Enhancing the Security of Software Defined Mobile Networks (SDMN) Based on Blockchain Technology

https://doi.org/10.3991/ijim.v17i04.37807

G. K. Sandhia[1](✉), S. Nithyaselvakumari[2], V. Saidulu[3], Nor Hissam B. Sulaiman[4], Anas A. Salameh[5]

[1] SRMIST, Chennai, India

[2] Department of Medical Instrumentation, Saveetha school of Engineering, Thandalam, India

[3] Department of Electronics and Communications Engineering, Mahatma Gandhi Institute of Technology, Hyderabad, India

[4] School of Creative Industry Management and Performing Arts (SCIMPA), Universiti Utara Malaysia, Kedah Darul Aman, Malaysia

[5] Department of Management Information Systems, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

ksandhia@gmail.com

Abstract—The blockchain involves future developments and new technologies. The emergence of a blockchain is a challenge for the conventional social organization and mode of activity. Data latency and mobile network capacity would no longer be a limitation for mobile users in next-generation networks of Software Defined Mobile Networks (SDMN). But there are many benefits to Software Defined Mobile Networking, it also contributes to certain security problems like DDoS / DoS attacks, unauthorized access, and single data point error. To enhance the security and privacy of the SDMN control plane, this paper proposes a new SDMN-based "Simplified Byzantine Fault Tolerance (SBFT)" algorithm to send signals between controllers and also set up an analysis study to investigate SBFT's security and results. However, there are many benefits of Software Defined Mobile Networking (SDMN), and then it helps to resolve other security concerns including DDoS / DoS attacks, unauthorized access, and single point failure. Blockchain, an evolving revolutionary technology, will offer creative approaches to address security issues in Software-Defined Mobile networks in an efficient way. This study proposes an SDMN-based Simplified Byzantine Fault Tolerance (SBFT) for enhancing the mobile network's security and privacy.

Keywords—blockchain, SDMN-based Simplified Byzantine Fault Tolerance (SBFT), software defined mobile networks, security, privacy

1 Introduction

The next generation of technology is a hybrid of emerging technologies and structures which are required to arrive in future Mobile networks in terms of meeting optimum efficiency and output criteria [1]. The architecture of SDMN networks is

required to turn across virtualization, including the programmability of different networking services [2]. It is described how today's new technologies, like "Blockchain, Software Defined Mobile Networking (SDMN), Network Functions Virtualization (NFV), the Internet of Things (IoT), Mobile Edge Computing (MEC), and Fog Computing (FC)," would simplify the move to recent technology. Additionally, SDMN supports emerging technologies that might improve rigidity in network design [3].

The development of technology is considered as just a case to theoretically enjoy the benefits of properly functioning systems from the blockchain. The integration of SDMN and blockchain technologies would have tremendous potential to deactivate an intrinsic value explosion. Furthermore, the strength of network access by its lowered latency, high speeds, and capability would allow IoT devices to be commonly used [4]. The "Communications Service Providers (CSPs)" include the understanding of heterogeneous types of access nodes as well as various access strategies for the exciting multi-network environment access [5]. And the selection of the quickest access node to every other node (device) will become a main issue in the future. Therefore, the blockchain technology illustrated in Figure 1 supports a future generation of frameworks for network infrastructure collection which is important for SDMN networks.

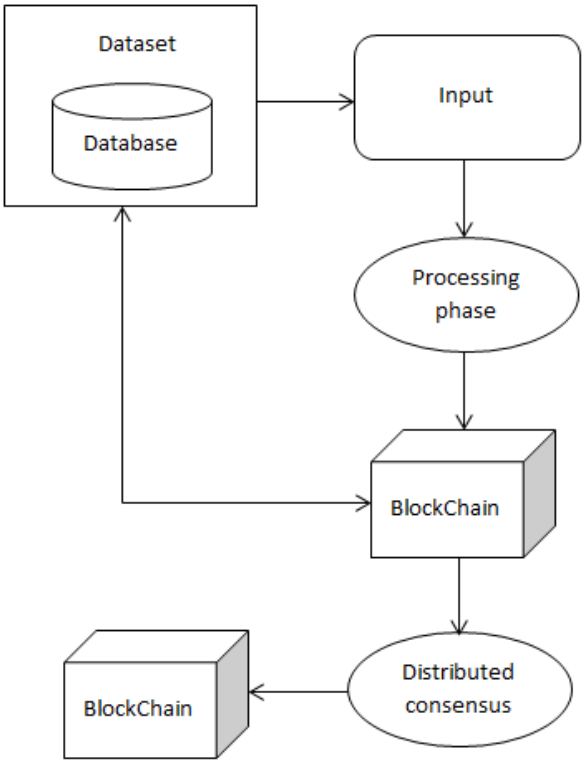

Fig. 1. Block Diagram of Blockchain Technology

Using the blockchain technique for SDMN will save huge amounts of money in operating expenses for businesses. Moreover, this would also effectively prevent future legal costs from rising out of conflicts. Find a smart contract prototype in a traditional supply chain system which might streamline the supply chain system and also allow products to be charged automatically after delivery. This will remove the need to respond with receivables accounts and pay department staff for billing to track distributors with unpaid invoices [2]. The need for Blockchain technology also improves monitors a shipment because both the supplier and the dealer will automatically know roughly where they fall regarding a volume benefit return. The knowledge is placed into the blockchain immediately. This allows both the supplier and dealer to do in real-time how often these units of a given product are being distributed in a region to determine whether or not the previous criteria were achieved for receiving a volume bonus return. Thus, if the data submitted to the blockchain indicates that the distributor satisfies any of the preceding requirements, the refund will be given to the distributor directly, without the distributor being required to check up with the payment supplier.

The users of the blockchain may either create the block data randomly or predefined. The "distributed consensus" protocol guarantees a lot of peers in the blockchain network accept the exact state of the distributed ledger. “Some of the distributed consensus algorithms that run inside the network without a central manager, in which the blockchain nodes validate a transaction in a variety of consensus ways, such as PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Stake Proof), PBFT (Practical Byzantine Fault Tolerance) and Raft [8],[9]. The essential use of the blockchain is used in the Bitcoin and crypto-currency, where the PoW is used as a consensus protocol and the computational capacity as a method for determining the selected peer [7]”.

SDMN is a novel approach that distinguishes control planes from data planes so that Mobile networks can be virtualized. “Compared with traditional Mobile networks, SDMN has many advantages including controller and information layer separation, modifiability, dynamic flow control, and centralized control”. Blockchain refers to the technology of collectively controlled, decentralized, and non-trust, to provide a stable ledger. It is simply a set of frames of data generated by the cryptographic correlation. For every data, a block provides data to validate large transactions as true. This process of storage makes it hard to alter information while it is being registered. “Attributes of the blockchain, including de-confidence, openness, and un-destructive information, comply with the requirements of the decentralized SDMN architecture.” Also, Smart Blockchain transactions could be designed stronger within SDMN programmability.

2 Literature survey

Related to the new SDSN protection situation, the benefits and disadvantages of the SDSN are evaluated from a security perspective, and potential attack activities are demonstrated from 3 levels, like DDoS and unauthorized anomalous attacks on the controller plane [10]. Those specific keys will be included in such a paper's analysis of the nature of a protection system.

Dargahi, T., et al.,[11] authors define and evaluate the security issues generated by the configurable broadband connection and identify possible vulnerabilities in the modern information plane. Protection framework systems were presented depending on SDSN [12, 13] but no details were given about the concentrated safety system. Few authors find the approaches used to manage different DoS threats in SDSN that were effective for SDSN protection yet the loss of integrity[14,15]. Work on broadband connection protection for the center of SDSN technology is also quite other-sided, and some were reduced to a single control scenario or a particular form of threat.

Xia, Q., et al., [16] creates a blockchain-based electronic medical recording framework that introduces blockchains to optimization techniques and base nodes with regards to the usage of blockchains in protection. The system tracks all requester's information request activities via smart contracts to avoid theft of patient's medical data, making medical records traceable and verifiable. Herbaut, N., et al., [17] create a client-centric online delivery network with blockchain to introduce a distributed network framework that allows service providers (SPs) and technical enablers (TEs) to interact and compromise against one another to initialize the best product delivery session, however, it doesn't suggest a specific negotiation framework.

Rottondi et al., [18] create a distributed generation utility existing infrastructure which includes the blockchain as a bridge for data storage to maintain software authentication and accuracy. Using simple cryptographic objects enables the device safer and user-friendlier. For achieving multi-party protection protocols, it would enter user data privacy and avoid leakage and data misuse. Zhang, J., et al., [19] suggests a two-step protocol that efficiently communicates medical information in a pervasive social network (PSN) with the next node in the network; the author permits a security module as an authentication service for access control and node verification and claims which blockchain technology will also improve such system's security. Anjum et al., [20] suggest which blockchains have to adjust to various structures based on their features. It is stated that the potential path is to resolve constraints on the blockchain since many blockchains could only perform 7 transactions per second.

Toyoda et al.[21] developed a blockchain-based product control issue management architecture for anti-counterfeit goods connected to RFID to evaluate it in the common threat. They have established comprehensive safety procedures that will allow every person, namely business process stakeholders and marketers to pass through and prove "ownership of RFID tag-attached products" based on the "Electronic Product Code (EPC)."When the EPC is distributed across the whole process as a static portion, an attacker may follow the transfer of the RFID name-attached models depending on the transmitted EPC quality.

Mujahid et al.[22] suggested a simple ultra-light, recognized as the “pseudo-Kasami code.” The confidentiality of RFID models is obtained while using the unpredictable property of hidden links in their basics.

Thus, this study proposes a blockchain-based SDMN protection mechanism with a distributed SDMN framework. They are using network resources to build a blockchain platform for SDMN. The block records the activities of the significant-time system and the timestamps, thus making the organizations 'activities recognizable. A standardized consensus technique named SBFT is suggested to verify the communications

exchanged between blocks including contact time limit, the recovery process, and credibility evaluation. Additionally, they set up an evaluation process to test the safety and efficiency of common understanding protocols and to simulate the algorithms suggested for consensus.

3 Proposed work

This study broadly suggests the blockchain-based security mechanism, called SDMN- based Simplified Byzantine Fault Tolerance (SBFT), and operated in a decentralized way. The proposed approach uses a specification of Software Defined Mobile Networks (SDMN) to improve the security and privacy of networks.

3.1 Software-Defined Mobile Networking (SDMN) model

Software-Defined Networking (SDMN) has been obtaining huge significance over the past few years and has been seen as the main pillar of the future. SDMN is a modern technique, that separates control planes from data planes to enable the virtualization of Mobile networks. The network can be run using software rather than hardware, through software-specified Mobile networks. This also finds a split between control and data planes, adding speed and versatility to Mobile networks. To ensure the protection of the SDMN framework design, this also considers the understanding of basic features: consistency of the program, functionality, privacy of the data, and anti-repudiation. A schematic of the device is shown in Figure 2 [24]:

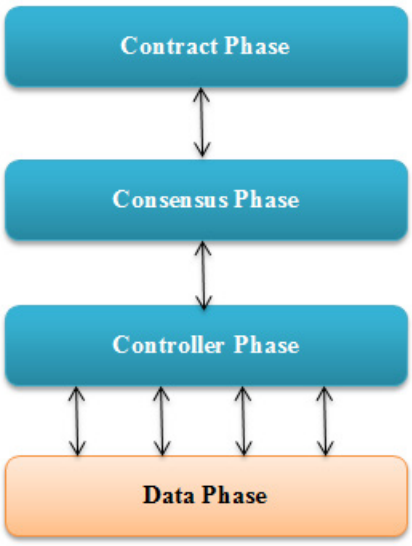

Fig. 2. Blockchain-based SDMN framework

The distributed horizontal controller model should be adopted to break the network into separate fields of study. Every field is individually monitored using a controller. Different controllers use a consensus algorithm to build the entire network view to avoid a single point of failure and increase device functionality. The Controller network is similar to the P2P network. Every controller is similar. From the world stability and transfer maintaining context, it is essential to continuously modify the network topology and link-state information including "switch port status, link utilization, and host CPU" consumption to establish a worldwide network overview. In blockchains, modified real-time data is registered, and global views may be generated in each controller.

The process may be split into 2 phases, the protection phase, and the transmission phase, for a controller. The protection technique of the SDMN control plane mostly covers 2 factors during the protection process. Prevents access by unauthorized controllers and prevents attackers from making false statements on shared databases. The principal method is to authenticate between SDMN controllers by transmitting data. The controller has certain verification information and holds other controllers' verification information. By transmitting the data encrypted, checking the information, and gaining consensus on counterfeiting. Uniform data distributed storage between controllers allows dealing with a single controller's information difficult. The controller senses suspicious traffic during the transmission phase and decides if an attack occurs. The mitigation of smart contracts will automatically respond to attacks by detecting the analytics center. In the scope, SDMN is designed to consider programmable networking services offered by Mobile networks, where traffic flows may be dynamically guided and managed to maintain optimum performance benefits.

3.2 SDMN security system model for DDoS/DoS Attacks

This study uses the SDMN security framework model of the Research Center and Attack Processing Center to independently achieve the design of DDoS / DoS assault defense contracts.

The control plane challenge is often affected by data plane DDoS / DoS attacks. Attackers transmit huge quantities of irrelevant packets to SDMN switches, such makes the switch often allows the controller to demand the flow list. There was perhaps some other way that the intruder deactivates or creates a link to allow suspicious people to drive to the other controller. Improper requests from the flow table and use of the controller resource must be known to trigger DDoS / DoS attacks.

"For DDoS / DoS attacks, smart contracts periodically test controller status with one-by-one traversal of the states, transactions, and trigger conditions found in each contract. The conditional transaction is then moved to the list for verification and awaits consensus. Transactions that do not meet the trigger condition will still be preserved on the blockchain." Once irregular traffic is detected, the Analysis Center activates and broadcasts the creation of a DDoS / DoS Warning Contract.1st phase is to check every controller's security and assure its validity. The confirmed controller must reach the agreed consensus. "After most verification nodes achieve a consensus, the most accurate primary controller is selected as per the consensus algorithm's confidence

process. The primary controller creates the DDoS / DoS mitigation deal and transmits it to other controllers to mitigate the DDoS / DoS attack by the alarm controller." The primary controller can never be re-elected in two consecutive positions for the sake of justice.

After the alarm has been silenced, the alarm controller must carry out a series of verification operations to minimize the safety risks at the control level. "At the same time, each controller transfers status information to the block to evaluate the alarming controller's current state, its mitigating effect, its effects on other controllers, and the origin of this assault." For systematic analysis, every event of the attack interval would also be documented in the block.

3.3 SDMN-Control plane scalability

This subsection will intend to evaluate the scalability of our decentralized control plane framework in addition to researching the outputs of our system. From the context of controlled SDMNs, it should concentrate primarily on assessing the scalability. Does $C_{j,k,\,i}$, represents the number of cloud intermediary nodes which exchange packets with the i^{th} IP address transfer from the D_j database to the D_k database, and f_j, f_k represents the number of Open Flow-enabled devices in the D_j and D_k database simultaneously. The number of SDMNs controlled by the BFT from the database D_j to the database D_k for the i^{th} transferred IP address is provided by the following formula:

$$R_i^{D_j D_k} = (f_i + f_k)\, C_{j,k,i} \tag{1}$$

The total number of SDS

Ns handled by the BFT for all IPs addressing migrations from the D_j database to the D_k database is the total of the rules described in (1) across i.

$$R_i^{D_j D_k} = \sum_i (f_i + f_k)\, C_{j,k,i} \tag{2}$$

The average number of BFT-managed SDMNs for other interface migrations of IPs originating from the D_j database is

$$R_i^{D_j D_k} = \sum_{\substack{k-1 \\ k \neq j}}^{N} \sum_i (f_i)\, C_{j,k,i} \tag{3}$$

The average value of BFT-controlled SDMNs for other IPs covering D_j database migrations is:

$$R^{D_*D_j} = \sum_{\substack{k-1 \\ k \neq j}}^{N} \sum_{i\prime} (\mathrm{f}_j) C_{j,k,i\prime} \tag{4}$$

For the D_j database, the average number of SDMNs controlled by BFT is:

$$R^{D_j} = R^{D_j D_x} + R^{D_x D_j} \tag{5}$$

$$R^{D_j} = \sum_{\substack{k=1 \\ k \neq j}}^{N} (\sum_{i} (\mathrm{f}_j) C_{j,k,i} + \sum_{i\prime} (\mathrm{f}_j) C_{j,k,i\prime}) \tag{6}$$

For all databases, the average number of SDMNs controlled by BFT is the total amount of the R^{Dj} for j

$$\mathrm{R^G} = \sum_{j=1}^{N} \sum_{\substack{k=1 \\ k \neq j}}^{N} (\sum_{i} (\mathrm{f}_j) C_{j,k,i} + \sum_{i\prime} (\mathrm{f}_j) C_{j,k,i\prime}) \tag{7}$$

It is observable from equations (1), (5), and (6) that the total of open Flow laws created for a D_j network is inversely related to the total amount of simultaneous inter-domain extinctions among D_j database and any other databases. The total amount of Open Flow systems for every other network to the one where open Flow rules become applied.The total amount of cloud-based corresponding Mobile networks that exchange data for each transferred message.

Because of this function, and to calculate the output of the routing protocol in their design, make use of their implemented BFT Rate parameter, which describes the amount of new open Flow standards controlled per second connected with IP address migrations stored in a D_j database. The BFT Rate function is a common attribute for every other network, it is strongly determined by the number of extinctions that the various Mobile networks receive.

For all Mobile networks, BFT Rate is measured and reported on the SDMN-based BFT collectively. If a BFT is implemented for a specific network it is often measured and documented as sustainable. The major goal of the BFT solution is really to establish the total device SDMN-based Rate quality both in the defined maximum period. Figure 3 shows the Standard working steps of SDMN-based SPBFT and PBFT This is performed via the complex evolution of the number of controllers over the operation/elimination of SDMN-based BFT on order by SDMN. If BFT Rate extends throughout the device will implement one or more BFT to maintain the SDMN is transferred. The expected result, it will delete all implemented BFT when SDMN Rate extends below the BFT to preserve device efficiency and the protection of services.

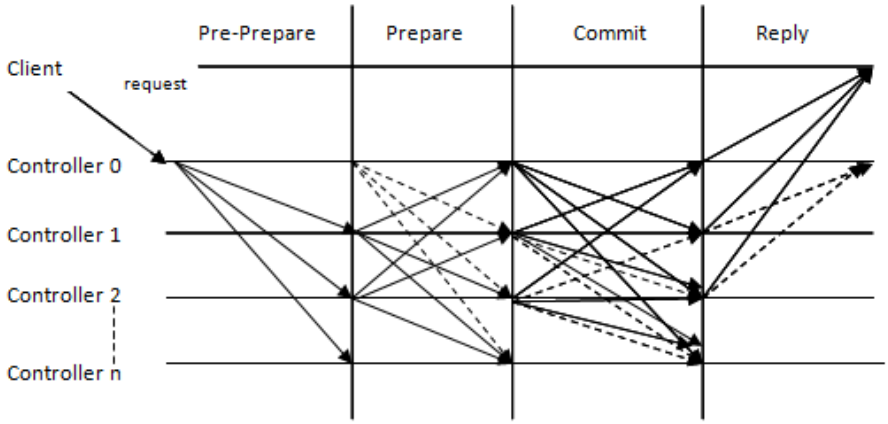

Fig. 3. Standard working steps of SDMN-based SPBFT and PBFT

3.4 SDMN-based Simplified Byzantine Fault Tolerance (SBFT)

This section discusses an analysis of the modern SBFT algorithm and explores its execution over a 5G network.The function is Γ= {I,S,U}. Here I = {a, p}is the user, a represents the attacker and p represents the protector, that is the controller.

S= $\{t_a, t_p\}$, identifies attacker and controller solution package. U= $\{u_a, u_p\}$, is attacker and controller utility function.

If there are 'n' controllers and the attacker targets 'r' controllers concurrently with the attack speed t_a, indicating the time to which the attacker bursts through the controller's firewall and interferes with the controller information itself. N (t_a), a hypothesis refers to the number of requests offered to send during the times t_a. The overall time is T. "During the process of the request processing the verification is introduced, so request activation interval equals verification interval. This paper suggests that the time interval of request initiation t_p, follows the exponential distribution with parameter, k. The amount of controllers retrieved at each time of the attack is Y."

In the next attack times t_a, the controller sends a request with the possibility of:

$$\mathrm{P}\,(\mathrm{N}\,(t_a)=1) = \mathrm{K}t_a e^{-kt_a} \tag{1}$$

More than one request with a chance of being sent in the next attack time t_a:

$$\mathrm{P}\,(\mathrm{N}\,(t_a)\geq 1) = 1\text{-}\mathrm{P}\,(\mathrm{N}\,(t_a)=0) = 1\text{-}e^{-kt_a} \tag{2}$$

For any period of attack t_a, the probability of a major attack is:

$$X = 1\text{-}P\ (N\ (t_a) \geq 1) = e^{-kt_a} \tag{3}$$

Hence, some controllers will be intruded on after this process. During the attack time, i can presume that M (i) could be intruded and M (i) will be transmitted:

$$M\ (i) = \sum_{j\in[1,i]}(P * r)\ -\ \sum_{j\in[1,i]}(Q) \tag{4}$$

The possibility of a major attack on that controller can also be achieved by:

$$PT = \frac{M\ (i)}{n} \tag{5}$$

In any intruder, it describes the "cost to include attack cost C_{a1}, which is the cost of intruding controllers, and the penalty cost $C_{a2,}$ which is the value of the detected attack. If the attack succeeds, then B_a would receive a positive intrusion. Will describes the cost $C_{d,}$ For any defender, which is the cost of the controller, lacking to avoid intrusion." If the controller is functioning properly, the regular cost $of\ B_{d1}$ is obtained. In the situation that the controller discovers the attack effectively, it'll get the B_{d2}, benefit. So the utility function of the attacker could be addressed as,

$$u_a = B_a\ *\ PT\ -\ C_{a1}\text{-}C_{a2}\ *\ (1\text{-}\ PT) \tag{6}$$

And the functional role of the defender is:

$$U_d = B_{d1}\ *\ (1\text{-}PT) + B_{d2}\ *\ \frac{Y}{r}\ -\ C_d\ \ *\ PT \tag{7}$$

A comparison of various consensus algorithms is shown in Table 1. The proposed SDMN-based SBFT has benefits in overdetection of error nodes as compared to BFT. This leads to this even though a maximum of one-third of nodes are attacked, only if the initial network has not been attacked will the network remain in good condition. It can have also seen that SPBFT possesses strong trading efficiency. "BFT could not satisfy the SDMN network's demand for a high volume of messages. SDMN-based BFT can also improve the verification and consensus process and decrease the number of signals."

Table 1. Comparison of Consensus Framework

Consensus Algorithm	Byzantine Fault Tolerance (BFT)	SDMN Based BFT
No. of nodes	3i+1	3i+1

Error node Tolerance	Anywhere from one-third nodes of malfunction, but mostly depends on the specific controller	With only around one-third of nodes in error
Consensus Performance	Common	Strong
Invulnerable	Common	Strong

In the invulnerability dimension, SBFT analyzes the verified data in the blockchain to identify the attacked controller and will have the system for dealing with the unknown controller, whereas BFT does not. In this case, this SDMN-based BFT will slow down the total device speed which is being affected. The framework will act rapidly if it is attacked and avoid it in time. Thus every block reports specific device actions and records timestamps, allowing the self-inspection and self-recovery of each organization in such attacks enforce. During the reduction of attacks, analyses of activity and the root analysis of the individuals that produce the activity are completed.

Also, distributed, "decentralized security systems in terms of design will prevent large-scale network anomalies caused by a single point of failure. However, other regular controllers help issue controllers get out of trouble. According to this design will use identification and traffic as the center of outer monitoring to maintain the controller's regular operation." SDMN's programmability provides an easy way to enhance the technology. In the security and information integrity dimension, every controller maintains its security code and uses blockchain technology to transmit the public key. Blocks hold encrypted fragments of controller information without access and control from any service provider, such that privacy security may be performed effectively. The blockchain includes a lot of distributed databases accessible, added, and anti-removable which maintains the record list of the block. Including time stamps and links to the preceding block, the blockchain contains a security guarantee that the information can never be changed if registered.

4 Experimental results

In this study, BFT is used as the algorithm's basis for comparison with the SDMN-based BFT proposed in this work to Matlab2018b. The request arrival intervals and the controller processing request intervals are all considered to be with exponential distributions. This study uses the run time of both algorithms in the program to evaluate the complexity of the algorithm. This section evaluates the standard controller consensus process with the BFT and SDMN-based BFT. Figure 4 illustrates the performance of the analysis. The n is the controller number, and the m is the average amount of consensus. The consensus time of the 2 methods, once the number of nodes will be less than ten, is not much different from the simulation findings. The SDMN-based BFT method's consensus time consumes around one-third of the BFT just as the amount of nodes is in reach often. Figure 5 indicates a contrast between the 2 techniques for operational cost signaling. The n is controller numbers, and the ordinate is the total operational costs signaling. Signaling operational costs improves with an overwhelming amount of controller networks. The SDMN-based BFT method's operational costs signaling is around fifty percent smaller than the BFT method.

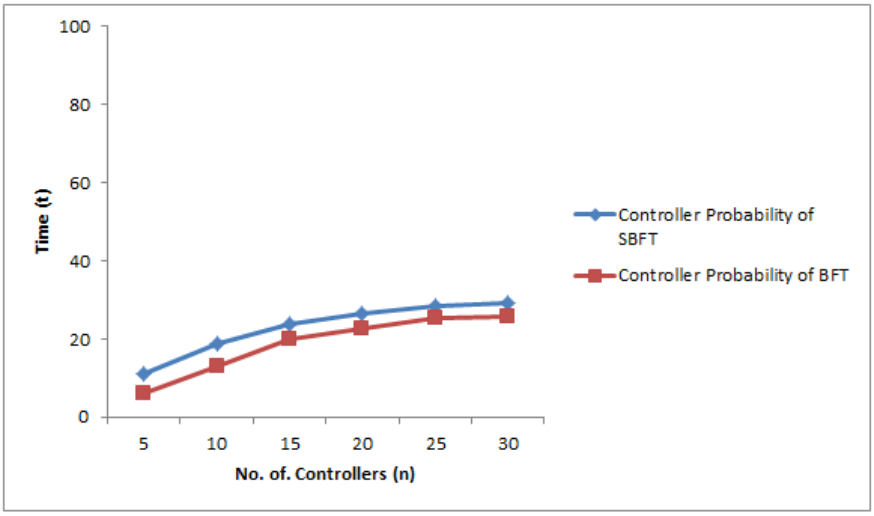

Fig. 4. Consensus Mean evaluation of the time

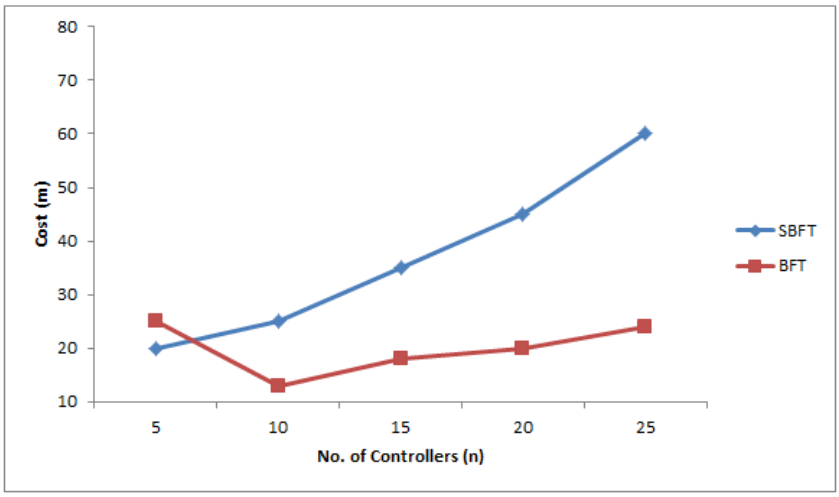

Fig. 5. Performance of Mean Value

A total of twenty runs are performed and combined to achieve the simulation results of complexity algorithms shown in Figure 6. The coordinate axis is controller numbers, and the complexity is the ordinate. Illustrated, algorithm complexity enhanced with controller numbers. The SDMN-based BFT algorithm's complexity is below that of the BFT algorithm. Additionally, the complexity of the SBFT algorithm grows more gradually than that of the BFT algorithm, as both, the number of nodes grows.

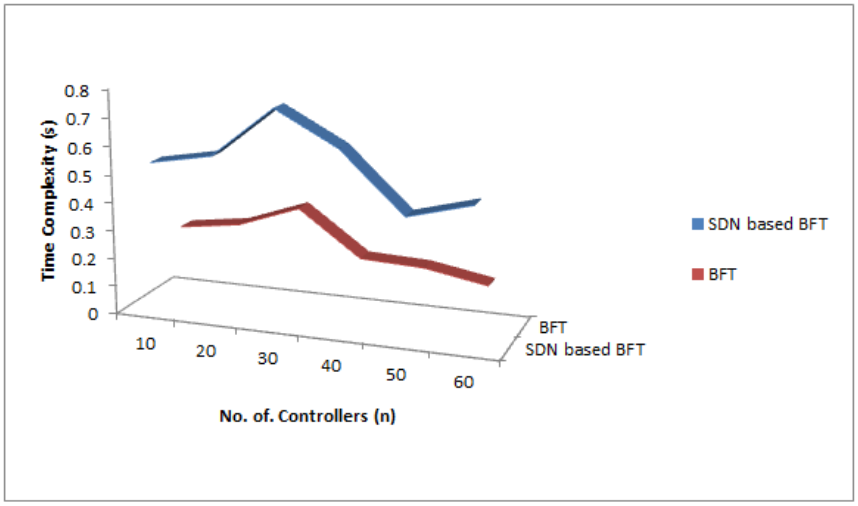

Fig. 6. Comparison of Time Complexity

Figure 7, compares the "invulnerability with and without the use of the SBFT algorithm based on the analysis model proposed in this study on the same attack power. The coordinate axis is the proportion of controllers that are targeted, and the ordinate is the number of regular cycles of operation. As the proportion of attackers targeting the controller improves, the controller reduces its normal operating cycle."

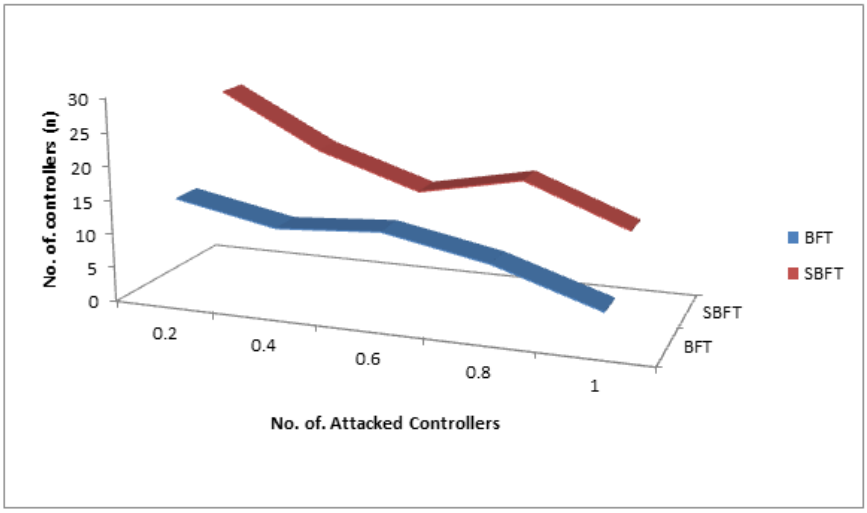

Fig. 7. Invulnerable Comparison

The recovery technique in this algorithm lets the control plane run with the same attack strength normally for a long time. "The SDMN-based BFT algorithm eliminates

the one-time broadcast consensus as opposed to the BFT algorithm, and the mean consensus time, bandwidth signaling, and time complexity are limited, which is more in line with the quick response SDMN criteria. Additionally, SBFT considers the primary controller as the basis of the execution of recovery steps." Therefore, the framework with an SDMN-based BFT algorithm will continue twice as long on the same attack intensity.

5 Conclusion and future work

This study proposes blockchain technology for enhancing the security and privacy of Software Defined Mobile Networks (SDMN) using the Simplified Byzantine Fault Tolerance (SBFT) algorithm. The most effective consensus algorithm to avoid unauthorized access and DDoS/DoS attacks are proposed to use SBFT and smart contracts to communicate information among controllers and to perform out requests. An SDMN-based framework would be used to analyze the system's security and effectiveness. "Simulation results indicate that the proposed SBFT algorithm in this paper may reduce or eliminate consensus time, overhead signaling, time complexity, and invulnerability, as opposed to the BFT algorithm".

6 Acknowledgment

This study is supported via funding from Prince Satam bin Abdulaziz University project number (PSAU/2023/R/1444)".

7 References

[1] Jangirala, S., Das, A. K., & Vasilakos, A. V. (2019). Designing a secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in a 5G mobile edge computing environment. IEEE Transactions on Industrial Informatics. https://doi.org/10.1109/TII.2019.2942389

[2] J. N. Dewey, R. Hill, and R. Plasencia, "Blockchain and 5GEnabled Internet of Things (IoT) will redefine Supply Chains and Trade Finance," https://www.hklaw.com/files/Uploads/Documents/Articles/Blockchain5GEnabledInternetofThings.pdf. Accessed on February 2019.

[3] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications, and issues," in Workshop on Mobile Big Data (Mobidata'15), Hangzhou, China, 2015, pp. 37–42. https://doi.org/10.1145/2757384.2757397

[4] B. Whittle, "The Implications of Fusing 5G and Blockchain," Accessed on April 2019. [Online]. Available: https://cointelegraph.com/news/ the-implications-of-fusing-5g-and-blockchain.

[5] "How Blockchain can impact the telecommunications industry and its relevance to the C-Suite," Blockchain Institute. https://www2.deloitte.com/content/dam/Deloitte/za/Docume–nts/technology-media-telecommunications/za_TMT_Blockchain_TelCo.Pdf. Accessed on January 2019.

[6] H. Min, "Blockchain technology for enhancing supply chain resilience," Business Horizons, vol. 62, no. 1, pp. 35–45, 2019. https://doi.org/10.1016/j.bushor.2018.08.012
[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85
[8] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry," IEEE Computer, vol. 50, no. 9, pp. 18–28, 2017. https://doi.org/10.1109/BigDataCongress.2017.85
[9] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in USENIX Annual Technical Conference (USENIX ATC'14), Philadelphia, PA, USA, 2014, pp. 305–319.
[10] Dabbagh, M., Hamdaoui, B., Guizani, M., Rayes, A.: Software-defined networking security: pros and cons. IEEE Commun. Mag. 53(6), 73–79 (2015). https://doi.org/10.1109/MCOM.2015.7120048
[11] Dargahi, T., Caponi, A., Ambrosin, M., Bianchi, G., Conti, M. A Survey on the security of stateful SDN data planes. IEEE Commun. Surv. Tutorials 19(3), 1701–1725 (2017). https://doi.org/10.1109/COMST.2017.2689819
[12] Liang, X.D., Qiu, X.F.: software defined security architecture for SDN-based 5G network. In: 2016 IEEE International Conference on Network Infrastructure and Digital Content (ICNIDC), pp. 17–21 (2016). https://doi.org/10.1109/ICNIDC.2016.7974528
[13] Liyanage, M., Ahmed, I., Ylianttila, M., et al.: Security for future software defined mobile networks. In: 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 256–264 (2015). https://doi.org/10.1109/NGMAST.2015.43
[14] Zhao, Z., Liu, F.L., Gong, D.F. An SDN based hopping multicast communication against DoS attack. KSII Trans. Internet Inf. Syst. 11(4), 2196–2218 (2017). https://doi.org/10.3837/tiis.2017.04.020
[15] Macedo, R., Castro, R.D., Santos, A., Ghamri-Doudane, Y., Nogueira, M.: Self-organized SDN controller cluster conformations against DDoS attacks effects. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2016). https://doi.org/10.1109/GLOCOM.2016.7842259
[16] Xia, Q., Sifah, E.B., Asamoah, K.O. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 5, 14757–14767 (2017). https://doi.org/10.1109/ACCESS.2017.2730843
[17] Herbaut, N., Negru, N. A model for collaborative blockchain-based video delivery relying on advanced network services chains. IEEE Commun. Mag. 55(9), 70–76 (2017). https://doi.org/10.1109/MCOM.2017.1700117
[18] Rottondi, C., Verticale, G.: A privacy-friendly gaming framework in smart electricity and water grids. IEEE Access 5, 14221–14233 (2017). https://doi.org/10.1109/ACCESS.2017.2727552
[19] Zhang, J., Xue, N., Huang, X.: A secure system for pervasive social network-based healthcare. IEEE Access 4(1), 9239–9250 (2016). https://doi.org/10.1109/ACCESS.2016.2645904
[20] Anjum, M., Sporny, A.: Sill: blockchain standards for compliance and trust. IEEE Cloud Comput. 4(4), 84–89 (2017). https://doi.org/10.1109/MCC.2017.3791019
[21] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply

chain," IEEE Access, vol. 5, pp. 17465–17477, 2017. https://doi.org/10.1109/ACCESS.2017.2720760

[22] Shao, Z., Zhu, X., Chikuvanyanga, A. M., & Zhu, H. (2019, January). Blockchain-Based SDN Security Guaranteeing Algorithm and Analysis Model. In International Conference on Wireless and Satellite Systems (pp. 348-362). Springer, Cham. https://doi.org/10.1007/978-3-030-19156-6_32

8 Authors

G. K. Sandhia M.E., Ph.D., is currently working as assistant professor in SRM Institute of Science and Technology. Her research areas are cryptography and network security, Block chain, Machine Learning (email: ksandhia@gmail.com).

Dr. S. Nithyaselvakumari presently working at Saveetha school of Engineering as Assistant professor SG in the Department of Medical Instrumentation and experienced around 11 years in teaching and 5 year in Industry. She has completed Bachelor of Engineering in Electronics and communication Engineering at Mahendra Engineering college Salem under madras university and done Master of Engineering in Sathyabama university in the department of Applied Electronics. In 2021, she has completed Ph.D under Anna University. Her area of research is in Bio Medical, wireless communication, Embedded system and Internet of Things (email: nithyaselvakumari.S@gmail.com).

Dr. V. Saidulu is a Senior Assistant Professor in the Department of Electronics and Communications Engineering in Mahatma Gandhi Institute of Technology, Hyderabad. He received B.Tech (ECE) and M.Tech (Microwave) Degree from Nagarjuna University, A.P and Indian Institute of Technology Banaras Hindu University, U.P in the year of 1998 and 2001 respectively. His Ph.D degree in Microstrip Antenns awarded from Jawaharlal Technological University, Hyderabad in 2016. He published 70 research papers in reputed journals and in National and International conferences. He awarded best papers in conference and Journals. He attended several FDP, STTP and Webinars which was organized by IIT's and NIT'S which is around 150. His a senior Fellow of IETE, IEI and ISTE and he obtained **Apprenticeship** by ECIL-Hyderabad. His research area in antennas, wireless communications, Cellular and mobile Communications (email: vsaidulu_ece@mgit.ac.in).

Nor Hissam B. Sulaiman is a Lecturer at School of Creative Industry Management and Performing Arts (SCIMPA), College of Arts and Sciences (CAS), Universiti Utara Malaysia since 2003, and currently the professional members of Malaysian Board of Technologist (MBOT), specialist in Telecommunication, Mass Media, and Broadcasting. He is also an Associate Member of the Film Directors Association of Malaysia (FDAM). His major research interest focusing on the area such as audience identification, media production, information communication technology (ICT), media law and ethic, and self-regulation of media content. (email: norhissam@uum.edu.my)

Anas A. Salameh is an Associate Professor at, Department of Management Information Systems, College of Business Administration, Prince Sattam Bin Abdulaziz University since 2016, and the current deputy director of the students'

activities committee as well as a member of the exams scheduling committee, PSAU. His major research interest focusing on the area such as e-commerce (m-commerce), e-business, e-marketing, technology acceptance/adoption, e-learning, e-CRM, service quality, and he evaluated service quality in many areas related to e-services aspects. (email: a.salameh@psau.edu.sa) Orcid: https://orcid.org//0000-0002-4694-3771

Article submitted 2022-11-19. Resubmitted 2023-01-03. Final acceptance 2023-01-05. Final version published as submitted by the authors.