Socializing Drones for Inter-Service Operability in Ultra-Dense Wireless Networks using Blockchain

Vishal Sharma, Ilsun You*
Department of Information Security Engineering
Asan-si, The Republic of Korea
vishal_sharma2012@hotmail.com, ilsunu@gmail.com

Gokhan Kul
University at Buffalo, SUNY
Buffalo, New York
gokhanku@buffalo.edu

ABSTRACT
Ultra-dense wireless networks require on-demand nodes which can trust each other and relay information despite the difference in their service providers. This paper presents the secure utilization of drones as on-demand nodes for inter-service operability between multiple vendors by exploiting the features of the blockchain. Various components and strategies for driving blockchain-based drones are also presented. Further, this paper features the threat implications of the blockchain-based drones and compares the deployment issues with the centralized and traditional drone-assisted wireless networks.

CCS CONCEPTS
- Networks → Network reliability, Security, Management;

KEYWORDS
Security, UAVs, blockchain, drones, threats, ultra-dense networks.

1 INTRODUCTION
The widening of the spectrum has improved the capacity of ultra-dense wireless networks. However, these networks require efficient interference mitigation policies for their efficient utilization. These networks are much affected by the density of users and services [1]. Most of the modern day vendors have started using on-demand drones for pulling the services and supporting uplink/downlink facilities between the users and the base stations. However, scenarios with a large gathering are subject to different vendors and each vendor tries to maximize its facilities by deploying more and more nodes (drones) [2] [3] as shown in Fig. 1A. Maximizing resources is good, but it comes with various challenges such as identification of the location, channel selection, interference-management and the availability of the line of sight. One of the efficient solutions can be the sharing of user-side resources and connect them with the core by per service charging approach. This solution is efficient, but comes at the cost of trust and requires policies for inter-service operability between the drones of different service providers. If a centralized approach is used for trust management, it will increase the cost of the network as well as induce excessive overheads and cause much latency in services. An efficient solution can be obtained by utilizing the concept of the blockchain, which can ensure trust between the drones from different vendors and also provide strategic concepts for their coordination and inter-service operations.

1.1 Blockchain
A blockchain is the distributed approach for managing records in the form of electronic ledgers as shown in Fig. 1B. These ledgers are distributed to all the peers who can add or delete the records without overwriting. Blockchain operates by addressing its blocks via a public key and can be particularized by the use of private keys. It aims at making permissible, accessible and open ledgers which can be operated by the entities who maintain trust by themselves without any centralized node. The blockchain operates with a parent, main chain, and orphans. The key components and trust entities are the parent and main chain, while others are the minorities and hold less than 51% of total blocks [4] [5].

Blockchain provides secure applications in case of networks and also helps in maintaining trust between the dynamic entities, which otherwise makes trust evaluation an expensive and complex task. Some of the applications of blockchain are distributed transaction validation, user-site security, smart laws and contracts for message exchange, shared trust, supply chain management, hybrid group formation in complex tasks, and drone socializing [6] [7].

1.2 Socializing Drones
The social networks are often seen among the users, which interact at their will by utilizing the features of the application platform. Similar to these, such networks can be formed between the drones which also unites together to perform common task depending on the features and configurations of their vendors. Socializing refers to a mutual agreement between the vendors for using drones for a specific task and for a specific duration. Social formation between drones can be done by using a set of specific coordinating rules or
pre-configured policies. These policies are driven by the service agreement between the service providers.

2 INTER-SERVICE OPERABILITY WITH DRONES

Inter-service operability refers to the drone sharing between multiple vendors for serving users in a highly dense environment. Drones have to be operated with non-overlapping coordinates such that there is minimal interference in the network. For instance, consider a scenario of a stadium or public gathering. Now, for a huge amount of users demanding service at the same moment from different service providers, every vendor looks for an on-demand solution of front hauling for users to base stations. Now, considering the density of users as well as service demands, every vendor aims at deploying enough drones that can serve all the users without many overheads. Considering that the crowd is huge and there are multiple vendors aiming at the same solution, there is a high probability of interference, overlapping coordinates, channel blocking, and security. The network can fall apart because of all these issues. Thus, it is important to form a common solution or platform that can unite these aerial vehicles from multiple vendors. Further, to maintain a balance in the service agreement, it is required to support vendor cost without any fault or compensation issues. This can be done through drone-trial balancing sheets by following its per-service usage, load, transaction history and actual capacity. Thus, inter-service operability can be seen as one of the challenging issues for drones in ultra-dense wireless networks.

Handling users and allowing access to other vendor’s drones are issues of trust, control, and authority. A minute loophole in the security can expose the entire security procedures of a particular vendor. Also, if a non-trust worthy drone joins the network by any means, it can redirect the traffic causing business loss to vendors. Such issues are to be handled efficiently without depending on the centralized body as it may cause excessive overheads and slow down the immediate demands of a particular area.

As discussed earlier, blockchain can resolve this complex issue with much fewer overheads and low-complexity. Drones from different vendors can form an aerial blockchain, thus, leading to the formation of a social circle of drones.

2.1 Weighted-Blockchain based drones

Blockchain-based drones are operated with the concept of weights in the process of their socializing. A single blockchain is used for one region with drones from multiple vendors. All the drones are subject to blocks with required contextual information. These blocks are united into a single blockchain with weight as a paradigm for managing forks and control over the chain. The context includes the public keys for drones, which are visible to all, private keys for each vendor. The location allocation can be done during the beginning of network, and there are no specific re-configurations required in the network. The parent selection can be done during the beginning of network, and it changes as the drones change their positions or load is shifted across the drone network. The parent will change as the resources of a particular drone changes with time. The advantage of blockchain is that it is easier to shift controls whenever the parent node changes and there are no specific re-configurations required in the network. The trial-balance service sheets for drones and transaction histories are recorded by the parent node and distributed to all. In this way, all the vendors are aware of the current situation and there is no fool-playing in terms of excess service charges and over-loading.

Once the initial blockchain is formed between the drones of all the vendors, the next step is the selection of the parent node. This parent node controls the blockchain of drones and it is responsible for broadcasting information ledgers to all the communicating drones. The selection of parent is done by trivial rule of numbers. The vendor with the highest number of drones or highest load will control the blockchain and its marked drone will serve as the parent. The parent selection can be done during the beginning of network, and it changes as the drones change their positions or load is shifted across the drone network. The parent will change as the resources of a particular drone changes with time. The advantage of blockchain is that it is easier to shift controls whenever the parent node changes and there are no specific re-configurations required in the network. The trial-balance service sheets for drones and transaction histories are recorded by the parent node and distributed to all. In this way, all the vendors are aware of the current situation and there is no fool-playing in terms of excess service charges and over-loading.

Once the blockchain is initialized and selection of parent node is done, the next step is load balancing between the blocks. This is done by checking the actual allocated users and the true load a drone can handle. The load balancing is performed by checking the supremacy of each chain of a common blockchain. Whenever a differences is identified for any block, the locations are shifted and the network tries to balance the load. In an alternative case, more drones are deployed and a new block is attached to the currently operating blockchain. The load balancing can be done on the principle of optimization, such that at a given instance:

\[ L(t) \leq \max (L), \]

subject to

\[ \min (I), \]

and

\[ S(t) \leq \max (S), \]

where \( L \) is the load, \( I \) is the interference level, and \( S \) is the size of the overall blockchain. Now, if there are \( N \) number of vendors each having \( U \) number of drones and the total strength of the area is \( Q \), then at a time instance \( t \),

\[ \left( \frac{L(t)}{N(t)U(t)} \right) \leq \left( \frac{Q}{NU} \right). \]
The proposed model is secured by the principles of blockchain. In the cases where there is no majority in the proposed model, the current load includes the users, which play a crucial role in deciding the majority as well as assigning this is one of the important terms and conditions included in all side chains. The same parent helps to check the matching of rules for initiating and regulating transactions between the blocks. Drone-smart contracts allow the for- 

\[ \frac{L(t)}{U(t)} \rightarrow \text{min}, \quad (5) \]

and

\[ \frac{U_p(t)}{U(t) + U_2(t) + \cdots + U_N(t)} \times 100 \geq 51\%. \quad (6) \]

Here, \( U_p \) refers to one of the vendors holding the above equation true at any instance (by definition of blockchain [6]).

### 2.4 Security of drones

The proposed model is secured by the principles of blockchain. There is no centralized authentication mechanism as the public key is used by the drones for identifying each other. Apart from this, when the vendors mutually agree for providing services in a defined area, they also share the pool of secret keys which are the private keys for the drones to exchange load information while socializing. The vendors also have the ability to update the pool of private keys in the case of identification of possible threats. It is noticeable that the blockchain fits appropriately in socializing drones as these aerial vehicles need not depend on the centralized body for regulating trust. However, in order to further enhance the trust between the drones and vendors, a separate set of keys can be used for drones to vendor and drone to drone transactions.

The private keys play a role in accessing the broadcasted information, depending on the authorization and access. Currently, the security is achieved only by the initial concepts of the blockchain, however, in future, the drone blockchain can be operated towards the role-based access and authorization. Such scenarios will be much complicated but more secure. However, the performance tradeoff between the complexity of blockchain and security requirements needs to be studied further before proceeding in this direction.

### 2.5 Drone-smart contracts

Smart contracts are the backbone of blockchain and drive the trans- actions between the blocks. Drone-smart contracts allow the for- mation of rules for initiating and regulating transactions between the drones and the vendors. The proposed model relies on load bal- ancing and location policies for smart contracts. The drone-smart contract is responsible for eliminating any dominance from the unintended group of drones and also maintains the distributive nature of drone social networks in ultra-dense environments. The key components of drone smart contract are:

- **Coordinate Information:** The first part of the contract checks the coordinate information and makes sure that it is aligned with the initial configurations. At any time in the network, if a drone tries to socialize with the drone of another vendor, it makes sure that coordinate information is clearly stated in the block and it matches the configurations of the blockchain [9].

- **Same Parent:** All the drones in the blockchain obey the rule of same parent irrespective of their belongings to a particular vendor. The length of the chain is considered from parent and parent is included in all side chains. The same parent helps to check the majority of the blockchain and decide who will control the blockchain.

- **Current Load:** This is one of the important terms and conditions in the formation of the drone-smart contract. The current load plays a vital role in deciding the majority as well as assigning the weights to the blocks. As discussed in the initial part of the proposed model, the current load includes the users, which form the weighted-blockchain. In the cases where there is no majority in a blockchain, weights help to identify the parent and balance the load.

- **Vendor Identification:** The smart contracts may have additional information and vendor-specific metadata. These are considered under vendor identification. The proposed model uses socializing concept and charges on the basis of services provided by drones of a particular vendor. The vendor metadata in the blocks helps to fix values against the particular service provider. It uses vendor public key to identify the service charges. It is to be noted that the service ledgers are available to all the drones, but the final values are obtained from the parent node. This looks centralized, but is distributed as addition and removal of records can be done by any drone, but the vendor interacts with the parent drone only for obtaining the current state ledger.

- **Witness Block:** The witness block is the access assignment au- thorization. This helps to signify the role of each vendor in drone networks. The witness block maintains the record for the minimum number of vendor drones which agree with the policies of location, load and channel control. As per the definition of the blockchain, at least 51% of all the blocks/drones must have a value 1 in the witness block, which signifies acceptance of the current situation. Alternatively, if the value is 0, the smart contracts are redefined and new policies are induced in the network.

### 2.6 Drone transactions and user association

Drone transactions help to decide the laws governed by the smart contracts for the exchange of information between the aerial vehicles. The drone transactions and user associations are attained by following laws:

- **Shuffling the blockchain:** This is the first part of the drone transaction that focuses on shuffling of the blockchain. Usually, it is done whenever the supremacy of a particular chain increases or decreases with the selection of new parent. In some cases, it is done periodically to lower the burden on a particular drone. This is also associated with the resource preservation as it is important to prevent a single drone from draining its resources.

- **Sharing of user and drone ledgers:** This defines the procedures for sharing the ledgers between all the blocks owning entities. The sharing of ledgers is governed by the time.

- **procedure of sharing:** Currently, the broadcast mechanisms are used for sharing ledgers and information across the blockchain-based drones. However, these can be operated by threshold conditions or by a particular communication protocol.

- **Frontend transactions:** All the users are associated with the drone on the basis of the line of sight and availability. Because of interoperability, any user can interact with any drone. However, this association is limited to front end only, and no inter-operability is allowed between the controlling stations and the core of a vendor. This is done to reduce the excessive burden of redundancy caused due to blockchain in drone networks. Also, the computational power and memory of drones’ onboard units play a crucial role in deciding the number of chains it can sustain and operate without many overheads.

### Table 1: Performance Factors

<table>
<thead>
<tr>
<th>Type</th>
<th>Operational Overheads</th>
<th>Latency</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized Deployment</td>
<td>High</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Traditional Drones</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>Blockchain-based Drones</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
At the moment, the performance of the proposed model is under-trol between one another, and how trust is ensured for the drones in Mobility and Identity management: How drones will shift con-

The actual context to be given to a particular chain. Overlapping of chains and make it difficult for the drones to identify the same time can have chains with a similar set of nodes that are overlapping. Drones serving more than one network at the same time can have chains with a similar set of nodes that are overlapping. Despite these features, there are certain threat implications of blockchain-based drones: Overlapping chains: Drones serving more than one network at the same time can have chains with a similar set of nodes that are identified by their common public key. Such scenarios can cause overlapping of chains and make it difficult for the drones to identify the actual context to be given to a particular chain. Mobility and Identity management: How drones will shift control between one another, and how trust is ensured for the drones in the absence of a line of sight with the control stations that provide a pool of public and private keys are still open issues. Violations of transaction laws: Self-amendments in the laws of the drone can violate the rules of the core blockchain. Thus, it is important to strictly handle the laws governing blockchain. Backhaul-blockchain: Since the majority of networks aims at provisioning services via front-haul blockchain, it is required to understand the impact of distributed trust via blockchain on the network backhaul. If private keys are used by depending on the vendor specific needs, dedicated algorithms will be required for non-repudiation of nodes. Access control and authorization: It is important to fix the level of access control for the drones in ultra-dense networks during inter-service operability. Also, it is required to analyze the authorization demand of blockchain by considering the patterns of ledger sharing and updating. This will help to analyze the blockchain from an external entity without becoming the part of the actual blocks.

3 PERFORMANCE CASE STUDY
Currently, this paper presents the ideology of considering blockchain-based drones for ultra-dense wireless networks as shown in Fig. 2. The performance of the proposed model is understood in terms of path length in comparison with the traditional networks with a central authority and the architecture considered in [2]. The details of these comparisons are presented in Table 1. As all the operations are performed at the user-side, the overheads in network formation are less and only depend on the number of drones deployed. This is because the amount of redundancy of ledgers that affects the performance is directly related to the deployed units of aerial vehicles. Similarly, the latency will be least as all the decisions are marked by the nodes themselves and the maximum distance traversed by a ledger for proof of work will be that between the parent and intended drone. The deployment cost remains same as no additional infrastructure is required in the applicability of the proposed model.

However, it is important to note that in this framework, the computation heavily depends on computing cryptographic pairings in parallel, especially for role-based access and authorization. Depending on the computing architecture of the drone, some optimizations in the processing unit may be required since existing CPU (central processing unit) architecture aims to provide fast computation heavily depends on computing cryptographic pairings in parallel, especially for role-based access and authorization. The paper illustrated the applicability of the proposed model.

Lee et al. [10] present a series of optimizations on CPU architecture to close the gap between CPUs and GPUs on processes that require high degrees of parallelism.

4 THREAT IMPLICATIONS OF BLOCKCHAIN-BASED DRONES
Blockchain-based drones are driven by the formation of network ledgers, drone-smart contracts, drone-transactions and user associations. Despite these features, there are certain threat implications of blockchain-based drones: Overlapping chains: Drones serving more than one network at the same time can have chains with a similar set of nodes that are identified by their common public key. Such scenarios can cause overlapping of chains and make it difficult for the drones to identify the actual context to be given to a particular chain. Mobility and Identity management: How drones will shift control between one another, and how trust is ensured for the drones in

5 CONCLUSION
This paper presented the ideology of secure utilization of drones for inter-service operability in ultra-dense wireless networks by exploiting the features of the blockchain. The paper illustrated the components and strategies for driving blockchain-based drones. Various features and threat implications of blockchain-based drones were also presented. The paper also illustrated the relevance of the blockchain-based drones in comparison with centralized and traditional drone-assisted wireless networks.

REFERENCES