffer from crucial challenges of secure and reliable resource allocation and content-caching as the involved entities are highly dynamic and there is no fine-tuned strategy to accommodate their connectivity. To resolve this quandary, cog-chain, a novel paradigm for secure and reliable resource allocation and content-caching in ATCNs, is presented. Various requirements, key concepts, and issues with ATCNs are also presented along with basic concepts to establish a cog-chain in ATCNs. Feed and fetch modes are utilized depending on the involved entities and caching servers. In addition, a cog-chain communication protocol is presented which avails to evaluate the formation of a virtual cog-chain between the nodes and the content-caching servers. The efficacy of the proposed solution is demonstrated through consequential gains observed for signaling overheads, computational time, reliability, and resource allocation growth. The proposed approach operates with the signaling overheads ranging between 30.36 and 303.6 bytes*hops/sec and the formation time between 186 and 195 ms. Furthermore, the overall time consumption is 83.33% lower than the sequential-verification model and the resource allocation growth is 27.17% better than the sequential-verification model.

INDEX TERMS Security, reliability, content caching, ATCNs, STINs, cog-chain.

I. INTRODUCTION

Aerial-Terrestrial Cloud Networks (ATCNs) include a system formed by the integration of aerial and terrestrial entities. ATCNs are the sub-type of Space and Terrestrial Integrated Networks (STINs) [1], which use multiple backbone formations in the sky as well as on the ground for enhancing the reachability of services to its users. ATCNs depend on the mutual collaboration between the aerial nodes [2]–[4], such as satellites or drones, and the terrestrial nodes, such as Ground Control Stations (GCSs), Base Stations (BSs), Ground Vehicles (GVs) or User Equipment (UE), for the transmission of services. ATCNs are capable of disintegrating themselves with sufficiently high-capacity of forming personalized or private sub-cloud infrastructures [5], [6]. In addition, ATCNs operate as a primary mode of content-sharing for public-safety communications. ATCNs help to assemble network intelligence, computational power, decisive capabilities, and resource-sharing as common parameters for collaboration between aerial and ground networks.

Moreover, ATCNs can use entities like satellites, airplanes (fixed wing, rotor-wing), drones, High Altitude Platform Systems (HAPS), GCS, GVs, User Equipment (UE), MicroCell (MC), and Macro Base Cell (MBS), as shown in Fig. 1. All these entities are capable of independent as well as dependent communications and require effective solutions for resource sharing/allocation, load-balancing and caching while supporting the reliable end to end transmissions.

In order to satisfy the operational-requirements of ATCNs, Cog-Chain, a novel paradigm for secure and reliable resource

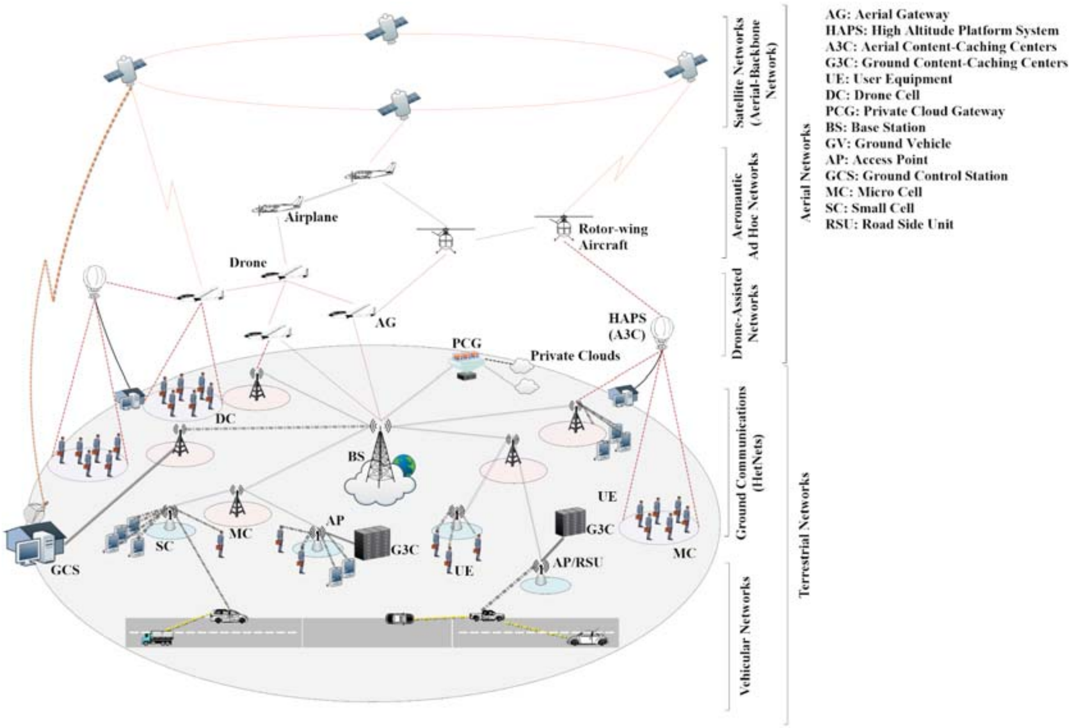


FIGURE 1. An exemplary illustration of ATCNs' architecture, components and dependencies.

allocation and content-caching is presented in this article. To realize such a formation the proposed architecture uses HAPS as Aerial Content-Caching Centers (A3C), and drones as Aerial Gateway (AG) for connecting terrestrial entities with other nodes. The aeronautical ad hoc formation is an intermediate layer between the drone-assisted networks and the satellite backbone networks. The Access Points (APs) operate similar to Road Side Units (RSU) for infrastructure-based vehicular networks, while some vehicles also possess the ability for infrastructure-less communications through the vehicle to vehicle mode. Private Cloud Gateway (PCG) helps to connect the private cloud systems to the regular network. In the given setup, APs or MC nodes can also serve the purpose of PCG for extending services between the core and the private networks.

II. PROBLEM STATEMENT AND OUR CONTRIBUTIONS

With a large number of nodes operating at the same instance in the aerial and the ground periphery, it is tedious to manage resources between them. This further demands efficient connectivity between the devices. There are solutions, which focus on resource allocation as well as caching in networks operating with UAVs [7]–[15]. However, coordinated networks, like ATCNs, suffer from another aspect of reliability and security that is missing in the existing solutions. Moreover, there is no common model that can support multi-factor security at the same instance that too with lesser overheads. Additionally, the available research works revolve around the formation of an optimization problem for improving connectivity to allow reliable resource allocation and caching. These solutions fail to accommodate the security and reliability of resource allocation and caching as an in-built mechanism. Such solutions need an external approach handling the extra operations, which may increase the cost of operations as well as overheads.

The major contributions of this work are as follows:

- At first, the article clarifies the requirement of a common solution for secure and reliable resource allocation and caching in ATCNs.
- Next, the article discusses the operational aspects and how existing literature is insufficient in handling the issues related to resource allocation in ATCNs.
- Then, a novel paradigm, ''Cog-Chain'' which supports multi-hierarchy security, resource allocation and caching in ATCNs, is discussed in detail.
- A Cog-Chain Communication Protocol (CCCP) is proposed, which the flow of actual virtual cog-chains and manages its operations.
- Finally, numerical evaluations and performance case study are presented to understand the implications as well as the advantages of using cog-chain in distributed networks like ATCNs.

The rest of the article is structured as follows: Section III provides the discussion on related works. Section IV discusses the architectural challenges of ATCNs. Section V discusses the service aspects of ATCNs. The proposed work is provided in Section VI and Section VII. Performance evaluation is given in Section VIII. Section IX discusses related

TABLE 1. A comparison of existing solutions for resource allocation and caching in UAVs. (C1: Reliability, C2: Resource Allocation, C3: Secure Resource Allocation, C4: Multi-tier Security, C5: In-build Security, C6: Caching, C7: Secure Caching).

Approach	C1	C2	C3	C4	C5	C6	C7
Subcarrier and power allocation for UAVs [7]	No	Yes	No	No	No	No	No
Joint caching and resource allocation for UAVs [8]	No	Yes	No	No	No	Yes	No
Resource allocation for UAVs [9]	No	Yes	No	No	No	No	No
Resources allocation mechanism for multi-layer UAVs [10]	No	Yes	No	No	No	No	No
Resource Allocation for UAV-assisted networks [11]	No	Yes	No	No	No	No	No
Resource allocation scheme for non-orthogonal transmissions [12]	No	Yes	No	No	No	No	No
Node placement and resource allocation [13]	No	Yes	No	No	No	No	No
Dynamic resource allocation for Social Internet of Vehicles [14]	No	Yes	No	No	No	Yes	No

technologies and open issues. Finally, Section X concludes the article.

III. RELATED WORKS

The resource allocation problem in the UAV networks has been explored in the form of various optimization problems by many researchers. Adequate resource allocation facilitates maximum throughput and efficient power consumption. The existing literature has studied a number of subproblems related to resource allocation and caching in the UAV communication networks.

Sun *et al.* [7] focused on the joint optimization in subcarrier and power allocation for solar powered multicarrier UAV communication systems [7]. The authors proposed a successive convex approximation-based algorithm for resource allocation, which is based on the mixed-integer nonconvex optimization. Chen *et al.* [8] emphasized on the Joint caching and resource allocation for UAVs and proposed a machine learning framework in the form of a Liquid State Machine (LSM) to predict the users' content request distribution when the limited information is available. The authors considered the problem associated with the user association and content replacement for resource allocations. Xu *et al.* [9] focused on the resource allocation problems for UAVs based on a non-convex optimization problem for total transmit power of a downlink.

Li and Han [10] focused on resources allocation mechanism in the multi-layer UAVs. The authors considered the packet delay problem and proposed a Voronoi based PV system. The authors modeled various properties to achieve a mean packet arrival rate in any UAV. The formulated optimization problem was solved with the Gradient descent method with the Bisection method.

Wang *et al.* [11] focused on the energy harvesting-based communications and formulated a problem of mixed integer nonlinear programming and gave a resource allocation algorithm to maximize the average throughput. Baek *et al.* [12] emphasized on the optimal resource allocation for non-orthogonal transmission. The authors focused on the maximum throughput of the user equipment and presented a resource allocation algorithm which helps to enhance the operation range of UAVs. Node placement and resource allocation problem were further discussed by Fan *et al.* [13]. Furthermore, a dynamic resource allocation for the social Internet of vehicles was explored by Zhang *et al.* [14]. The authors presented the optimization framework based on the joint allocation of transmitting power of the vehicle.

From the comparison presented in Table 1, it can be evidently stated that the existing research does not reveal any security paradigms in the resource allocation for UAVs. Moreover, various security domains for caching and resource allocation in the UAVs communication networks need a considerable research and advancement.

IV. ARCHITECTURAL CHALLENGES OF ATCNS

The inclusion of different types of entities makes the network ultra-dense while raising the requirements of low-complex and highly-reliable connectivity leading to secure transmissions between the end users. Considering such aspects, the architectural challenges associated with ATCNs are listed below:

A. COMMON INTEGRATION PLATFORMS (CIPS)

ATCNs rely on the efficient unification of all the layers resulting in a common cloud infrastructure which makes an entity believe as if it was operating on the same network. Such unification is dependent on the seamless integration of platforms and services, which results in the formation of a highly efficient integrated network. With the involvement of dynamic nodes, it becomes easier to facilitate the network with all-time connectivity, but this raises a need for efficient interfacing between the entities. Such an interfacing is achievable through Common Integration Platforms (CIPs), which enable to merge two or more networks without classifying them on the basis of their property or services, rather use only content-type and content-policing for deciding the rules of integration. CIPs can be fixated on different types of solutions like using a controller in Software-Defined Networks (SDNs) or slice-interface in Network Function Virtualization (NFV) [16], [17]. CIPs are also responsible for preventing any isolation as well as avoiding any redundant connectivity in the network.

B. ABOVE-ROUTING TRANSMISSIONS (ARTS)

Because of dynamic and frequently varying topologies, ATCNs suffer from the lack of control and require a solution for integrated network routing [1]. Although it is simpler to demand such a solution, integration of networks increases the risks of partitioning as well as broadcast storming that waste the resources of a network in excessive amount leading to a complete failure of services. Solutions, like ARTs, fit on top of any routing protocol and help in the smooth operation of integrated network irrespective of the topology changes or content-availability. ARTs take into account the situational awareness of the network and use a solution like the disintegration of addressing protocols for helping to attain a seamless flow of services. These further include the use of a dominance procedure, which allows regulating the traffic from the layer or subnetwork operating in an upper hierarchy in the unified ATCNs. For example, terrestrial isolation or network partitioning and broadcast storming can be prevented by forming access control and authorization policies with the above-operated drone-networks or HAPS. In certain scenarios like aeronautical ad hoc formations, ARTs are attained directly through satellite or command and control towers on the ground.

C. NODE PLACEMENT AND CONTROL

Placement of nodes and control over their actions are much crucial from the architectural point of view. An incorrect positioning of a node and the wrong calculations of waypoints for drones and HAPS w.r.t. satellite movement can lead to scenarios with No Line of Sight (NLoS) [18], [19]. Although there are solutions for handling transmissions in scenarios with NLoS, it is desirable to prevent such a situation by efficiently placing each node in the network. ATCNs are the integrated clouds, thus, control on position and identifying the likelihood of failure become extremely important for preventing transmissions losses. Efficient node placement and control over its transmissions help to prevent issues related to signal distortion, fading because of atmospheric conditions or vegetation losses, and even physical and signal interference [20]–[23]. In addition, from the security point of view, the position of a node is important to keep safe the topology of the entire network. Capturing a node which possesses a maximum context of the network causes its perimeter to be exposed leading to the threats of different types of cyber attacks.

D. MOBILITY MANAGEMENT AND SECURITY

Mobility management is one of the most critical aspects to be handled in ATCNs as it results in different types of variations in the topology. Mobility management is architectural dependent and security of movement is highly crucial as any loopback connectivity can cause an attacker to gain access to the involved entities. Node authentication, access control, and mitigation of handover interference are crucial factors related to mobility management in ATCNs [24]. In addition, signaling overheads, energy-efficiency, and cost of operations are other factors to control [22]. Use of secure encoding and modulation procedures can help to secure the mobility in ATCNs. The secure handover process should be emphasized to reduce the total transmission time and the packet loss rate. The excessive key distribution overhead is also a considerable parameter in ATCNs' mobility management.

V. SERVICE ASPECTS OF ATCNS

ATCNs facilitate connectivity between the networks which may get isolated in the absence of a gateway. With the advent of ATCNs on the backbone of STINs, different types of services, performance issues, and tradeoffs can be managed for networks which have the capability of working independently but also possess some architectural issues as discussed below:

A. RESOURCE ALLOCATION

Networks supporting 4G- and 5G-enabled devices demand efficient policies for resource allocation. In ATCNs, resource allocation is seen as an important paradigm of load balancing as it helps to efficiently facilitate the nodes which have sufficient computational capacity for handling incoming traffic. Resource allocation depends on different factors such as energy consumption, memory utilization, cost of operation, detection and processing time, network delays, and the lifetime of the nodes [25]–[28]. With the integration of different entities, resource allocation becomes more challenging as issues like scalability, node-authentication, transmission time and losses become more prominent for taking a decision. Accessibility, optimization, and process transitions are other factors which affect resource allocation in ATCNS. In addition, the hierarchical flow of information and dynamic topology make it more complex and tedious to optimally allocate the resources among the intended nodes. Thus, effective strategies are required which can help to allocate resources without compromising the accessibility and authorization of the network nodes.

B. CONTENT-CACHING

Accessing similar services, again and again, requires efficient storage medium to effectively provide content on-demand. In case the nodes argue for similar data over and over, and the content has to be traversed back from its original source, the performance of the network may degrade and there can be unintended delays that may result in huge amount of network failures. Such a situation can be resolved through content-caching, which helps to support the users with ready-to-provide requested information at a rapid pace [15]. In ATCNs, content-caching is required at different layers, however, to facilitate the operations of a network, two caching servers can be placed in one zone while the actual network may have n number of such servers depending on the metrics like, number of connections supported, energy and memory requirements, present load, and etc. In the given architecture, A3C and Ground Content-Caching Center (G3C) are used as caching servers, which help to facilitate both aerial as well as terrestrial entities at the same time without involving themselves in the issues related to mobility management. To attain a low-complex solution, ATCNs use HAPS for aerial content caching and use data centers directly connected to APs for terrestrial content caching. Content-caching and resource allocation can be together seen as one issue, which needs a secure and reliable mechanism to handle especially looking at the broader performance view of ATCNs. In addition, factors like joint-bandwidth allocation, per UE (node) capacity, throughput and average gains over SINR are of utmost importance [15], [29]. These issues further raise the bar once seen from the security point of view and require an effective strategy for achieving reliable and secure content-caching.

C. CAPACITY, COVERAGE, AND COMPLEXITY

As other general services are concerned, capacity, coverage, and complexity are three pillars of any type of operations, which are performed by the ATCNs' entities. Aerial components in ATCNs are responsible for enhancing the coverage of the network while leveraging on the modern network technologies, whereas terrestrial entities are responsible for mitigating any issue concerning cell overlapping, large latency or multiple-access interference [30]. Coverage of a network is often related to capacity and a network must ensure high capacity along with high coverage. It is a proven statement that a network with high coverage but low capacity is of no use as it may result in large delays and higher overheads [31]–[33]. Capacity and coverage further require a low-complex solution to accommodate a larger number of nodes at a low cost. In general, the integration of aerial and terrestrial networks must result in high capacity, enhanced coverage, and low-complex transmissions while maintaining the security considerations of the network.

D. SECURITY-PERFORMANCE TRADEOFFS

A critically secure network may not provide sufficiently high performance. Strict security policies may result in excessive overheads which prove to be a burden on the energy and memory requirements of a network [34]. The management of tradeoff between the security and performance is still an open issue and it becomes even bigger when more than one type of networks are involved in service layoffs. Technologies like Low-Power Wide-Area Network (LPWAN) [35], [36], IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [37] and Zigbee [38], [39] can be used for obtaining low-power and energy-efficient solutions especially in the deployment of service gateways in ATCNs.

Servers operating through these technologies can be used as gateways and can also help to decide the energy-efficient policies for secure and reliable content-caching [19]. Furthermore, solutions in terms of algorithmic strategies or software architectures, which can regulate the flow of services in the network without much dependent on a single entity, are also required. The developed approach must ensure that each and every component of ATCN is utilized for enhancing the Quality of Experience (QoE) for its users while preserving resources in such way that the possibilities of attack and network shutdowns due to traffic capturing and over-consumption of resources are eradicated.

VI. A MULTI-LAYER SECURITY AND RELIABILITY MECHANISM: COG-CHAIN

This article introduces a novel cog-chain concept which is inspired by the mechanical ''Cogs'', ''Chains'' and rules of ''Blockchain'' technology, however in a different context and application. A network operating with the principles of cog-chains can have main chains and multiple sub-chains, however, cog-chain[1] uses all its chains for security and reliability of the system. Further, there is no broadcasting and content sharing is done through CCCP which makes it more reliable and controllable. In addition, cog-chains provide solutions for feedback, control and policing, which are difficult to attain through a normal blockchain process. The proposed cog-chain technology introduces a new mechanism for multi-layer security and reliability, especially for integrated systems such as ATCNs, as shown in Fig. 2.

A. COG-CHAIN: FORMATION AND COMPONENTS

The Cog-chains comprises the N number of cogs each representing an entity of the network with a K number of chains between them. Each layer can have the M number of cogs out of which M' can be operated as a common cog between two or more cogs. The formation of cog-chain is dominated by the number of chains operating over each cog. These chains are the virtual path of connectivity between the actual entities in the network and a chain exists between the cogs (entities) if there is a high likelihood of the existence of a transmission path between the entities. Unlike mechanical cogs, the assumption can be made that each cog can have multiple chains each representing a different role in the system. Following rules help to clarify the formation of cog-chain:

- Number of chains: The number of chains helps to decide on the number of policies required to manage the network. If the network is based on a single property, the number of chains follows $1 \leq K \leq \left(\frac{M(M-1)}{2}\right)$, and follows $(L+1) \leq K \leq \left(L.\frac{M(M-1)}{2} + \sum_{i=1}^{L} M_i\right)$ for L-layered system. For the R number of properties, each entity in the above governing conditions is multiplied with R, which denotes the additional chains on each cog (entity) in the network.
- Chain-formations: Cog-chain is governed by rules, which form the virtual chain between the cogs and help to form a security and reliability-based decision-support system which takes into account the present condition of the network.
  - Timing-controlled chains: When the number of properties in a network is controlled by time and the chains appear or disappear through time-stamping, the type of chains is timing-controlled. Such chains facilitate connectivity with other cogs once a particular checkpoint is attained in the periodicity of the system.

[1] Cog and node are having a similar meaning in this article.

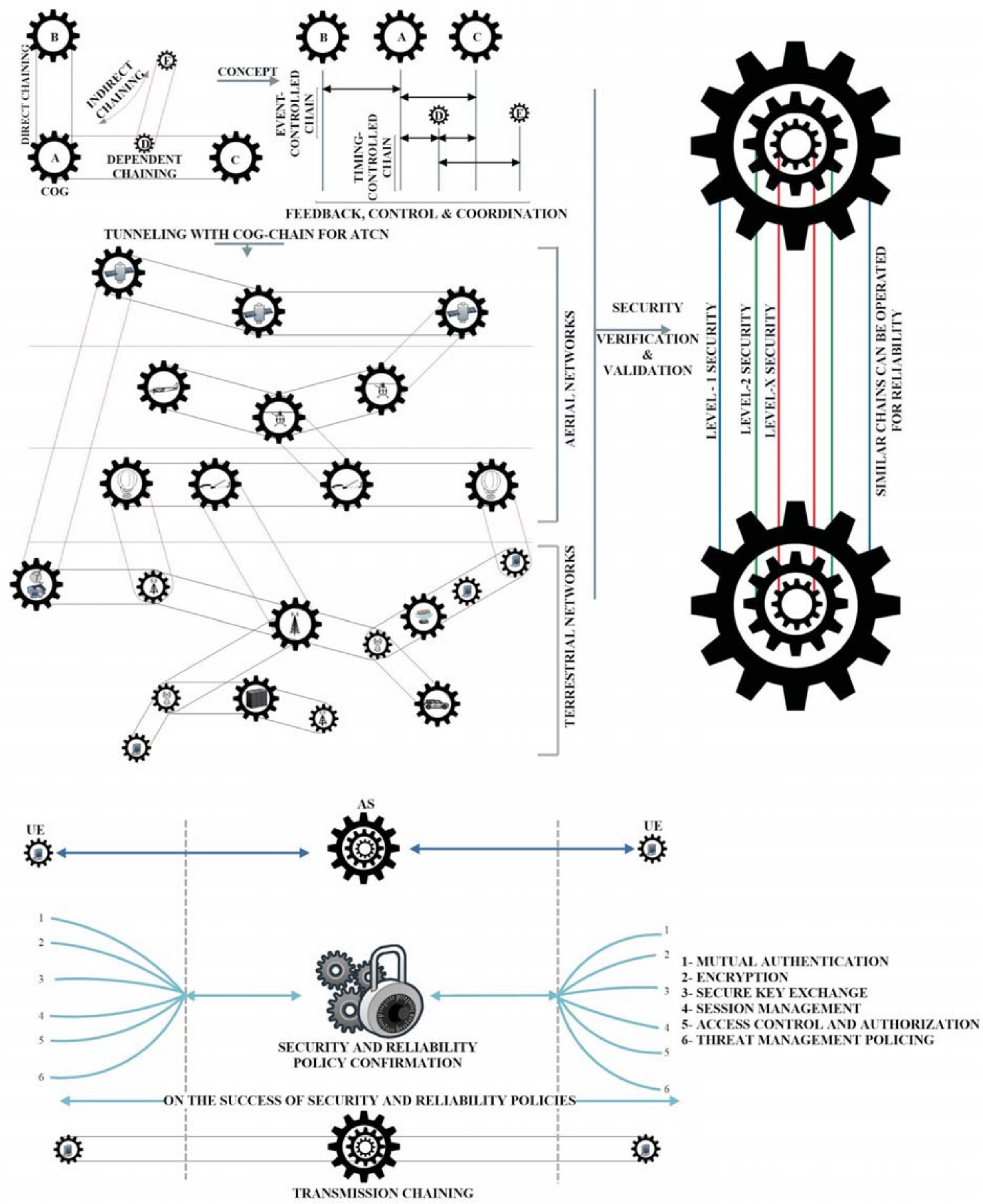


FIGURE 2. A detailed functional illustration of the proposed cog-chain concept for multi-layer security and reliable transmission in hierarchical networks.

– Event-controlled chains: When the number of properties in a network is controlled by the occurrence of an event and the chains appear or disappear through event marking, the type of chains is event-controlled. Various events that control the cog-chain can include a failure of a node, introduction of new rules, failures in security validations, excessive load, etc.

In addition to these, sub-classification can also be done on the formation of chains through sub-properties like flow control, access management; however, such a classification is beyond the scope of this article.

B. TYPES OF CONNECTIONS

The cog chaining helps to perform transmissions by authorizing each entity in the network and defining connections for access control and management. Based on the type of linking, the chaining process can be classified into following types[2]:

- Direct chaining: When two or more cogs have a direct connectivity between them and their transmissions are followed by simple handshakes, the type of chaining is termed as direct chaining.
- Indirect chaining: When two or more cogs depend on each other, but there is no direct chain between them due to a difference in types of properties, the type of chaining is termed as indirect chaining.
- Dependent chaining: When a cog operate as an intermediate between the two cogs while leveraging the services of other cogs, the type of chaining is termed as dependent chaining.

C. SELECTION OF TRANSPORTERS AND TUNNELING

The chains are the mode of transmissions, but these are virtual, thus, it becomes important to decide the components which will act as a transporter in the developed cog-chain system and tunneling can be used for connecting entities while enhancing the privacy of network. In general cog-chain, a transporter's role can be played by a process, function, base stations, servers, or gateways with multiple chains for a different set of incoming and outgoing requests. The inclusion of proxy servers can also help to disguise the active transporters in the network and can prevent the flow of information.

D. POLICIES AND PROCESS

Mode of operations is governed by the policies defined for connectivity between the cogs. Different solutions can be opted to decide the links between the cogs such as optimization principles [40], threshold procedures, fuzzy-rules [41], mobility protocols [42], and even architectural dependencies can be used for governing the policies in cog-chains. The processes available in cog-chains are divided into the following three categories:

- Feedback: This helps to operate the network while improving on the issues listed by the cogs. Feedbacks are obtained through logs based on the operations of each entity.
- Control: This helps to manage the policies which help to prevent any mismanagement of cogs, threat analysis, and introduces checks on the information-flow across the network.
- Coordination: This helps to define policies on how and on what basis two or more cogs collaborate. It also decides the common properties for combining cogs while generating a desirable output.

E. SECURITY AND RELIABILITY LAYERING

Cog-chain is responsible for managing security and reliability in a multi-layer network by defining policies for each cog. As stated earlier, each cog operates on a particular property and failure to support it helps to define reasons for an entity to deny connectivity. Cog-chain allows low-complex security and reliability verification by simple matching of operational rules. It also uses feedback, control and coordination policies to validate the entire network. For security, only those entities which possess similar property-interest and levels of security and reliability are authorized for connections. Sub-entities, which depend on the authentication of other major entities, are allowed to participate through dependent chaining. Entities which have a high risk of vulnerability, but are crucial to operating, are always connected through indirect mapping. The authentication through an Authentication Server (AS) is done by direct chaining, while the protocol for mutual communication is specific to the application and the scenario. The number of sub-cogs decides the level of security and reliability to be satisfied by each entity before possessing the virtual chain for participation. Only those entities, which satisfy the laid requirements with other entities, as well as the AS, are allowed to transmit leading a way to the formation of a secure and reliable network. Errors and unmatched policies help to maintain logs which are used for verification and validation procedures.[3] Once the nodes are authorized and pass the security requirements of the AS, the network is capable of operating towards the secure and reliable resource allocation and content caching in ATCNs.

VII. COG-CHAIN BASED RESOURCE ALLOCATION AND CONTENT CACHING IN ATCNS

A3C and G3C are responsible for managing activities related to caching whereas resource allocation is done by any entity which possesses more chains in a given layer of the network.[4] Resource allocation is performed based on current-demands of the network and usually, the load is considered as an observable entity which can be shared amongst the nodes. In the given system, the nodes with more number of requests are offloaded with priority provided they have a minimum number of direct mappings. In addition, the load on the cogs with a maximum number of sub-cogs must be minimum, which is similar to making lesser requests to a server with a maximum degree of connectivity as it serves as an important point in connecting the nodes, especially in a multi-layer setup. Further, the cogs with multiple sub-cogs should be allocated load in an ascending order to allow resource sharing at limited security controls.

[2] The type of chains helps to understand the path to be followed by the entities while authorizing each other for a possession of their services.

[3] The details on the verification and validation procedures are beyond the scope of this article and will be presented in future reports.

[4] Aerial CCS is observed through HAPS as these systems provide a fixed location which is key in the identification of a dynamic caching server.

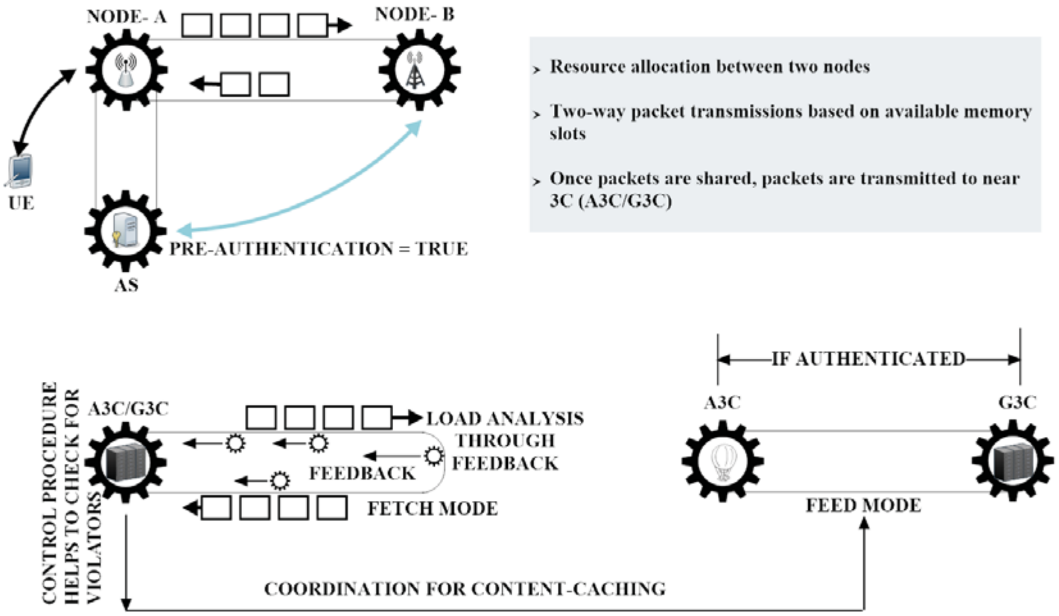

NODE- A
NODE- B
UE
AS
PRE-AUTHENTICATION = TRUE
› Resource allocation between two nodes
› Two-way packet transmissions based on available memory slots
› Once packets are shared, packets are transmitted to near 3C (A3C/G3C)
CONTROL PROCEDURE HELPS TO CHECK FOR VIOLATORS
A3C/G3C
LOAD ANALYSIS THROUGH FEEDBACK
FEEDBACK
FETCH MODE
IF AUTHENTICATED
A3C
G3C
FEED MODE
COORDINATION FOR CONTENT-CACHING

FIGURE 3. An illustration of detailed procedures of the proposed resource allocation and content caching through cog-chain. The figure shows communication between a UE and the node-A which operates with other node-B to check for resources and share the load to facilitate requests from incoming UE. This helps to manage excessive load in the network. Next, the three process policies and processes are demonstrated, which show how the fetch and feed modes are used for secure and reliable resource allocation and content caching.

If the security policies are increased, the load is allocated by following a dependent chaining and the content is shared with the cogs that already satisfied the security and reliability levels. In the absence of such a cog, the dominating cog, that first satisfies the security levels wins and is selected for transfers and load allocation.

It is recommended to have pre-fixed security levels with the A3C and G3C to ensure that there is no overhead while communicating with the Content-Caching Server (CCS). The content caching is performed over resource allocation by using cog-chains through following procedures:

- The content from the aerial network which is frequently requested by the UEs and aeronautical ad hoc users are available at both A3C and G3C depending on the lifetime of the requests.
- Once the network entities ensure the formation of a cog-chain, they also form a virtual chain with the CCS. If the policies are confirmed, caching is allowed and the requests for caching are submitted in feed and fetch mode. The feed mode is between the A3C and G3C in which the load is distributed on the basis of requesting entity. The frequent pages requested by the aerial nodes on aeronautical setup are fed to A3C and similar is performed for G3C to accommodate the requests coming from both drone-enabled as well as terrestrial setups. The fetch mode is for A3C and G3C to automatically update their history and logs while consistently checking the requests of their operational layer.
- Note that A3C and G3C also maintain cache as per their layered module and keep a record by making another cog-chain while supporting CCS through cog size. Here, cog size refers to the memory slots available at a cog for each chain. The chain for caching can be the connection or a particular application.

Content-caching through cog-chain helps to attain near user or edge-enabled caching which can considerably improve the performance of a network without compromising the security and maintaining the reliability of connections. All these details are provided through an easy to follow demonstration in Fig. 3, and the flow-chart depicting its procedures is presented in Fig. 4. Cog-chain is easier to implement and offers lightweight facilities for procedures related to authentication, access control, and authorization. Most of the devices in the network are considered to have a pre-established cog-chain at least with AS. This helps to easily accommodate requests from incoming entities without any further authentication. However, work is still needed in this direction and solutions are required to establish the core-security concepts, like mutual authentication, channel secrecy, and pre-shared keys, for cogs in cog-chain. For reliable and secure resource allocation and content-caching, it is required that a system must protect its feed and fetch operations. To do this, a cog-chain communication protocol (CCCP) is proposed in Fig. 5. This protocol is demonstrated for feed mode to cache contents between G3C and A3C. Similar operations can be extended to fit in the fetch mode as well. The details of this protocol are as follows:

- It is assumed that the initial principles of cog-chain ensure the formation of a secure channel between the G3C and AP, and between the BS (AS) and A3C.

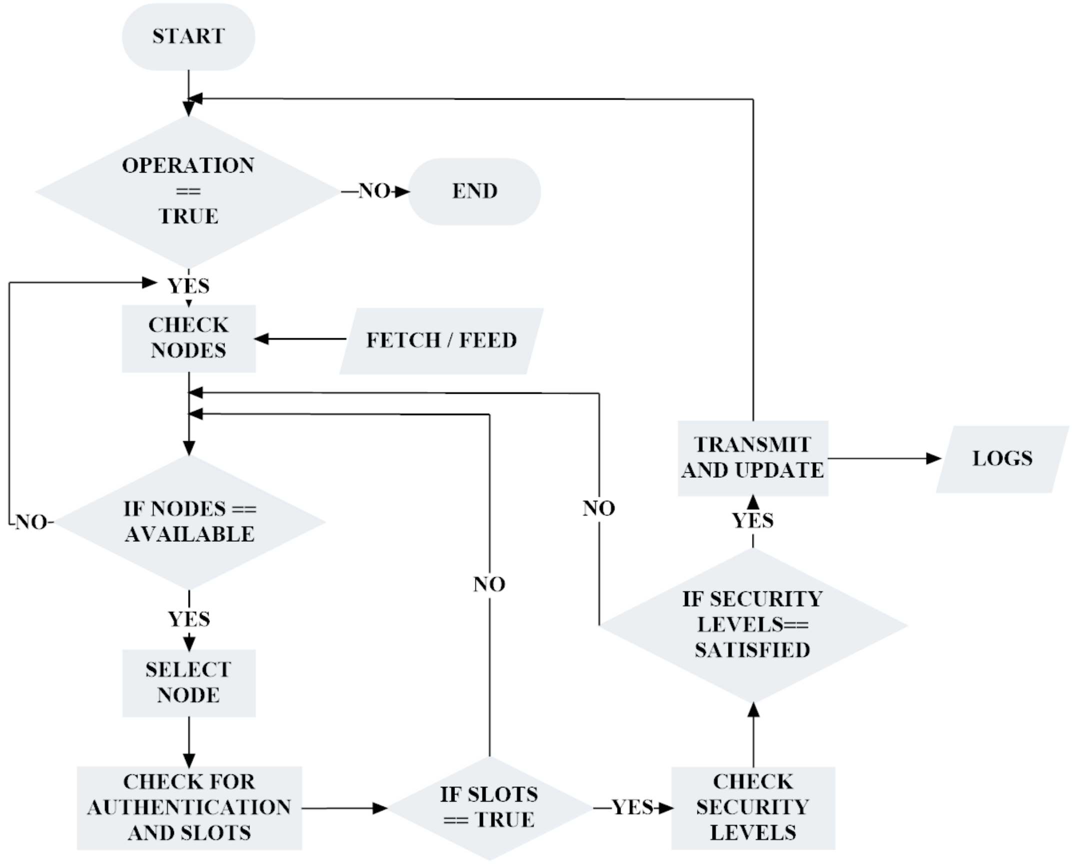


FIGURE 4. Cog-chain formation flow chart. The overall approach is demonstrated through the flowchart, which helps to understand the steps to be followed for facilitating cog-chains for secure and reliable content-sharing.

The crucial entities AP and BS have a pre-shared key K_{AP-BS} to secure their communication. Each cog-chain formed between these entities are marked with pseudo-ID as $\mathrm{CID}_1, \mathrm{CID}_2$ and CID_3. In order to mark the level of security guaranteed by these cog-chains as per the initial definition and principles, these IDs can be marked as CID_1^R, where R helps to determine the number of features. In such a case, cogs which possess similar R or its requested property can communicate while others have to build a virtual chain for communication. The channel security for each property is assumed through Advanced Encryption Standard (AES), while message protection is performed through a Hash Message Authentication Code (HMAC).

- Once the initial steps are finalized, and G3C has content to feed to A3C, it sends the (REQ_TO_FEED, A3C) message to AP, which asks for a presence of A3C in the nearby hierarchy to BS by using (CONF_VERIF_REQ, A3C) message.
- BS checks the database and sends the availability message to AP (AVAILABLE(N_{A3C}, ID_1, CID_3), which includes the network ID of A3C, a pseudo ID to be used for A3C, and the cog-chain ID between the BS and A3C. Note that CID_3 can further be divided into multiple routes, but the involved entities are unsure of such division, which helps to maintain the anonymity of the node as well as its route. Next, BS sends a READY message to A3C containing its pseudo ID (ID_1) and time stamp T_0. In addition, AP sends the confirmation message to G3C (CONFIRM_A3C, ID_1, SK_1, ID_2, CID_3), which includes a shared key generated through K_{AP-BS}, which helps to secure messages through HMAC operations. The message also contains the pseudo-ID of G3C and cog-chain details.
- Following this, AP sends the shared key to A3C along with details of the pseudo ID of transmitting G3C, which begins establishing the path through a decision message which is encrypted with a new timestamp. The message is decrypted at the A3C and verified for its content. Once verified, A3C also shares its decision on chaining and sends a similar message to G3C by using encryption. On approval, a virtual cog-chain is established between the two entities which are used for content-caching until the difference of time-stamps.

The CCCP can be operated for longer duration without re-establishing the virtual cog-chain by using Public Key Infrastructure (PKI), such as sending a Diffie-Hellman key in the decision to establish a long-term security between

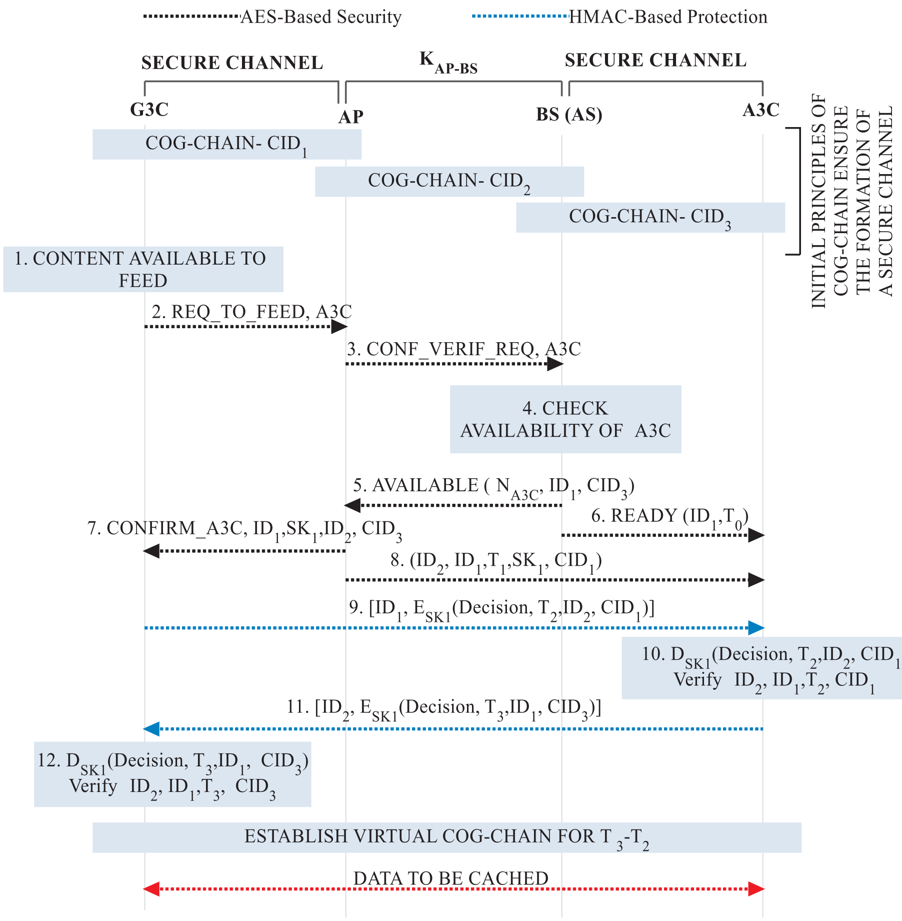

AES-Based Security
HMAC-Based Protection
SECURE CHANNEL
K_{AP-BS}
SECURE CHANNEL
G3C
AP
BS (AS)
A3C
COG-CHAIN- CID_1
COG-CHAIN- CID_2
COG-CHAIN- CID_3
INITIAL PRINCIPLES OF COG-CHAIN ENSURE THE FORMATION OF A SECURE CHANNEL
1. CONTENT AVAILABLE TO FEED
2. REQ_TO_FEED, A3C
3. CONF_VERIF_REQ, A3C
4. CHECK AVAILABILITY OF A3C
5. AVAILABLE (N_{A3C}, ID_1, CID_3)
6. READY (ID_1,T_0)
7. CONFIRM_A3C, ID_1,SK_1,ID_2, CID_3
8. (ID_2, ID_1,T_1,SK_1, CID_1)
9. [ID_1, E_{SK1}(Decision, T_2,ID_2, CID_1)]
10. D_{SK1}(Decision, T_2,ID_2, CID_1) Verify ID_2, ID_1,T_2, CID_1
11. [ID_2, E_{SK1}(Decision, T_3,ID_1, CID_3)]
12. D_{SK1}(Decision, T_3,ID_1, CID_3) Verify ID_2, ID_1,T_3, CID_3
ESTABLISH VIRTUAL COG-CHAIN FOR T_3-T_2
DATA TO BE CACHED

FIGURE 5. Cog-chain communication protocol for A3C and G3C content caching via Feed mode.

the servers. However, such an operation is computationally expensive, and given the fact that A3C can be a dynamic node, the availability of CCS becomes a challenge for such (PKI) operations.

VIII. PERFORMANCE EVALUATION

The proposed cog-chain for ATCN ensures reliable and secure resource allocation and content caching. However, to evaluate the performance-security tradeoff, a simulation study is presented in two parts. The first part analyzes the signaling overheads, computational time complexity, and reliability of forming a cog-chain and enabling communications in feed and fetch modes of the proposed approach. The second part compares the proposed approach with the general operative blockchain model and sequential-verification model with a variation in the number of layers when applied to ATCNs. The details of the parameters used in the evaluations are given in Table 2.

A. EVALUATION: PART I (NUMERICAL OBSERVATIONS)

The main task is to set up the cog-chain to start the procedures of secure and reliable resource allocation and content caching. The signaling overheads ($\mathcal{O}_s$) are evaluated by using model from [43] and calculated as $\frac{\mathcal{H}\times\mathcal{Q}}{\tau} + \frac{(\mathcal{H}-1)\times\mathcal{Q}}{\tau} + \frac{(\mathcal{A}-1)\times(\mathcal{H}')\times\mathcal{Q}}{\tau}$ and $\frac{\mathcal{H}\times\mathcal{Q}}{\tau} + \frac{(\mathcal{A}-1)\times(\mathcal{H}')\times\mathcal{Q}}{\tau}$ for feed and fetch modes, respectively. The value for hops ($\mathcal{H}$) is set at 10 between G3C and AP, $\mathcal{H}'$ at 1 between AP and BS, and at 10 between BS and A3C; message size ($\mathcal{Q}$) is set at 66 bytes, and number of addresses ($\mathcal{A}$) and stay time (τ) varies w.r.t. involved entities. The results, as shown in Fig. 6, present that feed mode causes 45.2% more overheads as the

TABLE 2. Parameter Configurations.

Parameter	Value	Description
$\mathcal{Q}$	66 bytes	Message size
$\mathcal{H}$	10	Number of hops
$\mathcal{A}$	4	Number of addresses
$\mathcal{H}'$	1	Intermediate hops
τ	5 to 50 s	Stay time of an aerial node
$\mathcal{P}$	6	Number of passes or links
$\mathcal{T}$	5 ms	Signaling time
τ_{LoS}	10 ms	Time to acquire LoS
τ_{E-D}	1 to 10 ms	Time to perform encryption/decryption
α_0	10	Initial resource value
η	1% to 3%	Request handling rate
K	6	Number of cog-chains

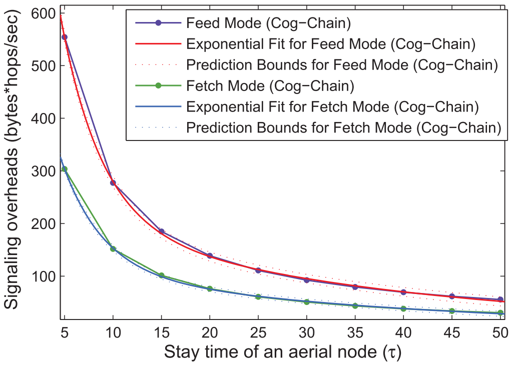


FIGURE 6. Signaling overheads vs. stay time of an aerial node.

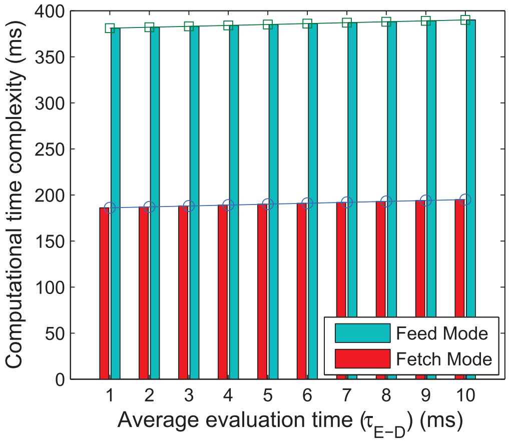


FIGURE 7. Computational time complexity vs. average evaluation time of encryption/decryption messages.

initiations are host-based compared with the fetch mode, which operates with a minimum signaling overhead of 30.36 and a maximum of 303.6 bytes*hops/sec with a varying stay time.

The computational time complexity is calculated as $\sum_{i=1}^{\mathcal{P}} (\mathcal{H}.\mathcal{T}.\mathcal{J})_i + \tau_{LoS} + \tau_{E-D}$, where $\mathcal{P}$ is the number of passes, which include, $\mathcal{P}_{G3C-AP}$, $\mathcal{P}_{G3C-BS}$, $\mathcal{P}_{G3C-A3C}$, $\mathcal{P}_{AP-BS}$, $\mathcal{P}_{AP-A3C}$ and $\mathcal{P}_{BS-A3C}$; $\mathcal{T}$ is signaling time, which is set at 5 ms for all passes, $\mathcal{J}$ is the number of messages (incoming/outgoing messages in CCCP) between the passes, τ_{LoS} is the time to acquire LoS and is set at 10 ms, and τ_{E-D} is the evaluation time including encryption and decryption processes and is varied to check the performance as shown in Fig. 7. The results show that the feed mode takes 50.5% more time to establish a cog-chain compared with the fetch mode, which operates in a range between 186 ms and 195 ms for a varying τ_{E-D}. The results in Fig. 8 help to understand the reliability of connectivity for cog-chain in both feed and fetch modes, where reliability is calculated as $\frac{\tau \times \psi_r}{1+(\tau-1)\psi_r}$ and ψ_r is the reliability coefficient equal to $\frac{\mathcal{H}}{\mathcal{H}-1}(1 - \frac{1}{(1+\frac{\mathcal{H}\mathcal{Q}}{\mathcal{O}_s})})$. The results suggest that the stay time of the aerial vehicle impacts the reliability and it increases as an aerial node stays for a longer duration in a particular zone.

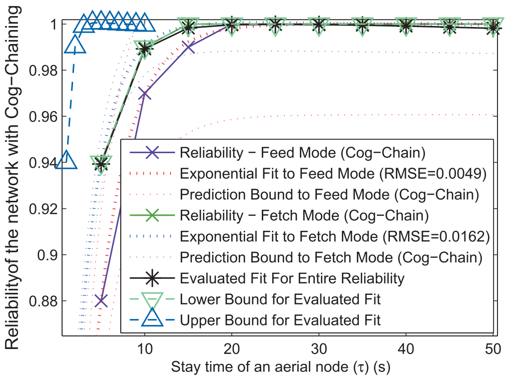


FIGURE 8. Reliability of operations for the cog-chain in feed and fetch mode vs. stay time of an aerial node.

B. EVALUATION: PART II (SYSTEM-LEVEL OBSERVATIONS)

The proposed approach relies on the combination of security solutions, which form the levels of the cog-chain and help to attain secure and reliable content-caching as well as resource allocation. The reliability is traceable from the earlier evaluations in Fig. 8. However, it is difficult to simulate the security as the adversaries in real time cannot be replicated to a system-level environment. Thus, to show the impact of the proposed solution, it is compared with the general blockchain operations and sequential-verification model between the two nodes. The observations are presented for the operational time and the impact of signaling time on the overall performance of the system. It is to be noted that in the cog-chain, the number of levels and the underlying protocols for mutual authentication and another layered phenomenon decide the performance of the network. In the blockchain-based network formation, the two nodes roughly consume 2.5 minutes to 10 minutes of timing cycles to accommodate a secure transaction between them as available in [44]. Although, there is no crisp system to detect its actual cost of operation, for ATCNs it is expected to increase because the stay time of a node is very less in a particular zone and probability of connectivity between aerial nodes after this much time is negligible. On the contrary, the cog-chain uses CCCP for connecting entities, and thus, the overall cost is the sum of timings utilized for mutual authentication and CCCP operations. In the result evaluations, Elliptical Curve Digital Signature Algorithm (ECDSA) is used for mutual authentication with a timing of 3180 ms [45]. In the case of sequential-verification, once the initial connection is established, the cost of operations is calculated as a sum of cycles consumed for each layer, which is usually very high compared to the cog-chain. The results for operational cost can be followed in Table 3.

Security procedures do affect the performance of a system. However, with the inclusion of proper steps, the performance of the system can be balanced and the network can be operated in a much reliable environment. To understand the feasibility and performance of the proposed cog-chain model, the comparisons of resource allocation growth are presented

TABLE 3. Operational cost (ms) comparison of cog-chain, sequential-verification and blockchain for communications between two nodes.

Operational Cost (ms)	Cog-chain (feed mode)	Cog-chain (fetch mode)	Sequential (feed mode)	Sequential (fetch mode)	Blockchain
Lower Limit	3561	3366	21366	20196	150000
Upper Limit	3570	3375	21420	20250	600000

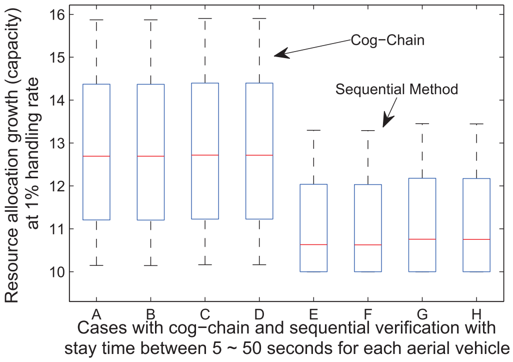


FIGURE 9. Resource allocation growth at 1% request handling rate vs. stay time of an aerial node for cog-chain and sequential-verification method. A: Cog-chain at lower feed time, B: Cog-chain at higher feed time, C: Cog-chain at lower fetch time, D: Cog-chain at higher fetch time, E: Sequential at lower feed time, F: Sequential at higher feed time, G: Sequential at lower fetch time, H: Sequential at higher fetch time.

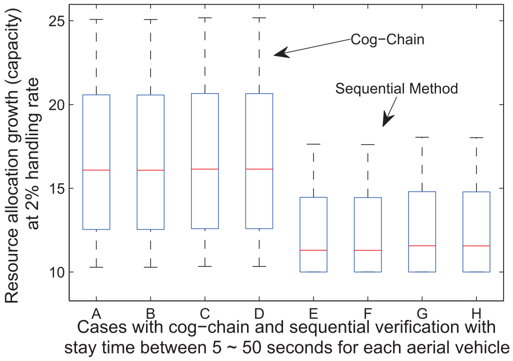


FIGURE 10. Resource allocation growth at 2% request handling rate vs. stay time of an aerial node for cog-chain and sequential-verification method. A: Cog-chain at lower feed time, B: Cog-chain at higher feed time, C: Cog-chain at lower fetch time, D: Cog-chain at higher fetch time, E: Sequential at lower feed time, F: Sequential at higher feed time, G: Sequential at lower fetch time, H: Sequential at higher fetch time.

with the sequential-verification model, which operates similar to cog-chain, but without any multi-hierarchal support for security features. This resource allocation growth (following the exponential growth [46] principle) is calculated as $\alpha_0\,(1+\eta)^{T_{useful}}$, where α_0 is the initial resource value, η is the request handling rate and T_{useful} is the useful time which is consumed for handling requests. It is calculated as a difference of the stay time and the algorithmic procedures of the respective approach. The results for resource allocation growth at 1%, 2%, and 3% request handling rate are shown in Fig. 9, Fig. 10, and Fig. 11, respectively. The average comparisons of these observations can be further studied in Fig. 12.

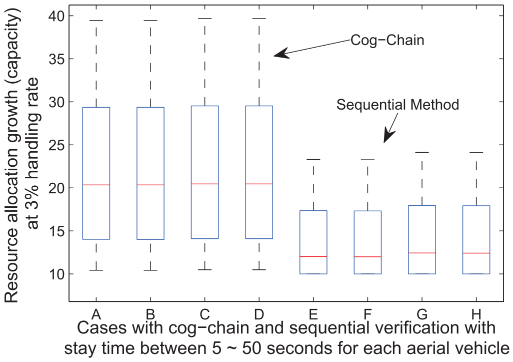


FIGURE 11. Resource allocation growth at 3% request handling rate vs. stay time of an aerial node for cog-chain and sequential-verification method. A: Cog-chain at lower feed time, B: Cog-chain at higher feed time, C: Cog-chain at lower fetch time, D: Cog-chain at higher fetch time, E: Sequential at lower feed time, F: Sequential at higher feed time, G: Sequential at lower fetch time, H: Sequential at higher fetch time.

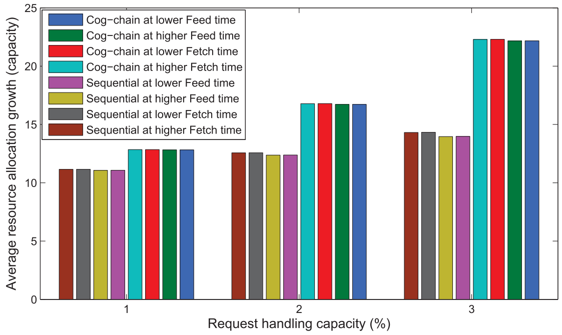
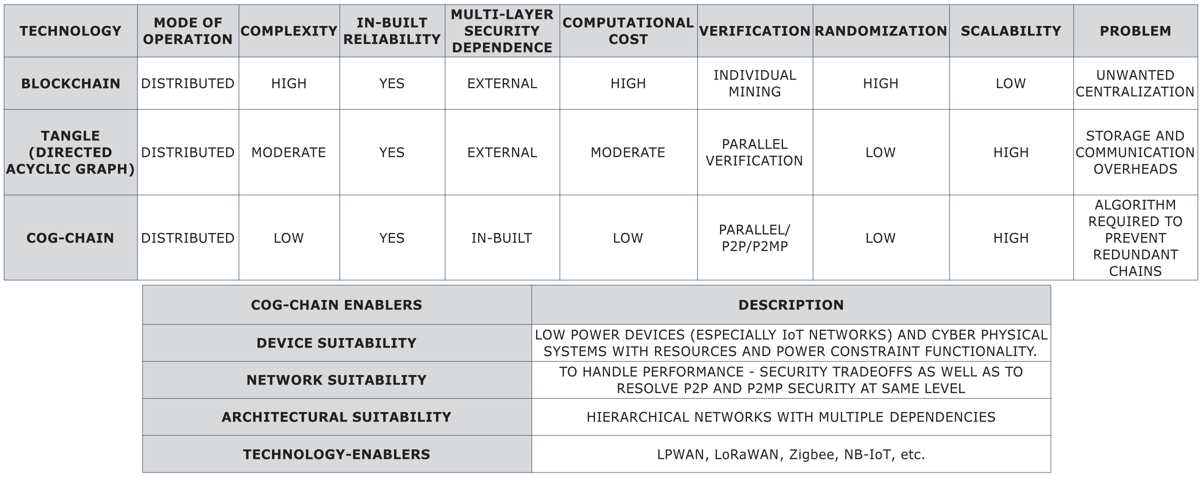


FIGURE 12. Average resource allocation growth comparison between the cog-chain and the sequential method vs. request handling rate for different timings of feed and fetch operations.

These results suggest that the lower fetch operation time offers better resource allocation than the feed operations, and collectively both these operations provide better resource allocation growth in comparison with the sequential- verification model. These results suggest that with the use of the cog-chain model, the resource allocation growth in ATCNs can be improved by 27.64% and 26.73% through only fetch and feed mode, respectively; and collectively the resource allocation growth improves by 27.17%, as shown in Fig. 12. Furthermore, it is to be noted that the general operations in blockchain consume sufficiently high time and no aerial node (unless configured rotor-wing) is expected to stay at a location for such a duration, which makes it unsuitable for ATCNs. However, with advanced topological solutions, blockchains can also be accommodated; but such verification is beyond the scope of this article.



TECHNOLOGY	MODE OF OPERATION	COMPLEXITY	IN-BUILT RELIABILITY	MULTI-LAYER SECURITY DEPENDENCE	COMPUTATIONAL COST	VERIFICATION	RANDOMIZATION	SCALABILITY	PROBLEM
BLOCKCHAIN	DISTRIBUTED	HIGH	YES	EXTERNAL	HIGH	INDIVIDUAL MINING	HIGH	LOW	UNWANTED CENTRALIZATION
TANGLE (DIRECTED ACYCLIC GRAPH)	DISTRIBUTED	MODERATE	YES	EXTERNAL	MODERATE	PARALLEL VERIFICATION	LOW	HIGH	STORAGE AND COMMUNICATION OVERHEADS
COG-CHAIN	DISTRIBUTED	LOW	YES	IN-BUILT	LOW	PARALLEL/ P2P/P2MP	LOW	HIGH	ALGORITHM REQUIRED TO PREVENT REDUNDANT CHAINS

COG-CHAIN ENABLERS	DESCRIPTION
DEVICE SUITABILITY	LOW POWER DEVICES (ESPECIALLY IoT NETWORKS) AND CYBER PHYSICAL SYSTEMS WITH RESOURCES AND POWER CONSTRAINT FUNCTIONALITY.
NETWORK SUITABILITY	TO HANDLE PERFORMANCE - SECURITY TRADEOFFS AS WELL AS TO RESOLVE P2P AND P2MP SECURITY AT SAME LEVEL
ARCHITECTURAL SUITABILITY	HIERARCHICAL NETWORKS WITH MULTIPLE DEPENDENCIES
TECHNOLOGY-ENABLERS	LPWAN, LoRaWAN, Zigbee, NB-IoT, etc.

FIGURE 13. **Related technologies, comparison and key enablers for cog-chain networks.**

From these results and discussions, it can be evidently concluded that the cog-chain offers a variety of hierarchical security solutions while establishing reliable connections which can be applied to a large variety of problems related to distributed networks. However, the work is yet in its initial phase and the solutions are to be thoroughly analyzed while leveraging on the latest technologies for real-time evaluations.

IX. RELATED TECHNOLOGIES AND OPEN ISSUES

Cog-chain can be related to solutions like blockchain [47], tangle [48], etc., on the basis of their role and type of solutions obtained from them, as shown in Fig. 13. Cog-chain is suitable for network operating at low and budgeted resources by consuming lesser overheads and storage. However, there are certain issues to be resolved for using cog-chain technology in much efficient, truly secure and highly reliable resource allocation and content-caching in ATCNS. These include,

- Real-time cog chaining: Despite being controlled by timing slots or an event, there are still some works required to define policies which can extend the operations of cog-chain to a real-time scenario. It is a conceptual work at the moment, which has to be verified through hardware-deployment, especially ATCNs, which involves highly dynamic nodes.
- Unified API and Accessibility: This is an open issue for cog-chains as there is no fixed standard or tool, which can be deployed for ensuring accessibility to nodes in ATCNs and there is a need for a unified API, which can establish cog-chains on-demand.
- Algorithms for Redundant Chain: ATCNs possess nodes which are mostly mobile and often change their locations, which may result in redundant chains between the same entities. Algorithmic solutions are required to avoid such issues and prevent networks from unnecessary computational overheads.
- Group-Authentication: ATCNs can be facilitated through group authentication for similar kinds of devices based on their location and operability. At the moment, such a concept is not considered in the proposed work and left for our future reports.
- Cog-failures and De-registration: Survivability and scalability are the key components of solutions which aim to support reliable and secure resource allocation and content-caching. In addition to the works presented in this paper, strategies should be developed to prevent the network from uncertain failures and also provide a competent solution for de-registration of virtually build cog-chains without allowing any information leakage.

X. CONCLUSION

This paper presented cog-chain, a novel paradigm, for secure and reliable resource allocation and content-caching in Aerial-Terrestrial Cloud Networks (ATCNs). The proposed approach was illustrated for its layer-wise security especially in hierarchical networks and presented with different sets of ideologies for achieving a reliable communication. In addition, various requirements, key concepts, and issues with ATCNs were also presented along with basic concepts to establish cog-chain in the networks. Feed and fetch modes were used depending on the involved entities and caching servers. A novel Cog-Chain Communication Protocol (CCCP) was also presented which helps to evaluate the formation of a virtual cog-chain between the nodes and the content servers.

The numerical analysis and system-based evaluations were used to prove the effectiveness of the proposed model. The results show that the proposed approach operates with a minimum signaling overhead of 30.36 bytes*hops/sec and a maximum of 303.6 bytes*hops/sec with the formation time between 186 and 195 ms. The overall time consumption is 83.33% lower than the sequential-verification model and the resource allocation growth is 27.17% better than the sequential-verification model, where fetch and feed modes improve it by 27.64% and 26.73%, respectively. These results show that the cog-chain possesses the ability to secure the processes associated with the resource allocation and can offer reliable content-caching with lower overheads and lesser computational complexity. Additionally, the technology comparisons and its core-ideology suggest that the cog-chain can be used in resolving different problems associated with the hierarchical and integrated networks.

REFERENCES

[1] H. Yao, L. Wang, X. Wang, Z. Lu, and Y. Liu, ''The space-terrestrial integrated network: An overview,'' *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 178–185, Sep. 2018, doi: 10.1109/MCOM.2018.1700038.

[2] T. Yu, X. Wang, J. Jin, and K. McIsaac, ''Cloud-orchestrated physical topology discovery of large-scale IoT systems using UAVs,'' *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 2261–2270, May 2018.

[3] Q. Wu, Y. Zeng, and R. Zhang, ''Joint trajectory and communication design for multi-UAV enabled wireless networks,'' *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 2109–2121, Mar. 2018.

[4] J. Chen, Q. Wu, Y. Xu, Y. Zhang, and Y. Yang, ''Distributed demand-aware channel-slot selection for multi-UAV networks: A game-theoretic learning approach,'' *IEEE Access*, vol. 6, pp. 14799–14811, 2018.

[5] E. Teller, R. W. DeVaul, C. L. Biffle, J. Weaver, and A. V. Staaf, ''Valuation of and marketplace for inter-network links between a high-altitude network and terrestrial network,'' U.S. Patent 15 679 145, Jan. 18, 2018.

[6] T. Li, H. Zhou, H. Luo, and S. Yu, ''SERvICE: A software defined framework for integrated space-terrestrial satellite communication,'' *IEEE Trans. Mobile Comput.*, vol. 17, no. 3, pp. 703–716, Mar. 2018.

[7] Y. Sun, D. W. K. Ng, D. Xu, L. Dai, and R. Schober. (2018). ''Resource allocation for solar powered UAV communication systems.'' [Online]. Available: https://arxiv.org/abs/1801.07188

[8] M. Chen, W. Saad, and C. Yin. (2018). ''Liquid state machine learning for resource and cache management in LTE-U unmanned aerial vehicle (UAV) networks.'' [Online]. Available: https://arxiv.org/abs/1801.09339

[9] D. Xu, Y. Sun, D. W. K. Ng, and R. Schober. (2018). ''Robust resource allocation for UAV systems with UAV jittering and user location uncertainty.'' [Online]. Available: https://arxiv.org/abs/1809.03706

[10] J. Li and Y. Han, ''Optimal resource allocation for packet delay minimization in multi-layer UAV networks,'' *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 580–583, Mar. 2017.

[11] H. Wang, J. Wang, G. Ding, L. Wang, T. A. Tsiftsis, and P. K. Sharma, ''Resource allocation for energy harvesting-powered D2D communication underlaying UAV-assisted networks,'' *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 14–24, Mar. 2018.

[12] J. Baek, S. I. Han, and Y. Han, ''Optimal resource allocation for non-orthogonal transmission in UAV relay systems,'' *IEEE Wireless Commun. Lett.*, vol. 7, no. 3, pp. 356–359, Jun. 2018.

[13] R. Fan, J. Cui, S. Jin, K. Yang, and J. An, ''Optimal node placement and resource allocation for UAV relaying network,'' *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 808–811, Apr. 2018.

[14] L. Zhang, Z. Zhao, Q. Wu, H. Zhao, H. Xu, and X. Wu, ''Energy-aware dynamic resource allocation in UAV assisted mobile edge computing over social Internet of vehicles,'' *IEEE Access*, vol. 6, pp. 56700–56715, 2018.

[15] M. Chen, M. Mozaffari, W. Saad, C. Yin, M. Debbah, and C. S. Hong, ''Caching in the sky: Proactive deployment of cache-enabled unmanned aerial vehicles for optimized quality-of-experience,'' *IEEE J. Sel. Areas Commun.*, vol. 35, no. 5, pp. 1046–1061, May 2017.

[16] V. Sharma, F. Song, I. You, and H.-C. Chao, ''Efficient management and fast handovers in software defined wireless networks using UAVs,'' *IEEE Netw.*, vol. 31, no. 6, pp. 78–85, Nov./Dec. 2017.

[17] G. Secinti, P. B. Darian, B. Canberk, and K. R. Chowdhury, ''SDNs in the sky: Robust end-to-end connectivity for aerial vehicular networks,'' *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 16–21, Jan. 2018.

[18] M. Gharibi, R. Boutaba, and S. L. Waslander, ''Internet of drones,'' *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[19] L. Wang, H. Yang, J. Long, K. Wu, and J. Chen, ''Enabling ultra-dense UAV-aided network with overlapped spectrum sharing: Potential and approaches,'' *IEEE Netw.*, vol. 32, no. 5, pp. 85–91, Sep./Oct. 2018.

[20] Q. Yang and S.-J. Yoo, ''Optimal UAV path planning: Sensing data acquisition over IoT sensor networks using multi-objective bio-inspired algorithms,'' *IEEE Access*, vol. 6, pp. 13671–13684, 2018.

[21] I. You, V. Sharma, M. Atiquzzaman, and K.-K. R. Choo, ''GDTN: Genome-based delay tolerant network formation in heterogeneous 5G using inter-UA collaboration,'' *PLoS ONE*, vol. 11, no. 12, p. e0167913, 2016.

[22] V. Sharma, F. Song, I. You, and M. Atiquzzaman, ''Energy efficient device discovery for reliable communication in 5G-based IoT and BSNs using unmanned aerial vehicles,'' *J. Netw. Comput. Appl.*, vol. 97, pp. 79–95, Nov. 2017.

[23] J. Sun, J. Tang, and S. Lao, ''Collision avoidance for cooperative UAVs with optimized artificial potential field algorithm,'' *IEEE Access*, vol. 5, pp. 18382–18390, 2017.

[24] I. Guvenc, ''Interference and mobility management in UAV-assisted wireless networks,'' U.S. Patent 15 443 147, Jun. 15, 2017.

[25] X. Chen, X. Li, D. Guo, and J. Grosspietsch, ''Resource allocation in public safety broadband networks with rapid-deployment access points,'' *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1660–1671, Feb. 2018.

[26] M. Chen, W. Saad, and C. Yin. (2018). ''Echo-liquid state deep learning for 360° content transmission and caching in wireless VR networks with cellular-connected UAVs.'' [Online]. Available: https://arxiv.org/abs/1804.03284

[27] F. Zhou, Y. Wu, Y.-C. Liang, Z. Li, Y. Wang, and K.-K. Wong, ''State of the art, taxonomy, and open issues on cognitive radio networks with NOMA,'' *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 100–108, Apr. 2018.

[28] V. Sharma, R. Kumar, and R. Kaur, ''UAV-assisted content-based sensor search in IoTs,'' *Electron. Lett.*, vol. 53, no. 11, pp. 724–726, May 2017.

[29] X. Wang, M. Chen, T. Taleb, A. Ksentini, and V. C. M. Leung, ''Cache in the air: Exploiting content caching and delivery techniques for 5G systems,'' *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 131–139, Feb. 2014.

[30] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, ''Drone small cells in the clouds: Design, deployment and performance analysis,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[31] S. A. R. Naqvi, S. A. Hassan, H. Pervaiz, and Q. Ni, ''Drone-aided communication as a key enabler for 5G and resilient public safety networks,'' *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 36–42, Jan. 2018.

[32] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovács, P. Mogensen, and M. Sorensen, ''Interference impact on coverage and capacity for low power wide area IoT networks,'' in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[33] T. Bai, A. Alkhateeb, and R. W. Heath, Jr., ''Coverage and capacity of millimeter-wave cellular networks,'' *IEEE Commun. Mag.*, vol. 52, no. 9, pp. 70–77, Sep. 2014.

[34] Y. Zhong, X. Ge, T. Han, Q. Li, and J. Zhang, ''Tradeoff between delay and physical layer security in wireless networks,'' *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1635–1647, Jul. 2018.

[35] R. Kirichek and V. Kulik, ''Long-range data transmission on flying ubiquitous sensor networks (FUSN) by using LPWAN protocols,'' in *Proc. Int. Conf. Distrib. Comput. Commun. Netw.* Cham, Switzerland: Springer, 2016, pp. 442–453.

[36] V. Sharma, I. You, G. Pau, M. Collotta, J. D. Lim, and J. N. Kim, ''Lorawan-based energy-efficient surveillance by drones for intelligent transportation systems,'' *Energies*, vol. 11, no. 3, p. 573, 2018.

[37] M. Bacco, L. Caviglione, and A. Gotta, ''Satellites, UAVs, vehicles and sensors for an integrated delay tolerant ad hoc network,'' in *Proc. Int. Conf. Pers. Satell. Services*. Cham, Switzerland: Springer, 2016, pp. 114–122.

[38] S. Moulik, S. Misra, and C. Chakraborty, ''Performance evaluation and delay-power trade-off analysis of ZigBee protocol,'' *IEEE Trans. Mobile Comput.*, vol. 18, no. 2, pp. 404–416, Feb. 2019.

[39] F. J. Velez *et al.*, ''Wireless sensor and networking technologies for swarms of aquatic surface drones,'' in *Proc. IEEE 82nd Veh. Technol. Conf. (VTC-Fall)*, Sep. 2015, pp. 1–2.

[40] F. Yang, P. Wang, Y. Zhang, L. Zheng, and J. Lu, ''Survey of swarm intelligence optimization algorithms,'' in *Proc. IEEE Int. Conf. Unmanned Syst. (ICUS)*, Oct. 2017, pp. 544–549.

[41] E. Bazhenova, S. Haarmann, S. Ihde, A. Solti, and M. Weske, ''Discovery of fuzzy DMN decision models from event logs,'' in *Proc. Int. Conf. Adv. Inf. Syst. Eng.* Cham, Switzerland: Springer, 2017, pp. 629–647.

[42] V. Sharma, R. Kumar, and N. Kumar, ''DPTR: Distributed priority tree-based routing protocol for FANETs,'' *Comput. Commun.*, vol. 122, pp. 129–151, Jun. 2018.

[43] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and energy-efficient handover in fog networks using blockchain-based DMM," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 22–31, May 2018, doi: 10.1109/MCOM.2018.1700863.

[44] M. Scherer, "Performance and scalability of blockchain networks and smart contracts," Ph.D. dissertation, Dept. Comput. Sci., Umeå Univ., Umeå, Sweden, 2017.

[45] T. Hu, J. Wang, G. Zhao, and X. Long, "An improved mutual authentication and key update scheme for multi-hop relay in Internet of Things," in *Proc. 7th IEEE Conf. Ind. Electron. Appl. (ICIEA)*, Jul. 2012, pp. 1024–1029.

[46] V. Stango and J. Zinman, "Exponential growth bias and household finance," *J. Finance*, vol. 64, no. 6, pp. 2807–2849, 2009.

[47] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018.

[48] S. Popov. (2017). *The Tangle*. Accessed: May 2, 2018. [Online]. Available: https://monbit.mn/wpcontent/uploads/2017/12/iota_whitepaper.pdf

VISHAL SHARMA (S'13–M'17) received the B.Tech. degree in computer science and engineering from Thapar University, in 2016, and the Ph.D. degree in computer science and engineering from Punjab Technical University, in 2012. He was with Thapar University as a Lecturer, in 2016. From 2016 to 2017, he was a Joint Postdoctoral Researcher with the MobiSec Lab, Department of Information Security Engineering, Soonchunhyang University, and Soongsil University, South Korea. He is currently a Research Assistant Professor with the Department of Information Security Engineering, Soonchunhyang University, South Korea. He has authored or co-authored more than 80 journal/conference articles and book chapters. His research interests include 5G networks, UAVs, estimation theory, and artificial intelligence. He serves as the Program Committee Member for the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. He was the TPC Member of ITNAC-IEEE TCBD'17 and serving as a TPC Member of ICCMIT'18, CoCoNet'18, and ITNAC-IEEE TCBD'18. He received three best paper awards from the IEEE International Conference on Communication, Management and Information Technology (ICCMIT), Warsaw, Poland, in 2017; from CISC-S'17 South Korea, in 2017; and from IoTaas, Taiwan, in 2017. He is the member of IEEE, a Professional Member of ACM, and a Past Chair for ACM Student Chapter-TU Patiala. He was the Track Chair of MobiSec'16 and AIMS-FSS'16, and a PC Member and Reviewer of MIST'16 and MIST'17, respectively. Also, he serves as a Reviewer for various IEEE Transactions and other journals.

ILSUN YOU (SM'13) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was with THIN Multimedia, Inc., Internet Security Co., Ltd., and Hanjo Engineering Co., Ltd., as a Research Engineer. He is currently an Associate Professor with the Department of Information Security Engineering, Soonchunhyang University. His current research interests include the Internet security, authentication, access control, and formal security analysis. He is a Fellow of the IET and a Senior Member of the IEEE. He has served or is currently serving as the main organizer of international conferences and workshops such as MobiWorld, MIST, SeCIHD, AsiaARES, and so forth. He is the Editor-in-Chief of the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. He is in the Editorial Board for *Information Sciences*, the *Journal of Network and Computer Applications*, the *International Journal of Ad Hoc and Ubiquitous Computing*, *Computing and Informatics*, the *Journal of High Speed Networks*, *Intelligent Automation & Soft Computing*, and *Security and Communication Networks*.

JUNG TAEK SEO received the Ph.D. degree in information security from the Graduate School of Information Security, Korea University, in 2006. From 2000 to 2016, he was with the National Security Research Institute as a Senior Researcher and the Head of the Infrastructure Protection Research Department. He is currently an Assistant Professor with the Department of Information Security Engineering, Soonchunhyang University. He has been a Principal Investigator of several government sponsored research project in SCADA, smart grid, and nuclear power plants. Recently, he has been actively working in the area of smart grid, in particular with respect to standard and policies. His research interests include SCADA, smart grid, nuclear power plants, smart city, and cyber physical system.

MOHSEN GUIZANI (S'85–M'89–SM'99–F'09) received the B.S. (Hons.) and M.S. degrees in electrical engineering and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He served in different academic and administrative positions at the University of Idaho, Western Michigan University, the University of West Florida, the University of Missouri–Kansas City, the University of Colorado Boulder, and Syracuse University. He is currently a Professor with the CSE Department, Qatar University, Qatar. He has authored nine books and more than 500 publications in refereed journals and conferences. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He is a Senior Member of ACM. He also served as a member, the Chair, and the General Chair for a number of international conferences. Throughout his career, he received three teaching awards and four research awards. He also received the 2017 IEEE Communications Society WTC Recognition Award and the 2018 AdHoc Technical Committee Recognition Award for his contribution to outstanding research in wireless communications and ad hoc sensor networks. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker and is currently the IEEE ComSoc Distinguished Lecturer. He serves on the editorial boards for several international technical journals and the Founder and an Editor-in-Chief of *Wireless Communications and Mobile Computing journal* (Wiley). He guest edited a number of special issues in IEEE journals and magazines. He is currently the Editor-in-Chief of the *IEEE Network Magazine*.