INTERNET 2018

The Tenth International Conference on Evolving Internet

ISBN: 978-1-61208-644-6

June 24 - 28, 2018

Venice, Italy

INTERNET 2018 Editors

Dirceu Cavendish, Kyushu Institute of Technology, Japan

Nicola Fabiano, Studio Legale Fabiano, Rome

INTERNET 2018

Forward

The Tenth International Conference on Evolving Internet (INTERNET 2018), held between June 24, 2018 and June 28, 2018 in Venice, Italy, dealt with challenges raised by evolving Internet making use of the progress in different advanced mechanisms and theoretical foundations. The gap analysis aimed at mechanisms and features concerning the Internet itself, as well as special applications for software defined radio networks, wireless networks, sensor networks, or Internet data streaming and mining.

Originally designed in the spirit of interchange between scientists, Internet reached a status where large-scale technical limitations impose rethinking its fundamentals. This refers to design aspects (flexibility, scalability, etc.), technical aspects (networking, routing, traffic, address limitation, etc), as well as economics (new business models, cost sharing, ownership, etc.). Evolving Internet poses architectural, design, and deployment challenges in terms of performance prediction, monitoring and control, admission control, extendibility, stability, resilience, delay-tolerance, and interworking with the existing infrastructures or with specialized networks.

While many attempts are done and scientific events are scheduled to deal with rethinking the Internet architecture, communication protocols, and its flexibility, the current series of events starting with INTERNET 2009 is targeting network calculi and supporting mechanisms for these challenging issues.

The conference had the following tracks:

- Internet challenges
- Internet of Things and Blockchain

We take here the opportunity to warmly thank all the members of the INTERNET 2018 technical program committee, as well as all the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated their time and effort to contribute to INTERNET 2018. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

We also gratefully thank the members of the INTERNET 2018 organizing committee for their help in handling the logistics and for their work that made this professional meeting a success.

We hope that INTERNET 2018 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the field of the evolving Internet. We also hope that Venice, Italy provided a pleasant environment during the conference and everyone saved some time to enjoy the unique charm of the city.

INTERNET 2018 Chairs

INTERNET Steering Committee

Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Dirceu Cavendish, Kyushu Institute of Technology, Japan
Steffen Fries, Siemens AG, Germany
Terje Jensen, Telenor, Norway
Cristina Alcaraz, University of Malaga, Spain
Parimala Thulasiraman, University of Manitoba - Winnipeg, Canada
Wladyslaw Homenda, Warsaw University of Technology, Poland
Onur Alparslan, Osaka University, Japan

INTERNET Industry/Research Advisory Committee

Michael Bahr, Siemens AG Corporate Technology, Munich, Germany
Marcin Markowski, Wroclaw University of Science and Technology, Poland
Hanmin Jung, KISTI, Korea
Paolo Barattini, Kontor 46, Italy
Yung Ryn (Elisha) Choe, Sandia National Laboratories, Livermore, USA

INTERNET 2018

Committee

INTERNET Steering Committee

Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Dirceu Cavendish, Kyushu Institute of Technology, Japan
Steffen Fries, Siemens AG, Germany
Terje Jensen, Telenor, Norway
Cristina Alcaraz, University of Malaga, Spain
Parimala Thulasiraman, University of Manitoba - Winnipeg, Canada
Wladyslaw Homenda, Warsaw University of Technology, Poland
Onur Alparslan, Osaka University, Japan

INTERNET Industry/Research Advisory Committee

Michael Bahr, Siemens AG Corporate Technology, Munich, Germany
Marcin Markowski, Wroclaw University of Science and Technology, Poland
Hanmin Jung, KISTI, Korea
Paolo Barattini, Kontor 46, Italy
Yung Ryn (Elisha) Choe, Sandia National Laboratories, Livermore, USA

INTERNET 2018 Technical Program Committee

Ala Al-Fuqaha, Western Michigan University, USA
Cristina Alcaraz, University of Malaga, Spain
Onur Alparslan, Osaka University, Japan
Ioannis Anagnostopoulos, University of Thessaly, Greece
Liz Bacon, University of Greenwich, UK
Mohamad Badra, Zayed University, Dubai, UAE
Michael Bahr, Siemens AG Corporate Technology, Munich, Germany
Zubair Baig, Edith Cowan University, Western Australia
Arijit Banerjee, Federated Wireless Inc., USA
Paolo Barattini, Kontor 46, Italy
Andrzej Beben, Warsaw University of Technology, Poland
Nik Bessis, Edge Hill University, UK
Maumita Bhattacharya, Charles Sturt University, Australia
Quentin Bodinier, SCEE/IETR - CentraleSupélec, Rennes, France
Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Fernando Boronat, Universidad Politécnica De Valencia-Campus De Gandia, Spain
Stefan Bosse, University of Bremen, Germany
Christos J. Bouras, University of Patras, Greece
Dirceu Cavendish, Kyushu Institute of Technology, Japan
Lianjie Cao, Purdue University, West Lafayette, USA

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Blockchain-based NAT Management for 5G Age

Younchan Jung

School of Information, Communications
and Electronics Engineering
Catholic University of Korea
Bucheon-si, Gyeonggi-do, Republic of Korea
Email: ycjung@catholic.ac.kr

Marnel Peradilla

Computer Technology Department,
College of Computer Studies
De La Salle University - Manila
Manila, Philippines
Email: marnel.peradilla@dlsu.edu.ph

***Abstract*—Full deployment of IPv6 addressing fails because nowadays Network Address Translation (NAT) devices are commonly used to extend internal private addressing from the global public IP addressing. The existing phone system uses the vertical model to solve issues relating to the NAT and mobility management. Also, the horizontal model has been studied, where a centralized Software-Defined network (SDN) controller is in charge of handling network functions such as NAT and mobility management. The goal of this paper is to propose a blockchain-based NAT management (BNATM) scheme to overcome the limitation that both the horizontal model as well as the vertical model face in relation with NAT and mobility management. Our proposal focuses on the idea that, if we use the blockchain technologies, each peer can easily obtain the necessary parameters required to handle the complicated NAT and mobility management procedures. Finally, this paper analyzes the latency comparisons among the proposed BNATM scheme, existing vertical model and centralized controller-based horizontal model.**

Keywords–NAT management; SDN horizontal model; Blockchain; Blockchain-based management; Hash address; Transaction access.

I. INTRODUCTION

The explosive growth of the Internet during 1990s signaled the danger of IP address exhaustion and also created an instant demand on IP addresses. The Internet Engineering Task Force (IETF) simultaneously introduced the IPv6 and Network Address Translation (NAT) [1] [2]. However, full deployment of IPv6 addressing fails because of the NAT's widespread use. Currently, NAT devices are commonly installed at network edges to modify the addresses of packets crossing the NAT.

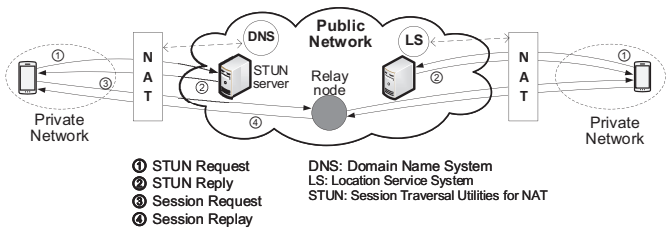


Figure 1. Vertical model for NAT management

NAT has one accessible public address which will be shared among End Nodes (ENs) inside the private network. NAT essentially extends internal addressing from the global IP addressing used over the Internet. NAT provides network resources to get over a shortage of the address space by mapping relatively public IP addresses to private IP addresses [3] [4]. However, the non-standardized characteristics of NAT cause traversal problems. Different NAT network products are available with different proprietary specifications. Therefore, NAT devices start to cause problems especially with the development of peer-to-peer applications [5]–[7].

Three issues are raised in implementing these application systems. First, a smart NAT management is needed in order to manage the private addressing of the local ENs in the private region and solve the NAT traversal issues. Second, the issue of mobility management, which focuses on ENs that use private IP addresses, should be solved. Most of the existing mobility management schemes only deal with the tracking of the location of the EN (that is, the addresses that are closely related to their locations) but not the use of private address [8] [9]. So, NAT management and mobility management functions need to collaborate in order that the application systems be operational. Lastly, for the joint operation of mobility management over the heterogeneous network, a significant portion of the existing work uses vertical model for network functions [10] [11]. As depicted in Figure 1, the existing vertical model for network functions for NAT management and mobility management has limitations in handling an integrated operation of heterogeneous network functions. The current trend for the NAT management and mobility management is to utilize the horizontal model of network functions [12]–[14]. The difference between the horizontal model and the vertical model depends on whether the processing of the network

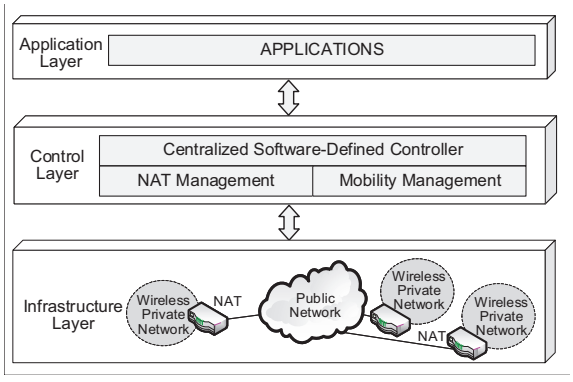


Figure 2. Horizontal model for 5G NAT management

 ISBN: 978-1-61208-644-6

functions takes place on the common control plane. In the horizontal model, all network functions are performed on the control plane, while in the vertical model, data processing and network function processing are performed in the same plane. Software-Defined Networking (SDN) is an emerging networking paradigm change from the vertical model to the horizontal model [15]. As shown in Figure 2, by separating the network's control plane from data plane, the control plane is implemented in a logically centralized controller. The centralized network controller in the control plane manages the intelligence and state of the entire network. However, the current network legacy devices, which operate based on the vertical model, are not yet ready to implement the horizontal model of network functions [16].

The goal of this paper is to develop a Blockchain-based Network Address Translation Management (BNATM) system which performs better in NAT management as well as mobility management than the horizontal model of network functions on the control layer. Figure 3 compares the BNATM system with vertical (or horizontal) model system from the viewpoint of naming and addressing for ENs. A BNATM address is a hash of the public key which is similar to the Bitcoin address in the blockchain-based payment system [17]. In terms of naming, the BNATM system uses the hash addresses differently from the existing system where the domain name is used. From the BNATM addressing point of view, public IP addresses and private IP addresses are used in the public network and a variety of private networks, respectively. However, in the IPv6-based horizontal model, addressing is based only on 128-bit public IP addresses.

		Identity Management	
	Network Service Protocol	**NAME**	**IP Address (Location Address)**
Vertical and Horizontal Model	IPv4 + NAT System	Domain Name	32-bit Public IP Address
		Domain Name	32-bit Private IP Address
	IPv6	Domain Name	128-bit Public IP Address
Proposed System	IPv4 + BNATM*	Hash Address	32-bit Public IP Address
		Hash Address	32-bit Private IP Address

BNATM: Blockchain-based NAT Management

Figure 3. Comparisons of naming and addressing

The BNATM structure is closed to the administrative control that SDN horizonal system operates with. However, a centralized Software-Defined controller on the control plane is in charge of the essential role in order to implement the application-based NAT and mobility management. The BNATM scheme utilizes one of the most innovative features of the blockchain where there is no central server running. It operates through a peer-to-peer network of connected computers or nodes. So, this idea gives significantly advantageous effects on NAT and mobility management by reducing the complexity of the system deployment and latency taken for the end-to-end session set up.

The rest of this paper is organized as follows. Section II proposes the blockchain-based architecture for NAT management. In Section III, this paper explains how to process a transaction to create a block and query/reply mechanism needed to access the transaction information from the blockchain. Section IV describes the improvement effects of the proposed management system. This paper concludes in Section V.

II. BLOCKCHAIN-BASED NETWORK ARCHITECTURE FOR NAT MANAGEMENT

A. Proposed network architecture

Together with explaining the BNATM network architecture (see Figure 4), the steps to run the network are as follows:

1) New transactions are sent to the nearest super node (SN). After a SN receive the transaction message, it broadcasts the message to all SNs. Each transaction message contains several data fields for NAT and mobility management, which will be described in the next section.
2) The SN collects new transactions into a block and performs on solving the proof-of-work for its block. Here, the SN maintains the full blockchain. There are two kinds of blockchains: full blockchain and block-header chain. The EN usually maintains the block-header chain. Later, when the EN needs a certain transaction information, it uses the query/reply mechanism by sending a query message to the nearest SN. Then, the SN searches the corresponding transaction data from the blockchain and returns the requested transaction information to the EN.
3) When an SN finds a proof-of-work, it broadcasts the block to all SNs and ENs.
4) SNs accept the block only if all transactions in it are valid.
5) SNs imply their acceptance of the block by working on creating the next necessary block in the chain, using the hash of the accepted block as the previous hash. SNs will always keep working on extending it. The main role of the EN is to update its NAT-related information by pushing it into the blockchain.
6) ENs accept the new block and extend the next necessary block header in the chain. This means that every EN maintains the block header chain rather than the full blockchain.

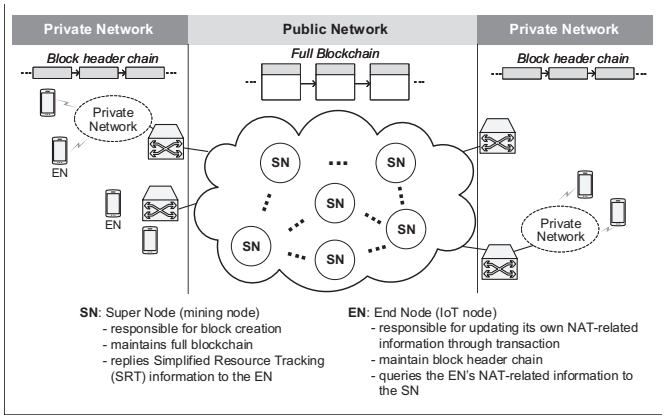


Figure 4. Proposed network architecture for Blockchain-based NAT management scheme

B. Time to get in the blockchain

An SN is responsible for the following functions:

- maintains the entire blockchain to store the entire transaction history,
- verifies incoming transactions by checking digital signatures and confirming the validity of the transaction,
- creates a block using recently collected valid transactions,
- finds a valid nonce to create a valid block header (the proof-of-work part) and,
- hopes that its created block is accepted by other nodes and not defeated by a competitor block created by other SNs.

If the proof-of-work is well designed, this price will be a minor inconvenience (like a short delay) for legitimate ENs but an economic deterrent to attackers of the service. Here, we define the user's waiting time from the moment a new transaction is announced to the network until the transaction successfully gets in the blockchain as Time-to-Get-in-Blockchain (TGinB). It is easy to adjust the average TGinB value by controlling the block creation difficulty. Our BNATM scheme adjusts this difficulty to target 5 seconds between blocks. The period of 5 seconds for TGinB means that it only takes 5 seconds for the blockchain to provide the NAT and mobility control to a certain EN since it moves and joins the new private network.

C. Obtaining public NAT address from the DHCP reply

Private IP addresses must be configured automatically for new ENs that moved from one network to another. Dynamic Host Configuration Protocol (DHCP) enables this entire process to be managed centrally. The DHCP server maintains a pool of private IP addresses and leases an address to any DHCP-enabled EN when it starts up on the network.

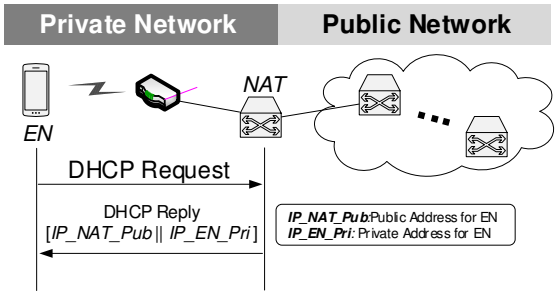


Figure 5. Obtaining public NAT address during private address assignment stage

A DHCP-enabled EN, upon accepting a lease offer, receives a valid private IP address for the private network to which it is currently connecting. There are additional parameters that a DHCP server is configured to assign to ENs. Some examples are router configuration (default gateway), Domain Name System (DNS) servers, and DNS domain name. In the proposed BNATM scheme, instead of using the DNS domain name, the NAT address, which is one accessible public address that will be shared among ENs inside the private network, is included in those parameters DHCP server offers. Figure 5 shows that the DHCP reply message contains the offered private address and the NAT address which will be used as the EN's source address when its packet enters the public network.

D. NAT port number as a function of the private address and port number

When EN sends a packet using its source private IP address and port number (IP_EN_Pri : $Port\_EN\_Pri$) to destination IP address and port number (IP_Dest : $Port\_Dest$), the NAT creates a map for EN's private address and port number (IP_EN_Pri : $Port\_EN\_Pri$) by assigning public $IP\_NAT_{EN}\_Pub$ and $Port\_NAT_{EN}\_Pub$ as public address and port number, respectively. So, incoming packets from [IP_Dest : $Port\_Dest$] destined to [$IP\_NAT_{EN}\_Pub$: $Port\_NAT_{EN}\_Pub$] are forwarded to [IP_EN_Pri : $Port\_EN\_Pri$]. As depicted in Figure 6, the BNATM scheme requires the important condition that $Port\_NAT_{EN}\_Pub$ should be derived from the hash function of IP_EN_Pri and $Port\_EN\_Pri$. EN is aware that NAT devices use the NAT port assignment function of **H16** where the first 16 bits are taken from the hash value.

E. Hash address used in BNATM scheme

Currently, the Long Term Evolution (LTE) communication system uses telephone numbers to identify each user while Voice over Internet Protocol (VoIP) applications use email addresses or domain names. However, in this paper, we propose to use the address derived from the public key to identify either a user or thing, that is, the hash address. A hash address is a hash of the Elliptic Curve Cryptography (ECC) public key. The hash address is the public part of a public-private cryptographic key. The private part of the key is under the control of the user. For example, when an EN moves and changes its private address, the EN creates a new transaction which contains its hash address and sends the transaction to the network. At this moment, the EN also uses its private key to sign the transaction, which results in the signature.

III. TRANSACTION PROCESS TO CREATE A BLOCK AND TRANSACTION ACCESS FROM BLOCKCHAIN

The wallet of EN monitors its state changes, such as private IP address changes. When any changes are found, the EN creates a new transaction and forwards it to the SNs. Then

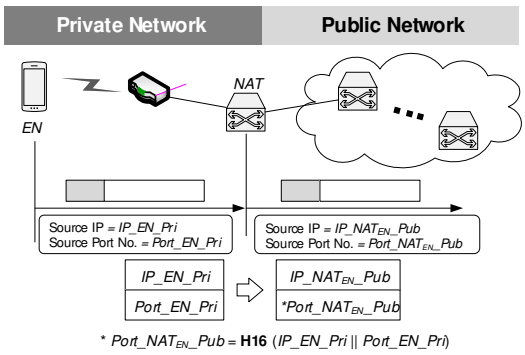


Figure 6. Public NAT port number determined as a function of EN's private IP address and port number

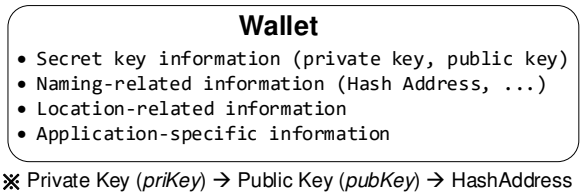


Figure 7. BNATM wallet information

SNs gather the transactions and compete to create the new block, which contains all the transactions after the previous block. Once an SN succeeds to create a block, it forwards the block to the other SNs and ENs. All the SNs maintain the full blockchain. On the other hand, when an EN receives the latest block, it updates the block header chain because the EN maintains chains of block header information excluding the body part of a block. When the SN receives the query from a certain EN, it searches the latest Tx information for the EN from the blockchain and replies to the EN with the information. The full details from transaction creation to the use of transaction information will be discussed in the following subsections.

A. Wallets in BNATM scheme

As shown in Figure 7, it is important for a BNATM user to have some knowledge of how a BNATM wallet software works. The wallet contains the following information:

- Secret key: private key ($priKey$), public key ($pubKey$)
- Naming-related: hash address ($HashAddress$)
- Location-related: IP_EN_Pri, $IP\_NAT_{EN}\_Pub$
- Application-specific: $Port\_NAT_{EN}\_Pub$, $AudioPort\_NAT_{EN}\_Pub$, encoder

The tasks performed by the wallet software also include:

- generates the corresponding public key ($pubKey$) and the hash address ($HashAddress$),
- updates its own location information that is, current private IP address (IP_EN_Pri) and current public NAT address ($IP\_NAT_{EN}\_Pub$) and,
- updates the necessary information for applications.

B. BNATM Transactions

EN's latest state information resides in the user's wallet. Their history is stored into a distributed database called the blockchain. Unlike centralized SDN controller, the blockchain stores a secure list of all transactions. A BNATM transaction is defined as the EN's state information during the period of dynamically assigned private IP address. So, the transaction change rate is the same as private IP address change rate. This means that EN updates its transaction when it moves and obtains a new private IP address. The transaction consists of Transaction Input (TxIn) and Transaction Output (TxOut). The TxIn contains the signature and the public key computed from the EN's private key which creates the transaction. The first field of TxOut contains the hash address that identifies the owner of this transaction.

As illustrated in Figure 8, the TxOut holds three types of fields:

1) Naming-related field: the $HashAddress$ is used for the purpose of searching a certain transaction from the blockchain. $TimeStamp$ is used to find the latest transaction for a given $HashAddress$. It is because among a series of transactions for a certain EN, only the latest transaction residing in the blockchain contains valid state information for the EN.
2) Location-related field: current public NAT address ($IP\_NAT_{EN}\_Pub$), which is important for NAT management and mobility management, indicates the EN's current location for the life of the transaction. The life will expire when the next transaction is issued.
3) Application-specific field: information such as application port number, audio port number and encoder type are included.

Once the EN creates a transaction (Tx) at the circumstance of location change, it sends the new transaction to the network. The first SN in the network that receives the Tx verifies the sent Tx if it is a valid Tx. If the Tx is correct, the SN relays it to other SNs in the network. Figure 9 explains the Tx verification process. To verify that a Tx is valid, an SN follows these steps:

- The script engine evaluates the $<scriptSig>$ of the $TxIn$. This $<scriptSig>$ just places two pieces of data into the stack, those are $<sig>$ and $<pubKey>$.
- The protocol now evaluates the $<scriptPubKey>$ of the $TxOut$ in the previous Tx. **OP_Duplicate** is a command that duplicates the last element of the stack, $<pubKey>$ of the $TxIn$ in the new Tx.
- Then, the **OP_HASHAddress** command computes the $HashAddressIN$ from the last element $<pubKey>$ on the stack.
- The command of **Place_HashAddress** places $<HashAddressOUT>$ onto the stack. This hash

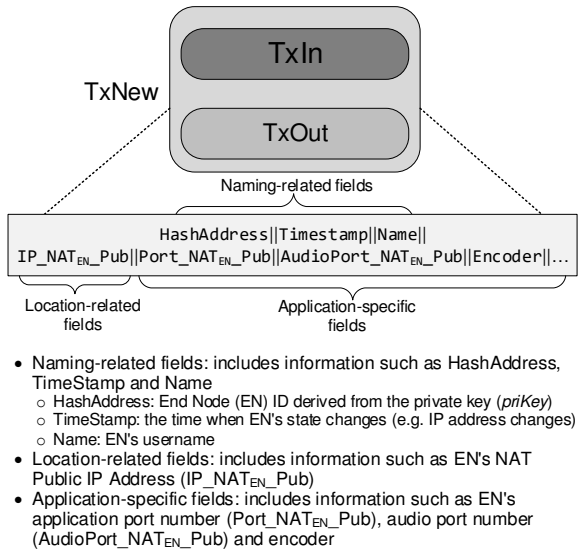


Figure 8. BNATM transaction architecture

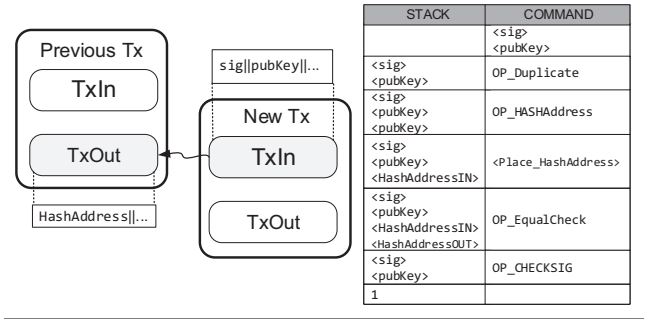


Figure 9. Transaction verification process

address is extracted from the $TxOut$ in the previous Tx.

- The next command is **OP_EqualCheck**. This command checks that the last two elements of $<HashAddressIN>$ and $<HashAddressOUT>$ are equal. If they are not, the Tx is tagged as invalid. After this verification, the two elements are withdrawn from the stack.
- The last command, **OP_CHECKSIG** checks that the Tx signature of $<sig>$ is correct. First, it hashes New Tx and checks that $<sig>$ is the correct signature for this hash. If the signature is correct, the Tx is valid. Otherwise, the Tx is rejected.

C. Blockchain and Proof-of-work

The blockchain is a distributed database holding all the BNATM transactions and keeping a secure list of all the transactions. The EN software that uses the blockchain has to send a query to an SN and receive the corresponding reply for a certain transaction. So, the SN is always ready to parse the blockchain to extract the relevant Tx information. This Tx information returned from the SN is used for the NAT and mobility management.

The blockchain uses proof-of-work to secure the distributed database. An attacker wishing to change the blockchain would have to apply a computational power equivalent to all the computational power spent from that point in time to the present. The blockchain is an ever-growing series of blocks where a certain block has a link to its previous block. Each block contains a group of new Txs created by the ENs. New Txs in the network are collected into a block which is appended to the blockchain. The mining SN is responsible for creating a new block. The scope of this paper does not include the selection protocol of the mining SN. Note that old blocks are never removed from the blockchain, thus the blockchain can only increase in length. The new block is secured with a partial hash inversion proof-of-work.

As shown in Figure 10, each block includes a group of valid Txs and block header information of the hash of the previous block, timestamp, a nonce and the root hash of all Txs. All the Txs in the block body are leaves in the Merkle Tree. Each Tx is hashed and hashes are hashed together to form a binary tree of hash pointers. So, the block header contains two hashes. One is related to the hash of the previous block and the other is the top hash in the binary tree of hash pointers, that is, the root hash. The nonce in a block solves the partial hash inversion problem. That is, the nonce is a number such that

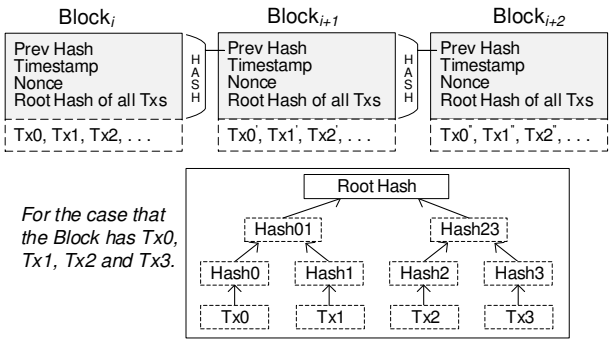


Figure 10. BNATM Blockchain

the hash of the entire block (including the nonce) starts with a certain number of zero bits. So, the block mining difficulty can be controlled by increasing the number of starting zero bits in the hash. The target block mining difficulty can be adjusted to control the TGinB period. This paper assumes that BNATM blocks are generated every 5 seconds. The target of 5 seconds means that on average it takes 5 seconds for an EN to be able to accept the session raised from the other ENs since the EN moves and joins the new private network. Reducing the average TGinB period increases the effective number of blocks updated globally per second, that is, block-creation rate. Our challenge is also to increase the block-creation rate as much as possible. This issue is beyond the scope of this paper.

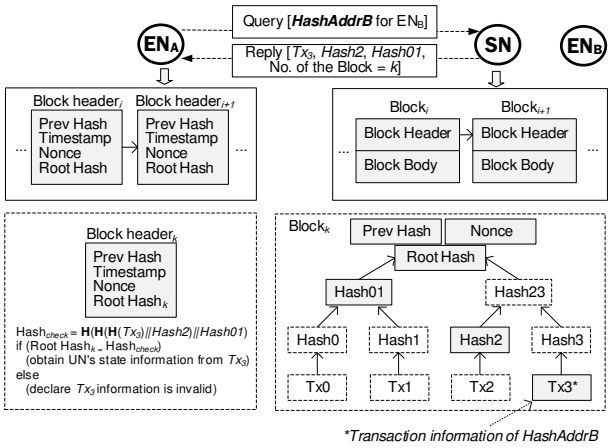


Figure 11. Transaction information access using query/reply mechanism

D. Query/reply mechanism to access transaction information

ENs only keep the block header chain while each SN maintains full blockchain. As shown in Figure 11, when an EN needs the transaction information for a particular hash address, that is, $HashAddrB$, it sends a Query to the nearest SN. Then, the SN parses the corresponding transaction $Tx3$ (it is assumed that $Tx3$ is the latest Tx for the hash address $HashAddrB$) from the blockchain and sends a Reply message to EN. The Reply message contains $Tx3$, $Hash2$, $Hash01$ and No. of the Block. When EN receives these pieces of information, it checks the validity of $Tx3$. It first calculates the

 ISBN: 978-1-61208-644-6

$Hashcheck$, that is, $\mathbf{H}(\mathbf{H}(\mathbf{H}(Tx3)||Hash2)||Hash01)$ where **H** means the hash function. Then, using the block number information contained in the Reply message, EN extracts the $RootHash_k$ at the $Blockheader_k$ in the block header chain. Lastly, the EN compares the extracted $RootHash_k$ to the calculated $Hashcheck$. If the two values are equal, the EN obtains the reliable Tx information for the $HashAddrB$. Otherwise, the EN declares the $Tx3$ information is invalid.

IV. BLOCKCHAIN-BASED NAT MANAGEMENT OPERATION AND IMPROVEMENT EFFECTS

A. Blockchain-based session establishment through NAT and mobility management

In Session Initiation Protocol-based (SIP) VoIP call operation, an end user sends SIP requests to initiate a session. Figure 12 shows a series of steps to complete a session set up between two ENs where they are located within the public network. This means that both of them use public IP addresses. Here, each EN changes its location dynamically. This dynamic feature of the EN requires to include the name and location resolution procedures. So, the DNS and Location Search (LS) system need to be involved to cause the latency problem. Because of the involvement of these two procedures, the vertical model, which passes through a series of these procedures, suffers from a relatively large amount of latency to complete a call set up.

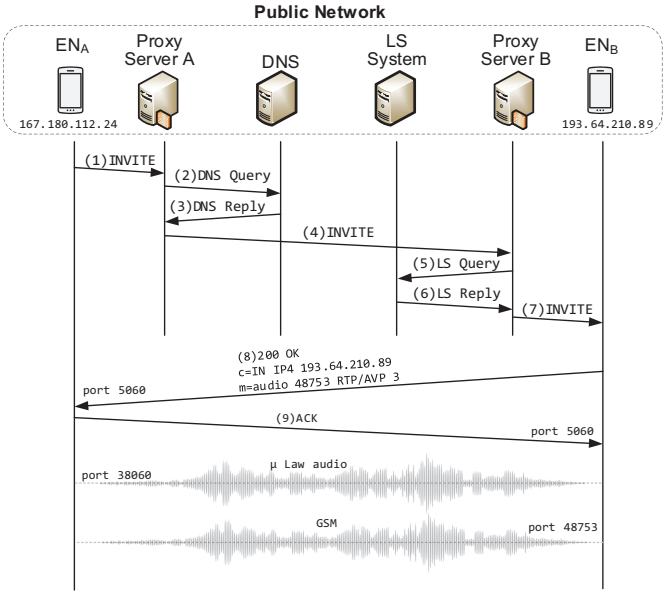


Figure 12. Existing SIP-based VoIP call operation

Figure 13 shows the proposed BNATM-based VoIP call operation. Here, we deal with the case that two ENs are located behind NAT devices. EN_A as well as EN_B belong to the private network. EN_A with the $HashAddrA$ wants to establish a session with EN_B with the $HashAddrB$. EN_A needs to obtain EN_B's state information. Then, EN_A sends (a) QUERY message which contains $HashAddrB$ to the nearest SN. When an SN, which has the full blockchain information, receives the QUERY, it seeks the corresponding Tx for $HashAddrB$. The SN sends back (b) REPLY message containing the Tx information for EN_B. This query/reply mechanism was explained in Subsection III. The query/reply procedure of ((a) and (b)) enables EN_A to obtain EN_B's state information: $HashAddrB$, Timestamp, Name, $IP\_NAT_{ENB}\_Pub$, $Port\_NAT_{ENB}\_Pub$, $AudioPort\_NAT_{ENB}\_Pub$ and encoder type. Here, EN_A resolves the current location of EN_B. Then, EN_A sends (c) INVITE message to $IP\_NAT_{ENB}\_Pub$. This INVITE message contains EN_A's hash address of $HashAddrA$. NAT_A translates the EN_A's private IP address and port number as $IP\_NAT_{ENA}\_Pub$ and $Port\_NAT_{ENA}\_Pub$. When NAT_B receives the packet, it translates the destination IP address and destination port number as $IP\_EN_B\_Pri$ and $Port\_EN_B\_Pri$. When EN_B receives the INVITE message from EN_A, it extracts the EN_A's hash address of $HashAddrA$. Now, the EN_B sends (d) QUERY message which contains the $HashAddrA$ to the nearest SN. When an SN receives the QUERY, it seeks the corresponding Tx for the $HashAddrA$. The SN sends back (e) REPLY message containing the Tx information for EN_A. The transaction access procedure of (d) and (e) enables EN_B to obtain EN_A's state information: $HashAddrA$, Timestamp, Name, $IP\_NAT_{ENA}\_Pub$, $Port\_NAT_{ENA}\_Pub$, $AudioPort\_NAT_{ENA}\_Pub$ and encoder type. At this moment, EN_B sends a Binding Request message toward its NAT device (NAT_B). Acknowledgement for this Binding Request is not necessary. The purpose of the Binding Request is to force the NAT_B to create a mapping entry of $[AudioPort\_NAT_{ENB}\_Pub : AudioPort\_EN_B\_Pri]$. At this moment, EN_B sends (f) 200 OK message to EN_A. After EN_A receives 200 OK message, it sends the Binding Request toward NAT_A. Similarly, the Binding Request from EN_A enables the NAT_A to create a mapping entry of $[AudioPort\_NAT_{ENA}\_Pub : AudioPort\_EN_A\_Pri]$. Finally, EN_A send (g) ACK message to EN_B. As a result, each side can reach the agreement on other session parameters such as audio encoder and others. Then, bidirectional session traffic travels through the established audio channels.

As shown in Figure 13, our blockchain-based session establishment scheme easily solves the problem of handling complex issues of NAT and mobility management. This advantage results from the fact that each peer can obtain the necessary parameters for peer-to-peer session establishment via simple query/reply mechanism between an EN and its nearest SN.

B. Improvement effects of BNATM scheme to complete network management

This paper calls the existing vertical model shown in Figure 12 and BNATM model in Figure 13 as "Vertical Model" and "BNATM Model", respectively. The following assumptions have been made to perform the comparative analysis for NAT and mobility management with respect to total latency to complete this network management between EN_A and EN_B, where each of them are located in different domains.

- The vertical model operates with the public IP addresses for ENs. On the other hand, the BNATM model operates with private addresses for ENs.
- Three types of delays exist, that is,
  1) T_I: intra-domain delay caused in intra-domain links,

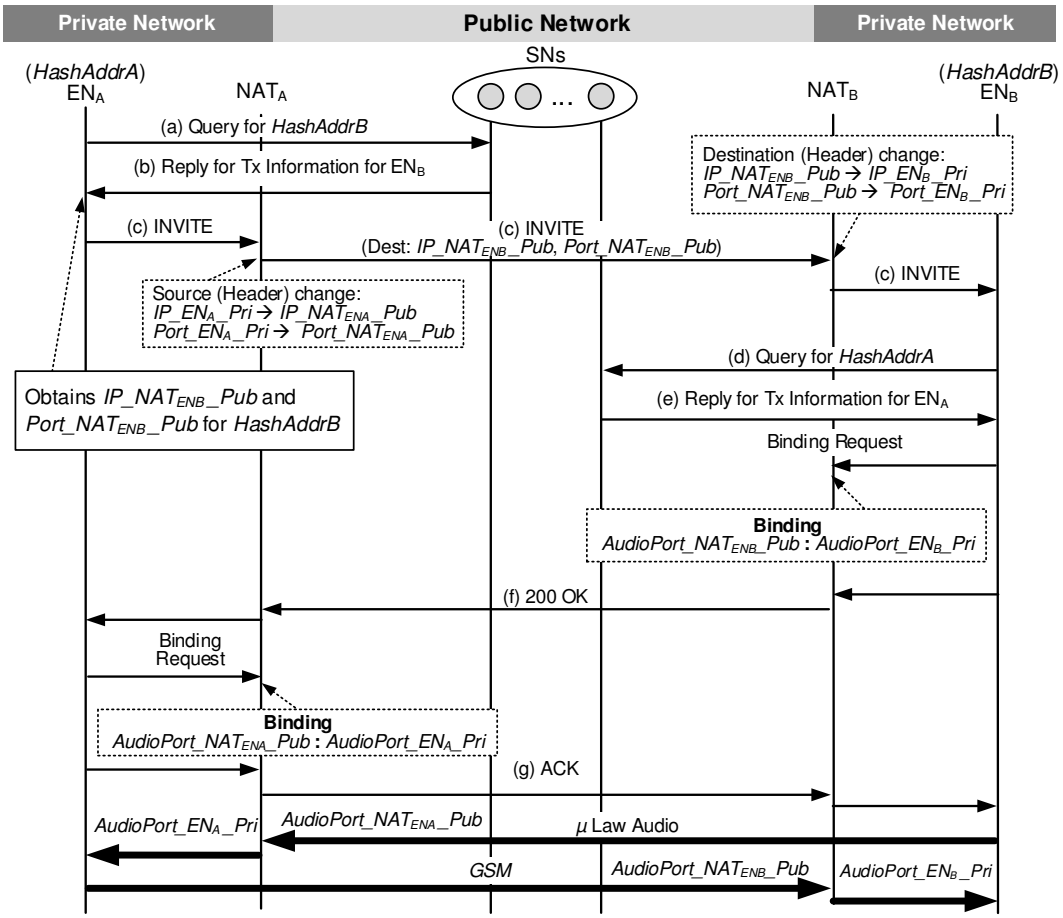


Figure 13. BNATM-based VoIP call operation

2) T_{II}: end-to-end delay caused in end-to-end path,
3) T_{III}: delay caused to collaborate with the distributed servers, which are spread in inter-domain regions.

- $T_{II} = 5T_I$ and $T_{III} = 10T_I$.

We summarize the comparison of the vertical model and BNATM model in Table I. The most interesting point is that the BNAT model does not have Type III delay components. This means that in the BNATM system, there is no need to collaborate with the query/reply procedures of (a), (b), (d) and (e) in Figure 13 to agree on necessary parameters to solve the issues relating to NAT and mobility management. Table I shows that, to reach an agreement on those parameters, the BNATM model requires $19T_I$ compared to existing SIP phone system's $57T_I$. It is very surprising that the BNATM system performs better by 300% than the existing vertical model. Recall that we assume the vertical model operates with the public IP addresses while BNATM model with private addresses for ENs. So, we argue that this 300% improvement on latency is lower bound because the vertical model excludes all the steps necessary for NAT management.

The 300% improvement on latency results from the simple query and reply mechanism to obtain parameters necessary to set up a session to the other side. When a source EN wants to establish a session to destination EN, the source EN sends a query to its neighbor SN to obtain the Tx information for the destination EN. When the SN receives the query from the source EN, it searches the latest Tx information for the destination EN from the blockchain and replies the information to the source EN. As shown in Figure 13, the reply messages of (b) and (e) enable to easily obtain the information of [$IP\_NAT_{ENB}\_Pub$, $Port\_NAT_{ENB}\_Pub$, $AudioPort\_NAT_{ENB}\_Pub$, encoder type, $\cdots$] and [$IP\_NAT_{ENA}\_Pub$, $Port\_NAT_{ENA}\_Pub$, $AudioPort\_NAT_{ENA}\_Pub$, encoder type, $\cdots$], respectively.

C. Performance tradeoff among vertical model, horizontal model and proposed BNATM system

Mid-call mobility management implies the handover process to provide seamless connection when an EN moves to a new network during an on-going session. Mid-call mobility management requires strict conditions on latency to maintain session quality when a handover occurs. According to the existing studies for latency comparisons for vertical and horizontal mobility management models [12], the vertical model yields a latency of 2,850 milliseconds for pre-call mobility management, assuming that the intra-domain delay of T_I is 50 milliseconds. Mid-call mobility solutions that are based on vertical model such as MIPv4 and MIPv6 produce latency performance of 268 milliseconds and 1,128 milliseconds, respectively. Here, the vertical model assumes

the ENs only use public IP addresses and operate without NAT devices. However, our BNATM system assumes that ENs are assigned with private IP addresses and operating behind NAT devices. In the BNATM model, a pre-call mobility management needs the latency of 950 milliseconds and a mid-call mobility management requires an average latency of 5 seconds.

In the proposed BNATM system, the blockchain extends a new block every 5 seconds. This is the reason why the BNATM system suffers from relatively high latency compared to the vertical model, especially in the case of the real-time network function of mid-call mobility management. Note again that the pre-call mobility management latency improves by 300% in the BNATM system compared to the vertical model. Such significant improvement inevitably needs to pay the price of real-time management issues such as the mid-call mobility management cases. As a result, the proposed BNATM system will show better performance over most of the network functions except for the real-time mid-call mobility management.

TABLE I. COMPARISON OF BNATM AND SIP PHONE SYSTEM

	BNATM Model (Proposed BNATM system)	**Vertical Model** (Existing SIP phone system)
Delay components	Type I: (a), (b), (d), (e) Type II: (c), (f), (g) Type III: None	Type I: (1), (7) Type II: (4), (8), (9) Type III: (2), (3), (5), (6)
Latency	$4T_I + 3T_{II} = 19T_I$	$2T_I + 3T_{II} + 4T_{III} = 57T_I$

$Note: T_{II} = 5T_I$ and $T_{III} = 10T_I$

V. CONCLUSION

Existing phone systems, such as the SIP-based VoIP call system, use the vertical model to solve issues related to the NAT and mobility management. As one candidate for future network architecture, the SDN horizontal model has been explored to control network functions such as NAT and mobility management. However, it is very difficult for the centralized SDN controller to replace all existing vertical model-based distributed servers, which are spread in inter-domain regions.

The goal of this paper was to propose a blockchain-based NAT management system to overcome the limitations that both the horizontal model and the vertical model face in solving issues related to NAT management as well as mobility management. Our idea focuses on the fact that, if we use blockchain technologies, each peer can easily reach agreement on the necessary parameters required to handle NAT and mobility management procedures. It is because our BNATM system works without either existing distributed servers in the vertical model or network controller in the horizontal model.

In this paper we proved that, from the latency viewpoint, the BNATM system performs better by 300% than the existing vertical model. As a result, the proposed BNATM system will show better performance over most of the network functions except for the real-time control cases such as mid-call mobility management.

ACKNOWLEDGMENT

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2017R1A2B4006086).

REFERENCES

[1] P. Srisuresh and G. Tsirtsis, "Network Address Translation - Protocol Translation (NAT-PT)," RFC 2766, Feb. 2000. [Online]. Available: https://rfc-editor.org/rfc/rfc2766.txt, accessed February 1, 2018

[2] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 8200, Jul. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc8200.txt, accessed February 1, 2018

[3] R. Ghafouri, A. Ashrafi, and B. V. Vahdat, "Security consideration of migration to IPv6 with NAT (Network Address Translation) methods," in 2015 23rd Iranian Conference on Electrical Engineering, May 2015, pp. 746–749.

[4] S. Kalwar, N. Bohra, and A. A. Memon, "A survey of transition mechanisms from IPv4 to IPv6; Simulated test bed and analysis," in 2015 Third International Conference on Digital Information, Networking, and Wireless Communications (DINWC), Feb 2015, pp. 30–34.

[5] P. Leppaho, N. Beijar, R. Kantola, and J. L. Santos, "Traversal of the customer edge with NAT-unfriendly protocols," in 2013 IEEE International Conference on Communications (ICC), June 2013, pp. 2933–2938.

[6] Y. Wang, S. Xu, J. Wang, Y. Xue, J. Fu, and B. Hu, "Research of NAT traversal based on RTP relay server under mobile internet environment," in 2015 4th International Conference on Computer Science and Network Technology (ICCSNT), vol. 01, Dec 2015, pp. 1370–1374.

[7] W. K. Jia, G. H. Liu, and Y. C. Chen, "NAT-Aware Peer Grouping and Chunk Scheduling for Mesh-Pull P2P Live Streaming Systems," in 2015 IEEE 39th Annual Computer Software and Applications Conference, vol. 2, July 2015, pp. 387–392.

[8] C. E. Perkins, "IP Mobility Support for IPv4, Revised," RFC 5944, Nov. 2010. [Online]. Available: https://rfc-editor.org/rfc/rfc5944.txt, accessed February 1, 2018

[9] D. B. Johnson, J. Arkko, and C. E. Perkins, "Mobility Support in IPv6," RFC 6275, Jul. 2011. [Online]. Available: https://rfc-editor.org/rfc/rfc6275.txt, accessed February 1, 2018

[10] Y. Jung and M. Peradilla, "Host mobility management using combined MIPv6 and DNS for MANETs," in 2013 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Aug 2013, pp. 100–105.

[11] M. B. Yassein, S. Aljawarneh, and W. Al-Sarayrah, "Mobility management of Internet of Things: Protocols, challenges and open issues," in 2017 International Conference on Engineering MIS (ICEMIS), May 2017, pp. 1–8.

[12] M. Peradilla and Y. Jung, "Combined Operations of Mobility and NAT Management on the Horizontal Model of Software-Defined Networking," in Proceedings of the International Conference on Internet of Things and Cloud Computing, ser. ICC '16. ACM, 2016, pp. 31:1–31:10.

[13] Y. Jung, M. Peradilla, and A. Saini, "Software-defined naming, discovery and session control for iot devices and smart phones in the constraint networks," Procedia Computer Science, vol. 110, 2017, pp. 290 – 296, 12th International Conference on Future Networks and Communications (FNC 2017).

[14] K. Tantayakul, R. Dhaou, and B. Paillassa, "Impact of sdn on mobility management," in 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), March 2016, pp. 260–265.

[15] J. H. Cox, J. Chung, S. Donovan, J. Ivey, R. J. Clark, G. Riley, and H. L. Owen, "Advancing Software-Defined Networks: A Survey," IEEE Access, vol. 5, 2017, pp. 25 487–25 526.

[16] S. Azodolmolky, P. Wieder, and R. Yahyapour, "Performance evaluation of a scalable software-defined networking deployment," in 2013 Second European Workshop on Software Defined Networks, Oct 2013, pp. 68–74.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," URL: https://bitcoin.org/bitcoin.pdf, accessed February 1, 2018.

 ISBN: 978-1-61208-644-6

TCP State Driven MPTCP Packet Scheduling for Streaming Video

Ryota Matsufuji, Shinichi Nagayama, Dirceu Cavendish, Daiki Nobayashi, Takeshi Ikenaga
Department of Computer Science and Electronics
Kyushu Institute of Technology
Fukuoka, Japan
e-mail: {q349428r@mail, o108076s@mail}.kyutech.jp {cavendish@ndrc, nova@ecs, ike@ecs}.kyutech.ac.jp

***Abstract*—Video streaming has become the major source of Internet traffic nowadays. Considering that content delivery network providers have adopted Video over Hypertext Transfer Protocol/Transmission Control Protocol (HTTP/TCP) as the preferred protocol stack for video streaming, understanding TCP performance in transporting video streams has become paramount. Recently, multipath transport protocols have allowed video streaming over multiple paths to become a reality. In this paper, we propose packet scheduling disciplines driven by underline TCP flow state for injecting video stream packets into multiple paths at the video server. We show how video streaming performance improves when packet schedulers take into account retransmission state in underlying paths in conjunction with current TCP variants. We utilize network performance measures, as well as video quality metrics, to characterize the performance and interaction between network and application layers of video streams for various network scenarios.**

Keywords*—Video streaming; high speed networks; TCP congestion control; TCP socket state; Multipath TCP; Packet retransmissions; Packet loss.

I. Introduction

Transmission Control Protocol (TCP) is the dominant transport protocol of the Internet, providing reliable data transmission for the large majority of applications. For data applications, the perceived quality of service is the total transport time of a given file. For real time (streaming) applications, the perceived quality of experience involves not only the total transport time, but also the amount of data discarded at the client due to excessive transport delays, as well as rendering stalls due to the lack of timely data. Transport delays and data starvation depend on how TCP handles flow control and packet retransmissions. Therefore, video streaming user experience depends heavily on TCP performance.

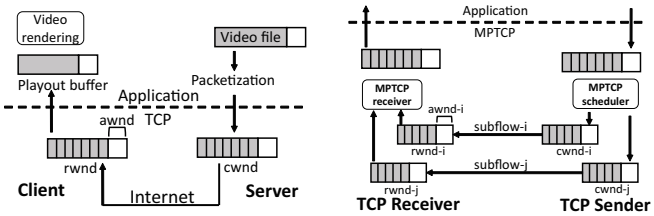
Recently, multipath transport has allowed video streamed over multiple IP interfaces and network paths. Multipath streaming not only augments aggregated bandwidth, but also increases reliability at the transport level session even when a specific radio link coverage gets compromised. An important issue in multipath transport is the path (sub-flow) selection; a packet scheduler is needed to split traffic to be injected on a packet by packet basis. For video streaming applications, head of line blocking may cause incomplete or late frames to be discarded at the receiver, as well as stream stalling. In this work, we introduce the concept of path schedulers based on current status of a TCP sub-flow and evaluate video streaming performance under this type of schedulers. To the best of our knowledge, there has not been a study of path selection mechanisms based on TCP sub-flow state. Specifically, we show that by avoiding paths in retransmission state, video streaming performance improvements can be obtained for different TCP variants and packet scheduler schemes.

The material is organized as follows. Related work discussion is provided on Section II. Section III describes video streaming over TCP system. Section IV introduces the TCP variants addressed in this paper. Section V introduces path schedulers used to support multipath transport, as well as our new TCP state driven path scheduling proposal. Section VI addresses multiple path video delivery performance evaluation for each TCP variant and multiple packet schedulers. Our empirical results in that section show that most schedulers benefit from TCP state awareness. Section VII addresses directions we are pursuing as follow up to this work.

II. Related Work

Although multipath transport studies are plenty in the literature, there has been few prior work on video performance over multiple paths [5] [13] [16]. Regarding multipath schedulers, there has been limited research activity. Yan et al. [18] propose a path selection mechanism based on estimated sub-flow capacity. Their evaluation is centered on throughput performance, as well as reducing packet retransmissions. Yan et al. [2] present a modelling of multipath transport in which they explain empirical evaluations of the impact of selecting a first sub-flow in throughput performance. Hwang et al. [9] propose a blocking scheme of a slow path when delay difference between paths is large, in order to improve data transport completion time on short lived flows. Ferlin et al. [7] introduce a path selection scheme based on a predictor of the head-of-line blocking of a given path. They carry out emulation experiments with their scheduler against the minimum Round Trip Time (RTT) default scheduler, in transporting bulk data, Web transactions and Constant Bit Rate (CBR) traffic, with figure of merits of goodput, completion time and packet delays, respectively. More recently, Kimura et al. [11] have shown throughput performance improvements on schedulers driven by path sending rate and window space, focusing on bulk data transfer applications. Also, Dong et al. [6] have proposed a path loss estimation approach to select paths subject to high and bulk loss rates. Although they have presented some Video Streaming experiments, they do not measure streaming performance from an application perspective. Finally, [17] has proposed a path scheduler based on prediction of the amount of data a path is able to transmit and evaluated it on simulated network scenarios with respect to throughput performance.

 ISBN: 978-1-61208-644-6



(a) TCP (b) MPTCP

Figure 1: Video Streaming over TCP/MPTCP

In contrast, our current work seeks multipath path scheduling principles that can be applied to different path schedulers to improve the quality of video streams. Previously [12], we have proposed new Multipath TCP (MPTCP) path schedulers based on dynamic path characteristics, such as congestion window space and estimated path throughput and evaluated multipath video streaming using these proposed schedulers. In this work, we propose to enhance path schedulers with TCP state information, such as whether a path is in fast retransmit and fast recovery state, to improve video quality in lossy network scenarios. For performance evaluation, we focus on video stream applications and use widely deployed TCP variants on open source network experiments over WiFi access links.

III. Video Streaming over TCP

Video streaming over HTTP/TCP involves an HTTP server, where video files are made available for streaming upon HTTP requests and a video client, which places HTTP requests to the server over the Internet, for video streaming. Figure 1 (a) illustrates video streaming components.

An HTTP server stores encoded video files, available upon HTTP requests. Once a request is placed, a TCP sender is instantiated to transmit packetized data to the client machine. At TCP transport layer, a congestion window is used for flow controlling the amount of data injected into the network. The size of the congestion window, $cwnd$, is adjusted dynamically, according to the level of congestion in the network, as well as the space available for data storage, $awnd$, at the TCP client receiver buffer. Congestion window space is freed only when data packets are acknowledged by the receiver, so that lost packets are retransmitted by the TCP layer. At the client side, in addition to acknowledging arriving packets, TCP receiver sends back its current available space $awnd$, so that at the sender side, $cwnd \leq awnd$ at all times. At the client application layer, a video player extracts data from a playout buffer, filled with packets delivered by TCP receiver from its buffer. The playout buffer is used to smooth out variable data arrival rate.

A. Interaction between Video streaming and TCP

At the server side, the HTTP server retrieves data into the TCP sender buffer according with $cwnd$ size. Hence, the injection rate of video data into the TCP buffer is different than the video variable encoding rate. In addition, TCP throughput performance is affected by the round trip time of the TCP session. This is a direct consequence of the congestion window mechanism of TCP, where only up to a $cwnd$ worth of bytes can be delivered without acknowledgements. Hence, for a fixed $cwnd$ size, from the sending of the first packet until the first acknowledgement arrives, a TCP session throughput is capped at $cwnd/RTT$. For each TCP congestion avoidance scheme, the size of the congestion window is computed by a specific algorithm at time of packet acknowledgement reception by the TCP source. However, for all schemes, the size of the congestion window is capped by the available TCP receiver space $awnd$ sent back from the TCP client.

At the client side, the video data is retrieved by the video player into a playout buffer and delivered to the video renderer. Playout buffer may underflow, if TCP receiver window empties out. On the other hand, playout buffer overflow does not occur, since the player will not pull more data into the playout buffer than it can handle.

In summary, video data packets are injected into the network only if space is available at the TCP congestion window. Arriving packets at the client are stored at the TCP receiver buffer and extracted by the video playout client at the video nominal playout rate.

IV. Anatomy of transmission control protocol

TCP protocols fall into two categories, delay and loss based. Advanced loss based TCP protocols use packet loss as primary congestion indication signal, performing window regulation as $cwnd_k = f(cwnd_{k-1})$, being ack reception paced. Most f functions follow an Additive Increase Multiplicative Decrease (AIMD) strategy, with various increase and decrease parameters. TCP NewReno [1] and Cubic [15] are examples of AIMD strategies. Delay based TCP protocols, on the other hand, use queue delay information as the congestion indication signal, increasing/decreasing the window if the delay is small/large, respectively. Capacity and Congestion Probing (CCP) [3] and Capacity Congestion Plus Derivative (CCPD) [4] are examples of delay based protocols.

Most TCP variants follow TCP Reno phase framework: slow start, congestion avoidance, fast retransmit and fast recovery. For TCP variants widely used today, congestion avoidance phase is sharply different. We will be introducing specific TCP variants' congestion avoidance phase shortly.

A. Multipath TCP

Multipath TCP (MPTCP) is a transport layer protocol, currently being evaluated by IETF, which makes possible data transport over multiple TCP sessions [8]. The key idea is to make multipath transport transparent to upper layers, hence presenting a single TCP socket to applications. Under the hood, MPTCP works with TCP variants, which are unaware of the multipath nature of the overall transport session. To accomplish that, MPTCP supports a packet scheduler that extracts packets from the MPTCP socket exposed to applications and injects them into TCP sockets belonging to a "subflow" defined by a single path TCP session. MPTCP transport architecture is represented in Figure 1 (b).

 ISBN: 978-1-61208-644-6

MPTCP packet scheduler works in two different configuration modes: uncoupled and coupled. In uncoupled mode, each sub-flow congestion window $cwnd$ is adjusted independently. In coupled mode, MPTCP couples the congestion control of the sub-flows, by adjusting the congestion window $cwnd_k$ of a sub-flow k according with parameters of all sub-flows. Although there are several coupled mechanisms, we focus on Linked Increase Algorithm (LIA) [14] and Opportunistic Linked Increase Algorithm (OLIA) [10]. In both cases, a MPTCP scheduler selects a sub-flow for packet injection according to some criteria among all sub-flows with large enough $cwnd$ to allow packet injection.

B. Linked Increase Congestion Control

Link Increase Algorithm (LIA) [14] couples the congestion control algorithms of different sub-flows by linking their congestion window increasing functions, while adopting the standard halving of $cwnd$ window upon packet loss detection. More specifically, LIA cwnd adjustment scheme is as per (1):

$$\begin{aligned} AckRec : cwnd^i_{k+1} &= cwnd^i_k + min(\tfrac{\alpha B_{ack} Mss^i}{\sum_0^n cwnd^p}, \tfrac{B_{ack} Mss^i}{cwnd^i}) \\ PktLoss : cwnd^i_{k+1} &= \tfrac{cwnd^i_k}{2} \end{aligned} \quad (1)$$

where α is a parameter regulating the aggressiveness of the protocol, B_{ack} is the number of acknowledged bytes, Mss^i is the maximum segment size of sub-flow i and n is the number of sub-flows. Equation (1) adopts $cwnd$ in bytes, rather than in packets (Maximum Segment Size - MSS), in contrast with TCP variants equations to be described shortly, because here we have the possibility of diverse MSSs on different sub-flows. However, the general idea is to increase $cwnd$ in increments that depend on $cwnd$ size of all sub-flows, for fairness, but no more than a single TCP Reno flow. The min operator in the increase adjustment guarantees that the increase is at most the same as if MPTCP was running on a single TCP Reno sub-flow. Therefore, in practical terms, each LIA sub-flow increases $cwnd$ at a slower pace than TCP Reno, still cutting $cwnd$ in half at each packet loss.

C. Opportunistic Linked Increase Congestion Control

Opportunistic Link Increase Algorithm (OLIA) [10] also couples the congestion control algorithms of different sub-flows, but with the increase based on the quality of paths. OLIA cwnd adjustment scheme is as per (2):

$$\begin{aligned} AckRec : cwnd^i_{k+1} &= cwnd^i_k + \frac{\frac{cwnd^i}{(RTT^i)^2}}{(\sum_0^n \frac{cwnd^p}{RTT^p})^2} + \frac{\alpha^i}{cwnd^i}, \\ PktLoss : cwnd^i_{k+1} &= \tfrac{cwnd^i_k}{2} \end{aligned} \quad (2)$$

where α is a positive parameter for all paths. The general idea is to tune $cwnd$ to an optimal congestion balancing point (in the Pareto optimal sense). In practical terms, each OLIA sub-flow increases $cwnd$ at a pace related to the ratio of its RTT and RTT of other subflows, still cutting $cwnd$ in half at each packet loss.

D. Cubic TCP Congestion Avoidance

TCP Cubic is a loss based TCP that has achieved widespread usage as the default TCP of the Linux operating system. During congestion avoidance, its congestion window adjustment scheme is:

$$\begin{aligned} AckRec : \quad cwnd_{k+1} &= C(t-K)^3 + Wmax \\ K &= (Wmax\frac{\beta}{C})^{1/3} \\ PktLoss : \quad cwnd_{k+1} &= \beta cwnd_k \\ Wmax &= cwnd_k \end{aligned} \quad (3)$$

where C is a scaling factor, Wmax is the cwnd value at time of packet loss detection and t is the elapsed time since the last packet loss detection (cwnd reduction). Parameters K drives the cubic increase away from Wmax, whereas β tunes how quickly cwnd reduction happens on packet loss. This process recovers its $cwnd$ quickly after causing loss event.

E. Capacity and Congestion Probing TCP

TCP CCP was our first proposal of a delay based congestion avoidance scheme based on solid control theoretical approach. The cwnd size is adjusted according to a proportional controller control law. The cwnd adjustment scheme is called at every acknowledgement reception and may result in either window increase or decrease regardless of loss event. CCP cwnd adjustment scheme is as per (4):

$$cwnd_k = \frac{[Kp(B - x_k) - in\_flight\_segs_k]}{2} \quad 0 \leq Kp \quad (4)$$

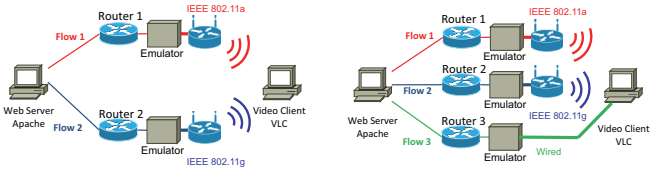
where Kp is a proportional gain, B is an estimated storage capacity of the TCP session path, or virtual buffer size, x_k is the level of occupancy of the virtual buffer, or estimated packet backlog and in_flight_segs is the number of segments in flight (unacknowledged). This fact guarantees a fast responsiveness to network bandwidth variations.

V. TCP State Driven MPTCP Packet Scheduler

MPTCP scheduler selects which sub-flow to inject packets into the network on a packet by packet basis. The default strategy is to select the path with shortest average packet delay. Herein, we introduce this conventional SPD, our previous LPC, LET path selection scheme, as well as a TCP state/retransmission aware packet injection mechanisms.

- **Shortest Packet Delay(SPD):** In shortest packet delay, the scheduler first rules out any path for which there is no space in its sub-flow congestion window (cwnd). Among the surviving paths, the scheduler then selects the path with small smooth round trip time (RTT). Smooth RTT is computed as an average RTT of recent packets transmitted at that sub-flow. Since each sub-flow already keeps track of its smooth RTT, this quantity is readily available at every sub-flow.
- **Largest Packet Credits(LPC):** Among the sub-flows with space in their cwnd, this scheduler selects the one with largest available space. Available space is the number of packets allowed by cwnd size minus the packets that have not been acknowledged yet.

 ISBN: 978-1-61208-644-6



(a) Two Path Network (b) Three Path Network

Figure 2: Video Streaming Emulation Network

- **Largest Estimated Throughput(LET):** In this case, among the sub-flows with large enough cwnd to accommodate new packets, the scheduler estimates the throughput of each sub-flow, as cwnd/sRTT (smooth RTT) and selects the one with largest throughput.
- **RTX Aware:** This supplemental scheme aims to avoid injecting packets into paths that are in retransmit/recovery mode, which would increase packet delivery delay due to head of line blocking. The strategy can be applied on top of any packet scheduler. In this work, it is applied to all previous schedulers (SPDX, LPCX and LETX, respectively). For instance, LETX first eliminates paths in TCP retransmission and among the remaining ones it selects the path of maximum estimated throughput. If all sub-flows are in retransmission state, no path is selected.

The rationale for these proposed schedulers is as follows. LPC addresses the path scenario in which a large RTT path has plenty of bandwidth. In default scheduler, this path may be less preferred due to its large RTT, regardless of having plenty of bandwidth for the video stream. LET addresses the scenario of a short path with plenty of bandwidth. The default scheduler may select this path due to its short RTT. However, if the short RTT has a smaller cwnd, LET will divert traffic away from this path, whereas default scheduler will continue to inject traffic through it. RTX Aware addresses network scenarios experiencing packet loss unevenly across multiple paths.

VI. Video Streaming Performance of Multipath Schedulers

Figure 2 describes the network testbeds used for emulating a network path with wireless and wired access links. On the first testbed, an HTTP Apache video server is connected to two access switches, which are connected to link emulators, used to adjust path delay and inject controlled random packet loss. A VLC client machine is connected to two Access Points, a 802.11a and 802.11g, on different bands (5GHz and 2.4GHz, respectively). On the second testbed, one extra all wired network path is added between the video server and the VLC client. All wired links are 1Gbps. No cross traffic is considered, as this would make it difficult to isolate the impact of TCP congestion avoidance schemes on video streaming performance. The simple topologies and isolated traffic allows us to better understand the impact of differential delays on streaming performance.

We list network settings and scenarios generated by network emulator in Tables I and II, respectively. Video settings are typical of a video stream. Its size is short enough to enable multiple streaming trials within a reasonable amount of time.

TABLE I: EXPERIMENTAL NETWORK SETTINGS

Element	Value
Video size	409 MBytes
Video rate	5.24 Mbps
Playout time	10 mins 24 secs
Video Codec	H.264 MPEG-4 AVC
MPTCP variants	CCP, Cubic, LIA, OLIA
MPTCP schedulers	SPD, LPC, LET, SPDX (rtX aware SPD), LPCX, LETX

TABLE II: EXPERIMENTAL NETWORK SCENARIO

Scenario	Emulator configuration (RTT, Bandwidth, Random loss rate)
3 path Equal Delay (3p-e)	Flow1) RTT 100 ms, BW 3 Mb/s, Loss 0 % Flow2) RTT 100 ms, BW 3 Mb/s, Loss 0 % Flow3) RTT 100 ms, BW 3 Mb/s, Loss 0.5 %
3 path Differential Delay (3p-d)	Flow1) RTT 100 ms, BW 3 Mb/s, Loss 0 % Flow2) RTT 100 ms, BW 3 Mb/s, Loss 0 % Flow3) RTT 50 ms, BW 3 Mb/s, Loss 0.5 %
2 path Equal Delay (2p-e)	Flow1) RTT 100 ms, BW 5 Mb/s, Loss 0.5 % Flow2) RTT 100 ms, BW 5 Mb/s, Loss 0 %
2 path Differential Delay (2p-d)	Flow1) RTT 50 ms, BW 5 Mb/s, Loss 0.5 % Flow2) RTT 100 ms, BW 5 Mb/s, Loss 0 %

For each scenario, path bandwidth capacity is tuned so as to force the use of multiple paths to stream a video playout rate of 5.24Mbps. We also inject 0.5 packet loss rate on the shortest path of each scenario, so as to contrast default packet scheduler (shortest RTT) with other schedulers. TCP variants used are: CCP, Cubic, LIA and OLIA.

Performance measures adopted, in order of priority, are:

- **Picture discards:** number of frames discarded by the video decoder. This measure defines the number of frames skipped by the video rendered at the client side.
- **Buffer underflow:** number of buffer underflow events at video client buffer. This measure defines the number of "catch up" events, where the video freezes and then resumes at a faster rate until all late frames have been played out.
- **Recovery Time from underflow:** amount of time a video playout buffer remains empty after an underflow event. This measure defines how long it takes for underflow event to recover and start rebuffering application data.
- **Sub-flow throughput:** the value of TCP Throughput on each sub-flow. This measure captures how MPTCP operates its scheduling packet injection and whether it is able to maintain a high enough throughput for the video playout rate.

We organize our video streaming experimental results in two network scenarios: i) Two path MPTCP; ii) Three path MPTCP. Each data point in charts represents five trials. Results are reported as average and min/max deviation bars.

A. Two Path MPTCP Performance Evaluation

Figures 3 a, b, c, d, report on video streaming and TCP performance in scenario 2p-e, 2path equal delay and a lossy path. For CCP variant (a), there is a small perceivable video performance (picture discard/buffer underflow) improvement by using RTX awareness on all schedulers. For Cubic TCP variant (b), there is a significant video performance improvement when RTX awareness is used in LPC, whereas LET seems to get worst. On the other hand, LIA and OLIA TCP variants (c,d) provide an appreciable video performance improvement when RTX awareness is used with all schedulers.

 ISBN: 978-1-61208-644-6

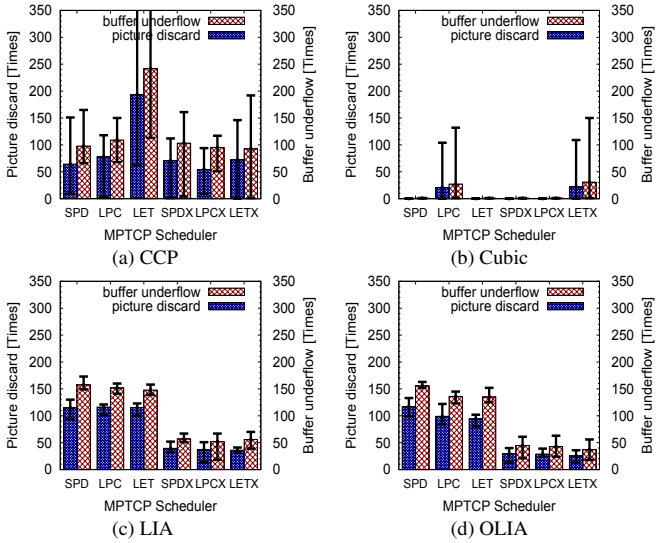


Figure 3: Scheduler Streaming Perf.; Scenario 2p-e

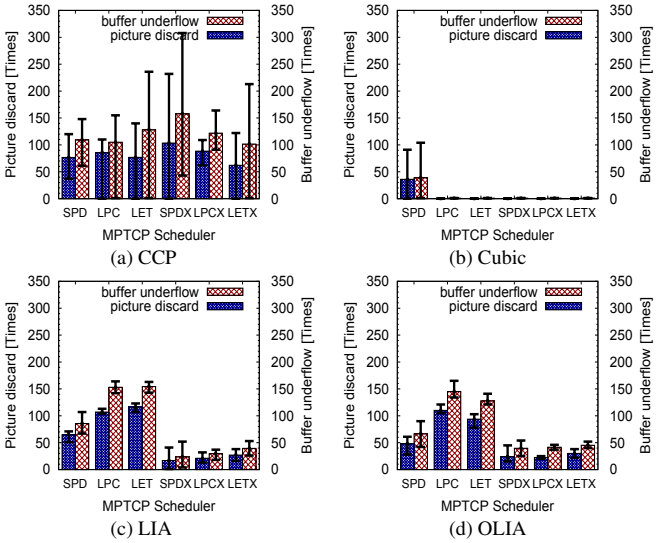


Figure 4: Scheduler Streaming Perf.; Scenario 2p-d

Figures 4 a, b, c, d, describe video streaming performance under network scenario 2p-d, where 0.5 % random packet loss is injected into the shorter delay path. Notice that the SDP scheduler gives preference to shorter delay path, regardless of its packet loss, which hurts performance. For CCP variant (a), there is no perceivable video performance difference among all schedulers. That is because CCP congestion avoidance often suffers from inaccurate estimation of path capacity. In contrast, Cubic often works well for video streaming independently of packet scheduler. On the other hand, coupled LIA and OLIA deliver best video performance when adopting RTX Aware strategy over all schedulers, while non-RTX schedulers cause a lot of video error events. In addition, Figures 5 a, b, c, d, report on corresponding recovery time of each scheduler and TCP variant. We can see that retransmission aware scheduling allows video client to refill quickly video receiver buffer, especially for LIA/OLIA TCP variants. There seems to be little impact on recovery time for more aggressive Cubic/CCP variants, due to their aggressive congestion window ramp up.

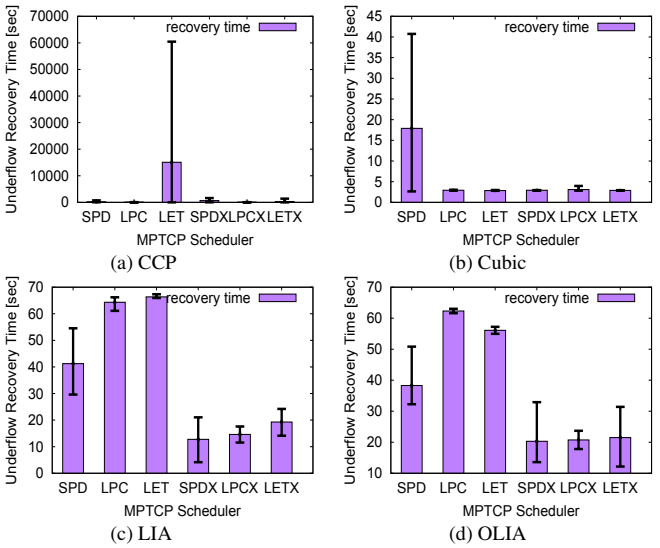


Figure 5: Scheduler Recovery Time.; Scenario 2p-d

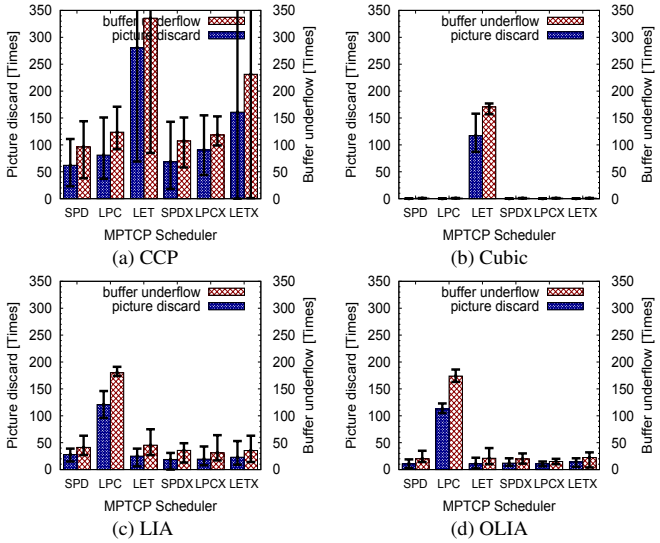
B. Three Path MPTCP Performance Evaluation

Figures 6 a, b, c, d, show video streaming and TCP performance under scenario 3p-e, three path equal delay RTT 100 msec with a 0.5 % random lossy path. In Figure 6 (a), no scheduler is able to improve CCP to deliver high video playout performance in 3 path network scenario. This is because CCP underestimates $cwnd$ in lossy and narrow bandwidth paths. Cubic (6 (b)), on the other hand, delivers best video performance under SPD and LPC schedulers. In addition, RTX Aware strategy increases LET video performance significantly. In contrast, RTX Aware strategy for LIA and OLIA decreases discard/underflow events when LPC scheduler is used.

Finally, Figures 7 a, b, c, d present video performance in scenario 3p-d, where shortest RTT flow3 has a 0.5 % packet loss condition. CCP and Cubic charts are similar as in previous scenario 3p-e, namely, little performance improvement by changing packet scheduler except for LET scheduler under Cubic TCP variant, which presents significant improvement. LIA and OLIA schedulers (Figures 7 c,d), on the other hand, provide only small improvements when RTX awareness is used. Figures 8 (c,d) shows that LET scheme injects a larger amount of packets into loss-less flow1 and flow2 than SPD and LPC, since total bandwidth of loss-less flow1 and flow2 is capable of 5.24 Mb/s video traffic in scenario 3p-e.

Overall, the above results show a consistent video streaming performance improvement when paths experiencing momentary retransmissions are avoided across most TCP variants as well as path scheduler schemes. In addition, more available paths does not always bring better performance, especially for aggressive TCP variants such as Cubic and CCP. Although these results were obtained for specific testbed topologies and network scenarios, we believe similar improvements can be attained on more generic network scenarios.

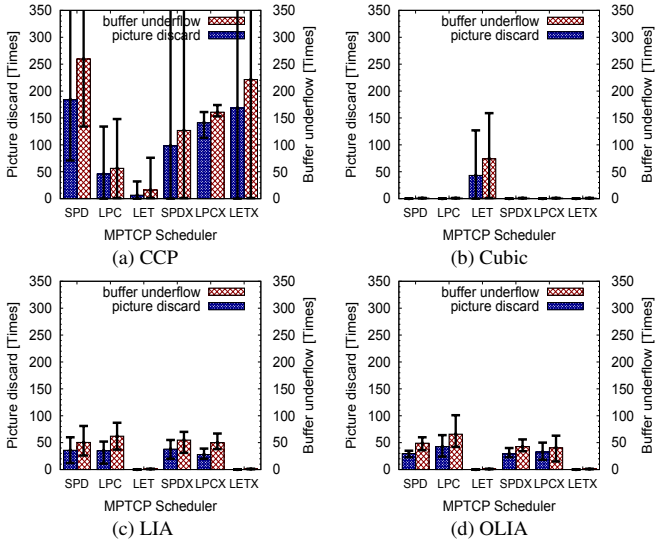
 ISBN: 978-1-61208-644-6



(a) CCP (b) Cubic

(c) LIA (d) OLIA

Figure 6: Scheduler Streaming Perf.; Scenario 3p-e



(a) CCP (b) Cubic

(c) LIA (d) OLIA

Figure 7: Scheduler Streaming Perf.; Scenario 3p-d

VII. Conclusion and Future Work

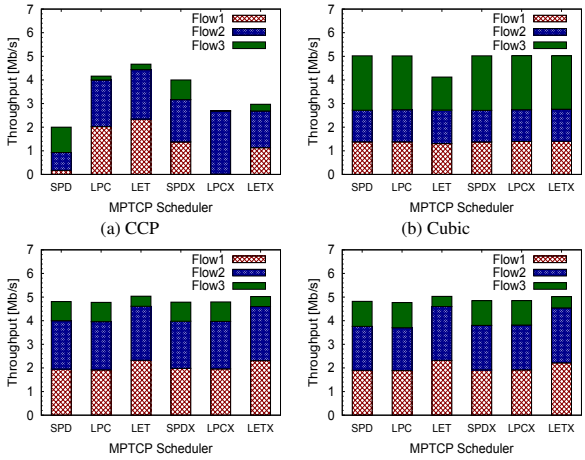
In this paper, we have proposed TCP state driven packet schedulers to improve the quality of streaming video over MPTCP. We have evaluated MPTCP performance with default and several packet schedulers which avoid injecting packets into paths experiencing retransmissions in lossy wireless network. Our results have shown that TCP state aware scheduling improves video streaming across most TCP variants, as well as coupled LIA and OLIA, for all packet schedulers studied. We believe that avoiding paths experiencing packet retransmissions may be applicable across a wide variety of schedulers and TCP variants. We are currently investigating other scheduling techniques to further reduce frame discard and video stalling to improve streaming video quality.

Acknowledgments

Work supported by JSPS KAKENHI Grant # 16K00131.

References

[1] M. Allman, V. Paxson, and W. Stevens, "TCP Congestion Control," IETF RFC 2581, April 1999.



(a) CCP (b) Cubic

(c) LIA (d) OLIA

Figure 8: Scheduler Throughput Perf.; Scenario 3p-d

[2] B. Arzani et al., "Deconstructing MPTCP Performance," In Proceedings of IEEE 22nd ICNP, pp. 269-274, 2014.

[3] D. Cavendish, K. Kumazoe, M. Tsuru, Y. Oie, and M. Gerla, "Capacity and Congestion Probing: TCP Congestion Avoidance via Path Capacity and Storage Estimation," IEEE Second International Conference on Evolving Internet, pp. 42-48, September 2010.

[4] D. Cavendish, H. Kuwahara, K. Kumazoe, M. Tsuru, and Y. Oie, "TCP Congestion Avoidance using Proportional plus Derivative Control," IARIA Third International Conference on Evolving Internet, pp. 20-25, June 2011.

[5] X. Corbillon, R. Aparicio-Pardo, N. Kuhn, G. Texier, and G. Simon, "Cross-Layer Scheduler for Video Streaming over MPTCP," ACM 7th International Conference on Multimedia Systems, May 10-13, 2016, Article 7.

[6] E. Dong et. al., "LAMPS: A Loss Aware Scheduler for Multipath TCP over Highly Lossy Networks," *Proceedings of the 42th IEEE Conference on Local Computer Networks*, pp. 1-9, October 2017.

[7] S. Ferlin et. al., "BLEST: Blocking Estimation-based MPTCP Scheduler for Heterogeneous Networks," In Proceedings of IFIP Networking Conference, pp. 431-439, 2016.

[8] A. Ford et. al., "Architectural Guidelines for Multipath TCP Development," IETF RFC 6182, 2011.

[9] J. Hwang and J. Yoo, "Packet Scheduling for Multipath TCP," IEEE 7th Int. Conference on Ubiquitous and Future Networks, pp.177-179, July 2015.

[10] R. Khalili, N. Gast, and J-Y Le Boudec, "MPTCP Is Not Pareto-Optimal: Performance Issues and a Possible Solution," IEEE/ACM Trans. on Networing, Vol. 21, No. 5, pp. 1651-1665, Aug. 2013.

[11] B. Kimura et al., "Alternative Scheduling Decisions for Multipath TCP," IEEE Communications Letters, Vol. 21, No. 11, pp. 2412-2415, Nov. 2017.

[12] R. Matsufuji et al., "Multipath TCP Packet Scheduling for Streaming Video," IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, pp. 1-6, August 2017.

[13] J-W. Park, R. P. Karrer, and J. Kim,, "TCP-Rome: A Transport-Layer Parallel Streaming Protocol for Real-Time Online Multimedia Environments," In Journal of Communications and Networks, Vol.13, No. 3, pp. 277-285, June 2011.

[14] C. Raiciu, M. Handly, and D. Wischik, "Coupled Congestion Control for Multipath Transport Protocols," IETF RFC 6356, 2011.

[15] I. Rhee, L. Xu, and S. Ha, "CUBIC for Fast Long-Distance Networks," Internet Draft, draft-rhee-tcpm-ctcp-02, August 2008.

[16] J. Wu, C. Yuen, B. Cheng, M. Wang, and J. Chen, "Streaming High-Quality Mobile Video with Multipath TCP in Heterogeneous Wireless Networks," IEEE Transactions on Mobile Computing, Vol.15, Issue 9, pp. 2345-2361, 2016.

[17] K. Xue et al., "DPSAF: Forward Prediction Based Dynamic Packet Scheduling and Adjusting With Feedback for Multipath TCP in Lossy Heterogeneous Networks," IEEE/ACM Trans. on Vehicular Technology, Vol. 67, No. 2, pp. 1521-1534, Feb. 2018.

[18] F. Yan, P. Amer, and N. Ekiz, "A Scheduler for Multipath TCP," In Proceedings of IEEE 22nd ICCCN, pp. 1-7, 2013.

 ISBN: 978-1-61208-644-6

Detection of Manipulated Communications in a Q&A Site by Considering Time Lags between Answer Submission and Problem Resolution

Yasuhiko Watanabe, Kenji Umemoto, Ryo Nishimura, and Yoshihiro Okada
Ryukoku University
Seta, Otsu, Shiga, Japan
Email: watanabe@rins.ryukoku.ac.jp, t070400@mail.ryukoku.ac.jp,
r_nishimura@afc.ryukoku.ac.jp, okada@rins.ryukoku.ac.jp

***Abstract*—Some users of Question and Answer (Q&A) sites use multiple user accounts and attempt to manipulate communications in the site. Manipulated communications, especially, manipulated evaluations, decrease the credibility of the Q&A site. In order to detect manipulated communications in a Q&A site, in this paper, we propose a method of detecting users suspected of using multiple user accounts and manipulating communications in a Q&A site by considering time lags between answer submission and problem resolution. We show our method is useful for detecting inadequate multiple account users and their submissions. In this study, we used the data of Yahoo! chiebukuro, one of the most popular Q&A sites in Japan, for observation and examination.**

Keywords–manipulated communication; multiple account user; Q&A site; time lag; credibility.

I. INTRODUCTION

These days, many people use Question and Answer (Q&A) sites. They share their information and knowledge by submitting questions and answers in Q&A sites. Q&A sites offer greater opportunities to users than search engines because of the following:

- Users can submit questions in natural and expressive sentences, not keywords.
- Users can submit ambiguous questions and still receive some answers from other users.
- Communications in Q&A sites are interactive. Users have chances to not only submit questions but give answers and, especially, join discussions.

Furthermore, Q&A sites are more convenient than Social Network Service (SNS) sites because of the following:

- Information in Q&A sites is reliable. This is because information in Q&A sites is generally checked and evaluated by questioners. Questioners in Q&A sites usually show which answers are useful to solve their problems.
- It is easy to retrieve communication records and find information for problem resolution. This is because information in Q&A sites is recorded in the form of questions and their answers.

As a result, Q&A sites are a promising media. Two of the essential factors in Q&A sites are anonymous submission and evaluation. In most Q&A sites, user registrations are required for those who want to join the Q&A sites. However, registered users generally need not reveal their real names to submit messages (questions, problems, answers, opinions, etc.). It is important to submit messages anonymously to a Q&A site. This is because anonymity gives users chances to submit messages without the potential privacy risks of disclosing personal information. However, some users abuse the anonymity and attempt to manipulate communications in a Q&A site. For example, some users use multiple user accounts and submit messages to a Q&A site inadequately. Manipulated communications (especially, manipulated evaluations) discourage other submitters, keep users from retrieving good communication records, and decrease the credibility of the Q&A site. As a result, it is important to detect users suspected of using multiple user accounts and manipulating communications in a Q&A site. Previous user identification methods can be categorized into two kinds of approaches.

- identity tracing based on user accounts and
- authorship identification based on analyzing stylistic features of messages.

In this case, identity tracing based on user accounts is not effective because inadequate users often attempt to hide their true identity to avoid detection. A possible solution is authorship identification based on analyzing stylistic features of messages. In recent years, a large number of studies have been made on authorship identification. However, few researchers addressed the identification issues of authors suspected of using multiple user accounts and manipulating communications in a Q&A site. To solve this problem, Watanabe et al. proposed a method of detecting users suspected of using multiple user accounts and manipulating evaluations in a Q&A site [1]. This method was based on one idea: inadequate multiple account users give too many good evaluations to their submissions. In other words, this method can be classified into authorship identification based on analyzing users' behaviors in anonymous communication services. This inadequate submission detection was useful but not enough because there are several types of inadequate submissions. To detect inadequate submissions more widely, in this paper, we propose a new method of detecting inadequate submissions by considering time lags between answer submission and problem resolution. We used messages in the data of Yahoo! chiebukuro [2], a widely-used Japanese Q&A site, for observation and examination.

The rest of this paper is organized as follows: In Section II, we survey the related works. In Section III, we describe multiple account users in a Q&A site. We explain Yahoo! chiebukuro which we take for an example of Q&A sites. In Section IV, we propose a method of detecting unnatural submissions in a Q&A site by considering time lags between answer submission and problem resolution. In Section V, we

 ISBN: 978-1-61208-644-6

TABLE I. THE NUMBERS OF USERS AND THEIR MESSAGES SUBMITTED TO PC, HEALTHCARE, SOCIAL ISSUES CATEGORY AND ALL 286 CATEGORIES IN YAHOO! CHIEBUKURO (FROM APRIL/2004 TO OCTOBER/2005).

category	U_{qst}	N_{qst}	U_{ans}	N_{ans}
PC	43493	171848	27420	474687
healthcare	29954	84364	38223	289578
social issues	13259	78777	25766	403306
all 286 categories	165064	3116009	183242	13477785

(Note) U_{qst} and U_{ans} are the numbers of users who submitted questions and answers, respectively. N_{qst} and N_{ans} are the numbers of questions and answers, respectively.

apply our method into a Q&A site and show that the method is useful for detecting inadequate submissions in a Q&A site. Finally, in Section VI, we present our conclusions.

II. RELATED WORKS

One of the essential factors of the Internet is anonymity. However, Internet users are generally concerned about unwanted audiences obtaining personal information. Joinson discussed the anonymity on the Internet from various points of view [3]. Fox et al. reported that 86% of Internet users are concerned that unwanted audiences will obtain information about them or their families [4]. Kambourakis pointed that anonymity is necessary in almost any protocol, application or service used in wired or wireless networks, and showed a survey on anonymity preserving solutions [5]. However, these days, many users abuse the anonymity. Take a Sybil attack for example. In a Sybil attack, the attacker intends to gain large influence on a peer-to-peer (P2P) network by creating and using a large number of pseudonymous identities [6] [7]. Sybil attack is a cheap and efficient way to gain large influence on P2P networks [8]. Similarly, in human online communities, such as, web-based bulletin boards, chat rooms, and blog comment forms, many users are thought to use multiple user accounts inadequately and submit inadequate messages, such as deceptive opinion spams. In recent years, a large number of studies have been made on authorship identification [9]–[14]. However, few researchers addressed the identification issues of authors suspected of using multiple user accounts and manipulating communications in the Internet. One of the difficulties of this problem is that we did not have sufficient number of examples of inadequate multiple account users and their submissions. To solve this problem, some researchers tried to extract inadequate submissions by using heuristic methods based on text similarities and ranking results [15] [16]. On the other hand, the authors of [17] pointed that these heuristic methods were insufficient to detect inadequate submissions precisely, and showed they could detect inadequate submissions precisely when they used large number of examples of inadequate submissions. However, they obtained examples of inadequate submissions by using Amazon Mechanical Turk [18]. The examples of inadequate submissions created by workers in Amazon Mechanical Turk have the following problems.

- Little is known about the purposes and methods of inadequate submissions. As a result, it is possible that their instructions to workers in Amazon Mechanical Turk were insufficient.
- There are unreliable workers in Amazon Mechanical Turk [19].

As a result, it is important to obtain inadequate submissions from the Internet. To solve this problem, we proposed methods of detecting inadequate multiple account users and their submissions [1]. This method can be classified into authorship identification based on analyzing users' behaviors in anonymous communication services. However, as mentioned, little is known about the purposes and methods of inadequate multiple account users. As a result, it is important to investigate these inadequate multiple account users and their inadequate submissions from various points of view.

III. MULTIPLE ACCOUNT USERS IN A Q&A SITE

In this section, we take Yahoo! chiebukuro for example and discuss reasons why and how some users in a Q&A site use multiple user accounts.

A. Yahoo! chiebukuro

Yahoo! chiebukuro is a Japanese version of Yahoo! answers and one of the most popular Q&A sites in Japan. In Japanese, chiebukuro means "bag of wisdom". Users of Yahoo! chiebukuro submit their questions and answers in the next way.

- User registrations are required for those who want to join Yahoo! chiebukuro.
- Users need not reveal their real names to submit their questions and answers.
- Each user can submit his/her answer only one time to one question.
- The period limit for accepting answers is one week. However, questioners can stop accepting answers before the time limits.
- After the time limits, questions with no answers are removed and cannot be referable. On the other hand, questions with answers can be referable.
- Each questioner is requested to determine which answer to his/her question is best and give a *best answer* label to it.

In this study, we used messages in the data of Yahoo! chiebukuro for observation and examination. The data of Yahoo! chiebukuro was published by Yahoo! JAPAN via National Institute of Informatics in 2007 [2]. This data consists of about 3.11 million questions and 13.47 million answers which were posted on Yahoo! chiebukuro from April/2004 to October/2005. In the data, each question has at least one answer

 ISBN: 978-1-61208-644-6

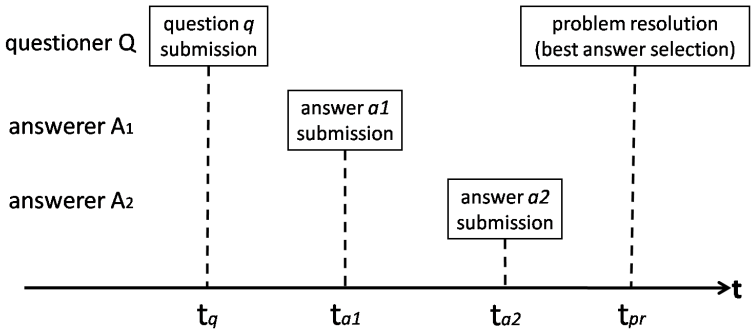


Figure 1. An example of a series of events that occur after a questioner submits his/her question to a Q&A site. Questioner Q submitted question q at t_q. Also, answerer A_1 and A_2 submitted their answers at t_{a1} and t_{a2}, respectively. Finally, questioner Q stopped accepting answers and determined which answer was the best answer at t_{pr}.

TABLE II. THE CUMULATIVE RELATIVE FREQUENCY OF TIME LAGS BETWEEN SUBMISSION TIME OF ANSWER T_A AND PROBLEM RESOLUTION TIME T_{PR} IN THE DATA OF YAHOO! CHIEBUKURO.

cumulative relative frequency (%)	0.5	1.0	1.5	2.0	2.5	5.0	$\cdots$	50.0
time lag between T_a and T_{pr} (sec)	49	87	123	158	194	391	$\cdots$	64848

because questions with no answers were removed. In order to avoid identifying individuals, user accounts were replaced with unique ID numbers. By using these ID numbers, we can trace any user's questions and answers in the data. Table I shows the numbers of users and their messages (questions and answers) submitted to

- PC category,
- healthcare category,
- social issues category, and
- all 286 categories in the data.

Furthermore, the following kinds of information are described in the data.

- submission time of question
- submission time of answer
- problem resolution time

Figure 1 shows an example of a series of events that occur after a questioner submits his/her question to a Q&A site. In Figure 1, the submission time of question q is t_q. Also, the submission time of answer a_1 and a_2 are t_{a1} and t_{a2}, respectively. Finally, the problem resolution time of question q is t_{pr}. At the problem resolution time, questioner Q stopped accepting answers and determined which answer was the best answer. We focus on time lag between answer submission and problem resolution. In case of answer a_2 in Figure 1, the time lag between answer submission and problem resolution is $t_{pr} - t_{a2}$. The average and median of these time lags of all answers in the data of Yahoo! chiebukuro were 187595 and 64848 seconds, respectively. Table II shows the cumulative relative frequency of the time lags in the data of Yahoo! chiebukuro. As shown in Table II, in case of 1.0 percent of all answers (135705 answers), questioners stopped accepting answers and selected best answers within 87 seconds after these answers were submitted. These 135705 answers included 52798 best answers.

B. Submissions by using multiple user accounts

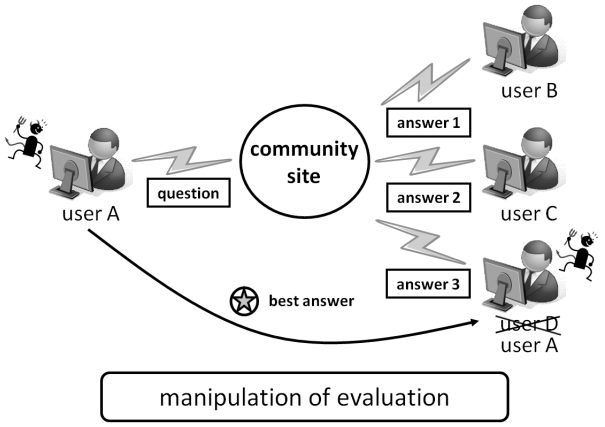
There are many reasons why users in a Q&A site use multiple user accounts. First, we discuss a proper reason. In Yahoo! chiebukuro, users need not reveal their real names to submit their messages. However, their messages are traceable because their user accounts are attached to them. Because of this traceability, we can collect any user's messages and some of them include clues of identifying individuals. As a result, to avoid identifying individuals, it is reasonable and proper that users change their user accounts or use multiple user accounts. However, the following types of message submissions by using multiple user accounts are neither reasonable nor proper.

a) TYPE QA: One user submits a question and its answer by using multiple user accounts (Figure 2 (a)).
We think that the user intended to manipulate the message evaluation. For example, in Yahoo! chiebukuro, each questioner is requested to determine which answer is best and give a *best answer* label to it. These message evaluations encourage message submitters to submit new messages and increase the credibility of the Q&A site. We think that the user repeated this type of submissions because he/she wanted to get many best answer labels and be seen as a good answerer.

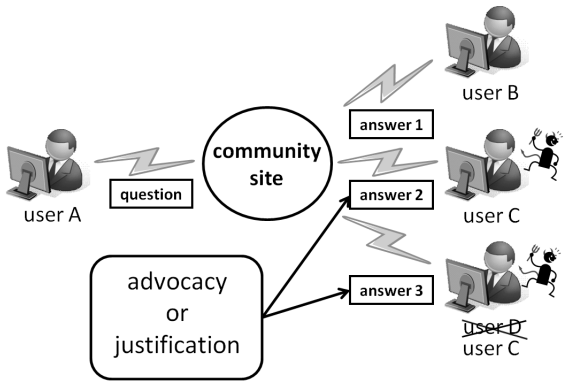
b) TYPE AA: One user submits two or more answers to the same question by using multiple user accounts (Figure 2 (b)).
We think that the user intended to dominate or disrupt communications in the Q&A site. To be more precise, the user intended to

- control communications by advocating or justifying his/her opinions, or
- disrupt communications by submitting two or more inappropriate messages.

These two types are not all types of inadequate submissions. However, these kinds of submissions seriously disrupt communications in a Q&A site. Especially, TYPE QA submissions are



(a) TYPE QA: one user submits a question and its answer by using multiple user accounts. (In this case, user A submits a question and its answer by using two user accounts.)



(b) TYPE AA: one user submits two or more answers to the same question by using multiple user accounts. (In this case, user C submits two answers by using two user accounts.)

Figure 2. Two types of inadequate submissions: TYPE QA and TYPE AA.

serious because users can manipulate evaluations of messages by repeating TYPE QA submissions. Manipulated evaluations discourage other submitters, keep users from retrieving good communication records, and decrease the credibility of the Q&A site. To solve this problem, Watanabe et al. proposed a method of detecting users suspected of using multiple user accounts and repeating TYPE QA submissions [1]. This method was based on one idea: if a user uses multiple user accounts and attempts to manipulate his/her evaluations inadequately, the user repeats TYPE QA submissions unnaturally and gives too many good evaluations to his/her submissions. This method of inadequate submission detection was useful but not enough because there are several types of inadequate submissions. Especially, Watanabe et al.'s method did not consider when questions and answers were submitted. In order to detect inadequate submissions more widely, in this study, we focus on time lags between best answer submission and problem resolution. As mentioned, in Yahoo! chiebukuro, the median time lag between answer submission and problem resolution was 64848 seconds. However, we found some cases where time lags between best answer submission and problem resolution were very short as if the questioners seemed to know when the best answers were submitted. We think that, if a certain user pair of questioner and answerer repeats this kind of unnatural submissions, the questioner and answerer are suspected of being one and the same user. In the next section, we propose a new method of detecting unnatural submissions by considering time lags between answer submission and problem resolution.

IV. UNNATURAL SUBMISSION DETECTION IN YAHOO! CHIEBUKURO

In Yahoo! chiebukuro, we found some cases where the time lags between best answer submission and problem resolution were very short as if the questioners seemed to know when the best answers were submitted. To determine whether this kind of unnatural submissions occurred, we test a hypothesis based on question and answer time lags (QAT): Hypothesis QAT. When this hypothesis is rejected by a one-sided binomial test, we determine that this kind of unnatural submissions occurred.

Hypothesis QAT If there are not too many cases where user i (questioner) determined that user j's answer was the best answer just after user j (answerer) submitted it, we would expect that there are at most $N_{QAT}(i, j, T_0)$ cases where user i determined user j's answer was the best answer within a shorter time lag than T_0.

$$N_{QAT}(i, j, T_0) = P_{QAT}(T_0) \times ans(i, j)$$

where $ans(i, j)$ is the total number of user j's answers for user i's questions and $P_{QAT}(T_0)$ is the probability that a user answers one question randomly and the answer is selected as best answer within a shorter time lag than T_0. Because each user of Yahoo! chiebukuro can submit his/her answer only one time to one question, $P_{QAT}(T_0)$ is

$$P_{QAT}(T_0) = \frac{N_{bestans}(T_0)}{N_{ans}}$$

where N_{ans} is the total number of answers and $N_{bestans}(T_0)$ is the number of best answers selected within a shorter time lag than T_0. Suppose T_0 was set to 87 seconds. This is because, as shown in Table II, the time lag between answer submission and problem resolution is 87 seconds when the cumulative relative frequency of answers is 0.01. When T_0 is sufficiently small, T_0 is independent of the categories in the data of Yahoo! chiebukuro. This is because, when T_0 is sufficiently small, questioners have not enough time to read answers in any category. We think 87 seconds is sufficiently small. When T_0 is sufficiently small and category-independent, N_{ans} and $N_{bestans}(T_0)$ can be set regardless of the categories. In this study, N_{ans} was set to 13477785. It was the total number of answers in the data of Yahoo! chiebukuro (Table I). On the other hand, $N_{bestans}(T_0)$ was set to 52798. It was the total number of best answers which were selected as best answers within 87 seconds after these best answers were submitted.

V. EXPERIMENTAL RESULTS

To evaluate our method, we conducted the detection of unnatural submissions in Yahoo! chiebukuro, which were suspected of being caused by multiple account users. In this experiment, the target users and submissions were all users and submissions in the data of Yahoo! chiebukuro, respectively. Also, the target categories were all 286 categories in the data of Yahoo! chiebukuro. T_0 was set to 87 seconds, and then, N_{ans} and $N_{bestans}(T_0)$ were 13477785 and 52798, respectively. The significant level of Hypothesis QAT was set to 0.000005.

 ISBN: 978-1-61208-644-6

This was extremely low because we intend to detect extreme unnatural submissions.

In this experiment, we tried to detect unnatural submissions in each category. Our method detected a total of 316 unnatural submissions caused by 258 user pairs. These 316 unnatural submissions can be classified into two types:

Type A this type of unnatural submission was caused by a user pair involved in unnatural submissions in two or more categories. For example, unnatural submissions in five categories caused by user pair (691911 ← 802184) were classified into this type. User pair (691911 ← 802184) means that user 691911 and 802184 are the questioner and answerer in this user pair, respectively. In this experiment, our method found 75 unnatural submissions of this type. These 75 unnatural submissions were caused by 17 user pairs. It is unnatural that one answerer submits answers repeatedly to the same questioner's questions in different categories. As a result, in each of these 17 user pairs, the questioner and the answerer were suspected of being one and the same user.

Type B this type of unnatural submission was caused by a user pair involved in unnatural submissions in only one category. In this experiment, our method found 241 unnatural submissions of this type. These 241 unnatural submissions were caused by 241 user pairs.

First, we discuss 17 user pairs involved in Type A unnatural submissions. As mentioned, these 17 user pairs were suspected. Furthermore, in questions and answers submitted by these 17 user pairs, we found many strange coincidence of opinions, mistype, expression selection, and so on. As a result, these 17 user pairs were deeply suspected. Moreover, it is notable that there were many questioners involved in Type A unnatural submissions submitted small number of answers. In the 75 type A unnatural submissions, we found 49 cases where the questioner submitted less than four answers. However, we think this is not unnatural. Suppose a questioner and answerer are one and the same user and his/her purposes is to manipulate the evaluation of the answerer. Questioner's answers are useless to manipulate the evaluation of the answerer, and consequently, the questioner submits no answer or small number of answers.

Next, we discuss user pairs involved in Type B unnatural submissions. We found suspected and unsuspected submissions in Type B unnatural submissions. In the unsuspected cases, we found five cases where the questioner and answerer used Yahoo! chiebukuro as an online chat system and communicated with each other in real time, for example,

question How can I get in touch with Mr. Kupo?
answer Yeah! Kupo is here!!!!

After submitting this question, the questioner received eleven answers in about 20 minutes. The last answer was submitted by Kupo. The questioner selected Kupo's answer as a best answer just after he/she received it. We think a considerable number of users enjoyed realtime communication frequently in Yahoo! chiebukuro. These users could be distinguished from inadequate users when our method was used in combination with other methods, such as, similarity analysis of writing.

VI. CONCLUSION

In order to detect unnatural submissions caused by inadequate multiple account users in a Q&A site, in this paper, we focused on time lags between answer submission and problem resolution. This is because we observed the data of Yahoo! chiebukuro, a widely-used Japanese Q&A site, and found some cases where the time lags between best answer submission and problem resolution were very short as if the questioners seemed to know when the best answers were submitted. The proposed method was based on an idea: if a user repeats submissions where the time lags between best answer submission and problem resolution are very short, the user is suspected of using multiple user accounts and attempting to manipulate his/her evaluations inadequately. In our method, unnatural submissions of this type were detected by a binomial test. We showed that our method detected many unnatural submissions. Unnatural submissions detected by our methods will give us a chance to investigate purposes and behaviors of users who use multiple user accounts and intend to manipulate evaluations in a Q&A site. We intend to combine our method with other methods, such as, similarity analysis of writing.

REFERENCES

[1] Y. Watanabe et al., "Investigation of users suspected of manipulating evaluations of answers in a q&a site," International Journal on Advances in Internet Technology, vol. 8, no. 3&4, 2015, pp. 50–63. [Online]. Available: https://www.iariajournals.org/internet_technology/inttech_v8_n34_2015_paged.pdf [accessed: 2018-5-1]

[2] "Distribution of "Yahoo! Chiebukuro" data," URL: http://www.nii.ac.jp/cscenter/idr/yahoo/tdc/chiebukuro_e.html [accessed: 2018-5-1].

[3] A. N. Joinson, Understanding the Psychology of Internet Behaviour: Virtual Worlds, Real Lives. Palgrave Macmillan, Feb. 2003.

[4] S. Fox et al., Trust and Privacy Online: Why Americans Want to Rewrite the Rules, The Pew Internet & American Life Project, 2000. [Online]. Available: http://www.pewinternet.org/˜/media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf [accessed: 2016-10-4]

[5] G. Kambourakis, "Anonymity and closely related terms in the cyberspace: An analysis by example," Journal of Information Security and Applications, vol. 19, no. 1, Feb. 2014, pp. 2–17. [Online]. Available: http://dx.doi.org/10.1016/j.jisa.2014.04.001 [accessed: 2018-5-1]

[6] J. R. Douceur, "The Sybil attack," in Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS '02), Mar. 2002, pp. 251–260. [Online]. Available: http://research.microsoft.com/pubs/74220/IPTPS2002.pdf [accessed: 2018-5-1]

[7] L. A. Cutillo, M. Manulis, and T. Strufe, "Security and privacy in online social networks," in Handbook of Social Network Technologies and Applications, B. Furht, Ed. Springer, Nov. 2010, pp. 497–522.

[8] L. Wang and J. Kangasharju, "Real-world sybil attacks in BitTorrent mainline DHT," in Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM 2012), Dec. 2012, pp. 826–832. [Online]. Available: http://dx.doi.org/10.1109/GLOCOM.2012.6503215 [accessed: 2018-5-1]

[9] O. de Vel, A. Anderson, M. Corney, and G. Mohay, "Mining e-mail content for author identification forensics," SIGMOD Rec., vol. 30, no. 4, Dec. 2001, pp. 55–64. [Online]. Available: http://doi.acm.org/10.1145/604264.604272 [accessed: 2018-5-1]

[10] M. Koppel, S. Argamon, and A. Shimoni, "Automatically categorizing written texts by author gender," Literary and Linguistic Computing, vol. 17, 2002, pp. 401–412. [Online]. Available: https://doi.org/10.1093/llc/17.4.401 [accessed: 2018-5-1]

[11] M. Corney, O. Y. de Vel, A. Anderson, and G. M. Mohay, "Gender-preferential text mining of e-mail discourse." in ACSAC. IEEE Computer Society, 2002, pp. 282–289. [Online]. Available:

 ISBN: 978-1-61208-644-6

http://dblp.uni-trier.de/db/conf/acsac/acsac2002.html [accessed: 2018-5-1]

[12] S. Argamon, M. Šarić, and S. S. Stein, "Style mining of electronic messages for multiple authorship discrimination: First results," in Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ser. KDD '03. New York, NY, USA: ACM, 2003, pp. 475–480. [Online]. Available: http://doi.acm.org/10.1145/956750.956805 [accessed: 2018-5-1]

[13] R. Zheng, J. Li, H. Chen, and Z. Huang, "A framework for authorship identification of online messages: Writing-style features and classification techniques," Journal of the Association for Information Science and Technology, vol. 57, no. 3, 3 2006, pp. 378–393. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/asi.20316/abstract [accessed: 2018-5-1]

[14] A. Abbasi and H. Chen, "Visualizing authorship for identification," in Proceedings of 2006 IEEE International Conference on Intelligence and Security (ISI 2006), 2006, pp. 60–71. [Online]. Available: http://dx.doi.org/10.1007/11760146_6 [accessed: 2018-5-1]

[15] N. Jindal and B. Liu, "Opinion spam and analysis," in Proceedings of the 2008 International Conference on Web Search and Data Mining (WSDM '08), Feb. 2008, pp. 219–230. [Online]. Available: http://doi.acm.org/10.1145/1341531.1341560 [accessed: 2018-5-1]

[16] G. Wu, D. Greene, B. Smyth, and P. Cunningham, "Distortion as a validation criterion in the identification of suspicious reviews," in Proceedings of the First Workshop on Social Media Analytics (SOMA '10), Jul. 2010, pp. 10–13. [Online]. Available: http://doi.acm.org/10.1145/1964858.1964860 [accessed: 2018-5-1]

[17] M. Ott, Y. Choi, C. Cardie, and J. T. Hancock, "Finding deceptive opinion spam by any stretch of the imagination," in Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies (HLT '11) - Volume 1, Jun. 2011, pp. 309–319. [Online]. Available: http://dl.acm.org/citation.cfm?id=2002472.2002512 [accessed: 2018-5-1]

[18] "Amazon Mechanical Turk," URL: http://www.mturk.com/ [accessed: 2018-5-1].

[19] C. Akkaya, A. Conrad, J. Wiebe, and R. Mihalcea, "Amazon Mechanical Turk for subjectivity word sense disambiguation," in Proceedings of the NAACL HLT 2010 Workshop on Creating Speech and Language Data with Amazon's Mechanical Turk (CSLDAMT '10), Jun. 2010, pp. 195–203. [Online]. Available: http://dl.acm.org/citation.cfm?id=1866696.1866727 [accessed: 2018-5-1]

 ISBN: 978-1-61208-644-6

SDN Based Cloud Platform for Smart Vehicles

Tijana Devaja, Živko Bojović, Anastazia Žunić
Faculty of Technical Sciences, University of Novi Sad
Novi Sad, Serbia
emails: tijana.devaja@uns.ac.rs, zivko@uns.ac.rs, anastazia95@gmail.com

Abstract- Over the past few years, the advances in wireless communications, the expansion of cloud computing applications and the implementation of intelligent terminal equipment, forced vehicle manufacturers to rethink the role of advanced Information and Communication Technology (ICT) in the vehicle industry. The process of designing, developing and deploying the new, smarter concept of vehicle management started by realizing the power of the collected data to improve vehicle services, to enable an integrated, effortless service experience, to engage with the drivers and implement the solutions for the well-being of all traffic participants. In this paper, we first define the key requirements for the integration of Smart Vehicle Computer System (SVCS) with cloud assisted automotive applications. Further, based on these requirements, we design a flexible and scalable cloud platform based on implementation of software defined networking into an architecture called Smart Vehicle to Cloud Integration Architecture (SVCIA). The goal is to provide a dynamic allocation of resources adjusted to the user needs and an easy implementation of new services, which makes driving safer and more comfortable for users. The validation of the suggested solution has been done through simulation, where we used a cloud application based on Dijkstra algorithm in order to dynamically route the traffic and avoid congestions. The obtained results show that the use of this kind of solution can significantly improve drivers' satisfaction and safety during the ride.

Keywords- cloud; Smart Vehicle to Cloud Integration Architecture (SVCIA); Smart Vehicle Computer System (SVCS); Software Defined Networking (SDN); Dijkstra algorithm.

I. INTRODUCTION

The future of the automotive industry is closely related to the development of advanced electronic systems and their integration with the applications on the cloud via Internet technology [1][2]. It is a part of new Internet of Vehicles (IoV) paradigm and the goal of this integration is to raise the level of intelligence of vehicles and to realize users' requirements [3]. They can generally be divided into two categories:

- The requirements of drivers to realize quality Information Systems (IS) and to ensure effective circulation of information necessary to improve traffic safety and efficiency.
- The passengers' need for greater comfort during the ride (vehicle as an office, entertainment), which means access to high-speed Internet.

The realization of these requirements implies the design and deployment of complex and intelligent computing systems in cars: Smart Vehicle Computer Systems (SVCS). Their implementation includes integration of the Geographic Information System for continuous vehicle tracking, traffic monitoring and other data collections, such as effective traffic signalization, weather conditions, etc. [4]. SVCS applications and services are provided by different communication technologies, computer platforms, sensors and other active devices [5][6]. Therefore, it is a major technological challenge to network the vehicles and to implement new telematics applications. From our point of view, the platform should enable vehicle networking with a built-in module for autonomous decision-making and control in the SVCS. We are convinced that the development of smart systems for networking of vehicles is crucial for a large-scale introduction of intelligent solutions; a prerequisite is a cloud environment [7]. The advent of cloud technologies, more than ever, creates the possibility to substitute conventional methods of collecting and processing sensory information approaches by: 1) decentralization of detection and data collection, assuming that sensor data are detected and collected from different locations; 2) collecting information and resources from the cloud; 3) analytics of those data; 4) ad-hoc exchange of detected information with other vehicles in the case of breakup of cloud connectivity and their subsequent forwarding to the cloud in order to update the existing databases; 5) elastic provisioning of secure access for a specific cloud provider, while the IP address of the link provider is constantly changing due to soft hand-off between base stations. It is assumed that the users can scale resources up or down in real-time based on requests.

We analyze how to enable the applications to use programmable dynamic interfaces to control and allocate network resources in order to differentiate the needs of users (such as SVCS) and the data types [8], and we propose the usage of Software Defined Networking (SDN) as a new solution for vehicle networking. This solution is a new and flexible combination of several existing contributions, including:

- Solution for providing the continuity of service,
- Ad-hoc communication between vehicles, important in case of interruption of the communication link between SVCS and traffic cloud,
- Centralized management and optimization of network resources, thus guaranteeing the reliability of services

 ISBN: 978-1-61208-644-6

(the concentration of routing information in the controller provides fast traffic redirection in case of failure, choosing the alternative route with minimum cost).

- Dynamic subscribing - dynamic user registration according to economic criteria (service on demand),
- Scalability, achieved by adding the SDN controller.

The remaining of the paper is elaborated as follows: Section 2 provides an overview of the research in the automotive industry with a focus on the field implementation of advanced ICT in vehicles and traffic management. In Section 3, we describe the proposed design of SDN-based architecture for vehicle to cloud integration. This concept, based on the SDN paradigm as an emerging technology, is described in Section 4. Section 5 provides an evaluation of the proposed solution from the traffic prediction standpoint. Section 6 concludes the paper and gives some details about how to reliably predict traffic.

II. RELATED WORKS

Today, there are many researches which deal with different aspects of application of advanced ICT solutions in the automotive industry and in traffic predictions. In ICT technologies, there are many new solutions. Different architectures are being developed, and the elements of an Intelligent Transport System (ITS) are being described. A large number of research papers have a goal to improve the implementation of Internet of Things (IoT) applications for smart traffic. Wibowo et al. [9] provide a multi-criteria analysis used to calculate the "smartness index", which represents the ability of the transportation system to help with a particular problem in order to develop a good strategy for a solution. Applications that solve traffic problems are often part of other projects, such as „smart city", which has as goal to improve the quality of life in the city environment. Examples of such applications include:

- Experimenting Acoustics in Real environments using Innovative Test-beds (EAR-IT) sub-project [10], in which the focus of the research is the analysis of the sound coming from the surroundings, with the aim to draw a conclusion about the traffic density, deadlock or occupancy of the lanes. A couple of hundreds of units have been installed around the city; they are connected to a central processor in order to process the sound. These units have microphones and computers installed in them, and they are connected to sensors, which allow precise location of the coming sound. When cars with priority pass are observed, the system has the ability to keep track of the siren and to locate the vehicle, and this information is used to facilitate the passage of the vehicle with priority to the desired destination.
- Applications which are developed to show the number and position of currently available parking lots in the city [11].

Some research papers point out the development of a smart transport system based on IoT solutions, which helps in solving traffic problems, and even enables vehicles to drive without human intervention (Google Car project [12]). The main idea in these papers is to use advanced solutions efficiently, to collect information about the location (for example, the number of moving vehicles in order to estimate the duration of travel, travel conditions, car accidents, etc.) in order to detect risks, to determine the best path to destination, to reduce the emission of harmful gases, etc. Pyykönen et al. [13] present a system based on the application of Road-Side Units (RSUs) for monitoring the connection between the sensors placed in vehicles and databases [13]. This system is collecting data, with adequate accuracy, from RSUs and moving vehicles and stores them in databases. This information is forwarded to the drivers, in order to adjust the speed, and to employees in the road service in order to easily locate the part of the road which has to be fixed. There are also papers which describe quantifiers for determining the current state in traffic. iRide [14] is an application, which enables real-time information coming from sensors located near the road. This information is being forwarded to the server, where it is processed and sent to the drivers to enable them to learn about the road conditions. Collecting information is a process that requires accuracy and takes into account a dimension of several timelines. This is the reason why Vehicular Adhoc Networks (VANET) are a part of this research and they do not only include communication between vehicles, but also communication between vehicles and the infrastructure. In [15], the authors propose a Systematic Management of Road Traffic (SMaRTDRIVE) application for mobile phones and smart systems to help with traffic prediction. It has an aim to help vehicles with priority pass. Vehicles are equipped with On Board Unit (OBUs), which are used to collect data about the status of vehicles from different sensors. The server contains a database and a Web application. The SMaRTDRIVE application can also be used by pedestrians. By clicking the button, they can report accidents on the road, congestions, or some other problems. The OBU unit placed in the vehicle can automatically detect the accident in which a car participated and informs the services. RSU has a task to control traffic signalization. Many papers explain the usage of „smart phones", and techniques such as "mobile crowdsourcing". In [16], the authors show how this technique can be successfully used in traffic for finding the optimal routes, where the ranking of a route is done by many users. In order to get the best results, when finding of optimal routes, the crowdsourcing technique is being used in combination with other algorithms.

III. DEVELOPING A PLATFORM FOR INTELLIGENT VEHICLES

The main prerequisite for the implementation of different applications, which should enable drivers to manage the vehicles more efficiently, is to ensure the reliable transfer and storage of data from the related vehicles and from the environment, to the location where they are installed. We believe that the cloud as a centralized location for storing a large amount of data with implemented applications provided by Telematics, Infotainment, Navigation, Fleet management and other services is an excellent location and solution. That is why the goal of our research is to develop a new intelligent platform that would enable the use of mobile network services (3G, 4G, and future 5G) to store and analyze the data from the connected cars. From the spatial aspect, we introduce a concept of four-layered hierarchical architecture, as shown in

 ISBN: 978-1-61208-644-6

Figure 1. The proposed concept of hierarchical SVCP architecture in the spatial sense consists of four different layers, described as follows:

- In the layer of vehicle clients, we are focused on three key areas:
  - monitoring the vehicles in motion,
  - internal and external sensing in order to collect the information which is needed for the prevention of failures, for improving safety in traffic,
  - internal and external sensing for the realization of solutions for the efficient interaction between the driver and the passenger with the embedded computer platform.
- At the transmission layer, we propose a solution which consists of a secure channel for information delivery from cloud through the available mobile network (3G, 4G, 5G) and ad-hoc solutions for resource and safety information shared between vehicles. For example, the information about an accident can be transmitted to the drivers who are near, to be warned in time about the situation on the road.
- The platform layer provides vehicle intelligence through the usage of different interfaces in order to take a great amount of differently structured information, which is collected from the internal and external sensing and provide the customized services and specialized applications for the drivers and passengers. At this layer, the content of video cameras is transmitted to the server via the nearest available network access to the Internet cloud. Virtual machines with significant resources (processor, memory, and network bandwidth) at cloud servers guarantee the quality of service. Different users, such as drivers, traffic controllers and passengers, can collect information from the multiple cloud services via different interfaces.
- The application layer enables the applications that include distribution of information about traffic congestions, the availability of parking spaces in certain geographic locations.

The core element of the platform is the internal (in-vehicle) virtual network, called SVCP, which provides the "smart" attribute [4]. A vehicle at the micro layer provides an efficient system for the real time collection and distribution of information from the vehicle and from the environment. This network consists of 1) different types of sensors, 2) a computer with a sensor aggregator which can perform a number of things in the computer itself like, store raw data locally, aggregate the raw data into data sets that can be more readily used, etc. and 3) a virtual switch that communicates through high data rate wireless communication links (e.g. Long Term Evolution (LTE) module) with the SDN controller on the cloud by the Open Flow protocol (see Figure 2.) [4]. The controller provides dynamic resource allocation and traffic routing in interaction with cloud network applications. It is designed so as to provide simple and efficient communications between virtual machines and the internal network in the vehicle, including humans and intelligent sensor devices. Virtual machines process the data collected on sensors, providing fast feedback to the vehicle user. Google economist evaluate that more data are being produced every couple of days now than in years before

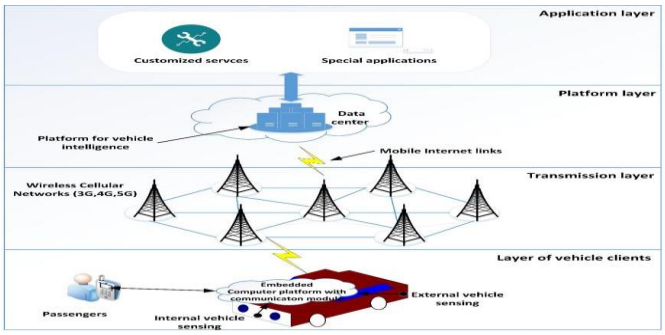


Figure 1. Concept of four-layered hierarchical architecture

2003. Some experts expect data volumes to reach 35 zettabytes by 2020. In 2013, 1.7 million billion bytes of data per minute were being generated globally. Due to a number of different driving technologies, we have explosive growth in data. The raw data, which is diverse, structured and unstructured in nature, is being sent to the cloud, where Big Data analytics correlate enormous amounts of data collected from a multitude of sources in real time, including millions of vehicles, drivers, weather, traffic, producers of parts (of types, windshields, bumpers, etc.) and other data in parallel. The relevant results of this Big Data analytics will be sent back to each vehicle in due time and either communicated to the driver or to the vehicle controlling algorithm [17].

IV. SVCP ARCHITECTURE SUPPORTED BY SDN BASED TRAFFIC IN CLOUD

In this paper, we design the SDN based SVCP architecture to provide more service contents (e.g., real-time traffic information, VPN service to the company location, gaming, etc.) for drivers, passengers and for better traffic control. The essential remark is that only SDN is responsible for central coordination of the quantity, speed and quality of data delivery, independently of the requests from the end user. The application of this platform significantly affects the safety, comfort and efficiency of driving. In order to explain the advantages of this platform, we have to clarify the processes that take place both locally and in the cloud. Different types of sensors are installed in vehicles, performing continuous measurements of a wide range of parameters, such as the state of individual functional units of the vehicle, the environmental conditions around the vehicle, the surrounding traffic signs, and the speed of vehicles coming from both directions, the state of health of the driver and passengers [18]. Usually, the degree to which vehicles are equipped with intelligent sensor devices as well as the quality of sensor devices vary. Therefore, it is justified to question the validity and extent of data obtained from the sensors. A particular challenge is the fact that from the available sample data, technologically limited local data processing systems, and with the available data analytics on board, it is not often possible to provide all the relevant information. Therefore, in the solution proposed in this paper, the emphasis is given to connecting the internal network to the cloud and processing them there as a part of evolution towards 5G [8].

 ISBN: 978-1-61208-644-6

The data arrive to the cloud at a high speed, proportional to the increase of the number of vehicles on the road. The amount of this data is great, and they are characterized by diversity and often structured differently. The result of the arrival of large amounts of data to the cloud is the formation of a much more representative data sample. The more precise data can be obtained in real time, with the important addendum that information is extracted and delivered to the vehicle using advanced Big Data analytics that no local system can observe individually. An important advantage of applying this solution is that this extra information can significantly improve the safety and efficiency of traffic, despite the fact that there is no expressed demand for it by the end user. By implementing SDN solutions with a centralized view on the system of networked vehicles, the information obtained by Big Data analytics is forwarded to local systems in vehicles even without the request message sent by the protocol on the user side. Based on this information it is possible to predict the movement of vehicles in the near future, the possibility of incidents on the road (e.g. due to a malfunction of the vehicle) and perform pro-active collision avoidance [8]. The information generated in the cloud can be of great importance for road safety and more efficient regulation of traffic on the roads. Their timely distribution to large groups of users is, therefore of paramount importance. This imposes the need for the dynamic changes in the network in order to provide the necessary resources since there is the redistribution of available network resources. Traditional IP networks are not able to provide the necessary dynamic, because any change in the network requires additional time and commitment of the human factor. Troubleshooting dynamic allocation of resources is closely linked with the problem of a more flexible traffic management, which requires that the IP network has brought a greater degree of programmability. For this reason, we have implemented SDN networking technology to help ensure a higher degree of automation in terms of the allocation of the necessary resources and more flexible traffic. The reasons for the occurrence of traffic stoppers may be different (August humidity, defects in vehicles, etc.) and they can cause the creation of kilometers long queues. The analysis of the data from the field and by applying efficient algorithms for prediction, the cloud can timely calculate the size of traffic stopper that could arise in the foreseeable future. To avoid the problem, the information is moving towards a concrete road in order to comply with some of the criteria (shortest path, minimum load on the road, etc.). This requires immediate changes in the configuration of the network, which are necessary for the dynamic allocation of bandwidth to users that can be provided only by the SDN controller to significantly affect the size of the plug and efficiency of traffic, which is shown in Figure 3. The vehicles can exchange information with the traffic infrastructure surrounding, which is very important in the case of failure of the network communication with traffic cloud, in order to avoid eventual accidents on the road. It is possible to establish ad-hoc, point-to-point or point-to-multipoint wireless communication (VANET) within a particular cluster [4].

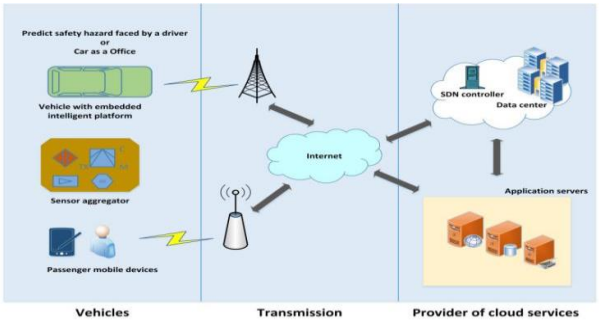


Figure 2. Concept of Smart Vehicle Computer System

V. SCENARIO FOR CLOUD SUPPORTED APPLICATION

In this paper we have done a validation of a suggested solution, with an application scenario on how to avoid traffic congestions on the road in cases when accidents occur.

In the previous section, we have proposed the architecture, and in this section we are evaluating one of the possible applications, dynamic vehicle routing, which is based on the earlier mentioned architecture. The main idea is to perform parameter minimization selected by the user to reach the desired destination. In defining the criteria for routes comparison, we started with predefined parameters, which describe each road section: length and maximal speed allowed.

We suggest an algorithm for realization, which will predict traffic using cloud technologies. Suppose that the traffic network which we are observing consists of 7 areas (theoretically it should be n areas: A1, A2…A7 which are shown in Figure 4.) Inside each area, we have more sections of the road. Each section can be characterized by different parameters:

- Quality of the road (whether it is a service, residential, tertiary, secondary or primary road) from point a to point b, it is denoted by Q(a, b). By primary road we think of highways, secondary roads are main roads in the city, tertiary are roads that lead to secondary roads, residential are roads through settlements and by service road we think of narrow roads which lead to residential roads. Each one of these roads has predefined speed limitations.
- Length of the section (road) expressed in kilometers-d(a, b).

The parameters of the quality of the road can have one of the values from the next set:

$$Q(a,b)\begin{cases} 0, & service\ road \\ 0.25, & residential\ road \\ 0.50, & tertiary\ road \\ 0.75, & secondary\ road \\ 1, & highways \\ +\infty, & unused\ road \end{cases}$$

The system starts to work when the event happens and SVCS sends information to traffic cloud. The undirected weighted graph is formed. If the road is not in the function or if there was an accident a value of the parameter Q(a,b) is set to infinity. Vector A (A1, A2… A7) is the range of areas which is shown in Figure 4. Each area consists of nodes collection (for example A1 has nodes S1, S2… Sn). For every area we continuously calculate weights of the path W(w1, w2,…, wn). The weights of the road should be calculated for every path. We are using Dijkstra's algorithm in this paper,

 ISBN: 978-1-61208-644-6

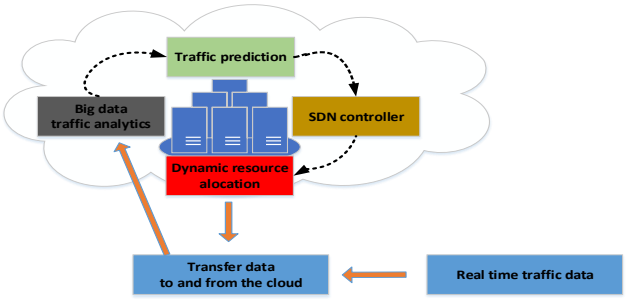


Figure 3. SDN platform for dynamic resource allocation on the cloud

which is adjusted to our needs. Dijkstra's algorithm finds the shortest path between the nodes in the graph, which are represented with different weights listed above w(a,b). The vector of weights is as follows:

$$W = w(a, b)$$

The weighted path can be expresses like a function:

$$W = Q(a, b) + c \cdot \frac{1}{d(a,b)}$$

Where c is a constant used for scaling, and d represents distance between points a and b.

Let us assume that we have a road system as it is shown in Figure 5. It is represented as a connected, undirected and weighted graph, with eight nodes. The weights are assigned with respect to the quality of the road Q(a,b). A user wants to find the shortest path from node A to node H. According to Dijkstra's algorithm, the user starts from the node A and is taking into consideration the paths to the remaining nodes. Since the nodes B, C and D are the neighbors of the node A, new ordered pairs are assigned to nodes B, C and D, respectively. By using the same idea, the algorithm moves through the graph and after a few steps the node H is reached. Analog to this, a user can choose other parameters (d(a,b), w(a,b)). In reality, the best road is not always the highway. In some occasions city road is a better choice, because route can be shorter than the route going along highway. If an accident occurs, our algorithm iteratively calculates a new route. The map was extracted from OpenStreetMap [19] which is a free editable map of the world. For experimental purposes, we have used the map of the University of Novi Sad campus, where the fluctuation of traffic is huge and there are often big congestions. It is very important to redirect cars through different paths in order to reduce the possibility of congestions.

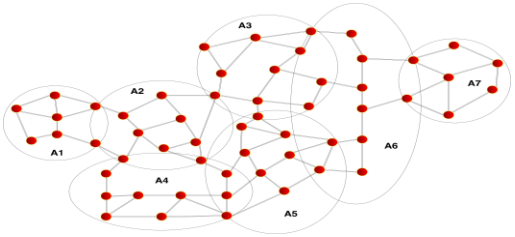


Figure 4. Range of areas

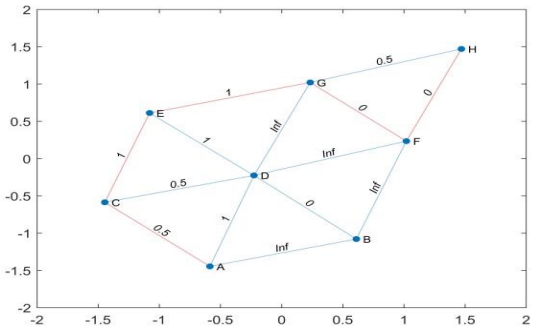


Figure 5. Example of road network

Figure 6. University of Novi Sad

Figure 7. Algorithm decides on the best path from starting to ending position

The model of the campus is shown in Figure 6. Taking into consideration that we have two possible routes from starting position to ending position, we apply our algorithm, and based on the assigned weights, the optimal route is calculated. The optimal route is shown in Figure 7. If an accident or congestion occurs, the cars are redirected to other route consisting of residential road.

 ISBN: 978-1-61208-644-6

VI. CONCLUSION

The usage of advanced ICT enables an easier integration of cyber-physical equipment in cars with the traffic cloud and provides enormous possibilities for the fast development of intelligent transport systems. In this article, the analysis is done, we provide a brief review of existing solutions in this field, and a new concept of an integrated platform for smart management of cars is proposed. We provide a detailed explanation that a basic concept consists of the applications for efficient management of cars, which are supported with the cloud, and we provide an explanation of the components, which affect the Quality of Service (QoS). In the end, in order to do a validation of suggested solutions, we have proposed an application scenario for the dynamic routing of traffic in cloud with a goal to avoid traffic congestions on the road in cases when accidents occur. Our belief is that SDN based traffic cloud will attract enormous attention from researchers in the near future, in order to ensure an efficient management of traffic, greater security and comfort for all the participants.

REFERENCES

[1] M. Qingxue and L. Jiajun, „The modeling and simulation of vehicle distance control based on cyber-physical system“. Proceedings of 7th Joint International Information Technology and Artificial Intelligence Conference (ITAIC 2014); Dec. 20-21 2014; Chongqing, China. IEEE.

[2] J. Bradley and E. Atkins, „Optimization and Control of Cyber-Physical Vehicle Systems“, Sensors, vol.15, pp 23020-23049 , September 2015

[3] J. Wan, J. Liu, Z. Shao, A. Vasilakos, M. Imran, and K. Zhou „Mobile Crowd Sensing for Traffic Prediction in Internet of Vehicles“, Sensors, vol.16, no.1, pp. 88-96, 2016 January,

[4] J . Wan, D. Zhang, Y . Sun, K . Lin, C. Zou, and H. Cai „VCMIA: A Novel Architecture for Integrating Vehicular Cyber-Physical Systems and Mobile Cloud Computing“ ACM/Springer Mobile Networks and Applications, vol. 19, pp 153-160, Apri 2014

[5] Y. Xu and J. Yan, „A cloud-based design of smart car information services“, Journal of Internet Technology, vol.13, no. 2, pp. 317-326 January 2012

[6] C. C. Chuang, W. L. Cheng, and K. S. Hsu, „A comprehensive composite digital services quality assurance application on intelligent transportation system“, Proceedings of 17th Asia-Pacific Network Operations and Management Symposium (APNOMS 2015); Aug 19-21 2015; Busan, South Korea. IEEE.

[7] M. Whaiduzzaman, M. Sookhaka, A. Gania, and R. Buyya, „A survey on vehicular cloud computing“, Journal of Network and Computer Applications, vol. 40, no.2, pp.325-344, November 2013.

[8] R. Trivisonno, R. Guerzoni, I. Vaishnavi, and D. Soldani, „SDN-based 5G mobile networks: architecture, functions, procedures and backward compatibility“, Transactions on Emerging Telecommunications Technologies, vol. 26, no.1, pp. 82–92. December 2014.

[9] S. Wibowo and S. Grandhi, “A Multicriteria Analysis Approach for Benchmarking Smart Transport Cities”, Science and Information Conference, pp. 94-101, July 2015.

[10] Ear-IT, Available at: https://ec.europa.eu/digital-single-market/en/news/ear-it-using-sound-picture-world-new-way

[11] M. D. Marquez, A. Lara, and R. X. Gordillo, “A New Prototype of Smart Parking Using Wireless Sensor Networks”, IEEE Colombian Conference on Communications and Computing, pp. 1-6, June 2014.

[12] Google Self-Driving Car Project, available at: https://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-0516.pdf

[13] P. Pyykönen, J. Laitinen, J. Viitanen, P. Eloranta, and T. Korhonen, “IoT for Intelligent Traffic System”, IEEE International Conference on Intelligent Computer Communication and Processing, pp. 175 – 179, 2013.

[14] M. Elkotob and E. Osipov, “iRide: A Cooperative Sensor and IP Multimedia Subsystem Based Architecture and Application for ITS Road Safety”, Proceedings of EuropeComm, vol. 16, no.3, pp. 153-162, 2009

[15] P. A. Sumayya and P. S. Shefeena, “VANET Based Vehicle Tracking Module for Safe and Efficient Road Transportation System”, International Conference on Information and Communication Technologies, vol. 46, pp. 1173-1180, 2015.

[16] J. Yu, K. H. Low, A. Oran, and P. Jaillet, “Hierarchical bayesian nonparametric approach to modeling and learning the wisdom of crowds of urban traffic route planning agents”, Inter. Conference on Intelligent Agent Technology, vol. 2, pp. 478–485, December 2012,

[17] M. Chen, S. Mao, and Y. Liu. “Big data: A survey. Mobile Networks and Applications”, vol.19, no.2, pp. 171-209, April 2014.

[18] M. Elkotob and E. Osipov, “iRide: A Cooperative Sensor and IP Multimedia Subsystem Based Architecture and Application for ITS Road Safety”,pp.153-162, 2009

 ISBN: 978-1-61208-644-6

European Data Protection Regulation and the Blockchain Analysis of the Critical Issues and Possible Solution Proposals

Nicola Fabiano
Studio Legale Fabiano
Rome, Italy
Email: info@fabiano.law

***Abstract*—The blockchain represents an Internet revolution in terms data usage, storage, anonymity, encryption, and so on. The technical evolution of the blockchain also has an impact on the Internet of Things (IoT) phenomena. However, we should take into account the legal issues related to the data protection and privacy law. Technological solutions are welcome, but it is necessary, before developing applications, to consider the risks to the fundamental rights and freedoms which we cannot dismiss. Personal data is a value. It is important to evaluate the European Regulation n. 2016/679, General Data Protection Regulation (GDPR) that applies from May 25th 2018. The GDPR introduces Data Protection by Design and by Default, Data Protection Impact Assessment (DPIA), data breach notification and significant administrative fines in respect of infringements of the Regulation. It is fundamental to evaluate the blockchain and its compliance with the GDPR principles. Regarding the data protection and security risks, there are some issues with potential consequences for data and liability. A correct law analysis allows evaluating risks preventing the wrong use of personal data. The contribution describes the main general principles according to the GDPR and the aspects related to the blockchain.**

Keywords–Data Protection; GDPR; Blockchain.

I. INTRODUCTION

Nowadays, the blockchain is a part of our life. More and more often people use the blockchain, especially in trading with crypto-currencies. We know that the blockchain is a distributed ledger database where encrypted data are stored. Several blockchain applications allow us to define this phenomenon as "blockchain as a service". In this context, it is important to consider the Regulation n. 2016/679 General Data Protection Regulation (GDPR) [4] about the protection of personal data. It is quite clear that the blockchain has been analysed only from a technical point of view, but there is another side to be considered that is the data protection law. In fact, the current blockchain framework considers technical aspects related to each kind of node and to the security measures adopted by avoiding disclosure of information. It is crucial to develop the blockchain infrastructure and set up the structure of the node. However, the developers pay attention to the technical aspects always ignoring the way to design the blockchain following the law obligations especially regarding the protection of personal data. This aspect is becoming increasingly relevant since the application of the GDPR starting from May 25th 2018.

The rest of the paper is structured as follows. In Section II, we describe the current European legislation on the processing of personal data. In Section III, we describe the differences between privacy and data protection. In Section IV, we analyse the blockchain and the relationship among the principles provided by the European Regulation 2016/679, trying to address possible solutions to be compliant with the law.

II. THE EUROPEAN LAW ON THE PROCESSING OF PERSONA DATA

In Europe, the protection of natural persons in relation to the processing of personal data is a fundamental right. In fact, Article 8 of the Charter of Fundamental Rights of the European Union (the Charter) [1] is related to the protection of natural persons in relation to the processing of personal data [4] (Article 8 - Protection of personal data).

Furthermore, the Charter also considers the respect for private and family life [1] (Article 7 - Respect for private and family life) as a crucial aspect of privacy.

Moreover, the Treaty on the Functioning of the European Union (TFEU) [2] considers the right to the protection of personal data (Article 16(1) says: "Everyone has the right to the protection of personal data concerning them").

This is the general legal framework, and the protection of personal data is under the Directive the Directive 95/46/EC [3] until May 25th 2018.

Nevertheless, in 2016, the European Regulation number 679/2016 has been published. It entered into force on May 25th, 2016, but it will be applied starting May 25th, 2018 [4]. According to Article 94, this Regulation will repeal the Directive 95/46/EC [3] with effects from May 25th 2018. Therefore, the Directive 95/46/CE will be applicable until May 25th, 2018.

The GDPR obviously mentions the Charter of Fundamental Rights of the European Union in the first Whereas (*The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the Charter) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her*).

The primary goal is to harmonise the legislation of each Member State: the GDPR will be directly applicable in each European State, avoiding possible confusion among the domestic law. The GDPR introduces numerous changes, such as the Data Protection Impact Assessment (DPIA), the Data Protection by Design and by Default (DPbDbD), the data breach notification, the Data Protection Officer (DPO), the very high administrative fines in respect of infringements of the Regulation, and so on.

 ISBN: 978-1-61208-644-6

Regarding the protection of personal data, apart from the before mentioned GDPR, there is also the Directive 2002/58/EC [5] concerning the processing of personal data and the protection of privacy in the electronic communications. In fact, according to Article 95 of the GDPR, there is a relationship with this Directive (*Article 95 says: "This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC".*).

Directive 2002/58/CE has the aim "*to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community*" (Article 1).

In this legal panorama, it is clear that technology and law are not at the same level because the first one (technology) is always ahead than the second one (law). The actions on the part of the legislator always follow the technological solutions, and so the rules have to be able to consider the technology evolution.

GDPR applies on May 25th 2018, and it is crucial to analyse it to comply with the new data protection Regulation. In fact, GDPR represents an innovative data protection law framework because of several legal purposes on which it is based.

III. Data Protection and Privacy

Often, people erroneously consider "privacy" and "data protection" as synonyms, confusing the real meaning indeed. "Privacy" and "data protection" are not the same because, apart from the terminological definition, they are different concepts. Both are fundamental rights in Europe, but there are differences between them. On one hand privacy is related to the personal life; on the other hand, data protection concerns the personal information.

It is not possible to address data protection and privacy issues adopting only technical solutions without any legal reference. Apart from the highly technical solution, hence, we cannot dismiss the law obligations, where they are applicable, like in Europe, according to the GDPR [4]. In fact, in terms of legal framework, "security" is not equal to "privacy". A system could be very secure but not in compliance with the data protection law. On the contrary, a system could be compliant with the data protection law and, hence, very secure (obviously only by the adoption of security measures).

IV. Blockchain and Data Protection

The IoT evolution realises an ecosystem and inside it there is an emerging phenomenon, basically a technical system, named blockchain [6]. The blockchain was imagined by Satoshi Nakamoto [7] and, probably, it is well-known because it is the technical structure used for the bitcoin (a crypto-currency). The blockchain has been primarily used for the crypto-currencies and it is a shared, immutable ledger for recording the history of transactions; it is a ledger of records. The blockchain can work as a distributed database, and its structure guarantees any modification or alteration due to the strong link and timestamp among each block.

However, apart from the crypto-currencies, the blockchain allowed to develop several applications in different fields (i.e., smart contracts, electronic identity, keeping of digital documents, e-Government, etc.). Hence, any interaction among the several blockchain application is possible. In this context, we can qualify the blockchain phenomenon in terms of "*blockchain as a service*" due to the potential to carry out diverse services. In fact, this development denotes the blockchain evolution from a technical structure under the crypto-currencies to a proper IT infrastructure that can be used to deliver services.

However, a distinction must be made.
Generally, there are:

1) public blockchain
2) private blockchain
3) combined blockchain (consortium blockchain)

Now all the blockchains are based on systems of proof of work or proof of stake. In the public blockchain, everyone can access and make transactions. In the private blockchain, the control is under the power of the organisation. In the combined blockchain, the control is under some nodes.

This scenario is important to privacy and the protection of personal data. In this general context, what about data protection and privacy? Regarding privacy, Satoshi Nakamoto [7] argues that *privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous*. However, the author says also that *The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner*. That represents a significant chink in the data protection and privacy perspective. Ensuring privacy and data protection is one of the main aims of any project which has to addressed by design, not leaving any possibility to compromise personal data and/or personal information. Given the structure of the blockchain, it seems that any subject or person or owner (as defined by Nakamoto) should be a controller and consequently bound to respect the privacy or data protection laws. From a business perspective, probably, personal data or personal information does not receive adequate protection, thinking also to grow the security measures. To set up high-security measures is a good solution but it is not the only one. Each organisation, before designing a project, has to consider the principles provided by the article 25 of the GDPR (data protection by design and by default). According to these principles the controller, before starting the processing of personal data, has to implement appropriate technical and organisational measures. In this way, the controller shall be compliant with the data protection by design and by default". It is wrong to address a compliance process with the privacy or data protection law after the project output because any evaluation must be during the design phase.

The security solution is always used by scientists and technicians to address data protection issues. However, it is crucial to consider the Data Protection obligations provided for by law and especially the GDPR. According to the EU Regulation n. 2016/679 from May 25th 2018 it will be mandatory to respect principles and rules required by the GDPR. Among the several principles provided by the GDPR, some general one do not

 ISBN: 978-1-61208-644-6

seem to be applicable to the blockchain. In fact, according to the article 5, paragraph 1, of the GDPR, there is the need to respect the following principles:

1) lawfulness, fairness and transparency
2) purpose limitation
3) data minimisation
4) accuracy
5) storage limitation
6) integrity and confidentiality

Paragraph 2 of the above mentioned article 5 states: "*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)*". The principles mentioned above are so relevant that, in case of infringement, a hard administrative fine up to 10.000.000 EUR shall be applicable, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year.

Giving that, what about the blockchain?

In fact, in case of private blockchain or probably of the combined blockchain, it is possible to respect the principles as mentioned above, because there will be an identified controller. In case of a public blockchain, instead, it will be impossible to establish who is the controller. The identification of a controller is crucial for the "accountability", according to the article 5, paragraph 2, of the GDPR. The essential identification of the controller is closely related to the six principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality).

How is it possible to respect the principles as mentioned earlier without a controller?

The consequences will be that a public blockchain will not be in compliance with the data protection law (GDPR).

Another point is the respect of the first principle (lawfulness, fairness and transparency) and especially regarding the data subject's consent.

According to the article 6, paragraph 1, of the GDPR "*Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*".

In this scenario, there are some relevant questions, and the answers will be useful to correctly address the legal issues related to the compliance with the data protection law (GDPR).

In fact,

- to whom the data subject gives the consent?
- can the data subject withdraw the consent and how?
- how and to whom the data subject can ask the erasure of personal data or exercise the rights according to the GDPR?
- who are the parties and, mainly, who is the blockchain's representative party that is responsible and considered as a controller?

As mentioned earlier, none of the questions mentioned earlier have answers in compliance with the GDPR. It is not possible to consider every single node of a public blockchain based on a contract. If the data subject withdraws the consent, the node continues existing, and it will not be erased and removed. As there is no controller in the public blockchain, it is impossible for the data subject to address a request to erase personal data; the data subject will not be able to exercise the rights according to the GDPR. A public blockchain, giving its technical structure, is not configurable as a contract among the node's owners.

V. Applying the GDPR to the blockchain and possible solutions

As mentioned earlier, it is quite complicated to apply the GDPR fully to the blockchain because of its technical architecture. We want to highlight some critical issues related to the application of the GDPR to the blockchain and the possible solutions.

1) **The roles.** It is relevant to identify all the roles played in the processing of personal data and especially in the blockchain. In the blockchain, we absolutely must identify the controller and the processor(s), but this is impossible in the public blockchain. Who is the controller in a blockchain?
2) **The Data Protection Officer (DPO).** Moreover, by virtue of its nature, its scope and/or its purposes, the blockchain could imply regular and systematic monitoring of data subjects on a large scale, according to the article 37, paragraph 1 letter b) of the GDPR. In this case, it is mandatory to designate a data protection officer (DPO). However, due to the blockchain architecture and structure, it will not be easy - especially in a public blockchain - to identify the controller and consequently who is the subject obligated to designate a data protection officer. We think that this is criticality of the blockchain structure and it will be impossible to designate a data protection officer. Differently, in a private blockchain, the controller can and indeed must designate a data protection officer according to the GDPR. Designating a data protection officer means that this subject has to take at least the tasks mentioned in the article 39 of the GDPR. It is evident that the blockchain must allow the DPO to make all the tasks to be compliant with the GDPR.
3) **Transferring personal data to third countries.** Another key-point is related to the transfers of personal data to third countries or international organisations. In fact, according to the blockchain architecture, it is impossible to restrict its application to the European member States. According to the article 3, paragraph 2, (Territorial scope) of the GDPR
"*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union".
Hence, for example, if someone based outside the European Union offers goods or services to such

data subject in the Union, he must respect the GDPR rules. In this context, it will be challenging to localise a blockchain (better all the data) only inside the European Union. Consequently, the GDPR will apply to all over the world. The articles from 44 to 50 of the GDPR provide the rules for the transfer of personal data outside Europe. It is quite impossible to localise the data centre(s) where the blockchain data are stored, because of its technical structure and this can be a critical condition for the application of the GDPR rules in this matter.

4) **The liability.** Regarding liability, the article 82 states that "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"*. What kind of right is there to receive compensation in a public blockchain where there is no controller?
5) **Data breach.** According to the article 34 of the GDPR "*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*". In a public blockchain how is the rule applied? We must consider a data breach firstly and understand its causes. Secondary, we must know who is the controller according to the considerations as mentioned above.

Hence, there are a lot of critical issues in the application of the GDPR in the blockchain; in certain cases, it is possible to comply with the GDPR rules using some legal instruments as mentioned above, but, in other cases, it will be impossible. However, although it is difficult to consider a full application of the GDPR to the blockchain, we think that through some legal instruments, it is possible to be compliant with the data protection law. In fact, we can address some issues - where applicable - by policies and contractual solutions. It should be clear that it is not ever possible to use all these legal solutions because it depends on the kind of the blockchain. In a public blockchain, for example, we can use only policies applicable to all the participants (node owners'). Each policy should be issued according to the GDPR rules. In this way, each node owner's will be informed about the processing of personal data and eventually give the consent.

VI. Conclusion

On May 25th 2018, the GDPR starts applying. It is crucial to analyse now the GDPR to be ready and comply with the new data protection Regulation. In fact, the GDPR represents an innovative data protection law framework, because of several purposes on which is based.

As we have shown, in the public blockchain there is no supervisor and each subject working on the blockchain is the owner of his node(s). In this case, indeed, there is no controller because the node's owner cannot be the controller of himself. In this situation, apparently, could seem that the privacy and data protection law is not applicable. However, the node's owner could perform activities in the blockchain potentially harmful to the same blockchain and the other nodes. Therefore, there is the liability for the node's owner for any possible damages. Designing and setting up blockchain means that privacy and security policies should be created privacy and security policies applicable to all the node's owners. This solution could mitigate the lack of the law where it is not possible to apply it to the blockchain system.

In the private blockchain, instead, the privacy and data protection law shall apply to the organization with the consequence that it must respect all the legal obligations, including the information to the data subject, his consent and rights. However, it is highly recommended to set up privacy and security policies.

In the combined blockchain, due to the fact that the control is under some nodes, they could be considered controllers and, hence, they are required to respect the privacy and data protection law.

The adoption - by design - of data protection policies could overcome some critical issues of the blockchain addressing, in this way, the nodal points towards a true path of compliance with the data protection and privacy laws.

References

[1] Charter of Fundamental Rights of the European Union http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN retrieved: June 2018

[2] The Treaty on the functioning of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN retrieved: June 2018

[3] Directive 95/46/ec of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN retrieved: June 2018

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN retrieved: June 2018

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, 2002 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=en retrieved: June 2018

[6] IBM, Understand the fundamentals of IBM Blockchain - https://www.ibm.com/blockchain/what-is-blockchain.html retrieved: June 2018

[7] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system - https://bitcoin.org/bitcoin.pdf retrieved: June 2018

[8] AA.VV.: River Publishers, Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds, 2016

[9] L. Axon, University of Oxford - Privacy-awareness in Blockchain-based PKI (2015) - https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63bretrieved: June 2018

[10] K. Christidis and M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things - http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408 retrieved: June 2018

[11] M. Conoscenti, A. Vetr and J.C. De Martin - Peer to Peer for Privacy and Decentralization in the Internet of Things - In: 39th International Conference on Software Engineering, Buenos Aires (AR), May 20-28, 2017. pp. 1-3 - http://porto.polito.it/2665723/1/peer_to_peer_for_privacy_and_decentralization_in_the_internet_of_things.pdf retrieved: June 2018

[12] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou - Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts (2016) - https://eprint.iacr.org/2015/675.pdf retrieved: June 2018

 ISBN: 978-1-61208-644-6

[13] G. Zyskind, O. Nathan and A. Sandy Pentland - Enigma: Decentralized Computation Platform with Guaranteed Privacy (2015) - https://arxiv.org/pdf/1506.03471.pdf retrieved: June 2018

[14] European Convention on human rights - http://www.echr.coe.int/Documents/Convention_ENG.pdf retrieved: June 2018

[15] Gartner: Gartner Says 6.4 Billion Connected ”Things” Will Be in Use in 2016, Up 30 Percent From 2015 - http://www.gartner.com/newsroom/id/3165317 retrieved: June 2018

[16] Cyberhigiene project - https://www.petrashub.org/portfolio-item/cyberhygiene/ retrieved: June 2018

[17] A. Cavoukian: Springer, Identity in the Information Society. Identity in the Information Society, 2010

 ISBN: 978-1-61208-644-6

Blockchain Beyond Cryptocurrencies: A Real-World Use Case

A Non-Repudiable Supply Chain Tracking System

Filippo Bosi, Michele Cappelletti, Stefano Monti, Guido Ravagli
Imola Informatica
Imola (BO), Italy
e-mail: {fbosi, mcappelletti, smonti, gravagli}@imolainformatica.it

***Abstract*—Blockchains have recently emerged as an architectural style to overcome the intrinsic trust problem that arises when single central authorities are delegated the role to keep certification information for different parties and actors. By fueling a host of different cryptocurrencies, various forms of blockchains are revolutionizing the finance sector. However, blockchains are rapidly emerging outside of the finance sector, disrupting the business scenarios. This paper presents a novel Supply Chain Tracking system that eliminates fraud and counterfeits from a specific business sector, namely toner cartridge regeneration, where a recent European directive (and subsequent national regulations) has posed stringent limitations.**

Keywords-Blockchain; supply chain; tracking.

I. INTRODUCTION

In recent years, cryptocurrencies have paved the way for a new architectural model for distributed, decentralized (i.e., with no central authority/single point of failure) transactions based on so-called blockchains.

Due to their nature as a distributed, non-repudiable, non-centralized ledger, blockchain adoption has now extended well beyond cryptocurrencies and finance in general [1], and relevant use cases begin to emerge in disparate business sectors, specifically where challenging traditional central "trust" authorities open up new business opportunities [2][3].

Blockchain adoption in contexts other than cryptovalues is quickly gaining momentum, and may be disruptive both in technical and in business terms.

Blockchain architectural styles and implementations pose some stringent limitations as well, and taking them into account is crucial when planning their adoption in business contexts other than finance.

This paper presents an innovative approach to certification and tracking of cartridge regeneration process and logistics.

A recent European Union (EU) directive called Green Public Procurement (GPP) [16], and subsequent national regulations (e.g., the Italian Criteri Minimi Ambientali – CAM [17]) require Public Administrations to have a relevant share of the toner cartridges they buy be regenerated and supplied by certified providers.

However, nowadays toner cartridge regeneration suffers from a high level of forgery, and the verification of used toner cartridge life cycle (e.g., whether they have been refilled from certified partners or not) becomes nearly impossible.

Some studies report that in the last five years, original and refilled cartridge market share have both significantly dropped, in favor of a steady increase of cloned/fake cartridge (from 1% to 30%).

We partnered with Eco-Recuperi [4] – a major Italian player in the cartridge regeneration process, and we designed a Supply Chain Tracking System that eliminates the possibility to sell counterfeit cartridges as certified, recycled ones, thanks to the adoption of blockchain as a distributed notarization system for supply chain certification.

The rest of this paper is organized as follows. Section II describes related work and background knowledge. Section III details the business scenario and main business/technical requirements. Section IV addresses the process and architecture of our solution. Section V concludes this paper and summarizes our main findings.

II. BACKGROUND

This section provides some background knowledge about blockchains, and surveys their benefits, architectural styles and alternatives, and their growing business adoption in many business sectors.

A. Blockchain features, benefits, and issues

Blockchain architecture [5] is a network of computing nodes that share a common state. Blockchain architecture and protocols are designed so that at any given time, the majority of nodes should agree on the state of a blockchain itself.

Changes on the state of a blockchain are recorded as a series (chain) of transaction groups (block): each transaction relates to a specific user (identified by a unique identifier), and a specific point in time (timestamp).

Blockchain typically acts as a generic distributed ledger of transactions and guarantees some key characteristics that lend themselves well to our business case.

1) Non-repudiation: every transaction users register on the blockchain automatically becomes non-repudiable, e.g., once a transaction takes place, the user that actually performed the transaction will not, in any case, be able to refute its responsibility about the transaction itself;

 ISBN: 978-1-61208-644-6

2) Irreversibility: every transaction users register on the blockchain automatically becomes irreversible, e.g., users are not allowed to cancel/edit/undo a transaction;

3) Transaction timestamping: any transaction happens at a specific point in time, and blockchain records such instant in a non-modifiable, and always identifiable way;

4) Censorship resistance: single transactions and the status of a system as a result of a series of transactions cannot be denied, and are always publicly available and verifiable.

The above features make blockchains a distributed ledger that notarizes events, and makes them universally, perpetually accessible and non-repudiable.

B. Blockchain architectural styles

Blockchain is neither a specification nor a technology, and is rather considered a paradigm/architecture style.

The first blockchain specification was the Bitcoin one, released in 2008 [6] [7]; from then on, many other blockchain implementations have emerged, with very different characteristics.

The Bitcoin blockchain has been considered the reference implementation of the blockchain paradigm. The major capability to implement is to – statistically - solve Byzantine Generals Problem [8], that is a classic problem faced by any distributed system network. The Bitcoin original implementation is based on hashcash [9], a proof of work algorithm. It is a smart approach to reach distributed consensus, providing a strong protection from brute force attacks, achieving overall system reliability in the presence of a number of faulty processes.

A proof of work algorithm has two strong implications: it needs a high amount of energy to run and it makes it harder to deliver real-time results, since it is distributed among a large and ever-increasing number of nodes, and it is based on computation-intensive random processing. Due to these limitations, many attempts have been made since Bitcoin release, to avoid proof of work shortcomings. Those implications set strong limits on transaction throughput and significant operational costs of the network. Proposed solutions focus on performance improvement and cost decrease: the most significant changes focus on the centralization of the transaction validation process and on the adoption of a consensus algorithm that is not based on the computational brute force principle.

These 'improvement solutions' can be considered as some sort of relaxation of constraints of the original Bitcoin blockchain architecture; while those relaxations are not necessarily a limitation, they should be carefully taken into account when determining which blockchain style fits business requirements and context the most.

Categorization [10] can be made in order to simplify blockchain types understanding:

- 'Bitcoin-like' Blockchains: blockchains with distributed consensus algorithm and history of transactions persisted in a chain of mathematically linked blocks; those are the blockchains that implement the original idea of blockchain as it was proposed by Bitcoin and their focus is on transaction history immutability and consistency over transaction throughput;
- 'Enterprise' blockchains: characterized by a centralization of core functionalities like transaction validation, block creation, and naming service; focus is set on governance aspects such as access regulation and privacy mechanisms;
- Distributed Ledger Technology (DLT): state is shared among nodes of the network, but no chain of blocks is implemented. Other measures are set in order to enforce immutability of transactions, but focus is set on performance in order to reach near-real time information distribution in the network.

Blockchains - and DLTs - can also be categorized by governance model, i.e., the possibility to access the blockchain with or without the permission of a remote account issuing service:

- Permission-less: users independently create their own account using a deterministic process that ensures the account identifier is globally unique, enabling them to immediately access the blockchain. It is the typical approach of 'Bitcoin-like' blockchains;
- Permissioned: users registration has to be approved by the blockchain centralized service issuer, such as any traditional Information Technology (IT) service.

C. Blockchain use cases and business opportunities

As previously discussed, the blockchain paradigm addresses the big challenge of securely collecting events in a distributed scenario enhancing immutability, transactionality, and near-real time delivery; the following section describes real world scenarios that take advantage of the adoption of the blockchain paradigm.

First of all, the use case the whole world knows is the one the blockchain was born for: exchange of a new digital currency, both coined and exchanged inside the blockchain. The birth of the blockchain marks the introduction of a new type of currency, alongside traditional fiat currencies, where fiat means the currency has a legal value and is coined by a proper institutional entity.

Digital currency exchange use case has already many real-world business case, such as:

- Cross border money transfer: near real-time delivery of transaction in the network allows worldwide value transfer with significant time and cost decrease with respect to traditional processes;
- Pseudonymous [11] money transfer: as previously said, account creation can be done autonomously. In addition, account data are pseudonymous, which means accounts do not include any personal data. These two features allow enhancing privacy features in value exchange between users;

 ISBN: 978-1-61208-644-6

- Closed virtual currencies: since the blockchain enables issuing digital currency autonomously, organizations can take advantage of this feature to replace - or implement – closed loop exchange of value such as fidelity card for customer retention and food stamps for employers.

Notarization is a less explored use case for blockchains, and derives directly from three Bitcoin-like blockchain features, provided that they come together:

- Non-repudiation: transaction issuer cannot repudiate ownership of his transactions;
- Immutability: transactions inserted in the blockchain cannot be altered in any way after being considered validated;
- Timestamping: every transaction is timestamped with the blockchain time once considered valid by the network.

A blockchain implementing all those three features can be considered as a notary and transactions made on the blockchain can be considered as notarized events.

Many business cases and applications can enhance certification of their processes by enforcing trust using blockchain as a notary service: tracking processes phases on the blockchain means they become unmodifiable milestones. While few real world applications of this use case are already in production, the great majority are yet to come:

- Track phases of clinical trials [12];
- Track patents issuing, intellectual property and copyrights [13];
- Track supply chain of goods, such as the cartridge recycling process phases presented in this paper.

III. SCENARIO AND REQUIREMENTS

This section describes our scenario and requirements from both business and technical perspectives.

A. Objectives

The main business goal of this project was to provide a reliable/verifiable certification process for cartridges lifecycle, to limit regeneration frauds. This means being able to:

- track cartridge status change between the various stages of refill processes (e.g., collect, refill, package, distribute, sell);
- physically tag/associate each cartridge with such lifecycle information with easily readable, non-repudiable, and tamper-proof mechanisms;
- build a verification infrastructure that lets anyone publicly verify the status of each cartridge.

The verification infrastructure itself has stringent non-functional requirements:

- reliability and trust: the infrastructure should prevent anyone from introducing fake data to certify non-recycled cartridges;
- simplicity: to ease adoption, especially among Public Administrations;
- cost-effectiveness: physical tags and the associated verification process should pose a negligible cost overhead, to avoid posing refilled cartridges out of market;
- accessibility: the verification tools should be easily accessible, via e.g., Web Applications and Mobile Applications.

B. Actors and process

The main actors are:

- Certification Authority: independent actor that issues unique identifiers (UIDs) to tag and track refilled cartridges;
- Collector: economic subject that collects exhausted toner cartridges and selects them for regeneration;
- Refiller: economic subject that actually refills exhausted cartridges;
- Distributor: economic subject that distributes and sells refilled toner cartridges;
- Customers: private/public subjects that buy refilled cartridges;
- Recycling consortium: consortium of recycling supply chain participants whose recycling process has been reviewed and approved by the Certification Authority; any cartridge refilled from a Refiller of the Consortium is identified by a UID from the Central Authority.

Figure 1. Traditional cartridge recycling process and actors

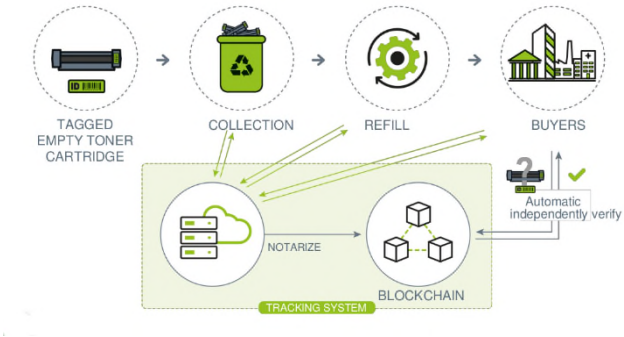


Figure 2. Blockchain-enabled, trusted recycling process and actors

Figures 1 and 2 depict traditional and blockchain-based processes, respectively.

The blockchain-based process steps are as follows:

- Step 0 – UID distribution: PACTO (Produttori Associati Cartucce e TOner) [18] Consortium distributes UIDs to certified Collectors, and keeps track of UID-Collector relationships;
- Step 1 – Cartridge collection: certified Collectors physically collect cartridges and cartridges, and tag them with physical, non-removable, low-cost medium (e.g., Near-Field Communication -NFC tags) that carry UIDs; from now on, each cartridge is uniquely identified by a UID and can be tracked throughout the whole process;
- Step 2 – Cartridge refill: certified Refillers receive exhausted cartridges from Collectors;
- Step 3 – (Optional) Cartridge Distribution: distributors are (optional) intermediary partners that facilitate cartridge sell;
- Step 4 – Sell: Distributors and Refillers are allowed to sell refilled, certified cartridges;
- Step 5 – Verification: Customers can verify cartridge refill process steps, from 1 to 4, hence being able to assess cartridge refill compliance.

C. The key blockchain role

From step 1 onwards, each step advance can be tracked and uniquely associated to a physical cartridge.

A traditional, centralized database of cartridges does not meet reliability and trust requirements: the owner of the database may easily alter database content, leaving other parties no option to verify the correctness of cartridge information.

This inherently distributed update and verification process lends itself well to the adoption of a blockchain-based approach; in our model, blockchain acts as the distributed, decentralized ledger that:

- keeps track of cartridges status advances, and uniquely identifies them (and each status change) via their UID;
- allows any party to verify each stage of the refill process, at any time, and with no option for anyone to alter/fake them.

D. Blockchain choice

Blockchain choice was a core activity of the analysis phase of the project. A huge effort has been spent on studying and researching to understand pros and cons of major public blockchain implementations. This phase was hard, because we were not even aware of the Key Performance Indicators (KPIs) to use for the evaluation. The blockchain is not just a software component: even the community surrounding it, which is defining its evolution roadmap has strong implications on several key aspects that have to be taken into consideration during the evaluation phase. Legal implications, constraints on the underlying service design, community principles, and so on, have to be included in the evaluation.

Key aspects to evaluate are:

- How the business service is considered critical: the most important element is understanding how service delivery failures can affect the real world. For example, using the blockchain in healthcare could be highly critical for humans, in supply chain or copyright protection it could result in considerable penalty to pay, and so on. In order to reasonably guarantee a reliable service, it is necessary to focus on the maturity level of the blockchain implementation, and the level of reliability of its distributed service network. On the other hand, if blockchain is used for a less critical use case, such as academic research, it is safe to adopt less mature technologies;
- Requirements on blockchain governance: should the access be regulated or not? Focus has to be set on governance processes at business level;
- Requirements on data to be written on the blockchain: first of all, data written on the blockchain are intended to be stored publicly, immutably and forever; this implicit feature has strong implications on privacy and data lifecycle, particularly if the blockchain is deployed and used in a public scenario;
- Requirements on performance and integrations: performance common KPIs are transaction validation time, transaction delivery throughput, and scalability of the blockchain; integrations aspects focus mostly on the quality and maturity of integration tools such as library and development environments;
- Cost of the blockchain infrastructure: blockchain costs can be divided in costs of transactions issued, intended as the fee related to those transactions and costs needed to run the infrastructure, intended as computational power to run nodes of the network,

 ISBN: 978-1-61208-644-6

computational power to generate the blocks, and other costs related to connection handling such as bandwidth.

Ultimately, a wider understanding and weighted evaluation on several aspects discussed above had led to consider the Bitcoin blockchain the best choice for this use case.

IV. ARCHITECTURE

The following section describes our Supply Chain Tracking System architecture main inspiring principles and design choices.

A. Architecture principles

Blockchain, as a distributed verifiable data storage, suffers from two main issues:

1. costs: registering transactions (events) on a blockchain usually has non-negligible execution times and transaction fees (costs), especially on public, permissionless blockchains;
2. storage space: Bitcoin blockchain allows storing custom payloads of 80kb: this means storing business-related pieces of information on blockchain is usually infeasible for real-world scenarios.

Due to the scope of our business scenario, we expect the number of transaction registrations to exponentially grow over time, since it depends on the number of certified refilled cartridges and on each status update event. In our model, transaction fees become a direct, proportional cost that contributes to the final cartridge price (as of today, this fee is upon the consortium itself). This is the main reason why cost efficiency throughout the whole recycling process is key in keeping refilled cartridges market-competitive, and we had to design a way for transactions on the blockchain to remain cost- and time-effective, no matter the increase in number of events. Our solution addresses both issues by adopting three key tenets.

First, we define an Event Common Tracking Model (ECTM) - a minimum set of pieces of information that each actor on the process agrees upon to keep track of cartridge status changes; this allows keeping business information strictly needed for notarization to a minimum, and contemporarily enabling interoperability between actors of the supply chain.

Second, we delegate storage of business information to traditional databases: Business Databases can either be centralized (e.g., a single database for the consortium) or distributed (e.g., each actor may have its own database). The only requirement on such databases is to keep track of the Common Tracking Model for each.

Third, to obtain cost efficiency and throughput, we group a set of multiple events into a single blockchain transaction; each group has the following characteristics:

- Each ECTM in a group gets hashed in an Event Hash (EH);
- Event Hashes are combined and hashed together via a Merkle-tree algorithm, producing a Group Hash (GH); this Merkle-tree-based approach is quickly becoming a major solution to provide a reproducible, hash based event grouping mechaninsm for blockchain efficiency, and is currently being adopted by a number of online blockchain based services, such as Eternity Wall [14] – the blockchain-based public message wall that promises messages lasting forever on the blockchain itself;
- The Group Hash gets stored on the blockchain.

This approach guarantees the following features:

- Flexibility: actors can save any business-related information into the Business Databases, provided the Common Tracking Model information are stored;
- Non-repudiability: any party that owns or knows a Common Tracking Model for an event, can easily verify against the blockchain its correctness; having Common Tracking Models hashed on the blockchain guarantees this model is tamper-proof and unmodifiable.

B. Architecture description

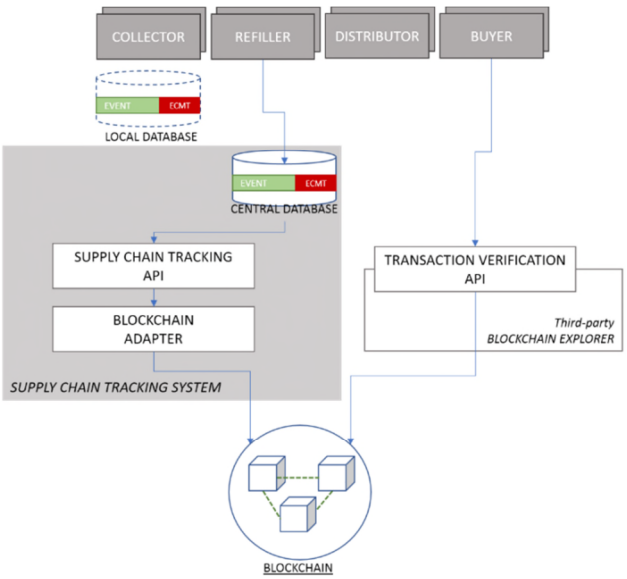


Figure 3. Architecture

Our Supply Chain Tracking System (see Figure 3) is based on the components described below.

Business database(s): in our first implementation, the PACTO Consortium holds a central database where business information related to recycling events are stored for any involved party; these is no need for this kind of

database to be central, and any single operator of any kind can adopt its own local database.

Transaction storage: this component holds the aggregation and hashing logic described in section IV.A

Blockchain adapter: this component acts as an abstraction layer that hides blockchain-specific transaction registration details, so as to let the architecture be portable between different blockchain implementations;

Blockchain Explorer: third-party service that allows to view information about blocks, addresses, and transactions on the Bitcoin blockchain. Our implementation relies on the open source Web portal BlockExplorer [15].

V. CONCLUSION AND FUTURE WORK

This work presents a novel Supply Chain Tracking System that relies on Bitcoin's blockchain to realize a notarization system supply chain goods status change and transitions.

This solution allows to overcome traditional fraud and counterfeit problems in a specific business sector, namely toner cartridge regeneration.

Future work will focus on investigating some new models and mechanisms (such as Lightning Network [19]) to keep Bitcoin's blockchain purest model, and simplify and speed up registration of transactions on the blockchain itself.

ACKNOWLEDGEMENT

This research was supported by Eco-Recuperi staff, whose insight and expertise greatly assisted the research, design and implementation of this work.

REFERENCES

[1] World Economic Forum, *The Future of Financial Infrastructure*, [Online] Available from: http://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services [retrieved: 2018.06.01]

[2] T. Aste, P. Tasca and T. Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry," in Computer, vol. 50, no. 9, pp. 18-28, 2017. doi: 10.1109/MC.2017.3571064

[3] M. Swan, "Blockchain: Blueprint for a New Economy", O'Reilly, 2015.

[4] Eco-Recuperi, *Eco-Recuperi website* [Online]. Available from: http://www.ecorecuperi.it/ [retrieved: 2018.06.01]

[5] A. Anjum, M. Sporny, and A. Sill, "Blockchain Standards for Compliance and Trust" in IEEE Cloud Computing, vol. 4, no. 4, pp. 84-90, July/August 2017. doi: 10.1109/MCC.2017.3791019

[6] S. Nakamoto, Bitcoin: *A Peer-to-Peer Electronic Cash System*, [Online] Available from: https://bitcoin.org/bitcoin.pdf [retrieved: 2018.06.01]

[7] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", Princeton Univ. Press, 2016.

[8] L. Lamport, R. Shostak, and M. Pease. 1982. "The Byzantine Generals Problem".ACM Transactions on Programming Languages. Syst. 4, 3 (July 1982), 382-401.

[9] A. Back, Hashcash – *A Denial of Service Counter-Measure*, [Online] Available from: http://www.hashcash.org/papers/hashcash.pdf [retrieved: 2018.06.01

[10] A. Lewis, *A Gentle Introduction to Blockchain Technology*, [Online] Available from: http://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Bitcoin-WEB.pdf. [retrieved: 2018.06.01]

[11] *Protect your privacy*. [Online]. Available from: https://bitcoin.org/en/protect-your-privacy [retrieved: 2018.06.01]

[12] Kodak. *Kodak Cryptocurrency and Blockchain Ledger Will Help Photographers Protect Their Copyright* [Online]. Available from: https://futurism.com/kodak-cryptocurrency-blockchain-ledger-help-photographers-protect-copyright/ [retrieved: 2018.06.01]

[13] *Distributed Ledger Technology in Clinical Trials* [Online]. Available from: https://tokeneconomy.co/distributed-ledger-technology-in-clinical-trials-fc2284bbe533 [retrieved: 2018.06.01]

[14] Eternity Wall, *How to independently verify notarization?* [Online] Available from: https://blog.eternitywall.com/2016/05/16/how-to-independently-verify-notarization/ [retrieved: 2018.06.01]

[15] Block Explorer [Online] Available from: https://blockexplorer.com/[retrieved: 2018.06.01]

[16] European Commission, *Green Public Procurement* [Online] Available from: http://ec.europa.eu/environment/gpp/index_en.htm [retrieved: 2018.06.01]

[17] Ministero dell'Ambiente e della Tutela del Territorio e del Mare, *Criteri Minimi Ambientali* [Online] Available from: http://www.minambiente.it/pagina/i-criteri-ambientali-minimi [retrieved: 2018.06.01]

[18] Associazione PACTO [Online] Available from: http://www.associazione-pacto.it/ [retrieved: 2018.06.01]

[19] Lightning Network [Online] Available from: https://lightning.network [retrieved: 2018.06.01]

 ISBN: 978-1-61208-644-6

Warm Wallets: A Safer Design to Achieve Business Automation for Blockchain-Based Services

A Novel Wallet Implementation Strategy for Enhancing Blockchain-based Online Services Security

Filippo Bosi, Michele Cappelletti, Guido Ravagli, Lorenzo Manzoni, Stefano Monti, Emanuele Pagliara
Imola Informatica
Imola (BO), Italy
e-mail: {fbosi, mcappelletti, gravagli, lmanzoni, smonti, epagliara}@imolainformatica.it

***Abstract*—Blockchain wallets are the user-facing, public/private key storage and signing/verification part of blockchains. Different architecture styles and hardware/software components are available on the market, with different trust and accessibility levels. This paper presents a novel wallet approach that fuses the accessibility benefits of online wallets with the security of air-gapped, cold-storage based wallets.**

Keywords-Blockchain; wallet.

I. INTRODUCTION

Blockchains are rapidly gaining momentum as a revolutionary architecture style that opens up novel, fully decentralized, trusted interaction schemes and unprecedented, unexplored business opportunities.

Blockchains rely on asymmetric cryptography schemes to sign transactions, and to guarantee immutability (i.e., once written to the blockchain, transactions cannot be altered) and non-repudiability (i.e., transactions cannot be entitled to users other than the one that originally signed the transaction).

Blockchain wallets are software/hardware components that act on the user side and offer: 1) blockchain connection facilities, 2) storage of users private/public key pairs, and 3) signing and verification features via the above private/public keys.

Different wallet styles and offering are available on the market, with different degrees of trust, accessibility, and convenience [1]; however, the most diffused solutions usually require relevant tradeoffs for users: online wallet services are the most convenient and accessible type (with supposed always-online availability), but require users to trust third party providers to hold their private keys (hence virtually being able to act on behalf of users themselves). Offline, air-gapped software/hardware components are supposedly the most secure solutions [3], but pose accessibility and convenience limitations.

This paper highlights the main wallet architecture styles, and proposes a novel, hybrid approach – called warm wallet – that aims at maximizing trust, convenience, and accessibility.

The rest of the paper is organized as follows. Section II describes blockchains and wallet alternatives. Section II surveys the main requirements and principles in designing blockchain wallets. Section IV describes warm wallet architecture and relevant implementation insights. Section V concludes our work with some hints at future work and research directions.

II. BACKGROUND

A. Blockchain and wallets

A wallet in a digital money world has the same issues of a wallet in real life. First, it must be secured, as if anybody has access to it, all the money contained in the wallet is at his/her complete disposal. Conceptually speaking, blockchains and wallets are secured with a single private key. If someone knows the private key, they have fullcontrol on the amount of money it holds. It is the owner's responsibility to put in place good security practices in order to secure the money.

A digital coin wallet is like a wallet with cash: people would not keep a large amount of cash in their pocket if they do not need it. In general, it is good practice to keep on the server only the amount of digital money needed for everyday use, that is, the amount of money usually needed for running the service for a reasonably long amount of time. The rest of the funds should be kept in a safer place, moving them to the online service only when necessary to refill the wallet in order to run the service without interruption.

B. Wallet alternatives

Hot wallets [3] are the simplest form of wallet since the private key is kept directly within the software wallet itself. While conceptually simple to manage, hot wallets provide a low level of trust, since compromising them means having the same direct, complete access to information (wallet status and balance) and features (e.g., signing transactions) as the owner himself/herself.

Hardware wallets [3] rely on dedicated devices that a) store owner private key in a (supposedly) tamper-proof, confidential way, and 2) sign transactions that are candidate to be placed on a blockchain, hence making them non-repudiable by the owner himself/herself. Hardware wallets usually have no mechanisms to directly interact with

 ISBN: 978-1-61208-644-6

blockchains and limit themselves to return the signed transaction; other pieces of software are then in charge of actually interacting with the blockchain. Cold storage and removable media can be used as a stripped-down hardware wallet whose sole responsibility is to safely keep a copy of the private key, and that delegates signature features to other pieces of software.

Multi-signature [3] wallets are designed to sign a transaction with multiple private keys at the same time, thus raising the challenge for transaction forgery. Each private key can be managed with different privacy and visibility strategies, and with different hardware/software components.

Cold storage [2] wallets hold the private key on air-gapped storage, i.e., an offline device/software component that is meant to always remain physically disconnected from the Internet. Cold storage wallets are able to sign transactions with the private key, but need to rely on stripped-down, secondary wallets to interact with the blockchain to initiate and receive transactions. Passing a signed transaction from the offline cold wallet to its online counterpart requires some kind of physical interaction to cross the "air gap" between the two.

Custodial wallets and Web wallets [3] are usually online, third party services that are supposed to 1) maintain private keys on behalf of their owners, and 2) allow users to operate on the blockchain (e.g., signing transactions) by interacting with functionalities exposed by such services, e.g., Application Programming Interfaces (APIs) or Web interfaces.

Paper wallets are physically printed versions of private keys (and any other user-related information): paper wallets obviously have no signing feature, and can be physically stored safely offline.

III. PRINCIPLES AND REQUIREMENTS

Choosing the right wallet architecture style for a blockchain-based application largely depends on business requirements rather than strictly technical considerations. The main driver usually is accessibility and business continuity. Cold storage wallets represent the most tamper-proof kind of wallet, since physical access to the medium is required to conduct any kind of attack. However, physical network disconnection becomes cold wallets most relevant drawback when business automation and continuity are at stake. The other key driver in wallet choice is trust and reliability: third party providers offer users the key features to store public/private key pairs, and sign/verify transactions; this approach, however, let malicious sysadmins (or any other malicious user that could gain privileged access) surreptitiously register transactions on behalf or real users. Main Bitcoin blockchain frauds, such as Mt. Gox hacker attack that led to roughly 630,000 bitcoins stolen, and ultimately determined Mt. Gox bankruptcy [6], relied exactly on stolen public/private key pairs from the provider hot wallets.

The cornerstones of cold wallet superior [2] security mainly relate to:

- Separation between private and public key;
- Separation between signing and verification functions.

Cold wallets implement such separation via a physical segregation (air-gap) of hardware/software components, and relegate signing functions (together with the necessary private key) to offline components.

Relaxing the physical segregation principle challenges wallet security, since, depending on the degree of connection and intercommunications, opportunities arise to access the private key (and associated signing features) via the online-facing public key holder logic component.

In our vision, however, such relaxation can

- Lead to strong benefits in terms of accessibility and business continuity;
- Be mitigated via usual security countermeasures and isolation principles (such as firewalling network connections, and running least-privileged processes).

The next section presents a warm wallet architecture and a proof-of-concept implementation that demonstrate the viability of a cold storage wallet that abandons physical air-gapping, in favor of logical separation and technical isolation.

IV. DESIGN AND IMPLEMENTATION

A. Warm wallet architecture

Conceptually warm wallet architecture relies on two logical components:

- Signing Wallet: offline (i.e., disconnected from the blockchain) component that holds user private key and transaction signing feature;
- Watching Wallet: online component that retains user public key and operates against the actual blockchain of choice.

This design strategy is independent from the actual blockchain implementation used to implement the online service. The following subsection deepens the description of implementation details of a first proof-of-concept warm wallet for Bitcoin blockchain.

B. Warm wallet implementation

The first consideration to take into account when building a blockchain wallet relates to how this component interacts with the blockchain itself. In the case of a Bitcoin blockchain wallet, the most straightforward way is to leverage a full Bitcoin Core node – a fully functional Bitcoin node – and leveraging its native signing, verification, and transaction registration facilities. Bitcoin Core nodes, however, are resource-expensive, both in terms of dedicated hardware requirements, and of runtime memory and CPU consumption.

This ruled out this design choice from the beginning, and we had to design an alternative solution. Simplified Payment Verification (SPV) [4] is a means to implement a

 ISBN: 978-1-61208-644-6

lighter-weight Bitcoin blockchain node that downloads only minimal transaction information, and retrieves full transaction details from blockchain nodes when in need.

Specifically, SPV clients only download the headers of blocks, and then request transactions from full nodes as needed; this approach allows computation cost to scale linearly with the height of the block chain, hence resulting in a more viable option, cost-wise.

We implemented the wallet in Java language, via the BitcoinJ library [5].

V. CONCLUSION

This paper presented an architecture solution to mix online, hot wallet accessibility and convenience, with the trust and security of air-gapped cold wallets. We are adopting this approach in some real-world, business cases of blockchain adoption outside of the traditional finance/cryptocurrency area, and specifically related to the tracking of supply chain goods. This approach is proving itself beneficial in terms of business continuity, convenience, and accessibility. Future work will focus on defining tools and best practices to guarantee logical network disconnection (e.g., enforcing specific software firewall rules) from the online and offline wallets parts, so that adopters of warm wallets are not forced to implement their own solutions.

REFERENCES

[1] S. Eskandari, D. Barrera, E. Stobert, and J. Clark, “A First Look at the Usability of Bitcoin Key Management,” Proceedings of the NDSS, Workshop on Usable Security (USEC), 2015

[2] M. Draupnir, “Bitcoin cold storage guide,” Available: https://www.weusecoins.com/bitcoin-cold-storage-guide/, 2016

[3] M. Conti, S. Kumar E, C. Lal,S. Ruj. A Survey on Security and Privacy Issues of Bitcoin
https://arxiv.org/pdf/1706.00916.pdf

[4] Simplified Payment Verification [Online] Available from: https://bitcoin.org/en/developer-guide#simplified-payment-verification-spv. Accessed on 2018-05-29

[5] BitcoinJ [Online]. Available from: https://bitcoinj.github.io/ Accessed on 2018-05-29

[6] The Inside Story of Mt. Gox, Bitcoin's $460 Million. [Online] Available from: https://www.wired.com/2014/03/bitcoin-exchange/ Accessed on 2018-05-29

 ISBN: 978-1-61208-644-6