N232-094, Blockchain-based, Highly Secure, Decentralized, and Immutable (DSI) Network System Protocol for Multifunction Advanced Data Link (MADL)

Responses to single question posted to DSIP Topic Q&A

A. Battlefield Sensing Layer Challenges

When a higher number of sensing devices are collectively working in the battlefield, the amount of Blockchain transactions generated will also be increasingly high. It raises several issues and bottlenecks for the overall system, which are as following.

A1) Fine/Coarse Grained Sensing: In practice, the physical entities in the battlefield arena may carry more than sensors/actuators, which have different sensing purposes and more than one node may have communication capability even if they are tied with the same physical object. In this situation, the number of data streams to transmit the information increases and thus the transaction count for a Blockchain network layer grows accordingly. Since adding a block of transactions into the distributed ledger requires consensus to be achieved, which is a time-consuming process, it can introduce performance overheads too. Therefore, fine-grained sensing might improve the accuracy, but the Blockchain infrastructure may not be able to handle such a large amount of transactions. Hence, multiple sensing streams may need to be aggregated and a balance between fine, and coarse-grained sensing needs to achieved, which can help in attaining optimal Blockchain performance.

A2) Interoperability: Military equipment and hardware used in the battlefield are typically manufactured from different vendors and the interoperability between these IoT devices is overlooked, which plays a major role in producing standardized transactions for the Blockchain platform. Furthermore, sometimes the high-end military equipment gets some critical parts replaced upon any damage, thus it may change the identity information of the device and require following a different standard to operate. Since it is difficult to have all the equipment follow the same communication standard, the important challenge here is to design a secure interoperable layer that can be generically used by every network-capable node to create globally-acceptable Blockchain transactions.

A3) Energy Efficiency: Power has a critical role in engaging military equipment to operate well in harsh situations. Sensing the terrain and physical conditions consumes energy. And, sending the data to other peers as well as the Blockchain network costs additional power. So, a right balance on sensing and transmission tasks is required as per the mission needs, and transaction frequency should be optimally selected for the Blockchain framework to minimize the overall energy cost.

B. Network Layer Challenges

The network layer creates the backbone of our Blockchain-enabled Internet-of-Battlefield-Things (IoBT) architecture, where the transaction gathering, block propagation, and Blockchain service-related communications take place. Hence, maintaining strong and reliable connectivity is important to avail all the benefits of Blockchain. The challenges involved in this layer are briefed below.

B1) Participants Selection: To have a distributed IoBT platform, it is important to have a consistent and reliable set of nodes, who can serve to maintain the Blockchain. Traditional IoT environment has ubiquitous network connectivity with which the nodes can send their data to cloud server that will perform the necessary analytics tasks and monitor the environment accordingly. However, the IoBT devices operate on stringent conditions, such a slow computational capability, lack of network connectivity, low/no energy supply, and so on. Thus, it is necessary to have a robust selection criteria to select nodes that can keep the Blockchain network active until a fixed period of time is reached. Also, mechanisms need to be established to periodically offload the responsibilities of existing nodes to another selected set of nodes for keeping the network alive until the mission completes.

B2) Dynamic Network Topology: Military missions are usually very dynamic in nature, where battlefield equipment and soldiers always change their locations. Thus, the network created by them will have both spatial and temporal topology variation. Furthermore, the energy drainage on the devices may even segment the network to multiple pieces. Considering these challenges, the adaptable communication protocols for the distributed ledger technology should be established to maintain consistency and ordering of transactions in Blockchain.

B3) Blockchain Parameter Tuning: The network layer mostly handles the sending and receiving of transactions and blocks among each node. Given the established tactical network may have a limited bandwidth, the size of transactions and blocks need to be optimally chosen so that overall latency in the consensus process can be minimized.

C. Consensus and Service Layer Challenges

Establishing the network of military things is not sufficient unless a robust distributed consensus mechanism is in place to maintain the Blockchain state. The traditional consensus algorithms have limitations to adapt in the IoBT environment. Therefore, applicability of different Blockchain consensus models needs to be investigated and revised appropriately to serve the needs of a Blockchain-enabled IoBT framework.

C1) The challenge is to find the right consensus model that will best work for the IoBT Blockchain, while considering the energy constraints, sparse connectivity issues, and transaction throughput requirements. Also, the dynamism of battlefield nodes poses the question of “who will be responsible to hold the Blockchain data (authenticated transaction data) permanently to make it available throughout?”

C2) Number of Nodes: As the nodes in battlefield enter and exit the network sporadically, the consensus requires a stable number of nodes to confirm the Blockchain state. If an insufficient number of nodes operate at the consensus layer, consistency of the Blockchain can be compromised. Although, fewer consensus participants can improve the transaction throughput, it may not be secure enough to prevent malicious exploitation of the consensus process.

C3) Performance and Privacy Considerations: Traditionally, each node verifies every single transaction in the Blockchain framework in parallel before the block mining occurs. This becomes a bottleneck when it comes to improving the scalability and transaction throughput in any IoT system. In addition to devising lightweight consensus mechanisms, several other techniques like sharding, off-chain computation, and state channels are considered for improving the Blockchain performance. However, it will be important to investigate their usefulness in improving the battlefield-specific Blockchain. In addition, privacy of transactions is critical to maintain when the ledger is shared among the participating military nodes.