Command and Control Platform using Private Blockchain

Kyoungmin Kim, Junwoo Seo, Mookyu Park, Moosung Park, and Kyungho Lee

Abstract— While developing its information technologies, the military of each country acquires information of other countries and tries to get the superiority of the defense. Through the data-fighting process of each country, it is possible to acquire the information of adversary on the battlefield and to steal military confidential such as operational plans by hacking. Based on its importance, command and control system became first target to those cyber attacks. Therefore, the military of each country have made efforts to use these systems on more secure channels, networks and storage media. This paper shows a schema of Command and Control Framework using private blockchain and explains why blockchain is used in the schema.

Research Keywords— Blockchain, Command & Control Platform, Decentralized Network

1 INTRODUCTION

Recently, as a variety of blockchain technologies have been evolved, a variety of decentralized applications have been created. In the military, there are an effort to utilize the blockchain technology to develop a self-defense framework, and to take advantage of the information defense.[1] In the past, it was difficult to construct a schema for implementing a decentralized application because there are few blockchain technologies. However, new blockchain technologies such as private blockchain and consensus algorithms make the military easier to envision a schema and develop the new idea. This paper suggests a new schema of Command and Control platform using private blockchain and the reason why blockchain is needed in military command and control platform.

2 RELATED WORKS

2.1 Permissioned, Private Blockchain [2]

Private blockchains are also called “Permissioned Ledgers”. Participants are allowed to participate in the reading, writing and consensus process, and specific subjects may be added or removed as needed. It is also possible to design a private blockchain with different versions depending on the design purpose. Therefore, although everyone can view the data, the data recording can be applied in a variety of ways.

Most of the private blockchains that have been produced so far are use algorithms that do not have hash competition, such as Federated Byzantine Agreement(FBA), Tendermint [3], Practical Byzantine Fault Tolerance(PBFT) [4].

3 THE BLOCKCHAIN BASED COMMAND AND CONTROL PLATFORM

3.1 Why blockchain is needed in C2 Platform

The enemy is likely to forge data on the command and control framework as part of information operations. Since a blockchain technology can prevent Single Point of Failure, it is a very good option for the military which thinks integrity is paramount value. Blockchain-based C2 Platform’s database cannot be modulated due to the decentralization of each participant node. Also, the new block

- *Kyoungmin Kim is with the department of Cyber Defense (CYDF), Korea University. E-mail: richard2104@korea.ac.kr.*
- *Junwoo Seo is with the department of Cyber Defense (CYDF), Korea University. E-mail: junuseo@korea.ac.kr.*
- *Mookyu Park is with the Institute of Cyber Security & Privacy (ICSP), Korea University. E-mail: ctupmk@korea.ac.kr.*
- *Moosung Park is with Agency for Defense Development(ADD), Republic of Korea. E-mail: parkms@add.re.kr.*
- *Kyungho Lee (corresponding author) is with the Institute of Cyber Security & Privacy (ICSP), Korea University. E-mail: kevinlee@korea.ac.kr..*

2014-2018 © ICRP. Published by the Institution of Creative Research Professionals

is connected with the previous block by hash, so data modulation and de-embedding in the whole block is practically impossible.

Errors and mistakes can be minimized in an unstable network situation, so time for correcting and correcting errors can be reduced. Network participants can monitor command and control transaction in real-time so that it can maximize visibility. Moreover, it is possible to maintain confidentiality by granting permission to each network participants.

3.2 Concept

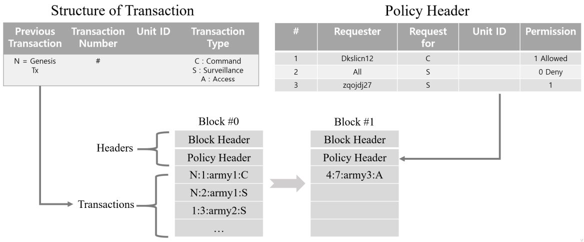
This paper suggested the Command and Control platform using the private blockchain. In this paper, the authority who can write to the block and the criteria for the instruction are stored in a new block header called a “Policy Header”. The policy header is used for authorizing each army’s node and enforcing owner’s control policy over one’s unit.

Each node refers to the network equipment that the military operates internally. Practical Byzantium Fault Tolerance(PBFT) is used for the block consensus. Each node votes for the node that will create the block, allowing all nodes participating in the distributed system to successfully negotiate asynchronously.

3.3 Block Headers

Block header contains the same header information as other existing blockchains such as version, previous block hash, merkle hash and time. The paper suggested a new header information called “Policy Header”. The policy header allows the system to set the access rights to the block and the request related to the command execution of the army.

As shown in the upper right corner of Figure 1, there are four parameters in the policy header. The “Requester” parameter refers to the requestor’s public key of the received overlay transaction. The second column in the policy header indicates the action requested in the transaction. The commander can set the type of transaction such as requesting surveillance, reconnaissance, and what kind of command is required. Additional information is stored in ASCII format in short sentences. The third column in the policy header, Unit ID, is the ID of the military unit or nodes, and the last column indicates that the transaction has permission.



Structure of Transaction

Previous Transaction	Transaction Number	Unit ID	Transaction Type
N = Genesis Tx	#		C : Command S : Surveillance A : Access

Policy Header

#	Requester	Request for	Unit ID	Permission
1	Dkslicn12	C		1 Allowed
2	All	S		0 Deny
3	zqojdj27	S		1

Fig. 1. Block Structure of suggested C2 Framework

3.4 Structure of Transaction

Command and Control platform’s transaction stores information that can intuitively understand. In this transaction history, all requests and the history of the nodes are stored regardless of the permission. Verification whether the transaction is executable is created in the policy header’s permission field. Also, when transactions related to authorization are stored, they are added to the policy header of the next block.

4 Conclusions

This paper proposed a concept and schema for developing a command control framework using a private block chain. The paper constructed the aggregation of network node with Practical Byzantine Fault Tolerance, which is the algorithm of private blockchain, and added "policy header" which can store the information necessary for military command and control.

By using the blockchain, the military can gain information advantage and the three elements of security will be satisfied. Confidentiality is satisfied through authorization of the private blockchain and Integrity is satisfied with the Merkle-hash. Also, network fault tolerance helps framework to satisfy availability. This will enable ally to establish a cyber strategy with the best defensive aspects.

However, it will not be able to show superior performance compared to the centralized cyber command control framework as a platform to utilize for gigantic and rapid command and control in an imminent wartime condition. Though, this schema and framework will be the cornerstone. As computing power to calculate hashes improves and each network device developed, the problem will be solved.

Acknowledgment

This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract. (UD060048AD)

REFERENCES

[1] Barnas, N. B. Blockchains in National Defense: Trustworthy Systems in a Trustless World. Blue Horizons Fellowship, Air University, Maxwell Air Force Base, Alabama 2016.

[2] Guegan, Dominique. Public Blockchain versus Private blockhain 2017.

[3] Kwon, Jae. Tendermint: Consensus without mining. *Draft v. 0.6, fall* 2014.

[4] Castro, Miguel, and Barbara Liskov. Practical Byzantine fault tolerance. *OSDI*. Vol. 99. 1999.

Kyoungmin Kim is currently a B.S student in the Department of Cyber Defense(CYDF) of Korea University since 2015. His research interests include Risk management and Blockchain.

Junwoo Seo is currently a B.S student in the Department of Cyber Defense(CYDF) of Korea University since 2015. His research interests include Risk management and Blockchain.

Mookyu Park received the B.S. degrees from Sejong University in 2014, Currently he is an Ph.D student in the Center for Information Security Technologies(CIST) of Korea University since 2014. His research interests include Data minig and Risk management.

Moosung Park received the B.S. degrees from Sogang University of in 1988 , M.S. degrees from Sogang University in 1990, Ph.D degrees from Kwangwoon University in 2004. Currently he works for Agency for Defense Development. His research interests include Cyber defense and Cyber sitautional awareness.

Kyungho Lee received the B.S. degrees from Sogang University of in 1989 , M.S. degrees from Sogang University in 1997, Ph.D degrees from Korea University in 2009. Currently he is Associate Professor in the Department of Cyber Defense and the Center for Information Security Technologies(CIST) of Korea University. His research interests include Risk management, Information security consulting, Privacy policy and Privacy impact assessment.