 CMC, vol.60, no.1, pp.1-14, 2019

A DPN (Delegated Proof of Node) Mechanism for Secure Data Transmission in IoT Services

Dae-Young Kim[1], Se Dong Min[2, †] and Seokhoon Kim[3, †, *]

Abstract: The importance of Blockchain and IoT technology have been highlighted in various fields. These are not unaccustomed words anymore in our lives. Although the technologies are in the infancy step and are still many remaining technical challenges, there is no doubt that it will be one of the major parts of the future Internet. The efficiency and security of data transmission scheme have always been major issues in the legacy Internet, and a data transmission scheme for the future Internet, including 5G and IoT environment should also provide and support these issues. Consequently, we propose a new data transmission scheme to successfully support the future Internet environment. The proposed scheme, which is named as S-DTS (Secure Data Transmission Scheme), supports a distributed transmission and decentralized access control. The S-DTS utilizes 4 synchronization zones, which are IoT network zone, aggregation zone, mining zone, and management zone, and these zones are operated by the DPN (Delegated Proof of Node) mechanism. Furthermore, all nodes are categorized to the 3 node groups, LDTG (Low Delay Tolerance Group), MDTG (Medium Delay Tolerance Group), HDTG (High Delay Tolerance Group), to provide an efficient data transmission, and the data in each group will be transmitted in accordance with their own traffic attributes. The evaluation results of this scheme show that it is very suitable for massive IoT environment scenarios, and IoT devices can take advantage of safe and efficient transmission by using the delegated proof of node technique. In addition, the S-DTS might be adaptable for various computing and networking environment with big data, edge cloud and cloud computing, and autonomous networking.

Keywords: Data transmission scheme, blockchain, delegated proof of node, public IoT service, synchronization.

1 Introduction

Nowadays, the 4th Industrial Revolution, which is based on various intelligent information

[1] School of Information Technology Engineering, Daegu Catholic University, 13-13, Hayang-ro, Hayang-eup, Gyeongsan, 38430, Republic of Korea.

[2] Department of Medical IT Engineering, Soonchunhyang University, 22, Soonchunhyang-ro, Sinchang-myeon, Asan, 31538, Republic of Korea.

[3] Department of Computer Software Engineering, Soonchunhyang University, 22, Soonchunhyang-ro, Sinchang-myeon, Asan, 31538, Republic of Korea.

[†] These authors have contributed equally to this work.

[*] Corresponding Author: Seokhoon Kim. Email: seokhoon@sch.ac.kr.

CMC. doi:10.32604/cmc.2019.06102 www.techscience.com/cmc

technologies such as IoT, Cloud, Bigdata, Mobile, Security, has been an inevitable phenomenon [Mohaisen, Mekky, Zhang et al. (2015); Scriber (2018)]. These technologies have been widely deployed to provide various services, and it has been one of the key factors of infrastructures in the various industrial fields, especially the future Internet. Among these technologies, the IoT technologies and its devices are main trigger to lead the new paradigm, because most of data in the future Internet environment will be generated by the IoT devices. As a well-known, the IoT related services have already influenced to the related business, and it has been created new global markets. In addition, the data, which are generated from multitudinous IoT devices, will be fundamental data to apply to creative services [Fang, Yao, Wang et al. (2018); Lin, He, Huang et al. (2018)].

Although the IoT technologies have been rapidly evolving in the past years, there are still a lot of technical challenges. Besides that, the network architecture in IoT environment has some important problems in terms of centralization and hierarchy. Generally, the IoT network architecture is very similar to the legacy Internet architecture, because it has been evolved in the expanded form of the existing architecture. It is also analogous in the aspect of the data transmission scheme. However, the legacy network architecture and data transmission scheme are not adequate for the IoT environment, because most of IoT devices with various constraints differ from legacy Internet nodes in computing power, power consumption, and so on. To solve these problems, the architecture and data transmission scheme can have to support a decentralized and distributed accessibility in the IoT environment. Moreover, the architecture and data transmission scheme are more easily to embrace numerous IoT devices, which has various limitations [Kim and Kim (2017); Ryoo, Na and Kim (2015); Kang, Yu, Huang et al. (2017); Zhang, Wang, Wang et al. (2018)].

In this paper, we propose a new secured data transmission scheme for various IoT services. The proposed scheme is based on a delegated proof of node, which is very similar to the blockchain technology. By adopting delegated proof of node, the proposed scheme not only supports a secure transmission in IoT environment, but also provides an efficient data forwarding by using accurate and precise synchronization within their synchronization zone. By doing this, it can support decentralized access and control, distributed information and authority, secured and efficient data forwarding, and so on.

The remainder of this paper is organized as follows. In Section 2, related works on IoT architecture and service are described, and the proposed scheme and its performance evaluation are discussed in Section 3 and Section 4, respectively. Finally, finally Section 5 is brought to concluding remarks.

2 Related works

2.1 Consensus algorithms

In the blockchain system, all nodes must keep the same transaction records for the transaction. To do this, the blockchain system uses consensus algorithms, which are consisted of the proving work of the transaction and the selecting policy of the block. Although there are some differences between permissionless and permissioned blockchain, the consensus algorithms are certainly needed to achieve a goal of blockchain technology for providing a decentralized control and distributed information [Yim, Yoo, Kwak et al. (2018); Yu, Arifuzzaman, Wen et al. (2015)]. However, these consensus algorithms in the

permissionless blockchain system have many limitations in terms of performance, power consumption and so on. There are some works to surmount these limitations in the past a few years, and these are followings.

2.1.1 PoW (Proof of Work)

As a well-known, the PoW is a mechanism, which is operated to find a specific hash value to create a new block in the blockchain system [Christidis and Devetsikiotis (2016)]. In the mechanism, the miners have to compete to discover the hash value, and then a new block will be created whenever a specific miner finds a defined hash value. In the bitcoin system, the hash value is expressed as followings.

$$hash\ (Block) \leq Max/D \tag{1}$$

where *hash (Block)* is the hash value of the block, *D* is the difficulty, and *Max* is the maximum value of difficulty (*D, 2^{256}-1*). The difficulty of hash value will be periodically adjusted to keep the new block creation cycle in the bitcoin system. Notwithstanding the bitcoin system is using the random block creation mechanism, the fork status, which has 2 or more children blocks concurrently, can be generated. In this case, the bitcoin system will choose the longest chain to solve the discordance of blockchain.

2.1.2 PoS (Proof of Stake)

The PoS was proposed one of the alternatives of the PoW to settle a high energy consumption, it is also one of the consensus algorithms to reflect holding asset of participants [Li, Liu, Cheng et al. (2018); Cebe, Erdin, Akkaya et al. (2018)]. In the PoS mechanism, miners can create a new block in accordance with their holding asset, and it is different from the PoW in this aspect. The hash function in the PoS mechanism is expressed as followings:

$$hash\ (\ hash\ (Block_{prev}), A, TS) \leq Bal\ (A)\ Max/D \tag{2}$$

where $Block_{prev}$ is the previous block, *A* is the address, *TS* is the timestamp, *Bal (A)* is the balance of address *A*, and *Max* and *D* are the same as the PoW hash. As shown in the expression (2), stakeholders with many holding assets can easily make a new block. In this mechanism, there are some compensation methods of applying the coin age and weight because rich stakeholders have always advantage than the others. Although these compensation methods have been developed to revise a block generation ratio, there are still weak points in the PoS mechanism which cannot quickly make a valid consensus. The DPoS (Delegated Proof of Stake) mechanism was suggested to resolve the weak points. In the DPoS mechanism, a stakeholder delegates their block generation authority to a delegator by using an election system, and then the delegators will generate the new valid block and verify the consensus. Consequently, the DPoS is used to the various recent system because it can reduce cost and time than the other mechanisms [Uriarte and De Nicola (2018); Rosa and Rothenberg (2018)].

2.1.3 PoET (Proof of Elapsed Time)

The PoET is a latest mechanism which can reduce energy consumption and guarantee

analogous security level to the PoW. The PoET is a kind of consensus algorithm based on the security module (Intel SGX). In the PoET mechanism, many practicable nodes will be participated to elect a leader fairly and efficiently. It uses the CPU commands to provide randomness and security when the nodes elect a leader. Although the PoET can provide a robustness of valid consensus, it has a disadvantage, which has to use an Intel SGX.

2.2 Pub/Sub communications

Nowadays, the ICN (Information Centric Networking) has been one of spotlighted networking technology. This networking technology is different from the legacy TCP/IP networking technology in aspect of data handling, and it works routing and forwarding based on the information name. In addition, it is more efficient than TCP/IP networking technology because it utilizes the information caching method in their networks. Therefore, the ICN technology will be a main infrastructure of the future Internet. In these evolution direction, Pub/Sub (Publish/Subscribe) communication scheme is one of main technology, which can improve the efficiency of future Internet [Wan, Yao, Jing et al. (2018); Zali, Hashemi, Cianci et al. (2018)]. The Pub/Sub communication mechanism is an asynchronous communication method which the source and destination are divided into the publisher and subscriber, respectively.

There are 3 conceptual points to divide into spatial side, temporal side, and synchronous side of this mechanism. Firstly, a publisher and a subscriber do not need to recognize each other in the spatial side. Secondly, they don't need to operate concurrently. This is a different feature in temporal side. Finally, in synchronous side, a publisher and subscriber can proceed a publication process and subscription process separately. The communication scheme between publisher and subscriber is shown in Fig. 1. As shown in Fig. 1, they use an event bus, and it supports an asynchronous event-driven transmission.

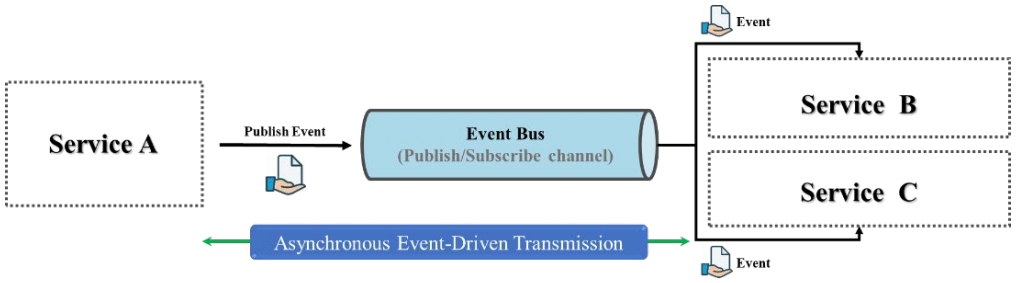


Figure 1: Pub/Sub communication scheme

It is very suitable for IoT communications because of these features. As well-known that the data in IoT environment will be commonly generated by designated events such as sensing, recognition, etc. It means that the generated data in IoT nodes need to transmit to their aggregation node by an asynchronous method, and it should work by using an event-driven method depending on the events. There are some representative Pub/Sub technologies to successfully accomplish to data transmission features for IoT nodes, and it is MQTT (MQ Telemetry Transport), DDS (Data Distribution Service) and so on. Besides these technologies, there are some limelight Pub/Sub researches which are content-based

Publish/Subscribe and ICN, COPSS (Content Oriented Publish/Subscribe System), PSync (Partial Synchronization), and notification in CCN (Content Centric Networking), etc.

3 DPN (Delegated Proof of Node) mechanism

The authority and auditability are very important issues in IoT services, because most of IoT applications will be utilized a decision based on the data from IoT devices. In addition, the aggregated data from IoT nodes can be used raw data to make a decision when they perform various learning algorithms. Hence, a data transmission scheme for IoT services should provide a secure and efficient route from the information publisher node to the information subscriber node.

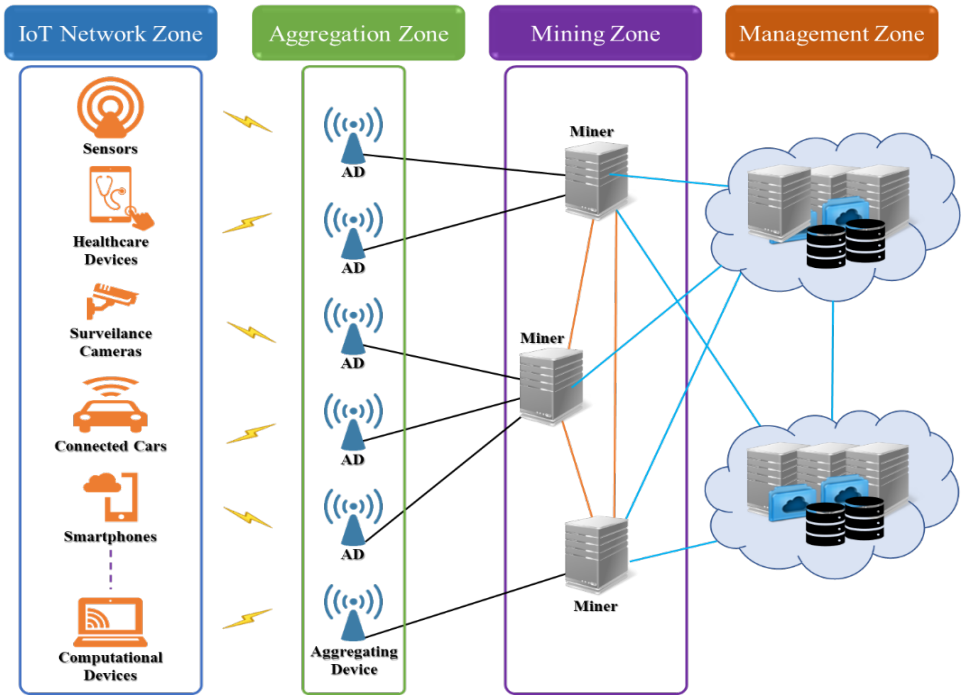


Figure 2: The Delegated proof node concept

As mentioned before, a secure and efficient transmission scheme is very important regardless of legacy Internet and future Internet environment including various IoT services. It is why we propose a new secured transmission scheme. The proposed scheme mainly consists the 2 parts, one is the Delegated Proof of Node (DPoN), the other is the Secure Data Transmission Scheme (SDTS) which includes the DPoN. In this Section 3, we will be focused on the descriptions in terms of the proposed DPoN, the descriptions of SDTS will be discussed in the next Section 4.

The proposed DPoN is very similar to the DPoS of blockchain technology. It also creates a blockchain using the delegation method from participating nodes. However, there are a few different points. The proposed DPoN does not consider to applying to a public blockchain. It means that the DPoN is focused on a service in a private blockchain. Most of

the IoT devices have many limitations in terms of computational power, energy consumption, and their traffic characteristic. These are the main reasons why the IoT devices cannot perform the mining process of blockchain by themselves. A blockchain technology in the DPoN will be only used to verify and to authenticate to each other nodes dues to the fact that the reasons. Furthermore, there is no necessity to use a coin in the blockchain which is generated by DPoN. Although the proposed DPoN has the same problems as the DPoS which are unfair to create to a new block in the aspect of block generation opportunity, it does not important matter because its target is the private blockchain which will be used to support to a specific IoT service from various IoT service providers.

As shown in Fig. 2, the proposed DPoN has several zones, and it is divided into 4 zones, IoT network zone, Aggregation Zone, Mining Zone, and Management Zone, respectively. Each zone has the different roles and functionalities, and the details are as followings.

3.1 IoT network zone

The IoT network zone is a kind of networking area where various IoT nodes are existed. In the DPoN, the roles and functionalities of IoT network zone are same as common IoT networks. There are many IoT nodes, and the node types are varied as shown in Fig. 2. Accordingly, they can easily join and detach to the IoT networks. The various IoT nodes, however, should be passed the authentication process to communicate with other nodes by using the DPoN mechanism, and this authentication process will be performed whenever they want to join or to detach to the IoT network. The IoT node will send an *authentication_request* message to a miner node via aggregation node. And then, the miner node will be sent an *authentication_reply* message to the IoT node with the authentication result. According to the authentication result, the IoT node can start their communications. Henceforth, the communications between IoT node and the aggregation node will be used the CoAP (Constrained Application Protocol).

3.2 Aggregation zone

The aggregation zone is an area where nodes gathering data of IoT nodes such as a sink node in an IoT network environment are congregated. Although there is only shown one type aggregating device in the Fig. 2, the aggregation device types are varied depending on the IoT devices, which the aggregating device should manage to. In this area, the aggregation device not only carries out a role of the anchor node of diverse IoT devices, but also it performs aggregation and management of delegation permission from IoT nodes and delivers the delegation information of IoT node to the miner. However, the aggregation node with low computing power does not carry out the management role to provide an efficient transmission performance, it just performs the delivery role same as the legacy anchor node. In this case, the management role will be processed by the upper mining node.

3.3 Mining zone

The genesis block and additional block in this mechanism are needed to make a blockchain, like as common blockchain technology, and the genesis block will be created by one of the miners which is designated by a managing node.

In this zone, there are many miner nodes which have enough computing power to make a blockchain, we called this area, mining zone. The mining node in this zone fulfills an authentication process of IoT nodes, whenever it receives the *authenthication_request* message from an IoT node. The miner node, which is received the *authentication_request* message, the received information is compared with the existing blockchain contents and node list. The blockchain contents have various information of nodes, which are included node ID, MAC address, duration, etc., and the node list contains a registered node information, which is gathered by an aggregating device. Since then, the miner node will create a new block in the blockchain, will send an *authentication_reply* message to the IoT node if the request information is valid, and will send a *blockchain_update_request* message to the management node. However, the miner node will send a reset message to the IoT node if not the request information is invalid. The hash function of this DPoN is also used to generate a new block, the expression is as followings.

$$hash\,(\,hash\,(Block_{prev}),\,A,\,TS) \leq D_{node}STA\,(A)\,Max/D \quad (3)$$

where $Block_{prev}$ is the previous block, A is the address, TS is the timestamp, $D_{node}STA\,(A)$ is the delegated stake of address A and, Max and D are the same as the PoW hash, respectively. The blockchain in the proposed DPoN is a kind of decentralized authentication and distributed transaction record, and a coin for compensation isn't need since the DPoN uses a private blockchain. In addition, the blockchain can be periodically reset by a management node to improve an efficiency and to save a storage space. Consequently, the DPoN can support very efficient and effective distributed authentication.

3.4 Management zone

This area is a supporting area to manage the DPoN. A management node can be a kind of server nodes, group of server nodes, or cloud. This management node or nodes will superintend a node list, crosschecking of the DPoN blockchain, designating a mining node for generating a genesis block, resetting the blockchain, and so on. In addition, the management node will set information for efficient data transmission for supporting a Pub/Sub mechanism and synchronized transmission scheme.

The Fig. 3 shows message processes in the proposed DPoN. As previously mentioned, the DPoN carries out the authentication process based on a blockchain. In these authentication processes, the delegation process of IoT node will be involved. As shown in Fig. 3, an IoT node sends an *authentication_request* message with delegation information of the IoT node, an aggregating node will perform the verification of delegation and permission based on the node list. Since then, the aggregating node will send a *SC_confirmation_request* message to a miner node. The miner node carries out the verification about the smart contract, which will be supervised by a management node and be synchronized between miner nodes and management nodes, and it will create and update a new block. To this end, the miner node will send a *SC_confirmation_reply* message to the aggregating node and send a *blockchain_update_request* message to the management node. The remaining message processes for updating the blockchain and smart contract information, and data transmission of the IoT node are common as a legacy message process.

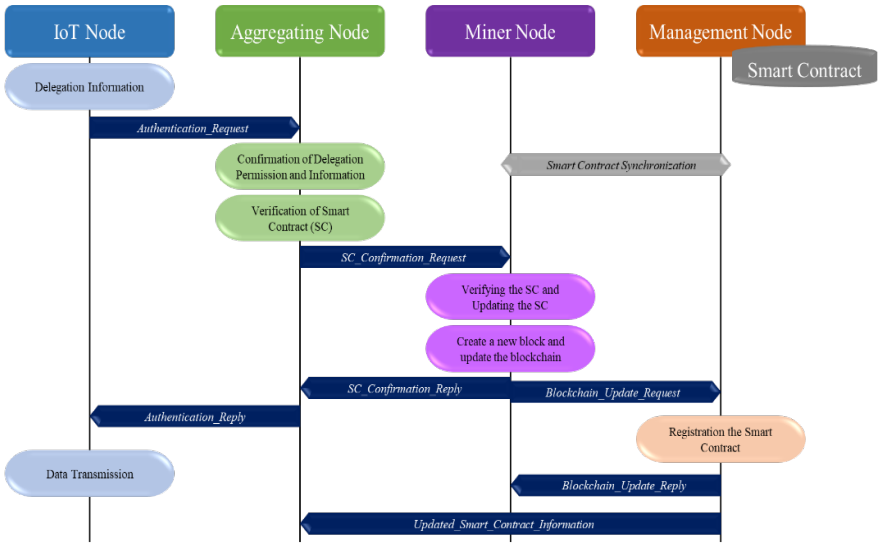


Figure 3: Messaging process in the DPoN

4 Secure data transmission scheme

As mentioned before, the authority, auditability, and efficiency are very important issue in IoT environment. Although the proposed DPoN can be provided the authority and auditability to IoT nodes, there are still insufficient things in the aspect of efficiency. Consequently, a new data transmission scheme is needed to make up for the efficiency, which can be used with the DPoN, and this is the main reason why we propose the new data transmission scheme. To this end, we proposed an enhanced data transmission scheme which is suitable for various IoT environments, and it is named secured data transmission scheme (S-DTS). The proposed S-DTS basically is synchronized data transmission methods, however, it supports the Pub/Sub operations, which are asynchronized data transmission methods. It means that the starting point of data transmission will be controlled by Pub/Sub mechanism, which is more suitable for IoT environment. However, the S-DTS utilizes a synchronization transmission scheme after the transmission start for providing an efficient data transmission.

The concept of proposed S-DTS is fundamentally similar to the concept of S-DTA (Safe Data Transmission Architecture) [Kim and Na (2016)], EPC-DFS (Efficient Peer-to-Peer Context awareness Data Forwarding Scheme) [Kim and Suk (2016)], and ESD-DTS (Efficient Software Defined Data Transmission Scheme) [Kim and Kim (2018)]. Although the S-DTS will be also operates synchronization zones same as the Kim et al. [Kim and Na (2016); Kim and Suk (2016); Kim and Kim (2018)], there are 3 different points mainly. Firstly, the S-DTS will be operated in synchronization zones which are different from the others. Secondly, the S-DTS utilizes new synchronization formulas when it sets up a synchronization time, as expressed in the equations below.

$$Node\_Delay_{all} = \sum_{n=1}^{n}(e_n + p_n + s_n + t_n + TI_n) \quad (4)$$

where e_n is an electronic delay of node n, p_n is a processing delay of node n, s_n is a serialization delay of node n, t_n is a transmission delay of node n, and TI_n is a time interval of node n for using the Pub/Sub mechanism. Therefore, the delay of arbitrary node i and the source-to-destination delay of all nodes are expressed as follows.

$$\begin{aligned} Node\_Delay_{i-node} &= (e_i + p_i + s_i + t_i + TI_i) \\ &\quad - (e_{i-1} + p_{i-1} + s_{i-1} + t_i + TI_i) \\ &\approx (p_i + TI_i) - p_{i-1} = ND_{i-node} \end{aligned} \tag{5}$$

$$Node\_Delay_{all} \approx \sum_{n=1}^{i} ND_{i-node} = Node\_Delay_{approx-all} \tag{6}$$

Based on these expressions (4), (5), and (6), the value of the synchronization initiation message (SIM_{set}) in the S-DTS can be set as follows.

$$SIM_{set} = \frac{\sum_{1}^{R_n} Node\_Delay_{approx-all}}{R_n} - \sum_{n=1}^{all-i} SCM_i + ET_i + TI_i \tag{7}$$

where, R_n is the number of repetitions, SCM_i is the synchronization calculation message (SCM) of node i, ET_i is the error tolerance of node i.

As previously stated, the basic scheme of S-DTS is almost same as the ESD-DTS, and the detailed procedures are described in Kim et al. [Kim and Kim (2018)]. The S-DTS accomplishes the synchronization processes by using SIMs. Although the SDN controller handles these SIMs in the ESD-DTS, the SIMs will be controlled by a management node in the S-DTS. And finally, the S-DTS is based on the DPoN mechanism, it is the most different point than the other schemes. As shown in expression (4), (5), (6) and (7), the value of TI_n is for utilizing DPoN mechanism in the synchronization processes. Therefore, all nodes, which are utilized the DPoN mechanism and are joined to the networks, can securely transmit to their data.

5 Performance evaluation

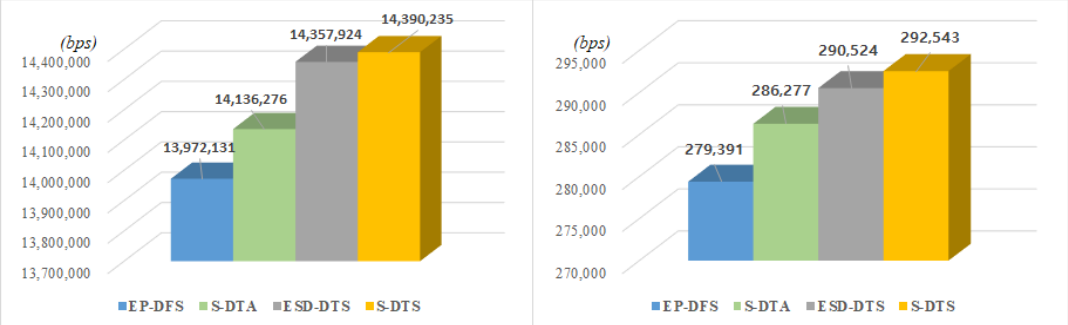
As is well-known, IoT services should consider various service scenarios, because IoT service environment is very dynamic and diverse. Consequently, we have divided the node type into 3 categories to reflect the IoT usage scenarios, and the 3 node types, HDTG (High Delay Tolerance Group), MDTG (Medium Delay Tolerance Group), and LDTG (Low Delay Tolerance Group), are described in the Tab. 1. In addition, we have carried out the computer simulations to verify the proposed S-DTS performance in various environments.

In this simulation, we perform comparisons with EP-DFS, S-DTA, ESD-DTS in the aspect of throughput, latency, and accessibility. This is because the proposed S-DTS is a kind of the evolved version of these schemes, EP-DFS, S-DTA, and ESD-DTS. Although there are 3 node types as shown in Tab. 1, we have only used 2 node types, LDTG and MDTG, to measure the throughput and latency in the simulations. These features are not important issue for HDTG, therefore we don't perform the measurements. Hence, we have performed the measurement of accessibility for HDTG. The accessibility feature is more important than throughput and latency, because the node, which is belong to the HDTG, should effectively utilize the limited resources such as power consumption, waking time. Therefore, we have performed the accessibility measurements for the HDTG in the simulations.

There are 50 nodes for each LDTG and MDTG in the source side in the simulation topology and the destination side have included 5 nodes. In addition, there is 1 server for supporting the edge computing in the destination side and the simulation topology of LDTG and MDTG are same. In the throughput and latency measurement simulations, the maximum bandwidth has been set to 15,728,640 bps (15 Mbps) for the nodes of LDTG and has been set to 327,680 bps (320 Kbps) for the nodes of MDTG. In addition, the streaming traffic type, which has high delay sensitivity, has been used the simulations, because we should verify the throughput and latency aspect.

Table 1: Node Types in the Simulations

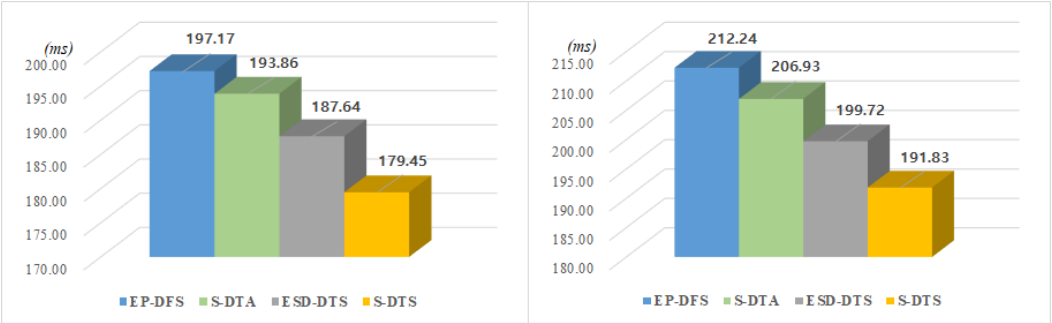
Node Type	Description
LDTG (Low Delay Tolerance Group)	• Required Bandwidth: upper Mbps class or higher • Requires low delay tolerance and high bandwidth
MDTG (Medium Delay Tolerance Group)	• Required Bandwidth: under Mbps class • Requires medium delay tolerance and medium bandwidth
HDTG (High Delay Tolerance Group)	• Required Bandwidth: under Kbps class • Requires high delay tolerance and low bandwidth



(a) Throughput Comparison for LDTG with others (b) Throughput Comparison for MDTG with others

Figure 4: Throughput Comparisons with EP-DFS, S-DTA, and ESD-DTS

Fig. 4 shows average throughput comparisons with EP-DFS, S-DTA, and ESD-DTS. The (a) of Fig. 4 shows an average throughput comparison for LDTG, the (b) of Fig. 4 demonstrates an average throughput comparison for MDTG. As shown in Fig. 4, the average throughput of LDTG and MDTG have not only been slightly increased than the ESD-DTS, but also been reasonably increased than the EP-DFS and S-DTA. Additionally, we have been performed the latency comparisons with other schemes, as shown in Fig. 5. It has been demonstrated in the results of these comparisons, which are also similar to the throughput comparisons, and the average latency of LDTG and MDTG have also been improved than the others.



(a) Latency Comparisons for LDTG with others (b) Latency Comparisons for MDTG with others

Figure 5: Latency Comparisons with EP-DFS, S-DTA, and ESD-DTS

Although the DPN mechanism has been added to the S-DTS, the S-DTS did not degrade than the other schemes in terms of throughput and latency. It means that, the S-DTS has been more efficient mechanism than the others, and the synchronization process and method have been more optimized than the others.

Contrariwise, the simulation topology for HDTG is differ to LDTG and MDTG. There are 500 nodes for HDTG, these nodes have randomly distributed to the source side by using the Poisson Distribution Model. The detailed reference parameters and variables are shown in the Tab. 2.

Table 2: Reference parameters and variables for HDTG

Feature	Description
Contention Slots	384
Data Distribution	Poisson, CBR (Constant Bit Rate)
Data Packet Size	30~300 bytes
Default Buffer Size	2,048 KB
(Threshold Value)	(1)
Duty Cycle	20%
Frame Length	1 ms
Probability Variable	$0 \leq \mathrm{P}(\varrho) \leq 1, 0 \leq \mathrm{P}(\tau) \leq 1$
Threshold Variable	$0 < k_2 \leq 1$
Total Packet Length	10 bytes

In the simulations for HDTG, we did not measure the throughput, because these aren't an important attribute for the nodes of HDTG [Novo (2018)]. Therefore, we provided the simulations in the aspect of timeout in place of the throughput. However, we didn't show the results of timeout ratio measurement, because all schemes have been represented almost same results which are around 47%.

Fig. 6 shows a latency comparison with other schemes for HDTG. It is also similar for the LDTG and MDTG, and this figure demonstrates outperform results than the others.

Although the S-DTS consists more complex mechanism than the other schemes, it has been performed outstanding results. It also means that the S-DTS can support various traffic conditions, even though the nodes have the very high delay tolerance. Consequently, the S-DTS can provide and support diverse data transmission ways, and it is more suitable for massive future Internet environments including IoT and 5G.

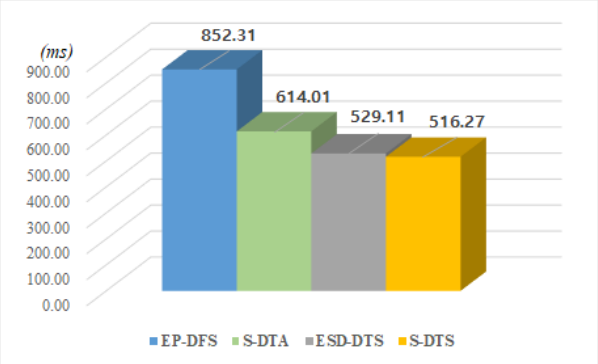


Figure 6: Latency Comparison with EP-DFS, S-DTA, and ESD-DTS for HDTG

6 Concluding remarks

The proposed secured data transmission scheme is mainly consisted 2 parts, one is the delegated proof of node method which is based on a blockchain technology, and the other is the synchronized data transmission mechanism which is supported a Pub/Sub method and operated time synchronization zone. The proposed S-DTS is very suitable for various IoT environments, which is a novel, secure, and scalable. Furthermore, it has not only a decentralized and distributed architecture, but also a secured and efficient data transmission scheme. The superiority of S-DTS has been already demonstrated by various performance evaluations. Consequently, IoT nodes can safely and efficiently transmit their data, and utilize diverse services, through the S-DTS. In addition to this, we will intend to address more efficient and secure data transmission architecture, and we will upgrade a function of management node for supporting more autonomous computing and networking in further researches. Finally, we will proceed the furthermore study for combination of SDN technology and DPoN technology.

Acknowledgement: This research was supported by the MSIT (Ministry of Science, ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2015-0-00403) supervised by the IITP (Institute for Information & Communications Technology Promotion), and this work was supported by the Soonchunhyang University Research Fund.

References

Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. (2018): Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50-57.

Christidis, K.; Devetsikiotis, M. (2016): Blockchains and smart contracts for the Internet of Things. *IEEE Access*, vol. 4, no. 1, pp. 2292-2303.

Fang, C.; Yao, H.; Wang, Z.; Wu, W.; Jin, X. et al. (2018): A survey of mobile information centric networking: research issues and challenges. *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2353-2371.

Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y. et al. (2017): Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154-3164.

Kim, D. Y.; Kim, S. (2017): Dual-channel medium access control of low power wide area networks considering traffic characteristics in IoE. *Cluster Computing*, vol. 20, no. 3, pp. 2375-2384.

Kim, E.; Kim, S. (2018): An efficient software defined data transmission scheme based on mobile edge computing for the massive IoT environment. *KSII Transactions on Internet and Information Systems*, vol. 12, no. 2, pp. 974-987.

Kim, S.; Na, W. (2016): Safe data transmission architecture based on cloud for Internet of Things. *Wireless Personal Communications*, vol. 86, no. 1, pp. 287-300.

Kim, S.; Suk, J. (2016): Efficient peer-to-peer context awareness data forwarding scheme in emergency situations. *Peer-to-Peer Networking and Applications*, vol. 9, no. 3, pp. 477-486.

Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W. et al. (2018): CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204-2220.

Lin, C.; He, D.; Huang, X.; Khurram-Khan, M.; Choo, K. R. (2018): A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems. *IEEE Access*, vol. 6, no. 1, pp. 28203-28212.

Mohaisen, A.; Mekky, H.; Zhang, X.; Xie, H.; Kim, Y. (2015): Timing attacks on access privacy in information centric networks and countermeasures. *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 675-687.

Novo, O. (2018): Blockchain meets IoT: an architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184-1195.

Rosa, R.; Rothenberg, C. E. (2018): Blockchain-based decentralized applications for multiple administrative domain networking. *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 29-37.

Ryoo, I.; Na, W.; Kim, S. (2015): Information exchange architecture based on software defined networking for cooperative intelligent transportation systems. *Cluster Computing*, vol. 18, no. 2, pp. 771-782.

Scriber, B. A. (2018): A framework for determining blockchain applicability. *IEEE Software*, vol. 35, no. 4, pp. 70-77.

Uriarte, R. B.; De Nicola, R. (2018): Blockchain-based decentralized cloud/fog solutions: challenges, opportunities, and standards. *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 22-28.

Wan, M.; Yao, J.; Jing, Y.; Jin, X. (2018): Event-based anomaly detection for non-public industrial communication protocols in SDN-based control systems. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 447-463.

Yim, J. C.; Yoo, K. H.; Kwak, J. Y.; Kim, S. M. (2018): Blockchain and consensus algorithm. *Electronics and Telecommunications Trends*, vol. 33, no. 1, pp. 45-56.

Yu, K.; Arifuzzaman, M.; Wen, Z.; Zhang, D.; Sato, T. (2015): A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid. *IEEE Transactions on Instrumentation and Measurement*, vol. 64, no. 8, pp. 2072-2085.

Zali, Z.; Hashemi, M. R.; Cianci, I.; Grieco, A.; Boggia, G. (2018): A controller-based architecture for information centric network construction and topology management. *China Communications*, vol. 15, no. 7, pp. 131-145.

Zhang, J. J.; Wang, F. Y.; Wang, X.; Xiong, G.; Zhu, F. et al. (2018): Cyber-physical-social systems: the state of the art and perspectives. *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 829-840.