Decentralized Authentication Mechanism for Mobile Ad hoc Networks

Hafida Khalfaoui, Abderrazak Farchane and Said Safi

***Abstract*—Covid 19 has dramatically changed people's lives around the world. It has shut down schools, companies and workplaces, forcing individuals to stay at home and comply to quarantine orders. Thus, individuals have resorted to the Internet as a means for communicating and sharing information in different domains. Unfortunately, some communities are still unserved by commercial service providers. Mobile Adhoc Network (MANET) can be used to fill this gap. One of the core issues in MANET is the authentication of the participating nodes. This mechanism is a fundamental requirement for implementing access control to network resources by confirming a user's identity. In recent years, security experts worldwide proposed distributed authentication for MANET due to the lack of a central authority to register and authenticate nodes. In this article, decentralized authentication based on the technology of fog computing and the concept of the blockchain is proposed. The evaluation of this mechanism satisfies the diverse security requirements and strongly protects the networks from attacks.**

***Index Terms*—Authentication, Blockchain, Community network, Fog computing, Mobile Ad hoc Network.**

I. Introduction

South Africa is one of the most underdeveloped societies in the world. Around 55.5% of the population is poor, with rural areas accounting for 80%. The majority of poor Africans cannot afford basic necessities or have access to resources, adequate education or essential services. Community networks give rural and underprivileged communities the chance to own, control and market their communication services, which could help bridge socioeconomic.

Zenzeleni ("Do it yourself" in isiXhosa) is the first community network in South Africa, founded in 2013 by the University of the Western Cape (UWC) PhD students and the Mankosi community's tribal government. Due to a shortage of electricity, Zenzeleni began as a local wireless network for delivering free calls by connecting analog phones via solar-powered routers. It was later updated to add an external internet connection for making calls to national numbers via a 3G modem [1]. The above has not happened without challenges: This project took six years to complete, and communities have faced several legal, technological, financial and social restrictions, which have necessitated collaboration to overcome them.

Mobile Ad hoc network (MANET) is a good solution to reduce communications costs in these community networks. They are composed of various computer systems or mobile phones called nodes, which can connect autonomously by radio waves without needing a fixed infrastructure such as routers or access points. This solution can open the door to many individuals to communicate, share information and have novels of what happens in their society with less cost and effort.

A. Problem statement

MANET has advanced dramatically due to the proliferation of mobile devices and enhancements in wireless communication. In some situations, people need to set up an instant and temporary multimedia network where devices can communicate immediately, such as in conferences, classrooms, home networks or other civilian locations like a sports stadium, ship or small aircraft [2].

The specifics of MANET show how these networks are, by nature, a great challenge for IT security. The operating approach for nodes is to receive packets and transmit them to the next-hop through intermediate nodes until they arrive at their destination [3]. They are resource-constrained devices that cannot secure and defend themselves, making them vulnerable to hacking and compromise. Indeed, the security of nodes and exchanged messages is essential. This work will focus precisely on authentication as a starting point of security, as it is required for both old and new nodes to connect to the network for communication. This security objective will protect the network by permitting only legitimate nodes to gain access to their resources and will defeat all attacks using the identity or role impersonation. Consequently, the authentication scheme must be robust, scalable and resistant to known threats. For MANET, many theoretical studies exist, but ultimately few practical applications can satisfy all the constraints inherent in Ad hoc networks.

One of the most popular authentication mechanisms in MANETs is clustering, such as proposed in [4], [5]. This algorithm separates the network into clusters, with the cluster head (CH) is chosen from the node with the highest weight. The CH then utilizes the AUCRES (authentication response) technique to authenticate nodes using unique identification and long keys. The problem with this algorithm appears when the cluster head is attacked. To improve this technique, security experts worldwide have been concentrating on the blockchain. This technology is well suited for MANET authentication and access control services due to its decentralized system, its cryptographic features and other characteristics such as enhanced unforgeability, reliability and fault tolerance.

B. Paper's contributions

This work proposes and evaluates the security of an authentication mechanism based on blockchain technology for

The authors are with the LIMATI Laboratory, Department of Mathematics and Computer Science, Polydisciplinary Faculty, Sultan Moulay Slimane University, PO Box 592, Beni Mellal, 23000, Morocco. (E-mail: hafidakhalfaoui1996@gmail.com, a.farchane@gmail.com, safi.said@gmail.com)

DOI: 10.36244/ICJ.2022.3.4

MANET's nodes. The architecture of this system includes mobile nodes and Ethereum Blockchain managed by smart contract rules. Fog nodes are also used to synchronize data associated with registered nodes. This paper's principal contributions can be outlined as follows:

- A decentralized authentication approach is presented without needing an intermediary or trusted third party. It uses the blockchain to register and authenticate devices, with access tokens calculated by the smart contract.
- The complete system is shown in detail, including the architecture, sequence diagrams and the explication of different interactions between nodes and the smart contract.
- Security analysis and discussion are explained about how this proposed authentication method satisfies security goals (identification, confidentiality, integrity and non-repudiation) and resists certain types of attacks.

C. Paper structure

The rest of this paper is shown as follows: Section II shows a brief overview of MANET and defines blockchain and fog computing technologies. Section III discusses a view of decentralized authentication methods in the literature. Section IV spots the light of the proposed mechanism. Section V presents its implementation and talks about the evaluation of results. Finally, Section VI gives the conclusion and the future work.

II. BACKGROUND

This section gives a summary of MANET, blockchain and fog computing technologies.

A. Mobile Ad hoc Network

A Mobile Ad hoc Network is an instant network of the mobile nodes without a fixed infrastructure. There are two modes of MANET: The first mode is when the nodes can directly interact with other nodes in their radio range. The second one is called multi-hop communication, when the intermediate nodes are employed to communicate with the nodes beyond their radio ranges [6].

MANET is vulnerable to various security attacks because of its characteristics, including dynamic topology, lack of central management and unsecured medium. The absence of a centralized administration pushes the nodes to communicate on a level of mutual trust. This property renders MANET more vulnerable to exploitation by internal attackers. Moreover, wireless links make it also more accessible for malicious nodes to get network resources.

There are two classifications of attacks according to [7], [8]. On the one hand, the attacks in MANET can be classified according to the attack's behavior as passive or active attacks:

- **Passive attacks**: Intercept data when it transits a network. It is difficult to detect the intrusion because this type of attack does not cause any noticeable perturbation or malicious activity disrupting the network's normal function. Traffic analysis, Traffic monitoring and Eavesdropping are examples of these attacks.
- **Active attacks** : Are more disruptive because the malicious nodes affect the network traffic and the transmissions by generating congestion and false routing information. Still, the dynamic nature of these attacks is quite easy to detect and prevent. Modification, Impersonation and Fabrication are examples of active attacks.

On the other hand, attacks can also be classified as either internal or external:

- **External attacks**: Are launched by unlicensed nodes that aren't part of the network, and they may flood the network with fake packets and sometimes imitate legitimate nodes. External malicious nodes mainly aim to create congestion or disrupt normal network operations.
- **Internal attacks**: Are initiated by the network's legitimate nodes; these malicious nodes take resources from other network nodes arbitrarily and selfishly like battery power, processing power and bandwidth.

B. Blockchain technology

Blockchain is a distributed ledger for storing cryptographically signed data. When a user creates a transaction over a blockchain network, the new transaction is grouped with others to form a block as shown in Figure 1. Once the block is created, active nodes, known as miners, ensure that transactions inside the block follow predetermined criteria using a consensus procedure like proof of Work (PoW). After, the miner who validates the block is rewarded, and the blockchain stores the verified block. Finally, to avoid a single point of failure, each node in the network keeps a copy of the blockchain on hand. These copies are simultaneously updated and verified [9].

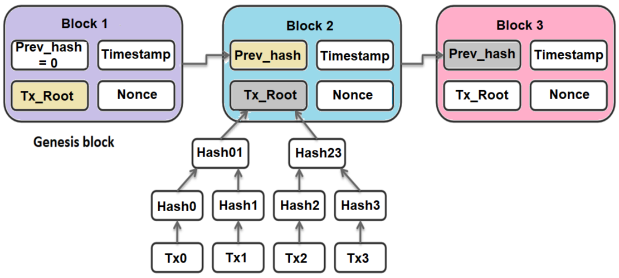

Fig. 1. Blockchain

C. Fog Computing

Fog computing is an extension of cloud computing, in which data processing is transferred to the near of devices instead of sending it to the cloud. This mechanism will lessen the burden of the Internet and give quick processing. The basic instruction of Fog computing consists of three layers: End devices, fog nodes and cloud servers [10].

III. STATE OF THE ART

Authentication is an essential step to ensure the legitimacy of nodes and the network's safety. Current state-of-the-art authentication solutions are not adequate for MANET due to the open environment, resource-constrained devices, centralization and high energy consumption. For this reason, low-power, low-storage, low-latency and low-communication-overhead authentication techniques are required. Recently, to fill gaps in existing technologies, current researchers have focused on blockchain mechanisms, each in their perspective.

Jarjis and Kadir [11] presented a blockchain implementation for Ad Hoc On-Demand Distance Vector (AODV). The AODV is considered an excellent routing protocol in MANET because it employs the least overhead by reducing information exchanged in messages. However, this weakens the authentication and checking integrity mechanism as nodes do not have enough knowledge about the identities of neighboring nodes. As a result, the authors modify the AODV protocol to BAODV, adding an extra field to the Route Request (RREQ) and Route Reply (RREP) options. This procedure begins by including a field called (Bnode) to the RREQ packet's header. This field stores the malicious node's address if it breaks into the network or tries to exploit its resources. Then, each node verifies that the previous node's address matches (Bnode). This solution provides node verification features and uses a chaining technique to detect Impersonation and Black-hole attacks as a secure system. It removes the malicious node involved path without extra processing that affects network performance with additional overhead.

Yang and Hwanseok [12] proposed a decentralized protocol for authentication by integrating blockchain and an area-based hierarchical structure. After dividing the entire network into regions, the region's most reliable node is designated as a Region Certificate Authority (RCA). The highest reliability node among the RCA will be elected and selected as Top Certificate Authority (TCA). Then, the RCA node issues a group key to the TCA node and a member key to the member nodes in the area. Only nodes that give the corresponding key can participate in data transmission. This protocol was implemented using blockchain technology through transaction creation, block packaging and verification processes. Blockchain, as a peer-to-peer network with a hierarchical structure of nodes, provides a decentralized solution for node authentication that can prevent a single point of failure of centralized mechanisms and the forgery of authentication information for nodes participating in the network.

The blockchain is also implemented in the other types of MANET like Flying Ad hoc Network (FANET) and Vehicular Ad hoc Network (VANET).
VANET is widely regarded as the main platform for vehicle-to-vehicle communication. This system improves transportation security and reduces the number of accidents [13]. However, it is more vulnerable to attacks due to its high mobility and dynamic topology. As a result, with VANET, a secure and anonymous authentication mechanism is critical. Azees et al. [14] proposed an anonymous authentication mechanism based on blockchain in which RSUs can anonymously authenticate the vehicles and perform future communications through the shared session key. Moreover, the reauthentication of automobiles between roadside units became faster thanks to the secure transfer of authentication codes between adjacent Road Side Units (RSUs). Among the advantages of this mechanism, the integrity of the transmitting message is preserved due to the support of the blockchain. In addition, the performance analysis done by the authors of this work proves its efficiency in terms of communication, computational and storage costs. So it is convenient for real-time applications.

For FANET; the network of unmanned aerial vehicles (UAVs) that can execute many activities, for example, delivery of goods, rescue missions and terrain monitoring; Kashish et al. [15] proposed a decentralized network authentication approach that adopts a blockchain-based public key infrastructure. The blockchain allows for shared public keys and the necessary information for the authentication process. This decentralized scheme reduces major security risks associated with a single point of failure. The experimental results show that this method works with constant throughput, latency and approximately constant message overhead as transaction size increase for a given network size. In addition, the authors mention that this architecture presented in the context of flying nodes can apply to other types of ad hoc network nodes.

The studies mentioned above demonstrate the utility of blockchain for different types of MANET. Also, the Internet of Things uses this technology as cited in [9]. For this reason, this work benefits the advantages of this technology and Fog computing to obtain a suitable authentication solution for MANET.

IV. PROPOSED MECHANISM

A. Architecture

This project aims to create a distributed authentication mechanism based on the blockchain that permits communication between nodes from different groups in the network. Figure 2 depicts the architecture of this mechanism divided into two layers: the device layer and the fog layer.

The device layer contains two types of mobile nodes installed in the network in clusters: admins and devices.

- **Admins**: They are in charge of controlling devices access, and they serve as the certification authority in each group. These admins should have high-performance RAM, a faster processor and a high storage capacity. In addition, It is preferable to be fixed computers connected to redundant power supplies as servers to stay permanently in service to register and authenticate nodes at any time. Many algorithms in the literature are created to select suitable admins as cited in [16]. Artificial Neural Networks (ANNs) are established to develop a clustering algorithm using weight-based parameters to choose cluster heads utilizing four inputs: mobility, packet drop, energy and the number of neighbor nodes. ANNs are computer systems inspired by the biological neural networks that form human brains [17]. This work does not focus on how selecting admins. The network creator chooses the other admins, and each one of them is assigned to the nearest fog node that helps share the blockchain between all admins.

- **Devices**: Each device is identified by its unique identified information and can be added by one admin.

The fog layer contains, in general, a network of fog nodes that enable the implementation of fog services. It also performs localized storage and processing locally to the devices in order to reduce cloud latency and response time. Each group in the network is associated with the nearest fog node. These fog nodes communicate to ensure data synchronization for authentication. When an admin registers any device, it will add a block to the blockchain and share it with its associated fog node. This latter updates the blockchain and distributes it to other fog nodes. As a result, all admins can receive the novel copy of the blockchain and will be able to authenticate all network nodes in the case of node mobility than a group to other groups.

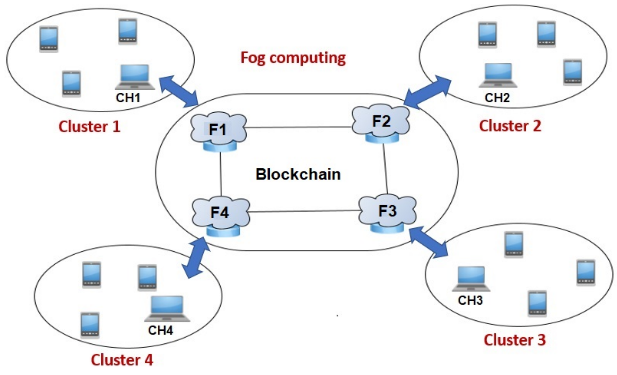

Fig. 2. The architecture of the proposed mechanism

B. Systems functioning

The network's function is to communicate by forwarding packets between nodes without any security guarantees. As a result, focusing on the authentication strategy allows reliable communication between several nodes over an untrusted network and prohibits the access of malicious users. In this paper, the transaction includes the node's registration and authentication request. The hash value of the latter is stored in the blockchain. The following sections will describe the different algorithms of the authentication mechanism.

1) Assumptions:

In this proposed mechanism, we assume that:
- Admins are trusted and all their actions are legitimate.
- Each admin chooses its cluster identifier (CID) and will share it only with trusted nodes. A new node can not sign up in the cluster if it does not have its CID.
- Each node has a private/public key pair for data encryption and integrity in the system.

2) Initialization phase:

This approach starts with an initialization phase. In the smart contract's constructor, the first admin is created using the address of the smart contract's creator, a unique identifier AID and a cluster head identifier CID. Then, the smart contract calculates the token of this first admin and saves it in the blockchain. Nodes credentials will be saved using their hash instead of keeping them in plain text.

3) Registration phase:

In the registration phase, each group with its associated nodes is registered in the blockchain. This phase is divided into two stages: Admin registration and device registration.

a- Admin registration

During this phase, each admin chooses a unique identifier (CID) to register its cluster on the blockchain. This operation is only restricted to administrator nodes. The following steps and the sequence diagram of Figure 3 describe the phase of admin registration.

1) A new admin can sign up by sending its information, including the address AIP, the cluster identifier CID and the unique identifier AID to an old admin using **addAdmin**(AIP, CID, AID) function.
2) After, the smart contract checks if the admin in question is already registered in the blockchain or not by searching the hash of its AID, AIP and CID.
3) If this admin does not exist in the blockchain, a token= **keccak256**(AIP, CID, AID) will be created, and the new admin will be saved in the blockchain. Keccak256 is a hash function.
4) Finally, the smart contract accepts the transaction triggering the **AdminAdded** event and generates a new block designated successful registration of the admin node. The event is a broadcast to all nodes in the blockchain.

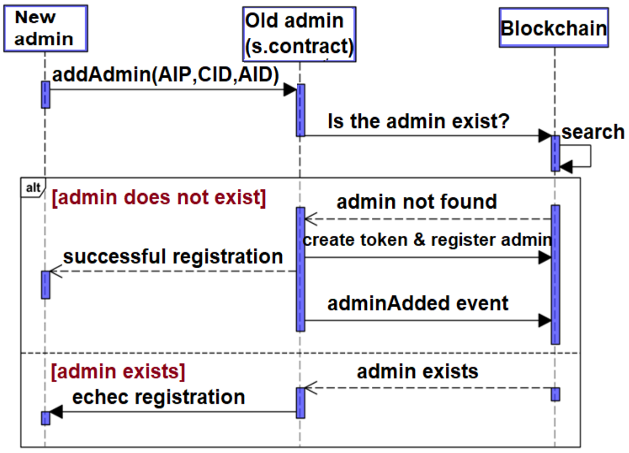

Fig. 3. Sequence diagram for clusters registration

b- Device registration phase

After the successful registration of the cluster in question, devices can register. The following steps and the sequence diagram of Figure 4 describe the device registration phase.

1) Admin can add a device to the network by sending the information, including the address of device DIP, the

cluster identifier CID and the unique device identifier DID to **addDevice**(DIP, CID, DID) function.

2) The function initially verifies if the CID presented corresponds to the adding admin. If not, the transaction will be terminated by error.
3) If yes, the function checks if this device is already existed by comparing the hash of its DIP, CID and DID to the nodes list saved in the blockchain.
4) If the device does not exist in the blockchain, a token = **keccak256**(DIP, CID, DID) is created, and the new device is registered.
5) Finally, the smart contract accepts the transaction triggering the **DeviceAdded** event and generates a new block designated successful registration of the new device.

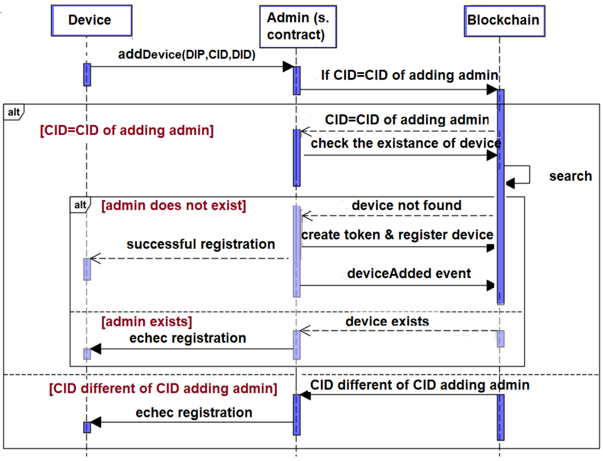

Fig. 4. Sequence diagram for devices registration

4) Authentication phase:

In the authentication phase, any admin can authenticate the devices registered in the blockchain to communicate with each other. The following steps and the sequence diagram of Figure 5 describe the device authentication phase.

1) The device sends a request authentication containing its DID, DIP and CID to any admin. This latter uses the smart contract to verify the received packet's legitimacy by creating its token and comparing it with the list of tokens stored in the blockchain.
2) If the token corresponding to the DIP exists, the admin successfully authenticates the device, and the event Authenticated is shared. Otherwise, it shares the NoAuthenticated event.

V. Implementation and Evaluation

A. Implementation

For implementing this strategy, Remix IDE is used in the first step. It is an open-source web tool that aids in the testing, debugging and deploying smart contracts and serves as a learning and teaching environment for Ethereum blockchain. The selection of Ethereum is based on the following criteria:

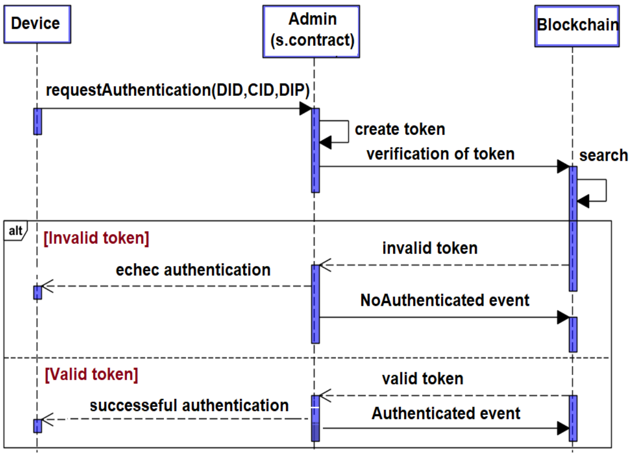

Fig. 5. Sequence diagram for the authentication phase.

1) Firstly, Ethereum is the most popular blockchain platform that simplifies the construction of decentralized applications (DApps).
2) Secondly, it allows creating, deploying and testing smart contracts.
3) Thirdly, it provides secure transactions using a lightweight and robust signature for restricted devices called Elliptic Curves Cryptography (ECC).
4) Fourthly, many Ethereum test networks do not need a faucet or mining; they can reset accounts instantly with a fixed amount of fake Ether for developing and testing the smart contract.
5) Finally, it is widespread and adopted by a large community.

In the following step, ReactJS was used to build a decentralized application (Dapp) that allows interaction between users and Ethereum. The smart contract's compilation and deployment were implemented by Hardhat. Ganache-CLI was used as an Ethereum emulator, which provided accounts with 100 ethers for testing smart contracts. It is very close to a real Ethereum implementation and shows the transactions and blocks created in the blockchain. Then, Metamask created a wallet to manage different accounts and connect the current user to the blockchain. Table I resumes the different tools adopted to validate the suggested mechanism.

TABLE I
DIFFERENT TOOLS USED IN THE IMPLEMENTATION.

Tool	Description
Remix IDE, Hardhat	Smart contracts compilation and deployment
Ganache-cli	Ethereum emulator
ReactJS	development of the front-end application
Metamask	Managing accounts

B. Evaluation

This study does not interest the proposed mechanism's execution time or power consumption because it depends on the type of Ethereum network, the communication protocol and the node specification. This study's interest concerns the impact of the mechanism on the security of nodes and the network in general. The security mechanism was created to authenticate nodes with limited MANET resources. The blockchain used SHA-256 and ECC algorithms as solid cryptographic proof for data integrity and authentication. All transactions in the blockchain were digitally signed and validated by admin nodes in the network and then were stored and organized in blocks using timestamps and hashes. These blocks were linked together to build a chain. The ECC algorithm is suited to the MANET environment, particularly in terms of key sizes and signature times. Also, it consumes less power and has the same level of security as Rivest Shamir Adleman (RSA)[18].

This part describes how the suggested strategy satisfies the various security requirements and protects against attacks.

- **Identification**: (ID) is required for any node trying to access the network. Each node in a cluster has a unique identifier DID, a unique public address and the CID that can associate it with its unique group.
- **Confidentiality**: This requirement was satisfied by encrypting all nodes' requests to keep the privacy of identification credentials. Each admin in the network has an Ethereum address that includes asymmetric public key pairs. It shares its public key with nodes for encrypting their messages request.
- **Integrity**: Each node uses its private key to generate a signature for each request message, while the admin can use the node's public key to verify the signature. Also, transactions in the blockchain were signed using the admin's private key produced by the Ethereum-supported ECDSA. This algorithm ensures the integrity of messages and the legitimacy of nodes. Besides, the identifiers of nodes are saved using their hash to keep their privacy because hashing is an irreversible function that cannot be converted back into the original information.
- **Non-repudiation**: Private keys sign all data in the system; as a result, sending and receiving parties can never deny ever their executing a transaction.
- **Resistance against attacks**: Each node can only have one identity and only one key pair in this model. The private key associated with this identity should sign all its transactions. The cluster admin must approve all its nodes identities; as a result, an attacker cannot impersonate another node's identity because he always needs its private key. Furthermore, it will be impossible to attack the blockchain if one admin is compromised because services are distributed and duplicated over all network admins and fog nodes.

C. Open issues

The approach proposed in this article is not adapted to real-time applications because registration and authentication times rely on admins availability. This problem is due to the limited storage capacity of the nodes. The blockchain system has a scalability problem that limits its practical use for all nodes in the network; i.e., if the number of nodes increases, the number of transactions increases, and the file size of the blockchain will require a large amount of storage capacity. As a result, only administrators can maintain the blockchain and control access by other nodes. In addition, this approach also relies on the type of blockchain used. According to the consensus protocol, the transactions will be validated only after the time of consensus. This step represents a critical and challenging issue in MANET due to the limited power and computation resources. High financial costs that involve the amount of cryptocurrency spent on transaction fees are another problem in this approach. In conclusion, for blockchain to operate seamlessly in MANETs, more personalized versions are needed that require fewer resources without losing the built-in security and that handle the changing topology of the network more efficiently.

VI. Conclusion and Future work

This paper proposed a decentralized authentication mechanism for allowing secure access to network resources. The suggested technique used the distributed nature and the cryptographic characteristics of blockchain technology. Besides, fog computing was used to assure communication between admins by delivering the update of blockchain anytime nodes are added to the network. Furthermore, this study defined the security requirements to analyze and evaluate the approach's resistance against attacks. The future work will be interested in protecting the admin from flooding attacks that aim to shut down the cluster. An intrusion detection system will be integrated to detect DOS/DDOS by checking the time of sending authentication requests. Suppose a node transmits more than several authentication requests to the admin in a short time. In that case, the admin will consider it a malicious node and immediately terminate any sort of communication with it and send an alert to all the admins in the network.

References

[1] S. D. Tena and C. Rey-Moreno, *Global information society watch 2018, Community networks*, 2018.

[2] A. O. Bang and P. L. Ramteke, "Manet: History, challenges and applications," *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, vol. 2, no. 9, pp. 249–251, 2013.

[3] M. Anand and T. Sasikala, "Efficient energy optimization in mobile ad hoc network (manet) using better-quality aodv protocol," *Cluster Computing*, vol. 22, no. 5, pp. 12681–12687, 2019. DOI: 10.1007/s10586-018-1721-2.

[4] N. Sharma and A. Gangal, "Mobile node authentication in manet using enhanced cluster based aucres algorithm," *Far East J. Electron. Commun*, pp. 1–12, 2016. DOI: 10.17654/ECSV3PI16001.

[5] M. Er-Rouidi, H. Moudni, H. Faouzi, H. Mouncif, and A. Merbouha, "Improving performance of mobile ad hoc network using clustering schemes," vol. 6, pp. 69–75, 2017. DOI: 10.11591/IJICT.V6I2.PP69-75.

[6] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, "A survey on manets: architecture, evolution, applications, security issues and solutions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, pp. 832–842, 2018. DOI: 10.11591/IJEECS.V12.I2.PP832-842.

[7] K. Gupta and P. K. Mittal, "An overview of security in manet," *International Journals of Advanced Research in Computer Science and Software Engineering ISSN*, vol. 7, pp. 2277–3128, 2017. DOI: 10.23956/IJARCSSE/V7I6/0254.

[8] M. Ichaba, "Security threats and solutions in mobile ad hoc networks; a review," *Universal J. Commun. Netw*, vol. 6, no. 2, pp. 7–17, 2018. DOI: 10.13189/ujcn.2018.060201.

[9] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018. DOI: 10.1016/j.cose.2018.06.004.

[10] A. A. Laghari, A. K. Jumani, and R. A. Laghari, "Review and state of art of fog computing," *Archives of Computational Methods in Engineering*, vol. 28, no. 5, pp. 3631–3643, 2021. DOI: 10.1007/S11831-020-09517-Y.

[11] A. Jarjis and G. Kadir, "Blockchain authentication for aodv routing protocol," in *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*. IEEE, 2020. DOI: 10.1109/BCCA50787.2020.9274452, pp. 78–85.

[12] H. Yang, "A study on hierarchical structure and blockchain-based node authentication mechanism in manet," *Convergence Security Journal*, vol. 19, no. 3, pp. 13–19, 2019. DOI:10.33778/kcsa.2019.19.3.013.

[13] H. Garmani, D. AitOmar, M. ElAmrani, M. Baslam, and M. Jourhmane, "Joint beacon power and beacon rate control based on game theoretic approach in vehicular ad hoc networks," *INFOCOMMUNICATIONS JOURNAL*, vol. 13, no. 1, pp. 58–67, 2021. DOI: 10.36244/ICJ.2021.1.7.

[14] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "Bbaas: Blockchain-based anonymous authentication scheme for providing secure communication in vanets," *Security and Communication Networks*, vol. 2021, pp. 1–11, 2021. DOI: 10.1155/2021/6679882.

[15] K. Khullar, Y. Malhotra, and A. Kumar, "Decentralized and secure communication architecture for fanets using blockchain," *Procedia Computer Science*, vol. 173, pp. 158–170, 2020. DOI: 10.1155/2021/6679882.

[16] B. Chatterjee and H. N. Saha, "Parameter training in manet using artificial neural network." *International Journal of Computer Network & Information Security*, vol. 11, no. 9, 2019. DOI: 10.5815/ijcnis.2019.09.01.

[17] D. Bisen, S. Mishra, and P. Saurabh, "K-means based cluster formation and head selection through artificial neural network in manet," 2021. DOI: 10.21203/RS.3.RS-667651/V1.

[18] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power iot devices," in *2016 international conference on advances in computing, communications and informatics (ICACCI)*. IEEE, 2016. DOI: 10.1109/ICACCI.2016.7732296, pp. 1725–1729.

Hafida Khalfaoui obtained her B.Sc. in Electronic and Telecommunication Engineering and her M.Sc. in Telecommunication Systems and Computer Networks from Sultan Moulay Slimane University, Beni Mellal, Morocco, in 2017 and 2019, respectively. She is following her Ph.D. in Mathematics and Computer Science at Sultan Moulay Slimane University. Her research interests include computer science and network security.

Abderrazak Farchane received his B.Sc. in Computer Science and Engineering in June 2001 and M.Sc. in Computer Science and Telecommunication from the university of Mohammed V Agdal, Rabat, Morocco, in 2003. He obtained his Ph.D. in Computer Science and Engineering at ENSIAS, Rabat, Morocco. He is currently an Associate Professor of Computer Science in the Polydisciplinary Faculty, Sultan Moulay Slimane University, Morocco. His areas of interest are Information Coding Theory, Cryptography, and Security.

Said Safi received his B.Sc. degree in Electronics from Cadi Ayyad University, Marrakech, Morocco, in 1995. He obtained his M.Sc. and Ph.D. from Chouaib Doukkali University and Cadi Ayyad University in 1997 and 2002, respectively. He is currently a Professor of Science at the Multidisciplinary Faculty, Sultan Moulay Slimane University, Beni Mellal, Morocco. His general interests span the areas of communications and signal processing, estimation, time-series analysis and system identification. Safi has more than 160 publications. His research currently focuses on transmitter and receiver diversity techniques for single and multi-user fading communication channels and on broadband wireless communication systems.