Secured SDN Based Blockchain: An Architecture to Improve the Security of VANET

Original Scientific Paper

Swapna Choudhary
G H Raisoni College of Engineering,
Research Scholar, Department of Electronics Engineering, Nagpur, India
swapna.choudhari@raisoni.net

Sanjay Dorle
G H Raisoni College of Engineering,
Faculty of Electronics Engineering, Department of Electronic Engineering, Nagpur, India
sanjay.dorle@raisoni.net

Abstract *– Vehicular Ad-hoc networks (VANETs) during the communication process, nodes are always varying and the process is always under security threats like Sybil attacks, masquerading attacks, etc. In order to reduce the probability of these attacks and to regulate traffic flow in the network, a software-defined network (SDN) is used. The SDN is used for implementing protocols like OpenFlow and reducing the routing load in the network, but it doesn't provide a high level of security to the network, hence protocols like encryption, hashing, etc. are applied to the VANET. In the paper, SDN based blockchain-inspired algorithm is implemented, which coordinates network traffic and improves the overall security of the network. Security analysis of the proposed algorithm shows that the combination of blockchain with encrypted SDN is removing more than 95% of the network attacks as compared to its non-blockchain counterparts.*

Keywords*: Vehicular Ad-hoc Network, Software-Defined Networks, Encryption algorithm, network security, blockchain*

1. INTRODUCTION

Security has always been a major research issue with wireless networks. This is due to the fact that packets transmitted between wireless nodes are intercepted by adversaries, and a wide variety of malicious operations are performed on them. The malicious packets are then re-communicated via the network for affecting other nodes, thereby reducing the network's optimum per formance capability.

The design of Vehicular ad-hoc networks [1] requires that a vehicular node must do the following operations:

a. Register on the network once it comes in the range of either a network vehicle node or a network infrastructure node (hub)

b. Perform communication either directly in a peer-to-peer manner or using infrastructure hub as a hopping node

c. Periodically broadcast information regarding events that are sensed by the vehicle

d. Inform the neighboring nodes and the infrastructure once the node is leaving the ad-hoc network

e. Send heartbeat packets to the neighboring nodes and the infrastructure hub regarding the current parameters of the node (energy levels, location, etc.)

Based on these operations, each vehicular node communicates with other nodes in an effective manner. In some cases, attacker nodes without register in the network try to interact with healthy nodes. In such cases, the attacker sends the critical information outside the network or changes the information and tried to insert malicious packets in the network which decreases the efficiency of networks.

In order to protect the networks from various attacks, different control mechanisms like bandwidth & security are applied. Protocols like Open flow and SFLOW of SDN can control the traffic of the network and reduce attacks. SDN protocols are not effective for the attacks like Sybil and masquerading. To protect the networks from these attacks which change the identity of nodes' secure hashing, Public Key Infrastructure (PSK) like algorithm can be used. These algorithms can improve the probability of attacks but algorithms like blockchain peer-to-peer communication are more efficient [2]. In the next section analysis of different architecture and algorithms are given and compared with proposed

encrypted blockchain open flow SDN architecture (ABOSS).

2. RELATED WORK

Blockchains are applied for securing VANETs extensively. The self-organized secure (SOS) framework [3] is based on a peer-to-peer network. The main advantage of this network is to secure the network even if there is no roadside infrastructure exist in the network. Shamir sharing combined with a trust-based routing scheme to achieve this objective. Due to the combination of these techniques Vehicles Authority, Message Integrity, Privacy, Non-Repudiation, Traceability, Anonymity, and Availability are improved. Moreover, attacks like Impersonation, Modification, ID Disclosure, Location Tracking, Repudiation, and denial of service (DoS) are removed. Similar work with improved cryptographic primitive attribute-based encryption (CP-ABE) is defined in [4]. In this work, due to attribute-based encryption, the overall network speed is improved along with a reduction of the attack probability in the network. A verifiable hidden policy CP-ABE with a decryption testing scheme is also proposed in [4], it allows nodes to be tested and authenticated before performing network communication. This work is improved by adding true blockchain solutions, which is described in [5], wherein blockchain is used for privacy preservation along with reduction of the computational complexity of the system. This work is implemented for the Internet of Things (IoT), but it can be extended to VANETs by replacing IoT-specific blocks like IoT platform providers with RSU and cloud services with VANET infrastructure services. This work can be further extended with the help of Shor's algorithm as described in [6], wherein a lattice-based conditional privacy-preserving & authentication scheme is defined. The lattice-based scheme is able to combine data from RSUs, vehicles, application providers, and trusted-third parties as shown in Fig. 1.

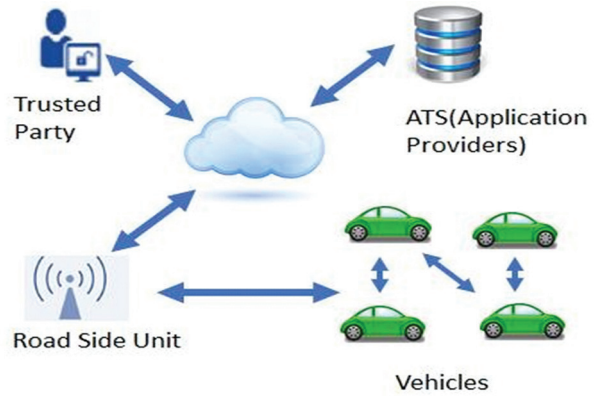

Fig.1. Lattice-based security mechanism

Due to lattice computations, the delay of the system is reduced, thereby improving the speed of communication along with providing security to the network. But, all these schemes mentioned in [3-6] suffer from inherent drawbacks, which are given as follows:

a. Limited area of applicability, because each of these protocols requires either the presence of a control unit or a high-powered computational unit.

b. Limited security performance due to the lack of decentralized control.

In order to eliminate these problems, the work in [7] presents efficient decentralized management mechanism with Blockchain. The solution employs managing the security of VANET by using a decentralized key-management mechanism. Bi-variate polynomial for a key agreement which is based on light-weight authentication is used. This technology can manage user identity and public key material which will improve the efficiency and cost as compared to traditional schemes of VANET. An example of the network is shown in Fig.2, wherein vehicles are connected to each other with the help of a decentralized blockchain model.

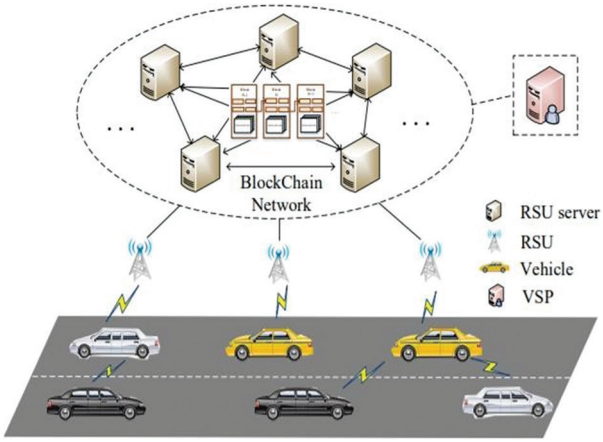

Fig. 2. Blockchain-based VANET

Due to the use of distributed blockchain-based authentication and communication, the overall communication cost is reduced by 50% of the cost of a standard public key infrastructure (PKI) system. This enables the network to be used for a larger set of users without increasing system cost. This work is modified in [8], in which trust-based routing and location privacy schemes are added to the VANET. Due to the addition of these schemes, the quality of service (QoS) performance of the network reduces, therefore there is a need to improve it with the help of machine learning models. The location privacy is maintained using k-copy scheme while the trust-based routing is maintained with the help of the same decentralized scheme as mentioned in [7].

The work in [8] can be further optimized in terms of QoS parameters with the help of an incentive scheme as mentioned in [9]. In this scheme, the node decisions regarding communication, channel selection, packet rate, etc. are monitored, and the parameters combination responsible for improving the QoS is incentivized using a scoring mechanism. Due to this, there is a balance between the security offered by the network and

the overall QoS of the network. The parameter combination which has the best score can communicate events in the network to the nearby nodes with the highest security and QoS. The event is mitigated with the help of the best possible route and parameter combination to each of the nearby nodes.

A combination of these schemes [7-9] is given in [10], wherein privacy-preservation is maintained using blockchain-powered trusted authorities. These authorities are responsible for node registration, node communication, and node termination from the network. All this data is stored in the form of the Merkle Patricia tree (MPT) for faster storage and retrieval performance. The system also supports conditional privacy by allowing each vehicle to have multiple certificates, and each certificate is responsible for a particular communication scenario in the network. A sample of this process is shown in Fig.3, the certificate for every special access for segregation is given to the vehicle in the network. This enables the vehicles to get better security performance, as the memory and computational requirement of these certificates is very low, therefore the QoS of the network is also maintained at an optimum level when compared to single-certificate computation systems.

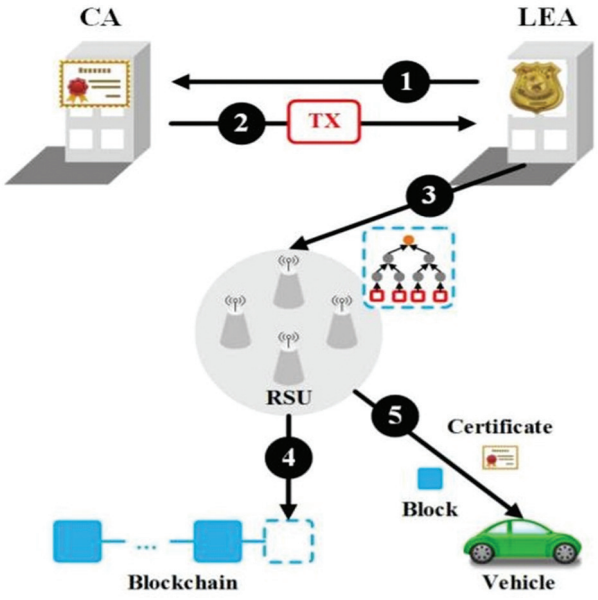

Fig. 3. Blockchain-based individual certificate scheme

In order to add features like bandwidth control, dynamic addressing, etc. VANETs are coupled with SDN. SDN is responsible for controlling the communication between nodes in the network. In order to eliminate these problems, the work in [7] presents efficient decentralized management mechanism with Blockchain. The solution employs managing the security of VANET by using a decentralized key-management mechanism. Bi-variate polynomial for a key agreement which is based on light-weight authentication is used. This technology can manage user identity and public key material which will improve the efficiency and cost as compared to traditional schemes of VANET. An example of the network is shown in Fig.2, wherein vehicles are connected to each other with the help of a decentralized blockchain model. An application of [10] and [11] can be observed in [12], in which blockchain and distributed ledger systems along with SDN are used for securing high-performance cyber-physical systems.

A similar trust-based model based on blockchain is also described in [13]. In this paper, a blockchain-based anonymous reputation system (BARS) is used to protect distribution of fake messages and privacy of the vehicles. The privacy preserving mechanism Lexicographical Merkle tree (LMT) is used to provide linkability between public key and identity of the vehicle through the certificate authority without disclosing private information of the vehicles. Law Enforcement Authority (LEA) is used to store the public key and identities of the vehicles. The reputation evaluation algorithm safeguards the vehicles from exposed behaviors thereby improving efficiency , robustness and security of the system.Work in [14] uses a blockchain-based Trust conditional privacy preservation announcement scheme (BTCPS]. It allows the vehicle to send messages to non-trusted environments. RSUs calculate reliability of the messages as per the reputation values of the vehicles. It can trace the malicious vehicle identity with associated public address . Proof of Work algorithm is used to improve the efficiency and QoS performance of the network.Due to conditional privacy, each node-to-node communication can be traced back to its source. It allows the system to trace the attacking node and eliminate it.

This scheme can be extended to include Group Mobility Management as given in [15]. In this work, handover latency and signalling costs during authentication can be reduced using aggregate message authentication code and one-time password authentication. Due to these techniques, the proposed scheme is not only fast but also supports faster handoffs whenever nodes are shifting between different internal mini-networks. This results in reducing the signalling overhead and handover latency of the system, which improves the QoS of the proposed system. In order to evaluate the system under different security threats, possible solutions are discussed in [16]. In this survey, it is observed that blockchain technology is the most useful when it comes to removing attacks from VANETs. It is used as the base security model for this underlying research. While security is a major aspect of any VANET, an effective data collection process must also be taken into consideration while designing networks. The work in [17] reviews a wide variety of data collection mechanisms for VANETs, and observe that topology-based methods have the best performance in terms of reducing delay and increasing the overall throughput performance. Using this mechanism, the QoS performance of VANETs can be improved. While using blockchain with topology-based methods, it is required that not more

than 51% of nodes must be clubbed together for communication. This results in a highly secure blockchain network, which is given in [18]. Due to topology issues if the blockchain network is attacked with more than 51% of users, then the network rules can be changed. These changes can allow an attacker to inject malicious rules into the network, and make backdoors in the system. It is also observed that when less than 51% of nodes are active then proper data dissemination can take place in the network. The overall performance and storage capabilities of the network depend on the memory and computational power needed per-node basis. The higher number of dissemination nodes will require a larger memory for storage, and will also require a higher computational power when compared to a network with a moderate number of participating dissemination nodes. This can be observed from [19], in which nodes within a radius of 1-hop distance are considered ideal candidates for data dissemination. This indicates that all kinds of topology constraints must always keep less than 51% nodes in close vicinity with each other.

Another attribute-based blockchain algorithm with privacy preservation and authentication is indicated in [20]. In this work, due to the decentralized nature of blockchain, there is no need to perform pre-authentication in the network. Moreover, the network provides high security without the presence of any roadside unit or infrastructure components. The network also demonstrates trust management considerations, which are improved with the help of SDN as observed in [21]. Trust based Deep Enforcement Learning Framework with SDN uses deep enforcement learning algorithm to find the highest routing path of the network. The trust model is used to evaluate behavior of neighboring nodes of the forwarding packets which helps to improve QoS parameters. These techniques can be extended to 5G networks as given in [22], wherein it is observed that network security is improved if SDN architectures are applied to high-speed 5G networks. While each network type has its own design requirements, the work in [23] indicates that SDN-based VANET networks require a lot of integrations before real-time deployments. For instance, to support Privacy violations the SDN-based VANET must implement 'Disclosing sensitive information module from SDN and 'Revealing the identity of vehicles module from VANET. In order to improve the security performance of stand-alone SDN systems, the work in [24] indicates the usage of broadcast encryption mechanisms. These mechanisms allow the system to secure new and existing SDN networks. The broadcast encryption mechanism is based on the Advanced Encryption Standard (AES) in 256-bit mode (AES-256). The security performance of this network is found to be far superior to other SDN networks, and thereby the same AES-256 implementation is used by the underlying research. Network safety can also be improved with the help of cooperative communication similar to P2P networks, this is given in [25]. To improve the network performance ,roadside Open Flow switch (ROFS) is used. SDN based Medium Access Control protocol is classified into two levels as follows:

a. Controller and management of vehicles is used to control Road Side Units .

b. Controller is used to schedule the cooperative time slot sharing between Road Side Units. Slots are allotted based on sharing information between control and data plane.

SDN based blockchain can improve vehicle density fluctuation which helps to improve agility and speed of the network which further improves the security. To improve network performance and better security, The Open Flow protocol is connected in tandem with ROFS, and a distributed communication architecture is implemented.

For improving security, the energy consumption of the network is considered in [26]. In this work, a small change in the learning function with the inclusion of energy consumption results in routing solutions that have greater energy efficiency than the ones which do not include energy consumption into the equation. The energy consumption can be further improved by offloading all the security and related computations on fog devices. This is observed in [27], wherein mobile edge nodes are utilized for performing complex encryption calculations, while the main communication and event-triggered processing are done on the main vehicular node. A device-to-device clustering (D2DC) method is described, which provides coverage to nodes that are not in the coverage radius of the main infrastructure node. This D2DC method does not only provides better coverage but also improves the overall energy efficiency of the network. The nodes which are not in coverage range do not require sending unnecessary communication packets in search of the infrastructure nodes. Due to this, more than 74% of the unserviceable nodes come under proper service of the network, which improves the QoS performance of the network. A similar approach that uses multi-agent architecture is given in [28]. A hybrid SDN based geographic routing protocol allows selection of reliable nodes to avoid communication problems between source and destination. By using load balancing criteria allows to form hierarchical topology of the network by creating group and selecting the group leader. Routing protocol provides the better network flexibility and resource management which helps to improve QoS parameters. The geographic routing protocol can be further modified as per the survey done in [29], in which it is suggested that VANET routing can be best adopted with key management-based trust & secure routing protocols for better routing efficiency.

The future of VANETs is the integration of the network with cloud-based approaches [30].Integration of Fog computing with SDN enhances the flexibility and programmability of the network. It will help minimize

future challenges in VANET. Blockchain- based SDN in combination with different protocols can improve inherent security of the network. The proposed Encrypted Blockchain based open Flow SDN architecture is explained and the performance evaluation of the given protocol and comparison with other standard algorithms is described in the next section.

3. PROPOSED ENCRYPTED BLOCKCHAIN OPEN FLOW SDN ARCHITECTURE (ABOSS)

The proposed encrypted blockchain open flow SDN architecture is described by dividing the entire VANET traffic flow into 3 different parts which are given as:

a. Securing node to node communication using AES- 256 & ad-hoc on-demand distance vector (AODV) routing protocol.

b. Improving security for the entire network using blockchain-based data transfer.

c. Adding QoS improvement layer with network control using Open Flow SDN.

A Block diagram of the entire system is shown in Fig.4, where node-to-node communications are shown.

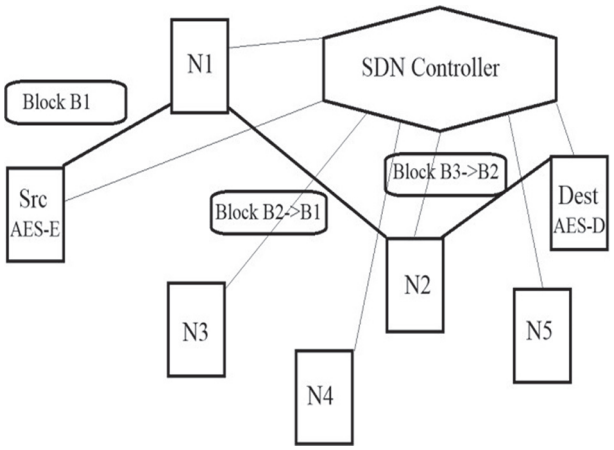

Fig. 4. Proposed encrypted blockchain open flow SDN architecture (ABOSS)

The input data originates from the source node, is encrypted with the AES protocol. The private key of AES is shared with the source and destination nodes. This key is moved into a secure block using public-key cryptography and is sent in the network. The block diagram of AES is shown in Fig.5. AES follows the given steps for encryption of data:

AES is a standard encryption algorithm that follows the given steps for encryption of data:

a. Add round key

b. Substitute bytes

c. Shift rows

d. Mix columns

e. Add round key

For decryption the same process used in reverse order using AES, the input data is altered to cipher text , and is kept ready for broadcast from the source node. Once the data is encrypted, to set the best routing paths between the source and destination packet is send to nearby nodes. These packets sent are known as Route Request (RREQ) packets as shown in Fig.6, where node 'A' is the source and node 'F' is the destination.

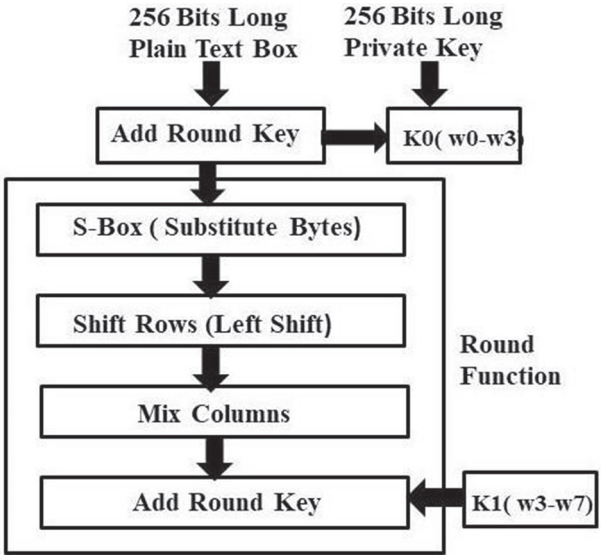

Fig. 5. AES block diagram

The nodes which are near, send Request reply (RREP) packets. Based on the reception of RREP packets, a path is selected between source 'A' and destination 'F' as A—B—D—F. This path is selected and kept stored on the SDN node. The source node then applies a blockchain based data transformation protocol. Using this protocol, the input data is converted into the following block structure which is given in Table 1.

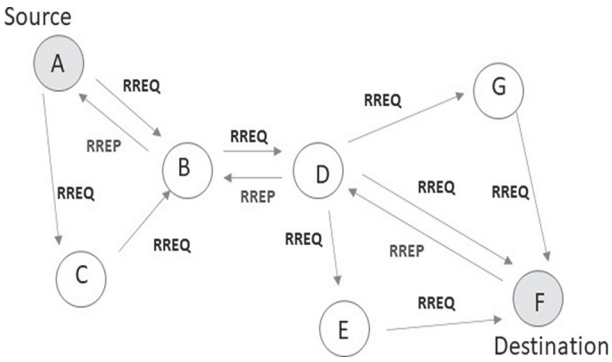

Fig. 6. Routing process

Table 1. Structure of the blocks in the blockchain

Previous Hash	Source	Destination	Current Node
Timestamp	Nonce	Data	Hash

The above structure gives the information of source node and destination nodes along with the timestamp of the transfer, current hash value and previous blocks

hash values and nonce value saved in the respective blocks. How the nonce value is responsible for creating the unique hash value. How to find the nonce number in blockchain the steps are shown below:

a. Initialize a random nonce value
b. Store the value in a block
c. Find the SHA256 hash of block
d. Check whether the hash value is repeated, if yes then discard and restart.
e. Check whether the hash value is following blockchain rules, if not then discard and restart.
f. If both rules (d, e) are followed, then store the nonce in the blockchain.

With above pseudo steps, the nonce number is evaluated and put in the blockchain. Which update the hash table's data and transferred it from source node to the next nearby nodes. As the data transmit to the next hopping nodes, whole blockchain is checked for authentication.

The blockchain, checking process is done using the following steps:

a. Check the current hash of the block
b. Check the previous hash of the next block
c. If these hashes match, then continue with the Checking,
d. If these hashes do not match, then discard the blockchain and re-start the communication
e. Once the blockchain is verified, then the communication proceeds to the next node.

Each blocks should follow the blockchain rules once the hash values of previous and current blocks is checked and verify. Proof –of –Work consensus algorithm is used to verify all these process. Once the verification done, packets send from any nodes using Open Flow SDN Protocol. This protocol has the following rules:

a. Remove the nodes which are not found in registered node list during communication process.
b. Set of 'N' packets allow to be transmitted within the nodes, where 'N' is link of maximum capacity to handle the packets.
c. k is the maximum hopes between the source and destination nodes decided. During the communication only k hoping is allowed in the network.

All these rules are applied to each of the communication packets. After application of SDN rules, the network will have the following advantages:

a. The network will be resilient to denial of service (DoS) attacks, due to SDN rules.
b. The network will not be affected by Spoofing (Masquerading) attacks, because of a combination of SDN rules and the blockchain verification process.
c. The network will not be affected by spying attacks due to blockchain verification, due to which there will be no communication of any node with unwanted nodes, thereby removing any chances of spying or spoofing.

Once all these verifications are completed, then data communication proceeds on a node-to-node basis. A comparison of the results obtained for these protocols with other standard methods is done and conclusions are derived from these results in the next section.

4. RESULTS EVALUATION & ANALYSIS

In order to evaluate the results for the given protocol, the network is simulated under similar conditions as directed in the standard VANET simulation networks in [10]. Due to the use of blockchain, it is observed that the proposed model has high security, and is able to identify Sybil, Masquerading, DDoS, and Smurf attacks with 100% efficiency. The reasons for this high efficiency are traceability, immutability, and improved trust levels of blockchain. Thereby making the network 100% efficient in terms of attack detection. The QoS parameters were evaluated by changing the number of communications, and averaging the values. The number of communications was varied between 10 to 100. The following network parameters are decided for simulating the network,

Channel Type:	Wireless Channel
Propagation Mode:	Two Ray Ground
Network interface:	Wireless Physical
MAC Protocol:	Mac/802.11
Interface Queue type:	Drop Tail Priority Queue
Antenna Type:	Omnidirectional
Routing:	AODV
Network X Size:	300
Network Y Size:	300
Packet Size:	1000 bytes per packet
Packet Interval:	0.01 seconds per packet

Parametric values for the end-to-end delay, throughput, energy consumption, and packet delivery ratio are evaluated based on the following formulas,

$$D = Tr - Tt \tag{1}$$

$$E = Et - Er \tag{2}$$

$$\text{Thr} = \frac{Psr}{D} \tag{3}$$

where, D is the end-to-end communication delay, E is the energy consumed during communication, Thr is Troughput and T_t are the reception and transmission time for the packet, E_t and E_r are the transmission and reception energies in the network, P_{sr} are the number

of packets successfully received and P_t are the number of packets transmitted. Using these values, the following parameters were evaluated. Delay performance of the network using different protocols are given in Table 2 where NSV is Non-Secured VANET, ASV is AES Secured VANET, ASS is AES Secured SDN, ABOSS is AES Blockchain Open flow Secured SDN.

Table 2. Delay Performance

No. of Nodes	Delay (ms) NSV	Delay (ms) ASV	Delay (ms) ASS	Delay (ms) ABOSS
10	34.09	45.80	25.02	21.40
20	31.09	44.80	32.02	22.40
30	34.31	44.82	27.79	25.72
40	37.94	42.04	47.56	24.31
50	54.93	45.33	28.31	27.47
60	57.02	35.06	26.39	22.30
70	47.45	33.66	25.39	24.71
80	32.69	29.54	29.89	21.89
90	49.29	44.80	32.02	21.40
100	61.24	51.27	22.20	21.69

From Table 2, it is observed that the Average delay of NSV is 44ms, ASV is 41.7ms, ASS is 29.6ms, and delay of ABOSS is 23.2ms. Thus, the delay using ABOSS is improved by 44% when compared to VANET secured systems, and the delay using ABOSS is improved by 22% when compared to SDN secured systems. Similar comparisons are made for energy and throughput. These values are given in Table 3 and 4 respectively.

From Table 3, it is observed that the Average Energy consumption of NSV is 25.48mJ, ASV is 39.73mJ, ASS is 18.3mJ, and energy consumption of ABOSS is 15.85mJ. Thus, the energy consumption using ABOSS is improved by 60.1% when compared to VANET secured systems, and the energy consumption using ABOSS is improved by 13.4% when compared to SDN secured systems.

Table 3. Energy performance

No. of Nodes	Energy (mJ) NSV	Energy (mJ) ASV	Energy (mJ) ASS	Energy (mJ) ABOSS
10	20.3	38.3	19.2	16.2
20	21.9	39.1	19.4	16.4
30	22.6	42	20.2	16.3
40	23.6	41.8	18.8	15.5
50	29.5	42.5	17.4	13.2
60	28.5	26	17.3	17.5
70	26.7	40.1	18.3	16
80	22.2	41.5	17.8	14.2
90	27.5	42.5	17.6	16.9
100	32	43.5	17	16.3

From Table 4, it is observed that the Average Throughput of NSV is 12.74Tbps, ASV is 16.34Tbps, ASS is 262.6Tbps and the Throughput of ABOSS is 442.6Tbps. Thus, the Throughput using ABOSS is improved much more than 100 % when compared to VANET secured systems, and the Throughput using ABOSS is improved by 68.5 % when compared to SDN secured systems.

Table 4. Throughput performance

No. of Nodes	Thr (Tbps) NSV	Thr (Tbps) ASV	Thr (Tbps) ASS	Thr (Tbps) ABOSS
10	19.8	19.3	163	423
20	18.8	17.3	173	435
30	15.3	8.83	240	620
40	12.3	8.78	287	354
50	5.4	8.5	244	429
60	7.73	14.2	261	372
70	16.6	22.1	256	447
80	7.91	40.2	466	469
90	4.8	6.94	363	442
100	18.8	17.3	173	435

5. CONCLUSION AND FUTURE SCOPE

The QoS parameters are improved by combining SDN with Open Flow with blockchain, and AES encryption 256 standards of the network. The network is secured from DOS, Masquerading, and Spying attacks due to the SDN rules and blockchain verification process. Due to the incorporation of AES, there is a further improvement in the security performance of the network in terms of data confidentiality. The work can be carried out on the cloud by unloading computations associated with security and blockchain and thus improving the parameters of the network. By the addition of machine learning in the routing process, the routing algorithm can be improved, which will further improve the QoS and security performance of the network.

6. REFERENCES:

[1] Y. Yang, D. He, H. Wang, L. Zhoc, "An efficient blockchain-based batch verification scheme for vehicular ad hoc networks", Transaction on Emerging Telecommunications Technologies, 2019, pp. 1-12.

[2] S. V. Akram, P. K. Malik, R. Singh, G. Anita, S. Tanwar, "Adoption of blockchain technology in various realms: Opportunities and challenges", Security Privacy, Vol. 3, No. 5, 2020.

[3] F. M. Salem, A. S. Ali, "SOS: Self- organized secure framework for VANET", International Journal Communication System, Vol. 33, No. 7, 2020.

[4] Y. Zhao, X. Zhang, X. Xie , Y. Ding, S. Kumar, "A verifiable hidden policy CP-ABE with decryption testing scheme and its application in VANET", Transaction on Emerging Telecommunications Technologies, 2019. (in print)

[5] M. D. Firoozjaei, R. Lu, A. Ghorbani, "An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms", Security Privacy, Vol. 3, No. 6, 2020.

[6] Dharminder, D. Mishra, "LCPPA: Lattice-based conditional privacy-preserving authentication in vehicular communication", Transaction on Emerging Telecommunications Technologies, Vol. 31, No. 2, 2019.

[7] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, W. He, "An Efficient Decentralized Key Management Mechanism for VANET with Blockchain", IEEE Transaction on Vehicular Technology, Vol. 69, No. 6, 2019, pp. 5836-5849.

[8] B. Luo, X. Li, J. Weng, J. Guo, J. Ma, "Blockchain-Enabled Trust-based Location Privacy Protection Scheme in VANET", IEEE Transaction on Vehicular Technology, Vol. 69, No. 2, 2020, pp. 2034-2048.

[9] M. S. Iftekhar, N. Javaid, O. Samuel, M. Shoaib, M. Imran, "An Incentive Scheme for VANETs based on Traffic Event Validation using Blockchain", Proceedings of the International Wireless Communications and Mobile Computing Conference, Limassol, Cyprus, 15-19 June 2020.

[10] Z. Lu, Q. Wang, G. Qu, Senior Member, IEEE, H. Zhang, and Z. Liu, "A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs", IEEE Transactions on Very Large Scale Integration Systems, Vol. 27, 2019, pp. 2792-2801.

[11] D. Zhang, F. R. Yu, and R. Yang, "Blockchain-Based Distributed Software-defined Vehicular Networks: A Dueling Deep Q-Learning Approach", IEEE Transactions on Cognitive Communications and Networking, Vol. 5, No. 4, 2019, pp. 1086-1100.

[12] M. Wagner, B. McMillin, "Cyber-Physical Transactions: A Method for Securing VANETs with Blockchains", Proceedings of the IEEE 23rd Pacific Rim International Symposium on Dependable Computing, Taipei, Taiwan, 4-7 December 2018.

[13] Z. Lu, W. Liu, Q. Wang, G. Qu, Z. Liu, "A Privacy-preserving Trust Model based on Blockchain for VANETs", IEEE Access, Vol. 6, 2017, pp. 45655-45664.

[14] X. Liu, H. Huang, F. Xiao, Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs", IEEE Internet of Things Journal, Vol. 7, No. 5, 2019, pp. 4101-4112.

[15] C. Lai, Y. Ding, "A Secure Blockchain-Based Group Mobility Management Scheme in VANETs", Proceedings of the IEEE/CIC International Conference on Communications in China, Changchun, China, 11-13 August 2019.

[16] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, M. S. Obada, "A systematic review on security issues in vehicular ad-hoc network", Security and Privacy, Vol. 1, No. 5, 2018.

[17] B. Pourghebleh, N. J. Navimipour, "Towards efficient data collection mechanisms in the Vehicular ad hoc networks", International Journal Communication System, Vol. 32, No. 5, 2019.

[18] R. Shrestha, S. Yeob, "Regional Blockchain for Vehicular Networks to Prevent 51% Attacks", IEEE Access, Vol. 7, 2019, pp. 95033-95045.

[19] R. Shrestha, R. Bajracharya, S. Yeob Nam, "Blockchain-based Message Dissemination in VANET", Proceedings of the IEEE 3rd International Conference on Computing, Communication and Security, Kathmandu, Nepal, 25-27 October 2018.

[20] Q. Feng, D. He, S. Zeadally, K. Liang, "BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad-Hoc Networks", IEEE Transactions on Industrial Informatics, Vol.6, 2019.

[21] D. Zhang, F. R. Yu, R. Yang, "A Machine Learning Approach for Software-defined Vehicular Ad Hoc Networks with Trust management", Proceedings of the IEEE Global Communications Conference, Abu Dhabi, United Arab Emirates, 9-13 December 2018.

[22] A. Hussein, I. H. Elhajj, A. Chehab, A. Kayssi, "SDN VANETs in 5G: An Architecture for Resilient Security Services", Proceedings of the 4th International Conference on Software Defined Systems, Valencia, Spain, 8-11 May 2017.

[23] W. B. Jaballah, M. Conti, C. Lal, "Security and Design Requirements for Software-Defined VANETs", Computer Networks, Vol 169, 2020.

[24] J. S. Weng, J. Weng, Y. Zhang, W. Luo, W. Lan, "BENBI: Scalable and Dynamic Access Control on the Northbound Interface of SDN-based VANET", IEEE Transactions on Vehicular Technology, Vol. 68, No. 1, 2019, pp. 822-831.

[25] G. Luo, J. Li, L. Zhang, Q. Yuan, Z. Liu, F. Yang, "SDN MAC: A Software-Defined Network Inspired MAC Protocol for Cooperative Safety in VANETs", IEEE Transactions on Intelligent Transport Systems, Vol. 19, No. 6, 2018, pp. 2011-2024.

[26] J. Joshi, K. Renuka, P. Medikonda, "Secured and Energy Efficient Data Transmission in SDN-VANETs", Proceedings of the 22nd International Computer Science and Engineering Conference, Chiang Mai, Thailand, 21-24 November 2018.

[27] A. Muthanna, R Shamilova, A. Ateya, A. Paramonov, M. Hammoudeh, "A mobile edge computing/software-definednetworking- enabled architecture for vehicular networks", Internet Technology Letters, Vol. 3, No. 6, 2019.

[28] L. Alouache, N. Nguyen, M. Aliouat, R. Checotah, "HSDN-GRA: A hybrid software-defined networking-based geographic routing protocol with the multi-agent approach", International Journal Communication System, Vol. 33, No. 15, 2020.

[29] L. Alouache, N. Nguyen, M. Aliouat, R. Chelouah, "Survey on IoV routing protocols: Security and network architecture", International Journal Communication System, Vol. 32, No. 2, 2019.

[30] R. Shrestha, R. Bajracharya, S. Y. Nam, "Challenges of Future VANET and Cloud-Based Approaches", Wireless Communication and Mobile Computing, 2018.