Sharding Enabled Blockchain for Software-Defined Internet of Unmanned Vehicles in Battlefield

Bimal Ghimire, Danda B. Rawat, Chunmei Liu and Jiang Li

***Abstract*—Internet of Unmanned Vehicles (IoUV) is regarded as an emerging technology for military applications not only to make surveillance system and battlefield operations fully coordinated and automated but also to provide significant strategic advantages. All the UVs form a coordinated network for exchanging information in IoUV which enhances context awareness, risk analysis and improves response time to make the mission effective. This article provides a perspective of fusion of blockchain technology with software defined IoUV, *aka* extended 5G, for battlefield scenario. Software defined IoUV dynamically configures the network parameters and provides the network visibility for better security and manageability of the network in IoUV. Blockchain technology helps to provide trustworthy command and control operations in IoUV and stores those operations in tamper-resistant digital ledgers in the form of transactions. Unmanned Vehicles (UVs) with high computing, storage, battery life and transmission power act as miners that validate every transaction and are responsible for creating blocks of the blockchain. However, current blockchain technology suffers from scalability, thus we propose sharding enabled blockchain to address the issue where shard of lightweight UVs maintain the required number of miners/auditors to handle the issues when the miner gets destroyed or damaged in the battlefield. Some participating UVs are used as wireless stations to provide persistent wireless connectivity in IoUV. The proposed framework aims to increase the trust and accountability, and to reduce business friction among different units involved in the battlefield.**

***Index Terms*—Internet of Unmanned Vehicles (IoUV), Internet-of-Battlefield Things (IoBT), unmanned vehicles, blockchain technology, sharding, scalability.**

I. Introduction

With the exponential growth of wireless subscriptions and number of Internet of Things (IoT) devices, networked world has been transforming in a way that was possibly not imagined before. Billions of IoT devices are already connected to the internet for different applications like smart city, smart energy, smart transportation systems and so on. Internet of Unmanned Vehicles (IoUV) is emerging as Internet of Battlefield Things (IoBT) for military applications, particularly in battlefield scenarios. This paper presents a perspective of combining blockchain with the software defined IoUV for battlefield scenario. The objective of our approach is to make all the battlefield operations automated and keep the communication secure enough among trusted parties by not letting the adversaries join the IoUV. Multiple UVs such as drones, fighter jets, tankers are sent to the battlefield where they exchanged information for an automated attack without involving soldiers in the battlefield. Fig. 1 shows our proposed two-layer system architecture for the blockchain empowered IoUV. The upper layer represents the blockchain implementation. The bottom layer consists of UVs such as tankers, fighter jets, drones which are connected to the blockchain network through either single-hop or multi-hop communication links. All the information exchanged between involved entities are validated by the blockchain and eventually stored permanently in the blockchain. Blockchain technology stores all the command and control operations in IoUV in tamper-resistant digital ledgers in the form of transactions. The stored transactions enhance better trust and accountability and reduce business friction among different units involved in the battlefield [1]–[4].

Many countries are conducting extensive research to make use of IoUVs and IoBTs for the effectiveness of their strategies and attacks on the battlefield. The most common approach of attack used in battlefield scenarios is to perform coordinated attacks. In this form of attack, all the participating parties exchange information with each other to get detailed information about the battlefield scenario. They analyze the exchanged information to make informed decision about the situation. When the central authority or command and control center (CC) sends an instruction, all parties make sure the command and control operations are legitimate and then perform a simultaneous coordinated attack. However, the distributed nature and massive scale of IoUV devices create several security challenges as the adversaries can intercept wireless communications and use it against the IoUVs. Thus, the availability of accurate and timely information only within the trusted group is always an utmost priority in IoUVs (e.g., [2]).

The main objective of this paper is to present a fusion of blockchain technology with software defined IoUV for battlefield scenario where i) software defined IoUV, *aka* extended 5G, dynamically configures the network parameters and provides the network visibility for better manageability of the network (e.g., [5]) and ii) blockchain technology helps to provide trustworthy command and control operations in IoUV and stores those operations in tamper-resistant digital ledgers in the form of transactions (e.g. [6]). Note that, for coordinated battlefield scenarios consisting of IoUVs,

Manuscript received Day Month Year.

Authors are with the Data Science & Cybersecurity Center (DSC^2), Department of Electrical Engineering and Computer Science at Howard University, Washington, DC 20059, USA. Corresponding E-mail: db.rawat@ieee.org, danda.rawat@howard.edu.

This work is partly supported by the U.S. NSF under grants CNS 1650831, CCF-0939370 and HRD 1828811, and by the U.S. Department of Homeland Security under grant DHS 2017-ST-062-000003 and DoE's National Nuclear Security Administration (NNSA) Award # DE-NA0003946.

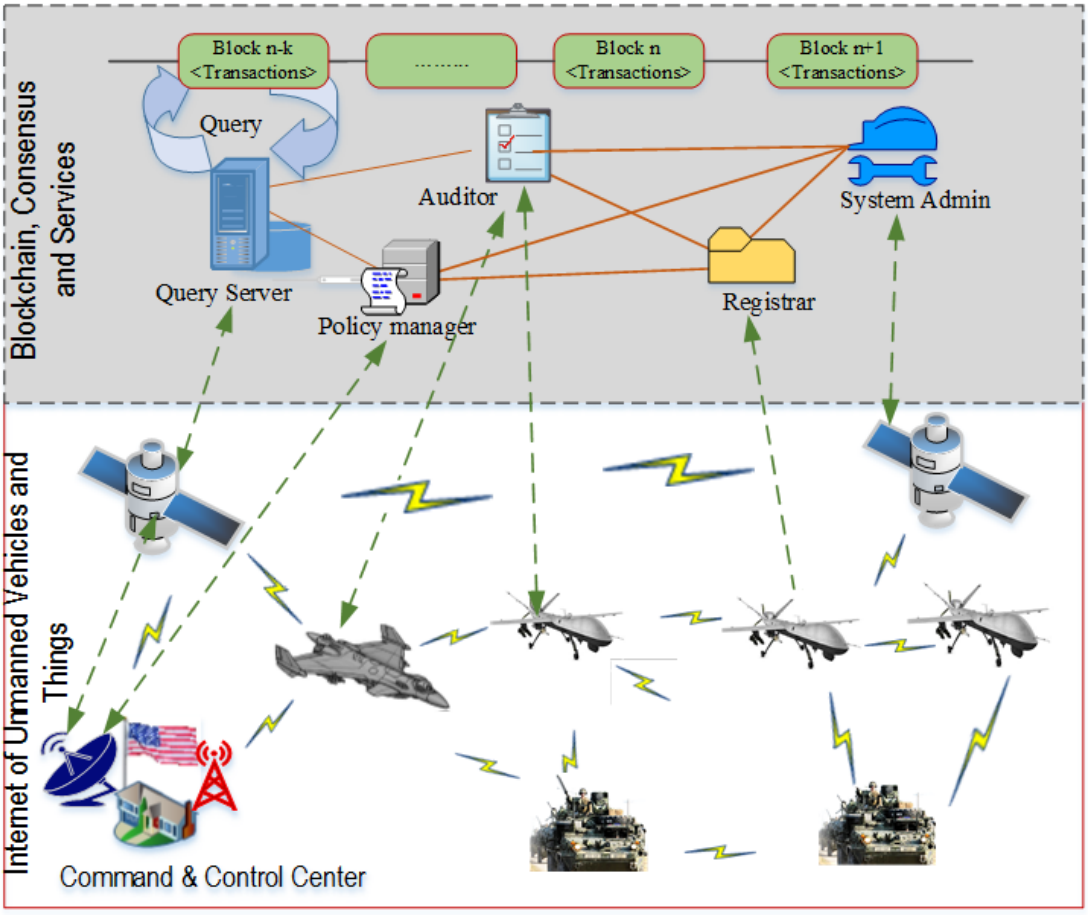

Fig. 1. Blockchain-Enabled Unmanned Internet of Unmanned Vehicles and Battlefield Things.

blockchain is a suitable platform for trustworthy operations to implement strategies, policies and decision making. Smart contracts (executable codes that reside in the blockchain) [7] could make the whole command and control operations trustworthy, coordinated and automated that could help to make informed critical decisions [8], [9].

For instance, recently, by mistake, airstrike hit the crowded hospital in Afghanistan where team of doctors without borders was working to treat war wounded people [10]. Later it was realized that the command and control operation had provided a wrong target and it was not clear who gave such command to hit the hospital. These type of command and control operations can be easily verified by using temper-resistant blockchain which could help reduce such mistakes and make involved units accountable.

Furthermore, current blockchain technology suffers from scalability, thus we propose sharding enabled blockchain to address the issue. Two different approaches of sharding are discussed in this paper. In one approach, subsets of UVs are grouped to form shard based on the type of transactions. Instead of validating each transaction by all blockchain nodes (UVs), a particular shard performs this task. The second approach of sharding is proposed as a backup plan to maintain the required number of miners in the blockchain system. In this case, group of lightweight UVs (UVs with limited computing, storage and communication resources) are used to form shard based on their needs in terms of computing, communications and storage capacities and needs.

In the following section, a novel architecture for blockchain enabled software defined IoUV followed by some analysis, discussions, some open research issues and conclusions, is presented.

II. Sharding Enabled Blockchain meets the Internet of Unnamed Vehicles (IoUV) for Battlefield Scenarios: An Architecture

A. System Architecture

The proposed system architecture consists of: i) several UVs (such as drones, fighter jets, unmanned tankers, unmanned flying vehicles and battlefield surveillance sensor nodes) with embedded storage, computing, communications and control units deployed for a mission oriented battlefield scenario where UVs adapt networking parameters for robust communications using software defined networking; and ii) blockchain implementation for storing command & control operations and interactions in the digital ledgers where UVs form clusters

based on their a) computing, storage and communications capabilities and b) needs to participate in sharding enabled blockchain based IoUV, as shown in Fig. 1

Current blockchain protocol requires each node to store the entire state of the blockchain in a distributed manner and processes each transaction in the blockchain network without the help of the (trusted) third-party, which is the important feature to provide robust security. However, this phenomena over the time limits scalability of the blockchain technology [11]. Specifically, the blockchain system suffers from the trilemma of having decentralization, security and scalability [12]. To address the scalability issue, the proposed architecture leverages the sharding approach where multiple UVs that have limited capabilities in terms of computing, communications and storage form clusters to participate in sharding based blockchain, as shown in Fig. 2. Furthermore, we are dividing our network into multiple shards based on transaction types and the transaction only propagates to a particular shard. This makes process of validation as well as mining (creating/validating blocks) fast in time sensitive operations in the battlefield (Section II-E). Each shard despite storing the complete state of the whole blockchain, only stores complete state for one particular ledger or type of transaction. Instead of forwarding each transaction to every UV (or node) in the IoUV network, the transaction is forwarded only to a particular shard which is supposed to validate this particular type of transaction. All the nodes of the particular shard verify the given type of transaction and then one successful miner/registrar creates a block to store the transaction in the blockchain as shown in Fig. 3. All the miners in the blockchain system do not need to spend their computing power trying to create blocks. Only miners in particular shard perform this task. This approach helps to resolve scalability issues in blockchain based IoUV.

B. Internet of Battlefield Things (IoBT) Scenario

IoBT consists of interconnected heterogeneous sensors, actuators, computing resources, analytical devices and software. Existing battlefield mission makes use of active sensors, intelligent sensors, camera sensors, Infra-red sensors, micro-electro-mechanical systems and so on. These sensors have the capability of using techniques like digital image/signal processing, machine learning and others to extract useful information. With such information, it can classify objects as ally or adversary even from very high noise levels. These sensors enable all the UVs to collect various critical information regarding target detection, its motion/movement, location, distance, types of objects, number of enemies, enemies' weapons and other parameters to provide situational awareness in the battlefield [1]. This information is relayed in real-time to the trusted peers more specifically to the blockchain in IoUV where every other peers can see all the exchanged information. The control and command center can also get timely information to make critical decisions. With this, it can decide whether to attack or add more unmanned vehicles or abort the mission or make any other kinds of tactical

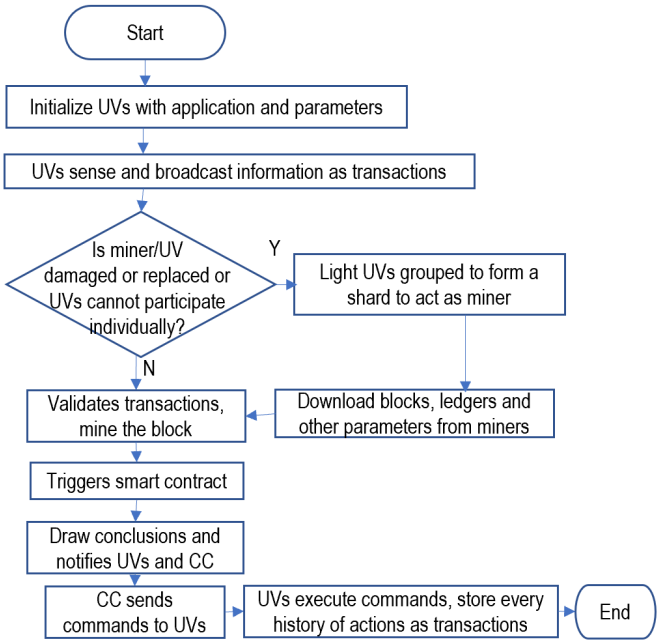

Fig. 2. Flow diagram for sharding for lightweight UVs and in case of damaged/replaced UVs.

decisions. This approach hugely helps to save human life and other resources. However, with the traditional communication approaches for IoUV, malicious nodes might intercept the exchange of information between unmanned vehicles and act as a genuine node and send false data.

However, with the traditional communication approaches for IoUV, malicious nodes might intercept the exchanged information between unmanned vehicles and act as a genuine node. Thus the ultimate goal of our proposed work is to make the communication secure enough by using blockchain so that untrusted node cannot join the network or eavesdrop to steal any kind of information or send any kind of false information into the IoUV.

For the blockchain based IoUV, command and control center deploys UVs by assigning a unique pair of keys consisting of public key and private key for blockchain operations. Public keys of every trusted peer in the group are distributed among the group and each UV stores this ledger with them. Furthermore, UVs are assumed to be equipped with software defined networking capabilities to adapt the networking parameters on the fly based on its operating environment [5].

C. Multiple Ledgers Based on Types of Transactions

We propose to use multiple ledgers to reduce the overall overhead in blockchain enabled IoUV since some information are not changed often and some information changed very often. In the blockchain enabled IoUV network, every UV maintains immutable distributed ledgers to store exchanged information as transactions. The proposed blockchain maintains multiple ledgers storing different types of information as transactions depending on the types of information it

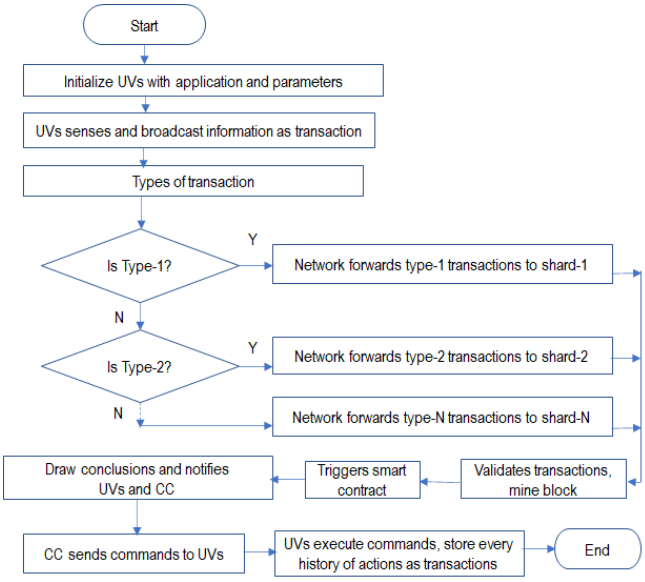

Fig. 3. Flow diagram for sharding of UVs based on transaction type.

exchanged. The transactions are stored permanently in the form of blocks created by miners by solving a cryptographic hash algorithm. One typical ledger stores transactions which reflect all the periodically sensed data by every UVs in the battlefield environment. It is obvious that the data depends on the sensors that every UV is equipped with. The common data gathered might be geo coordinate(location), line-of-sight, laser designation, electro-optical pixel and others for situational awareness of war-zone. The data collected by all the UVs in the environment is securely shared using digital signature among all the peers. With this information along with others, command and control center ultimately can decide and send instructions. The instructions might be whether to attack or abort the mission, send backup UVs or others. Each transaction is verified by the UVs and ultimately stored in block.

Another ledger holds public keys of all the peer UVs participating in the current battlefield situation and also of CC. Every UV stores this ledger and this ledger is updated whenever a new trusted UV joins or leaves the live battlefield scenario. The ledger is updated with the consensus from all the participating nodes while the joining or leaving node only sends the notification about its action. Each UV needs to notify its presence consistently either by sending sensed data or any information or just a beacon. This persistent communication is mandatory to identify the presence of each UV. The joining and leaving of UV on the battlefield might be planned or accidental (an UV might get hit by enemy force or lose its battery power). In case of accidental loss of UV, smart contract decides its absence if it does not receive any signal for a given threshold time and the ledger gets updated accordingly. This scenario is necessary to securely communicate only with all the participating peer UVs and will be ultimately helpful to create a trusted environment and analyze the war zone in detail with trustworthy information.

Another ledger holds all the public keys that are ever assigned to any UVs. This ledger gets updated whenever central authority assigns a new pair of private and public key to a new UV. This ledger keeps track of every UVs. Only miner nodes hold this ledger and update whenever required. This ledger facilitates identifying each UV and finding every detail regarding it that is ever associated with the blockchain network.

Other ledger maintains the current status of types and the number of weapons each UVs is having. The transaction in this ledger with timestamping provides the information about what types and numbers of weapons each UV were initialized with, what types and number of weapons ever used to attack by each UVs and how much each UV is left with. This gives useful and sensitive information to estimate or plan for current as well as future battlefield situations. Depending on the computing, storage, networking capability each UV possesses, it may store a particular ledger or combination of these or all.

D. Communications and Mining in Blockchain Enabled IoUV

Whenever UVs are sent for a battlefield mission, a persistent fast communication between all the UVs is of utmost priority. UVs carrying sensors and weapons can have the capability to act as wireless stations to provide the connectivity to broadcast every transaction. Some UVs also act as wireless stations to other UVs and provide wireless connectivity in IoUV for the battlefield. To broadcast a transaction in blockchain network, a UV should be able to transmit its information to a nearby wireless station. However, all UVs might not have sufficient transmission power to achieve this. In such a case, communication takes place using multi-hop routing. A nearby UV in proximity relays the transaction to the wireless station.

In our proposed model, each UV communicates in broadcast mode encrypting the message with its private key. Each communication is also stored in the blockchain as a transaction with timestamp. Every UV in the group communicates with each other encrypting its message with own's private key. With the public key pair of sender, (all public keys of trusted UVs are in ledger) each UV verifies the authenticity of the transaction. If any malicious node initiates the transaction encrypting with its private key, it is not decrypted as ledger contains the public key of the trusted UVs only. This is how the blockchain ensures whether any UV is trusted or malicious.

In blockchain, mining is a task of storing current transactions in a valid block on top of the previous blocks stored in chronological order. The nodes which perform this task are called miners. Miners solve a computation intensive cryptographic puzzle to find the valid address for each block [6]. Miners are special nodes in the network with high computing capabilities. In the proposed system, not all participating UVs may have enough resources like computing power, storage, battery power, bandwidth and communication range. Every node may not have the capability to validate every communications or transactions and store in the blocks. The UVs with sufficient resources act as miners to validate each transaction and eventually store in cryptographic block.

However, those with limited resources act as lightweight node in the blockchain system. These nodes only store public keys of UVs operating in current battlefield, where as miners store public keys of all the UVs which have been ever assigned with a pair of public and private keys. Each UV (of the trusted group) can join the closed blockchain network and initiate or forward communications (transactions) to the blockchain network. All UVs in the network validate the transactions and eventually miners create valid blocks to store transactions permanently. Note that, although all the miners participate in creating a block, the one which creates valid address for the block first, is considered as successful. Once the valid block is created, it is broadcasted to the blockchain network and all the other miners also update their ledger respectively.

Whenever a new UV joins the network of the live battlefield, it broadcasts request to join the network. The request is validated to identify whether it is a trusted UV or not. If found trusted, all the blockchain network nodes update its public key ledger to add newly joined UV. A similar approach is applied for any UVs that leave the battlefield. This is required as new UVs can join or existing UVs can leave the battlefield. Every blockchain nodes whether it is miner or lightweight UV, can see ongoing communication in blockchain as well as receive the encrypted command or information through the communication channel. The lightweight UVs, do not store all the transactions while the miners store all the transactions happened since the genesis block. The lightweight UVs only store block headers to validate the authenticity of any transactions if required. These UVs work as Simplified Payment Verification (SPV) nodes and can verify any transaction comparing stored Merkle root and generated merkle tree from block headers of that particular transaction [13].

Our approach also incorporates smart contracts on top of blockchain to draw automated tactical and critical decisions. If any of the participating UV does not respond for a threshold time, a smart contract (program running on blockchain network and checking the log of transactions continuously) notifies all the other participating UVs as well as the CC to make aware of the situation. The CC can take necessary actions as per the needs. The smart contract also issues commands to every nodes to update their ledger to exclude the lost UV. Similarly, whenever a new trusted party joins, it broadcasts its presence. Miners in the network validate this transaction of request to decide the authenticity of this new UV. If found authentic, smart contract issues instruction to all UVs to update their ledger. In this paper, we are assuming that the CC has the ultimate decision power regarding critical decisions like issuing attack command, aborting the mission, sending backup UVs. It can always override the automatic decision made by the consensus of all the UVs triggering some smart contract. Let us assume that the UVs have sufficient weapons and the sensors' data collected by all the UVs are sufficient and favorable to attack target(s) then a smart contract executing in the network issues hit the target instruction. However, the CC provides a final decision or notification to hit the target. All the instructions or commands sent by the CC are also stored as transaction in the blockchain.As mentioned before, all the participating UVs need to store every information collected or exchanged in the blockchain as a transaction so that each peer gets the situational awareness. Apart from this, each peer also acknowledges the information once it sees the transaction, which creates a tight coupling between all the peers and makes coordinated attack effective.

Apart from other information, logs of weapons is an essential element of any battle mission. Using blockchain to store every detail regarding weapons is significantly useful to analyze past battlefield scenarios as well as plan for future missions. In our approach, the CC initializes all types and number of weapons for every UVs before leaving for a war zone. This information along with the timestamp is stored in the blockchain. After receiving the command from the CC for a coordinated attack, UVs fire weapons and send the information about it to the blockchain network. These transactions are validated by UVs and the number of available weapons gets updated in the corresponding ledger. Miners store every such transaction permanently in the blocks. With this information along with sensors' data, CC can make the decision whether to send any backup UVs or not.

E. Sharding for Scalability Issue in IoUV

Existing blockchain technology provides security, trust and decentralization but the biggest problem with it is scalability. The size of the chain increases rapidly with time. The more nodes join the blockchain, the more transactions they do, the size of the chain keeps on increasing. Each transaction is broadcasted to the entire blockchain network for consensus. So with the rise in the number of nodes, the transaction validation time also increases.This problem is not severe in case of proposed private blockchain as there will always be a limited number of UVs. Moreover, UVs do not join or leave randomly as in public blockchain. Furthermore, all the hashing and encryption applied in communication (when we use a single ledger in blockchain) might cause a delay in time-sensitive operations like mission critical battlefield. This problem can be solved by using sharding based on types of transactions. As there are multiple types of information or transactions in our proposed blockchain and so are the respective ledgers in the blockchain. Not all participating UVs store all types of ledgers as mentioned before. Instead of UVs validating all the types of transaction, the use of shards for handling a particular type of transactions decreases the latency in the system and resolves the scalability problem to a great deal. This scenario can be best explained by an example. Suppose there is a blockchain system for job application system. In this scenario, there are multiple types and instances of companies or employers such as banks, information technology companies, hospitals, universities, automobiles and so on. All these employers connected to the same blockchain network accept and validate the candidate's application. Suppose a candidate wants to apply for the post of bank manager and submits his application in the blockchain network. In the present scenario of public blockchain, this application propagates to all types

of employers (nodes) to validate it. However, in our sharding approach, each employer listens to the application but the validation is done only by the shard of banks. The other types of employers do not need to waste computing power. Applying this idea on the proposed blockchain system for IoUV makes our system efficient in terms of time, computing and battery power.

It is always desirable and necessary to maintain sufficient number of nodes verifying transactions to make the system resilient. More the number of miners, the faster the block of transactions is created. However, in the battlefield it is likely that miners get destroyed by enemy forces. In such situations, lightweight UVs can form a shard to share the computing and communication resources and act as a miner. The shard then downloads all the copies of blockchain from other miners and starts performing the validation and mining task.

Note that the approach of sharding might cause security concerns in the blockchain network. The security issue occurs if attackers identify the nodes representing a shard. In such a case, they may compromise the shard when they demonstrate 51% attack against the network [14]. It might be possible to demonstrate it against a shard as it only consists of a subset of blockchain nodes. However in our proposed system, only trusted UVs can participate in the network and UVs operate only for a mission period which makes it resilient against such case.

III. Open Challenges and Research Perspectives

Previous sections show that sharding enabled blockchain for IoUV for providing security, trustworthiness and scalablility. However, the proposed architecture is in its early stage, thus there are several open challenges. Some key open challenges are discussed below.

Hardware Security Issues: The heterogeneous and distributed nature of UVs in IoUV possesses several security and privacy challenges through hardware used in UVs. There are multiple registered incidents in which hackers used these vulnerable devices to attack the networked systems. It is likely that adversaries can compromise the IoUV devices and gain access to the proposed blockchain system. If adversaries hacked multiple UVs and were able to join the network, the consequences might be disastrous as there are always limited UVs in any battlefield network. If adversaries gain access to the IoUV system, it can modify all the blocks or transactions of every node in the network. This issue could be resolved by having formally verified trustworthy hardware in UVs.

Heterogeneous Networking and Communications: Heterogeneous networking and communication infrastructure and protocols could lead to high overhead and less useful communications. Furthermore, due to the high mobility of UVs, maintaining fast and persistent connectivity and communications between UVs to achieve operational efficiency is a great challenge. These issues can be solved by using software defined networking to have better network visibility and manageability.

Limited Power: UVs are battery powered and might need to perform intense communication and computation in the proposed system. If the battle lasts longer than expected, UVs may run out of power. In such a situation, UVs will not be able to compute, communicate and do other important tasks. This will have a huge adverse impact on the whole mission. This issue could be solved by having a proper deployment of UVs in a round robin manner or replacing batteries in the sky with the help of another UV.

Latency: All communication and critical decisions are significantly time sensitive so, the validation of transactions should be instantaneous. In the public blockchain scenario, miners get rewards for verifying transactions. The difficulty level of mining is always adjusted in a certain time interval based on the expected time and actual time taken to mine certain number of blocks [15]. However, in case of proposed system, this approach might not work. Blocks need to be created frequently during battle missions, other times there might not be sufficient transactions to create blocks for a long period of time. Setting a difficulty level as in the public blockchain is not applicable in the case of IoUV scenario. It should be carefully selected or adjusted not to affect the time sensitive operation.

Scalabitily: The concept of sharding enabled blockchain resolves scalability issues to a great extent. However, the number of UVs in IoUV is always limited and each shard/cluster contains an even lesser number of nodes. If a malicious node with high computing resources becomes able to compromise any UVs to gain access to blockchain, then there will be a chance that it can forge the ledger in blockchain. However, this is almost impossible in case of the public blockchain like bitcoin [6] since there are numerous nodes in the entire blockchain network. To make a successful attack, an attacker needs to demonstrate the proof-of-work satisfying 51% attack [14]. This means the attacker must have control over more than 50 percent of network and/or resources of the entire network. In case of the proposed system architecture, the chance of forging ledgers of a shard by malicious node(s) is very low as the blockchain network is closed and the UVs remain active in the IoUV blockchain network only for the battlefield mission. Shard can always be mission specific and can be offloaded to CC for future reference. Moreover, the proposed battlefield mission basically consists of tankers, drones, firefighters jets, bombers and so on with high computing resources. So, it is difficult task for attackers to control more thank 50% computing resources of IoUVs.

IV. Future research work

Blockchain has been studied well in the literature. There are already plenty of applications developed in the world. Nevertheless, scalability has not gained an adequate focus on research. Today, even the most popular blockchain applications like bitcoin, ethereum, and others are experiencing scalability problems. These networks take significant time to validate transaction and consumes enormous electricity. Today, bitcoin consumes electricity more than that of some countries. This is an important area of research to make blockchain sustainably

applicable for varieties of use case scenarios. We have proposed how sharding can be utilized to overcome the issue in IoUV. While, the main challenge with the sharding in IoUV is to form a logical group of the mobile UVs dynamically and provide consistent connectivity. Assessing the battlefield gravity, identifying the required number of UVs, and the type of UVs for each shard is a big challenge. Each shard might have a different number of UVs based on the type of transactions it handles. The highly dynamic and volatile nature of the battlefield scenario makes it more difficult to maintain the number of nodes in each shard. Our future research direction will focus on all the challenges outlined in this paper. We also focus on extending the utilization of SDN in IoUV scenario to evaluate and adjust network parameters to form shard dynamically as per needs.

V. Conclusion

The proposed sharding enabled blockchain for software defined IoUV provides not only security and trustworthy information exchange in IoUV but also a complete audit trail of command and control operations and communications. The ledger of every communication ever happened in the IoUV could facilitate any government or defense system to analyze past and present battlefield operations and help to draw strategic decisions to plan for the future battlefield operations. Our approach creates an efficient, trustworthy, fully coordinated and automated battlefield environment for mission critical command and control operations. Sharding enabled blockchain empowered IoUV environment is scalable to execute time sensitive battlefield operations efficiently and timely. Furthermore, this paper has discussed several open challenges and provided possible future research directions to tackle the challenges.

Acknowledgments

This work is partly supported by the U.S. NSF under grants CNS 1650831, CCF-0939370, IIS-1924092 and HRD 1828811, and by the U.S. Department of Homeland Security under grant DHS 2017-ST-062-000003 and DoE's National Nuclear Security Administration (NNSA) Award # DE-NA0003946. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies.

References

[1] J. Zhu, E. McClave, Q. Pham, S. Polineni, S. Reinhart, R. Sheatsley, and A. Toth, "A Vision Toward an Internet of Battlefield Things (IoBT): Autonomous Classifying Sensor Network," US Army Research Laboratory Adelphi United States, Tech. Rep., 2018.

[2] U. Khakurel, D. B. Rawat, and L. Njilla, "FastChain: Lightweight Blockchain with Sharding for Internet of Battlefield-Things in NS-3," in *Proc. of the 2019 IEEE International Conference on Industrial Internet (ICII)*, Orlando, FL, USA, November 11 - 12.

[3] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3680–3689, 2019.

[4] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, "Blockchain-empowered secure Internet-of-Battlefield Things (IoBT) architecture," in *2018 IEEE Military Communications Conference*, 2018, pp. 593–598.

[5] J. McCoy and D. B. Rawat, "Software-Defined Networking for Unmanned Aerial Vehicular Networking and Security: A Survey," *Electronics*, vol. 8, no. 12, p. 1468, 2019.

[6] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, 2008.

[7] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2018.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] Q. Xu, Z. Su, and Q. Yang, "Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1098–1110, 2019.

[10] Alissa J. Rubin, "Airstrike Hits Doctors Without Borders Hospital in Afghanistan," Oct. 3, 2015, URL: https://www.nytimes.com/2015/10/04/world/asia/afghanistan-bombing-hospital-doctors-without-borders-kunduz.html.

[11] M. Bez, G. Fornari, and T. Vardanega, "The scalability challenge of Ethereum: An initial quantitative analysis," in *2019 IEEE Int'l Conf on Service-Oriented System Engineering*, 2019, pp. 167–176.

[12] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, 2020.

[13] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[14] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *2016 IEEE international conference on consumer electronics (ICCE)*, 2016, pp. 467–468.

[15] M. B. Taylor, "The evolution of bitcoin hardware," *Computer*, vol. 50, no. 9, pp. 58–66, 2017.

Bimal Ghimire is pursuing his PhD in Computer Science in the Department of Electrical Engineering & Computer Science and is associated with the Data Science & Cybersecurity Center (DSC^2) at Howard University, Washington, DC, USA. His research interests include cybersecurity, data analytics, blockchain, vehicular networks and age of information for cybersecurity.

Danda B. Rawat (S'07, M'09, SM'13) is a Professor in the Department of Electrical Engineering & Computer Science and Founding Director of the Data Science & Cybersecurity Center (DSC^2) at Howard University, Washington, DC, USA. Dr. Rawat is engaged in research and teaching in the areas of cybersecurity, machine learning and wireless networking for emerging networked systems. Dr. Rawat is the recipient of NSF CAREER Award, the US Air Force Research Laboratory (AFRL) Summer Faculty Visiting Fellowship, Outstanding Research Faculty Award and several Best Paper Awards.

Chunmei Liu is a Professor in the Department of Electrical Engineering & Computer Science at Howard University, Washington, DC, USA. Her research interests include graph algorithms, machine learning, big data analytics and security. She is the recipient of NSF CAREER Award.

Jiang Li is an Associate Professor in the Department of Electrical Engineering & Computer Science at Howard University, Washington, DC, USA. His research interests include computer networks, delay tolerant networks, data analytics, machine learning and security.