2021 4th International Conference on Advanced Communication Technologies and Networking (CommNet) | 978-1-6654-0306-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/CommNet52204.2021.9641959

Blockchain-based Model Against selfish Attacks in Mobile ad hoc Networks

Nada Mouchfiq[1], Ahmed Habbani[1], Chaimae Benjbara[1], and Halim Berradi[1]

[1]SSLab , ENSIAS, Mohammed V University of Rabat , Morocco
Emails: {nada_mouchfiq, ahmed.habbani, chaimae_benjbara, halim_berradi}@um5.ac.ma.

***Abstract*—Over the past several decades, the importance of security has been increasing, in particular in the area of research addressing the Internet of Things (IoT) and, implicitly, ad hoc networks since they are part of it. Researchers have adopted blockchain as an interesting and trendy research topic in the wireless ad hoc environment. Due to its strong characteristics, such as consensus, immutability, finality and provenance, it's used not only as a secure data storage for critical data, but also as a platform that facilitates trustless data exchange between independent parties. However, the main challenge of applying blockchain in an ad hoc network is what kind of nodes should be involved in the validation process and how to adopt the heavy computational complexity of block validation in an appropriate way while maintaining its authentic characteristics. In this paper, we propose a new blockchain-based model against selfish attacks in ad hoc networks and optimize it in this context, to this end, we investigate the presence of MPR nodes to adapt and integrate the blockchain principle in MANETs and based on this we conduct a security analysis to evaluate our model by discussing the ability of our model to meet major security issues related to confidentiality, integrity, availability, non-repudiation, and vulnerability to attacks.**

***Index Terms*—Security, MPR, Blockchain, IoT, Ad hoc networks, selfish attacks.**

I. Introduction

The notion of the digital environment is a fundamental aspect of society because humans and the digital environment are strongly associated, which drives the progress and enhancement of typical [1], relevant, and time-consuming methodologies and approaches to the environment. We now live in a world where infrastructure and large flows of information are indispensable features of contemporary life. The rapid growth of online services, from social media to e-commerce to e-collaboration, has come to structure our daily lives in ways that were inconceivable just ten years ago. To cope with technological advancements, research trends and concepts are thus centered on the intelligent environment.

The concept of the Internet of Things has evolved into an overarching term for a variety of technologies designed to improve the effectiveness of future cities and the lives of their citizens, not only by introducing novel applications, but also by introducing smartness to existing processes that make life softer and more peaceful for those individuals. It has become trendy to actually debate IOT, and several countries are attempting to develop it (Fig. 1).

978-1-6654-0306-1/21/$31.00 ©2021 IEEE

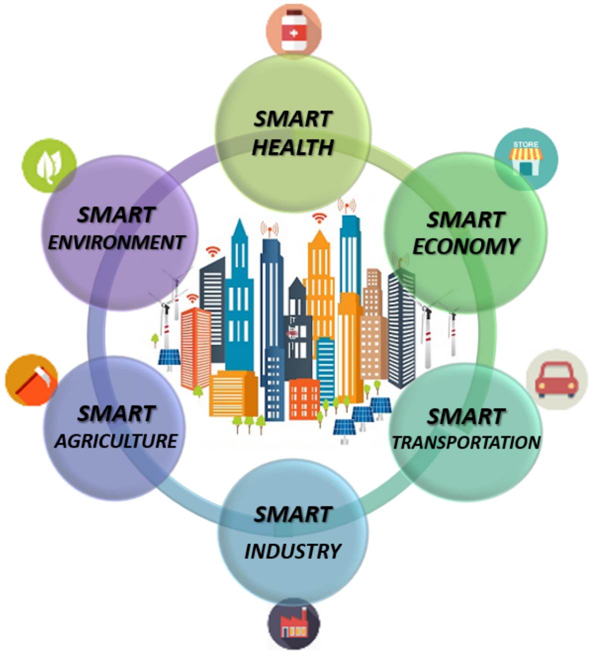

Fig. 1. IoT components.

An ad hoc network is a type of decentralised wireless network that does not rely on any predefined infrastructure, such as routers or access points [2] . In ad hoc networks, every node participates in routing by forwarding data to other nodes, and the choice of which node will forward the data is made dynamically using the connectivity of the network in conformity with the routing algorithm being implemented.

Several approaches have been proposed for connecting mobile ad hoc networks to the Internet. Because mobile ad hoc network nodes use IP addresses to define their routing, it might be appropriate to consider using these IPs to route a packet over the Internet.

Our team works on improving the performance of ad hoc networks (MANET ”Mobile Ad hoc Networks”, VANET ”Vehicular Ad hoc Networks”, FANET ”Flying Ad hoc Networks”, ...). Since ad hoc networks could integrate the new IoT technology, we will be able to take advantage of this type of network to improve ours.

The mobile ad-hoc networks (MANETs) are a system of mobile nodes connected with each other through wireless links without infrastructure maintenance. They are a tangible example of smart environments and also have multiple application domains (Fig. 2), as a set of wireless mobile nodes capable of communicating without pre-existing infrastructure. Each node forming this type of network contributes to the routing procedure [3].

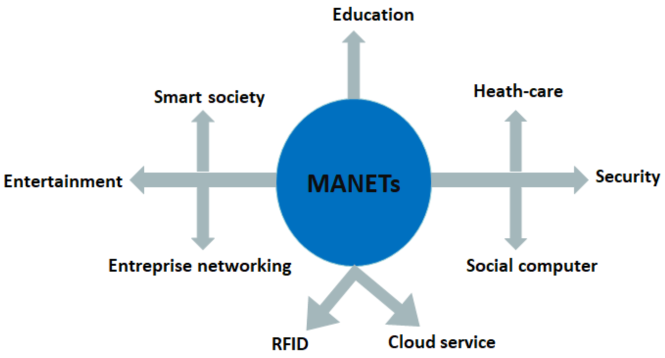

Fig. 2. MANETs application domains.

A. Motivation and Background

The decentralized nature of MANETs and the fact that they allow users to connect and trade information regardless of their geographical location or adjacency to the infrastructure makes them more flexible and robust and broadens their domains use [4] .

MANETs are defined as stand-alone systems that are configured using different devices without infrastructure and who or access point such as mobile phones . On the other hand, [5] MANET networks can face several challenges including :

- Energy constraint.
- Constraint of absence of fixed limits.
- Lack of protection against external signals.
- Routing constraint with the dynamics of the network topology.
- Constraint related to variation of link and device capabilities.
- Security.

MANETs are essentially identified by their active behavior , restricted frequency range, and the fact that they use low-power equipements, restricted processors, involved protocols, and restricted security. It has become necessary to improve the security side of MANET networks [6] .

The security solution must give full insurance spanning the whole protocol pile . There is no sole system that can arrange all the security sides in MANETs.

- Confidentiality : Ensure that data packets and configuration parameter information are not accessed or appropriated to an attacker or disclosed to unknown entities.
- Integrity : ensure that the packets exchanged (or stored) have not been modified in an unauthorized manner (ensure that the data is not modified by unauthorized agents).
- Availibility : Ensure that the packets exchanged are always available and that devices and agents are not prevented from having access to the information.
- Authentication : Authentication makes it possible to decide if a person is really what he claims to be in terms of information security by following an identity authentication procedure by checking the identification information presented compared to that stored.
- Non-Repudiation : Ensure that any person or any other entity engaged in communication by computer, cannot deny having received or sent a message.
- Access control : refers to the selective restriction of access to a place or other resource or network, while access management describes the process. The act of access can manifest itself as consumption, access or use; the operation of accessing a resource is called authorisation and in this process, two analogous access control mechanisms are locks and login identifiers.

The dynamic appearance of MANETs makes them vulnerable to multiple attacks, so many threats can harm the MANETs networks. Security should be taken into account at the early stage of design of basic networking mechanisms. In our study, we have identified the security threats in each layer. In the following list, we can find various attacks in each of the 5 layers in the MANETs :

- Application Layer :
  - Repudiation.
  - Malicious code.
- Transport Layer :
  - Session Hijacking.
  - SYN flooding.
- Network Layer :
  - Blackhole, Grayhole, Wormhole...
  - Message altering.
  - Routing attacks.
- Data Link Layer :
  - Jamming.
  - Selfish misbehaviour of nodes.
  - Malicious behaviour of nodes Traffic Analysis.
- Physical Layer :
  - Eaverdropping.
  - Active interference.

The remainder of this article is structured as follows. The second section introduces related works, and the third section describes the proposed approach for adapting blockchain principles to the context of mobile ad hoc networks. The discussion conducted in the fourth section includes a security analysis, our model potential performance against selfish attacks and an evaluation for the solution as a work in progress. And finally the paper is concluded in the section V.

II. Related Works

Several approaches and propositions have been put forward to deal with the security challenge in IoT and mobile ad hoc networks in various ways. The authors of [7] have designed a FLEAM (federated learning empowered and attackercentric architecture) consisting of monitoring, detection, analysis and filtering modules. The analysis module performs local learning combined with global learning to generate collaborative detection and intelligence information and actionable intelligence data in close proximity to the attackers.

The authors of [8] provide a two-layer IP hopping based MTD approach for enhancing the security of the MANET terminal device by using a combination of data encryption technology, the MANET terminal implementation offers three levels of network security : anti-intrusion in a normal environment, intrusion detection in an offending environment, and anti-eavesdropping in a threatening environment.

The authors of [9] have designed a federated learning based anomaly detection system for accurate identification and classification of attacks in IoT networks. The FL implementation part of the proposed approach of the suggested approach shares computational power with on-device learning and different layers of UGRs ensure higher degrees of accuracy in attack classification. The performance of the approach the approach is further improved by the ensembler that combines predictions from different layers of GRUs and enhances the confidentiality of IoT devices.

Recently with the increasing preponderance of integrated intelligent systems, the apparition of the notion of IOT, and the crucial importance of the some applications (such as surveillance, eHealth, network control, traffic control , emergency ...) reliable security is required as vulnerabilities are becoming more and more intense, hence the need to increase the level of network security to protect against possible attacks. And it is in this context that blockchain technology has emerged in recent years in order to benefit from the high level of security it offers to the network in which it is integrated , and as a part of the IOT environnement [10] , ad hoc networks have not been excluded from this evolution and have gained from the advantages provided by the blockchain. The blockchain technology [11] was conceived by Satoshi Nakamoto in 2008 , the first time use of this technology was in the banking and finance sector to support digital transactions and, provide access to the distributed ledger in a secure and trusted way. It was implemented as the main component of Bitcoin, where it serves as the public register for all transactions on the network.

A blockchain is a chain of blocks which contain specific information (database). In the case of the assigned network of blockchain , every contributor in the network manages, approves, and restores new accesses.All connected networks have a blockchain copy in stock. Due to the obvious high degree of security and accuracy, blockchain has been spread in various scenarios of functions and is recognized as one of the main approaches to evolving the world's evolution.Since the blockchain technology provides transparency, trustless, and secure transactions in the decentralized network, which helps in attaining robust and auditable records of all transactions, it is recently applied to different scenarios for Internet of Things (IoT) and especially Mobile Adhoc Networks (MANETs).

The integration of this technology into IoT environments and ad hoc networks has been the subject of interest for several researchers.For example,in the authors of [12] propose a lightweight architecture and the associated protocols for consortium blockchain-based identity management to address privacy, security, and scalability issues in a centralized system for IoT. Besides, they implement a proof-of-concept prototype and evaluate our approach. They evaluate their work by measuring the latency and throughput of the transactions while using different query actions and payload sizes, and they compared it to other similar works.

The approach proposed by [13] consists of integrating a lightweight blockchain architecture dedicated to IoT by eliminating the overhead expenses of the current blockchain while providing the security and the confidentiality as a solution, since the blockchain principle necessitates a high calculating capacity and a high calculating time. To do this, the author proposed a blockchain architecture with a centralized node to optimize the efficiency of the batteries and distributed approvals to reduce processing time and block checking, in addition to the implementation of functional blocks guaranteeing security and confidentiality.

The authors of [14] propose a decentralised attribute-based access control model with a complementary trust and reputation system (TRS) for IoT authorisation, which allows the trust and reputation values of each node in the network to be determined incrementally; the proposed system also integrates scores into the access control mechanism to achieve dynamic and fluid access control. They designed their system to run on a public blockchain, but separated the storage of sensitive information, such as user attributes, onto private sidechains to preserve confidentiality.

III. Proposed Model

Blockchain technology is made up of several technologies, including cryptography, math, consensus algorithms, and economic models. It is a safe, shared, and distributed ledger (database) that records all transactional data in the form of blocks. To solve the problem of distributed data synchronization, the blockchain employs peer-to-peer networks and consensus mechanisms, eliminating the need for a centralized trusted authority.

Each block can be recognized by a cryptographic hash algorithm on the header of the block. Generally, the block is composed of two parts :

- The body : contains the main transaction data.

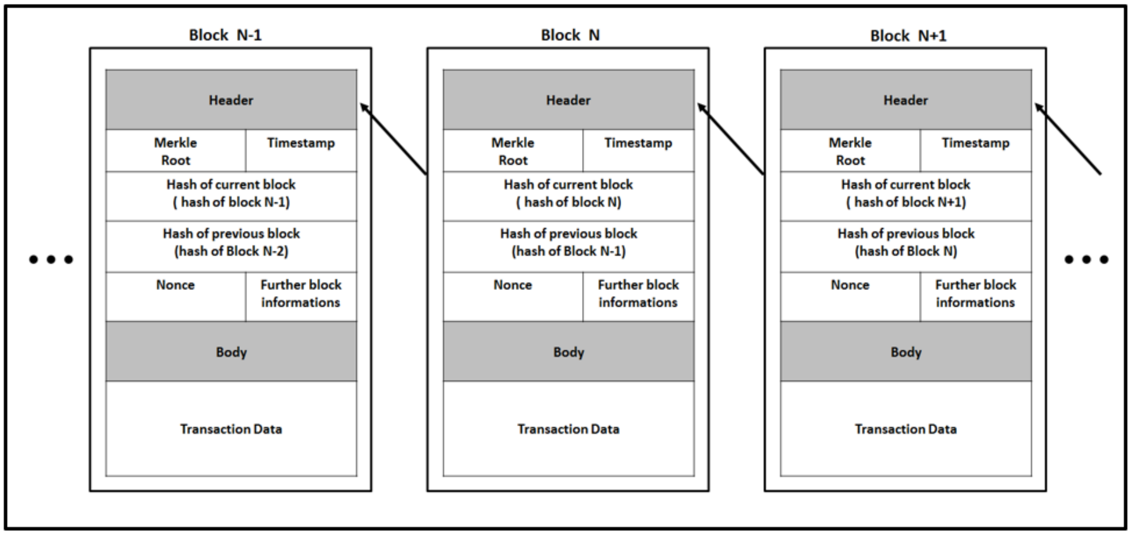
Block N-1
Block N
Block N+1
Header
Merkle Root
Timestamp
Hash of current block (hash of block N-1)
Hash of previous block (hash of Block N-2)
Nonce
Further block informations
Body
Transaction Data
Header
Merkle Root
Timestamp
Hash of current block (hash of block N)
Hash of previous block (hash of Block N-1)
Nonce
Further block informations
Body
Transaction Data
Header
Merkle Root
Timestamp
Hash of current block (hash of block N+1)
Hash of previous block (hash of Block N)
Nonce
Further block informations
Body
Transaction Data
• • •
• • •

Fig. 3. Block structure in blockchain.

- The header : includes a hash of the previous and current block, Merkle Root [15], timestamp, nonce, and further block information as shown in (Fig. 3).

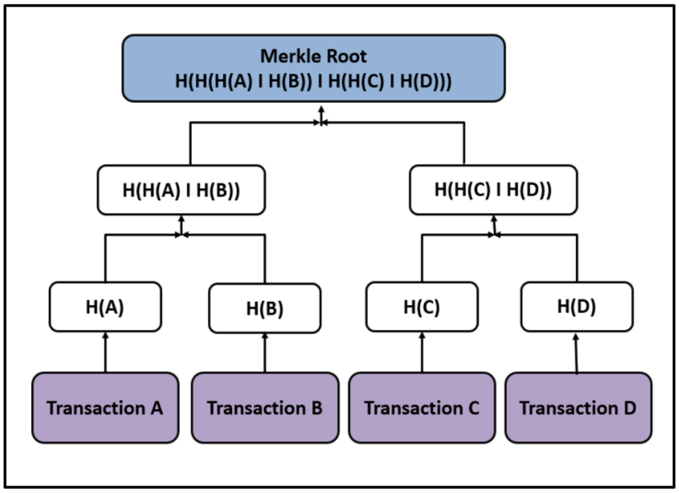

Fig. 4. Merkle tree structure.

Ralph Merkle presented the Merkle tree in 1979. It is a useful tree structure for a variety of applications, particularly cryptography. Throughout the history of computers, Merkle trees have been a critical component of data verification. Their structure aids in the verification of data consistency. Its architecture greatly helps in the acceleration of security authentication in big data applications. [16] It's a full binary tree, and each node is destined to hash the value from its leaf nodes. The Merkle tree structure is illustrated in (Fig. 4).

Each block in the blockchain has a Merkle root stored in the block header, as shown in (Fig .5). The Merkle tree enables every node on the network to validate individual transactions without downloading and confirming the entire block. If a copy of a block in the blockchain networks has the same Merkle root as another, the transactions in that block are identical. Because of the properties of the hash, even a small amount of incorrect data would result in vastly different Merkle roots. As a result, there is no need to verify the amount of required information.

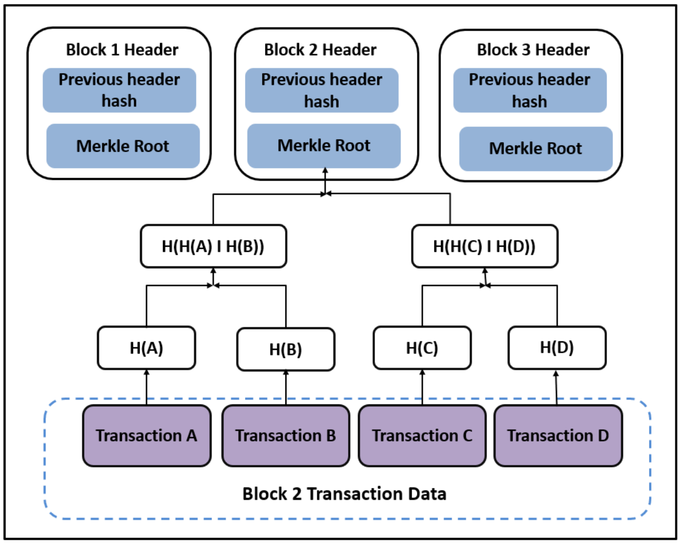

Fig. 5. Merkle tree structure in blockchain.

Based on the blockchain principle, we propose a model for preventing selfish attacks in MANETs. Our solution employs its fundamental principles and makes modifications to overcome these challenges and support in the mitigation of selfish attacks in mobile ad hoc networks.

The phenomenon of technology and data infrastructure, as well as vast amounts of data flows, have proven to be critical in determining the process of recent life. IoT will connect a variety of intelligent devices in the coming years.

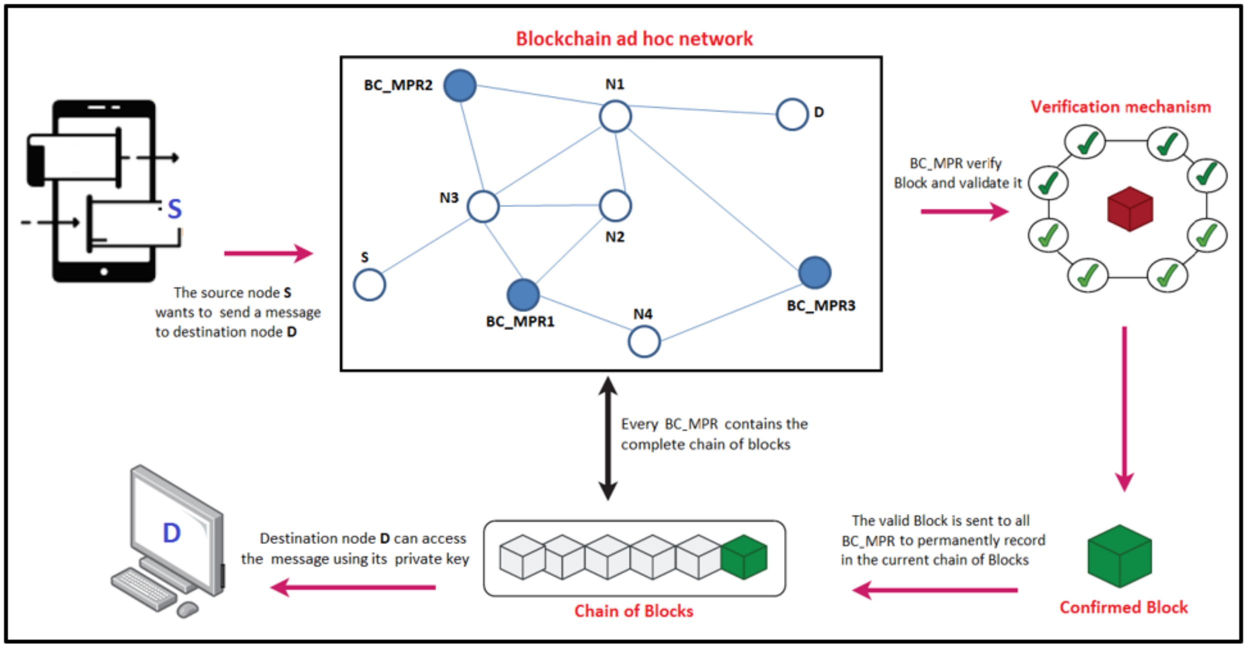
Blockchain ad hoc network
BC_MPR2
N1
D
N3
N2
S
BC_MPR1
N4
BC_MPR3
S
The source node S wants to send a message to destination node D
BC_MPR verify Block and validate it
Verification mechanism
Every BC_MPR contains the complete chain of blocks
D
Destination node D can access the message using its private key
Chain of Blocks
The valid Block is sent to all BC_MPR to permanently record in the current chain of Blocks
Confirmed Block

Fig. 6. Our proposed Blockchain-based model.

Many approaches for connecting mobile ad hoc networks to the Internet have been proposed. Given that mobile ad hoc network nodes have IP addresses for routing purposes, it comes down to the fact that those IP addresses can be used to route a packet over the Internet.

As a team, we specialize in ad hoc networks, particularly mobile ad hoc networks (MANETs), which are wireless networks with mobile elements that have no infrastructure and deliver configuration on a continuous basis. Each MANETs component can easily manage within the network and must always have traffic associated with its application, which is often what gives the MANETs the special ability to operate both as a router and as a host.

When compared to a traditional flooding mechanism in which each node forwards each message when it receives the first copy, the MPR (MultiPoint Relay) technique allows for a reduction in message overhead.

Only nodes designated as MPRs can generate link status information. Control messages TC are sent to nodes that have been designated as MPR by one or more neighboring nodes. As a result, a node informs the network that it is capable of reaching the nodes that have elected it as MPR.

These specific nodes are in charge of optimizing TC messages. Interaction between the source (S) and thus the destination (D) is provided by intermediate nodes (N), which select relay points among themselves and establish several properties such as energy state, node stability, and the view of developing control messages along the network in an optimized manner.

Our team is aiming to improve MANET protocols by developing solutions to address the issues that this type of network presents. Among the completed work, some examine the optimization of MPR selection based on various parameters, such as mobility quantification and minimizing broadcast redundancy, as well as improving communication and security in these networks [17,18,19,20,21,22].

According to our research, new security methods have been deployed in various networks, such as the blockchain in IoT that we described in our article. As a result, it has been recommended to test the impact of the blockchain security principle in ad hoc networks on the level of security that our MANETs network will provide. To ensure the continuity of teamwork and, in particular, to ensure network security using the improved protocols developed by our team, we introduce a method of security that is more suitable to our needs. This method is based on the principle of Blockchain hoc networks to determine its impact on the level of security that it will provide to our MANETs network.

The MPR is the verificator (validator) in our ”MPR Blockchain” solution to integrating blockchain in a MANETs network. The MPR is nominated by the nodes (N) that make up its neighborhood, each of which is furnished with a blockchain security algorithm. BC_MPR is the name we gave it based on our solution.

Our proposed model allows to detect malicious nodes after the verification phase and isolate them by adding them to a blacklist whose update will be broadcasted, our approach also offers an alternative of sending the data via another path that will also undergo the verification process before reaching the destination. Our model operates, as shown in the figures above (Fig. 6) and (Fig. 7) :

- A message is sent from the source node S to the destination node D through a path.
- Node S sends the packet to a peer-to-peer network of

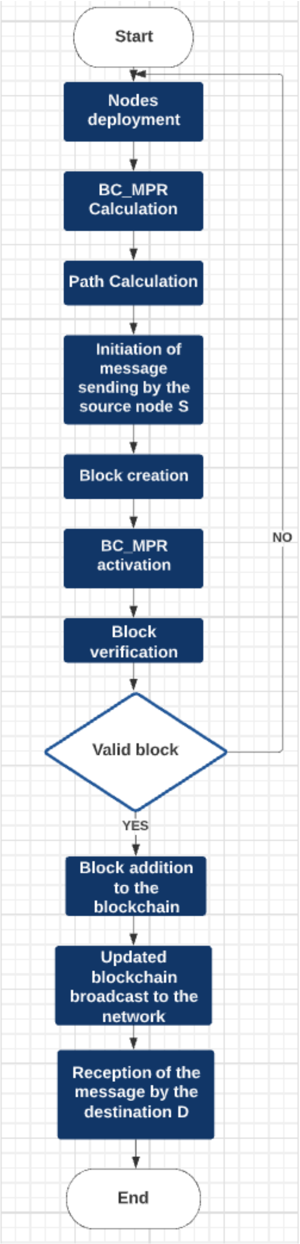
Start
Nodes deployment
BC_MPR Calculation
Path Calculation
Initiation of message sending by the source node S
Block creation
BC_MPR activation
Block verification
Valid block
NO
YES
Block addition to the blockchain
Updated blockchain broadcast to the network
Reception of the message by the destination D
End

Fig. 7. Flowchart of our proposed model.

nodes, which are high-level processing machines. On this network, blockchain protocols are used.

- The blockchain network's BC_MPR nodes broadcast it throughout the network. A block is created when a number of transactions are combined by the nodes.
- Only if a target hash code is created do all BC_MPRs add the block to the existing chain of confirmed blocks. The consensus mechanism is a method that varies in terms of computational cost and turnaround time.
- In the case where the block verification is not favorable, our solution follows the flowchart in (Fig. 8).
- Finally, using its private key, destination node D can access the message.

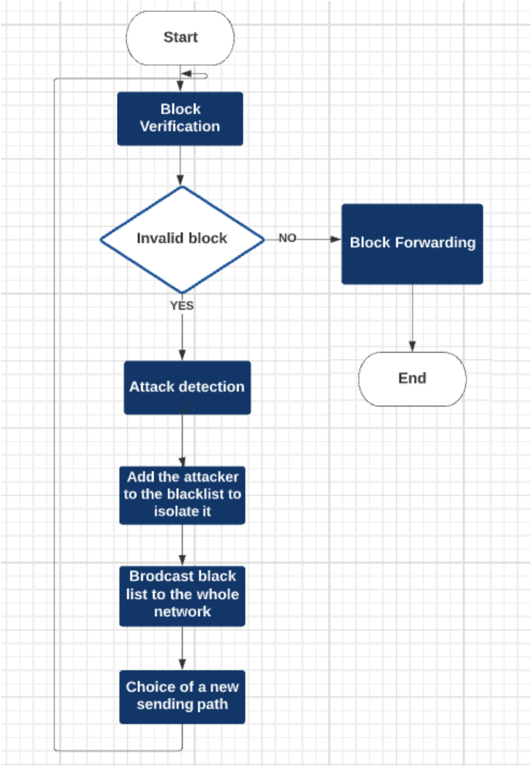
Start
Block Verification
Invalid block
NO
Block Forwarding
End
YES
Attack detection
Add the attacker to the blacklist to isolate it
Brodcast black list to the whole network
Choice of a new sending path

Fig. 8. Flowchart of attack detection according to our model.

IV. Discussion

A. Security Analysis

Every security system is designed to meet three main requirements, namely Confidentiality, Integrity, and Availability, abbreviated as CIA [23]. Confidentiality ensures that only authorized users can access the message. The message's integrity ensures that it reaches at its destination without modification or changes, and availability ensures that each service or data is available to the user when required.

1) Security criteria verification: The proposed blockchain-based model for ad hoc network device communications provides a robust and secure model for inter-device communication. This model also offers flexibility because any device that desires to communicate with another device can do so. Table I summarizes how our proposed scheme satisfy the security requirements mentioned below :

Confidentiality : Our blockchain-based model provides it through asymmetric cryptography, in which the receiving node generates an asymmetric key pair : a public key that is broadcasted to all users and a private key that the receiver keeps secret. The unique feature of this key pair is that each message encrypted with the public key can only be decrypted with the corresponding private key. As a result, messages encrypted with a receiver's public key are secure. Of course, the corresponding private key cannot be calculated from the corresponding public key. Furthermore, blockchain

TABLE I
SECURITY ANALYSIS.

Security requirement	*Applied mechanism*
Confidentiality	Accomplished through the use of encryption
Integrity	Hashing mechanisms are used to ensure the integrity
Availability	Accomplished by restricting the transactions that are validated by the verificator nodes.
Non-repudiation	The sender will not be able to deny having sent the message in the future since he is the only one who can generate the digital signature with his secret private key.
Authorization	Realised by making use of a policy header and shared keys.

transparency would enable viewing of all valid timestamped transactions while maintaining confidentiality.

Availability : According to our model, the incorporation of the blockchain ensures the high availability of transaction data that is stored. With thousands of nodes in a P2P blockchain network, transaction data is replicated and updated on each node. Even if one of the nodes leaves the network unintentionally, voluntarily, or otherwise becomes inaccessible, the network as a whole will continue to function. This ensures that the blockchain system is always available.

Non repudiation : Nodes in the blockchain network cannot deny an action or transaction that they have performed. This is useful because network members cannot deny that a specific set of data was not received or sent because all transactions are made available to all network members once they occur. In fact, a digital signature uses a cryptographic algorithm to confirm the validity of a data item. It is also a system for ensuring that a specific data element has not been changed. A digital signature scheme is made up of three basic components. The first component is the key generation algorithm, which generates two keys : one used for signing messages and kept private, known as the private key, and the other made publicly accessible, known as the public key, which is used to validate whether the message has the signature executed with the corresponding private key. The signature algorithm is the second core part. Using the provided private key, it generates a signature on the approved input message. The verification algorithm is the third essential component. It takes as inputs a signature, a message, and a public key, and approves the message signature using the public key. In this case, the sender cannot deny sending the message in the future because he is the only one who can generate the digital signature using his secret private key.

Integrity : Because data modification, addition, and deletion are not permitted in distributed systems, blockchain technology preserves the integrity and immutability of data. As a result, all participants can view the data history at any time. Furthermore, the data stored in the network is protected by cryptographic mechanisms. The hash function exists to ensure the integrity of data. The hash code is computed and stored at the start. This code is later recalculated and compared to the previously saved one. If the two values are identical, the data has not been altered; if they are not, the data has been changed. The integrity of the data is well maintained thanks to the use of blockchain. Once the data has been recorded in the blockchain, it is extremely difficult for anyone to tamper with it and change it. The fact that changing data in the blockchain is extremely difficult, if not impossible, is a significant advantage.

2) Our model potential performance against selfish attacks : DDos as an example : In this section, we evaluate the potential performance of our proposed model against selfish attacks, specifically DDos attacks (blackhole attack, wormhole attack, greyhole attack, Byzantine attack ...).

A mobile ad hoc network (MANET) is a spontaneous network that can be set up without a predefined infrastructure or topology. As a result, all of its nodes are routers and participate in route discovery and maintenance. Each MANETs component can easily manage within the network and must always have traffic associated with its application, which is often what gives the MANETs the unique ability to operate both as a router and as a host. Ad hoc networks have a wide range of applications in the military, commercial, health, agriculture, and other fields. They are especially useful in situations where installing an infrastructure network is not conceivable, where the network's purpose is too temporary, or even where the existing infrastructure network has been destroyed.

These networks' communication must be able to overcome the new challenges of an ad hoc network, such as node mobility, limited power supply, quality of service, bandwidth issues, topology changes, and security concerns. These challenges impose new requirements on MANET routing protocols, making them more vulnerable to attacks. There are numerous solutions that address attacks and provide some level of security in wireless networks, but these solutions are not always suitable for this environment, especially because the vulnerabilities that these networks can face are proportional to the evolution and importance of the domains using ad hoc networks.

We investigate the effectiveness of our solution in preventing a critical security attack, which is especially relevant for mobile ad hoc networks. It's a distributed denial of service (DDOS) attack [24] in which the attacker uses multiple malicious devices to overwhelm a specific target node. Several recent attacks that used devices to launch massive DDoS attacks have come to light.

The DDoS attacker has hundreds or thousands of useless packets flooding the victim's resources in order to make the network busy or disabled. The network's performance will suffer as a result, and it will be unable to perform its function. As a result, it is no longer able to provide services to legitimate nodes.

According to our research and the literature review we conducted in a previous section, we observed that new security approaches are being applied in order to ensure confidentiality, control access, or detect attacks, and while there is no doubt that ensuring these criteria is very important for smart networks, they are still insufficient because with the domains of application of the MANETs, than the need to provide more security criteria, in this case, the insufficient As a result, there is a need for a cooperative approach that ensures a higher level of security by allowing messages to be verified by special nodes, detecting attacks, ensuring an alternate route for sending packets so that the information reaches the destination, and isolating the node(s) responsible so that they do not affect future transmissions.

Our proposed solution offers hierarchical protection against these attacks. The first level of security can be attributed to the fact that an attacker would be unable to directly install malware on the devices because they are not directly accessible. At least one BC_MPR must verify all transactions. Assume for a moment that the attacker is still successful in infecting the devices. The second layer of security requires the validator to authorize all outgoing traffic by examining the policy header. The requests that constitute the DDoS attack traffic would be blocked because they were not authorized. As a result, any attempt at transaction falsification is only possible if the private key is known. Furthermore, because all blocks are chained together, the attacker cannot attack a specific block. If the verification is favorable, the packet is validated and continues on its way to the destination; if it is unfavourable, the nodes responsible for the attack are isolated and added to a black list that is broadcasted throughout the network, and the packet is sent via a new path that will go through the same verification process in order to validate the transmission.

B. *Evaluation of our model performance*

We decided to evaluate our model using two criteria : security criteria analysis and simulation-based performance analysis. We detailed our approach and evaluated the security criteria part in this paper, and we are currently developing the simulation part with NS3 to check the performances and also the security analysis we conducted in this paper.

We would like to underline that the simulation of our approach is currently in progress; we have implemented the blockchain part in our ad hoc network, and we are currently working on the attack part, with which we will test our approach in order to obtain results and compare them to those that already exist.

The proposed scheme's performance is evaluated using the NS-3 simulator [25]. Because the implementation stack in NS-3 is similar to a real implementation, it is expected that the modeled scenario will also work well in a real environment. It is reasonable to expect that the simulated scenario will also work properly in a real-world setting.

Furthermore, the simulator includes implementations of the majority of routing protocols used in MANETs and IoT environments in general. As a result, we used this simulator to test the proposed scheme's performance.

The metrics offered to evaluate the performance of our proposal presented below, In our simulation, we will observe these main metrics :

- Energy cost.
- Throughput : the time average of the number of bits that can be transmitted by each node to its destination.
- Delay (Latency) : the time it takes for a packet to be transmitted from the source to the destination.
- Packet Delivery Ratio : the ratio between the number of packets transmitted and the number of packets received.
- Lost Packets : the number of packets that have not been successfully transmitted.

V. Conclusion

IoT security has been the subject of much interest recently, both within the academic world and in industry. However, the existing security solutions are not necessarily adapted to the IoT nor to the MANETs network as long as they are part of the IoT context, due to the fact that the threats are evolving as much as the technology. In this article, we presented the description of IoT, we discussed mobile ad hoc networks architecture and infrastructure, and therefore the security of MANETs by mentioning security measures. We also revealed the work already wiped out the world of network security , after that we introduced blockchain technology then introduced our proposed model. We have also provided a comprehensive analysis to evaluate our solution and discuss its key properties to meet major security concerns related to confidentiality, integrity, availability, non-repudiation, and to selfish attacks. and then we introduced our current work whose purpose is evaluating the performance efficiency of our solution via simulation results.

References

[1] Z. Lv, L. Qiao, A. Kumar Sing, et al.,"AI-empowered IoT security for smart cities," *ACM Trans. on Internet Technol.* , 2021 , vol. 21, no 4, pp. 1-21.

[2] V. G. Menon, " A Comprehensive Survey on Opportunistic Routing Protocols for MANETs: Issues, Challenges and Future Directions," 2019, arXiv:201907.0239.v1.

[3] Quy, V.K., Nam, V.H., Linh, D.M. et al., " A Survey of QoS-aware Routing Protocols for the MANET-WSN Convergence Scenarios in IoT Networks," *Wireless Pers. Commun.*,2021, pp. 49–62 .

[4] A. Albeshri, " An Image Hashing-Based Authentication and Secure Group Communication Scheme for IoT-Enabled MANETs," *Future Internet* , 2021, vol. 13, no 7, pp. 166 .

[5] N. Mouchfiq, A. Habbani, C. Benjbara, " Security Issues in MANETs: A Survey," in *Proc. 5th Int. Congress on Inf. and Commun. Technol. (ICICT 2020).* Advances in Intelligent Systems and Computing , 2021, vol 1184 , pp. 288-295.

[6] N. Mouchfiq, C. Benjbara, A. Habbani, " Security in MANETs: The Blockchain Issue," in *Int. Conf. on Advanced Commun. Systems and Inf. Security* , 2019, pp. 219-232 .

[7] LI. Jianhua, LYU. Lingjuan, LIU. Ximeng, et al.," FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT," *IEEE Trans on Ind. Inform.* , 2021.

[8] P. Wang, M. Zhou, and Z. Ding., "A TwoLayer IP Hopping-Based Moving Target Defense Approach to Enhancing the Security of Mobile Ad-Hoc Networks," *Sensors* , 2021 , vol. 21, no 7, pp. 2355 .

[9] V. Mothukuri, P. Khare, R. M. Parizi, et al.," Federated Learning-based Anomaly Detection for IoT Security Attacks," *IEEE Internet of Things J.* , 2021.

[10] M. Abdelhafidh, et al. ”A Survey of Blockchain-Based Solutions for IoTs, VANETs, and FANETs,” Enabling Blockchain Technology for Secure Networking and Commun., *IGI Global* , 2021, pp. 110-148 .

[11] Nakamoto, Satoshi., ” Bitcoin: A peer-to-peer electronic cash system,”*Decentralized Bus. Rev.* 2008,pp. 21260.

[12] M. A. Bouras, Q. Lu, S. Dhelim, and H. Ning,” A Lightweight Blockchain-Based IoT Identity Management Approach,” *Future Internet 13* , no. 2 , pp. 24 , 2021.

[13] A. Dorri, S. S. Kanhere , and R. Jurdak, ” Towards an optimized blockchain for IoT,” in *IEEE/ACM Second Int. Conf. on Internet-of-Things Des. and Implementation* , 2017, pp. 173-178.

[14] G. D. Putra, V. Dedeoglu, S. S. Kanhere, et al., ” Trust-based Blockchain Authorization for IoT,” ‘*IEEE Trans. on Netw. and Service Manage.* , 2021.

[15] D. Mitra, L. Tauz, and L. Dolecek, ” Overcoming Data Availability Attacks in Blockchain Systems: LDPC Code Design for Coded Merkle Tree,”2021, arXiv:2108.13332.

[16] U. Chelladurai, S. Pandian, ” HARE: A new Hash-based Authenticated Reliable and Efficient Modified Merkle Tree Data Structure to Ensure Integrity of Data in the Healthcare Systems,” *J. of Ambient Intell. and Humanized Comput.* , pp. 1-15 , 2021.

[17] H. Berradi, A. Habbani, N. Mouchfiq, et al., ”Improvement of OLSR Protocol Using the Hello Message Scheme Based on Neighbors Mobility.” *J. Commun.* , vol. 15, no 7, pp. 551-557 , 2020.

[18] H. Berradi, A. Habbani, M. Souidi, F. Elmahdi and N. Mouchfiq., ”Optimize the QoS Metrics in Smart Mobile Communication using Multi-Objective Function.” in *3rd Int. Conf. on Adv. Commun. Technol. and Netw.* , 2020 , pp. 1-7 .

[19] C. Benjbara, N. Mouchfiq, and A. Habbani, ” Multipathing Communication in Heterogeneous Ad Hoc Network,” in Proc. *5th Int. Congr. on Inf. and Commun. Technol.* , 2021, pp. 270-278.

[20] F. El Mahdi, A. Habbani, N. Mouchfiq, et al., ” Study of security in MANETs and evaluation of network performance using ETX metric,” in Proc. *2017 Int. Conf. on Smart Digit. Environ.* ,2017, pp. 220-228.

[21] C. Benjbara, A. Habbani, F. El Mahdi, et al., ” Multi-path routing protocol in the smart digital environment,” in Proc. *2017 Int. Conf. on Smart Digit. Environ.*, 2017, pp. 14-18.

[22] N. Mouchfiq, A. Habbani, and C. Benjbara, ” SDN Based Security in Mobile Ad hoc Networks.” *J. of Advances in Comput. Netw.* , vol. 8, no. 1, pp. 31-35, 2020.

[23] I. K. Sahu , M. J. Nene , ” Model for IaaS Security Model: MISP Framework,” in *2021 Int. Conf. on Intell. Technol.*, 2021, pp. 1-6.

[24] N. Al-Bulushi, D. Al-Abri, M. Ould-Khaoua and A. Al-Maashri, ”On the Impact of Static and Mobile Wormhole Attacks on the Performance of MANETs with AODV and OSLR Routing Protocols,” in *15th IEEE Conf. on Ind. Electronics and Appl.*, 2020, pp. 1064-1069.

[25] Network simulator NS-3, Available : https://www.nsnam.org/