EasyChair Preprint

№ 13046

Problem of Integrating Blockchain Technologies into Wireless Mesh Networks: Application to Community Wireless Networks

Djotio Ndie Thomas and Dobe Abel

April 19, 2024

Problem of integrating Blockchain Technologies into Wireless Mesh Networks: Application to Community Wireless Networks

Thomas DJOTIO NDIÉ [1], Abel DOBE* [1]

[1] 1 National Advance School of Engineering Yaounde, University of Yaounde I/Cameroun,

{tdjotio, dobeabel}@gmail.com

Abstract. Wireless mesh networks (WMNs), because of their low installation costs compared to the network infrastructure, were seen as a relevant alternative to connect remote areas and poor regions where telephone companies have great apprehension to invest. However, WMNs have security vulnerabilities, including denial of service (DoS) and identity theft attacks. The most common methods for securing mesh networks are centralized systems, while WMNs are decentralized, open and flexible by design. The usual blockchain integration in WMNs is more oriented towards the construction of online payment platforms. This paper proposes BlockWMN, a model for integrating blockchain technology into WMNs with the ultimate goal of protecting them from the abovementioned attacks. Fundamentally, we address a consensus issue or a so-called "Byzantine Generals" or "Byzantine Fault Tolerance" (BFT) problem. Our approach uses the blockchain as a secure database to save the network graph and all the network nodes' credentials in real time. Each node has the ability to check in the blockchain all signaling information received from other nodes. Unlike other approaches, our solution is decentralized, open and flexible. The limits of our model are inherent to the nature of blockchains: high energy consumption for the calculation of the proof of work and memory space for the storage of blockchain information.

Keywords: BlockWMN, Wireless mesh networks, Wireless community network, blockchain, security.

Declarations

Conflict of Interest: Thomas DJOTIO NDIÉ declares that he has no conflict of interest. Abel DOBE declares that he has no conflict of interest.

1 Introduction

The virtual world offers new possibilities in the economy, health, and education, to name but a few. However, more than half (56%) of the world's population, the

majority of whom are from developing countries, still do not have access to internet coverage and therefore cannot benefit from the opportunities it offers [1].

Wireless mesh networks (WMNs) allow simplifying deployment and scalable coverage of the network. They are fault-tolerant and allow a significant reduction in initial installation and operating costs compared to other types of networks. With these advantages, WMNs would be the ideal solution for coverage of poor or sparsely populated areas not covered by the global network, allowing them to access the Internet at lower cost [2]. Despite all these advantages, very few WMNs are used by telecom operators. [3]. By construction, they are open and do not put a particular emphasis on security. Their operation is based on trust between members, which makes them vulnerable to several types of attacks due to the behavior of network users, such as denial of service (DoS) and identity theft [4].

In 2008, wanting to secure Bitcoin transactions, Satoshi Nakamoto opted for the total decentralization of the data to be processed. Thus, blockchain technology was born [5]. The consideration of security in network data processing depends on a mutual consensus among all network nodes. Several other decentralized applications that aim to ensure optimal security in the sharing of information within a network will be inspired by this technology. [6]. For example, the global architecture for domain name management and the associated domain name servers (DNS), which have been distributed and replicated in the Internet's "nodes" since the creation of ICANN (1998), have never failed [5]. How can the success of the blockchain be adapted to the security of WMN information? What factors should be taken into account to make WMNs more robust against the abovementioned vulnerabilities?

We propose BlockWMN, an approach to integrate blockchain technology into WMNs to reduce their vulnerability to the abovementioned attacks. BlockWMN uses the blockchain as a secure database to save in real time the network graph and all the network nodes' credentials. Fundamentally, we address a consensus issue or a so-called "Byzantine Generals" or "Byzantine Fault Tolerance" (BFT) problem. In our model, each node has the possibility to check in the blockchain all signaling information received from the other network nodes. Unlike other approaches, our model is decentralized, open and flexible. Its limits are inherent to the nature of the blockchains: high-energy consumption for the calculation of the proof of work and memory space for the storage of information of the blockchain.

The rest of this paper is organized as follows: in section 2, we present related works on securing WMNs with a focus on blockchain integration in WMNs. Section 3 presents our model of blockchain integration in a WMN. Section 4 presents an application of our model of integration in a wireless community network. Section 5 concludes and presents future works.

2 State of the art on securing WMNs

There are three WMN architectures: (1) **User mesh**, where each node acts as a router and repeater for its neighbours [7] [8]. (2) **Router mesh** where the meshing is done at the wireless router level. (3) **Hybrid mesh**, which combines both previous architectures. The router mesh ensures communication between mostly remote clients, as well as access to other types of networks. The client mesh ensures communication

between clients located in a restricted perimeter without going through the backbone formed by routers [7] [8] [9] [10].

All nodes are mobile and can therefore be connected dynamically and arbitrarily. They behave like routers and participate in the discovery and maintenance of routes to other network nodes. This avoids having access points that, in case of failure, isolate part of the network [11].

2.1 Wireless mesh network security

The basic security objectives for WMNs are the same as those for wired networks: confidentiality, integrity, availability, authentication and nonrepudiation of users [12].

They are vulnerable in their operations: a malicious node can compromise network operations at any layer: physical, MAC (medium access control), network, transport, or application. WMNs are exposed to attacks such as eavesdropping (or spying), interference and frequency jamming at the physical layer, selfishness at the MAC layer, or denial of service at the network layer [4].

2.2 Some of the security models proposed

Existing security models can be divided into two categories: centralized and decentralized models.

Centralized models are the most widely implemented [13]. They use the router or a user mesh node as a central server that (1) manages all authentication and validates transactions between nodes [18] and (2) observes and analyses network and/or node activities [4] [9] [14]. The vulnerability of this model is the central node, which acts as the server. In case of its failure, the whole network is affected.

Decentralized models do not have a central server node. All nodes are equal and have the same responsibilities for network functions. These security models are of two types: (1) supervised systems, where when a dedicated server admits new nodes, all other activities are performed collaboratively [13] [14]. (2) Autonomous systems where everything is done collaboratively and by consensus [13] [15] [16].

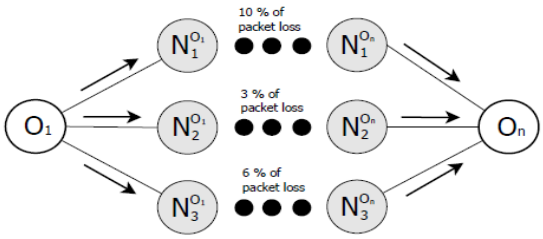
In terms of analysis and interrogation, autonomous decentralized security models are best suited for WMN operation. Here, security implementation is a challenge since (a) it is implemented by all network nodes; (b) if one node in the network is affected, the entire network is compromised; and (c) there is a lack of trust among the network nodes. The question is therefore how to deal with information whose source and transmission channel are questionable. This is the fundamental question of the so-called "Byzantine Generals" or "Byzantine Fault Tolerance" (BFT) problem [17] [35], which gave rise to the concept of the same name: BFT. It refers to systems in which there is trust through a consensus mechanism, despite the presence of a certain number of malicious nodes [19] [35]. There are several solutions for building a BFT system. Similarly, there are different approaches to enable a blockchain to achieve Byzantine fault tolerance, including consensus algorithms [36]. Several studies are being conducted on the integration of blockchain in WMNs, but they are more oriented towards the creation of platforms for securing goods exchange without intermediaries in WMNs [3].

2.3 Routing protocols for wireless mesh networks: case of BATMAN adv.

The reasons for our choice of the B.A.T.M.A.N.adv. (Better Approach To Mobile Ad hoc Network) protocol advanced [20] are because (a) it is developed for WMNs [11]; (b) it strictly follows a decentralized routing approach [21]; this corresponds to our goal of building a decentralized and cooperative security system that respects the basic principles of WMNs.

The approach proposed by B.A.T.M.A.N. is to choose the next hop on the most reliable route, i.e. the one with the least risk of packet loss, calculated based on the transmission quality (TQ) metric. Each node keeps a history of all the sequence numbers of all OGM (Originator Message) messages received from its neighbors. The neighbor with the most OGM sequence numbers of the recipient's OGMs in the routing table is considered the most reliable next hop. The disadvantages are (1) the rather slow reaction to changes in the network topology. If a link "breaks" between two nodes, the network has to wait until it receives the information on the topology change before it is notified of the problem; (2) massive exchanges of OGM signaling messages, which implies the memory needed to store the history of received messages [23] [24]. The information contained in an OGM can be summarized as follows [25]:

- Packet type: Initialize this field with the ELP packet type.
- Version: Set your internal compatibility version.
- TTL: Initialize with BATADV_TTL
- Flags: not used
- Sequence number: On the first broadcast, set the sequence number to an arbitrary value and increment the field by one for each following OGMv2.
- Originator Address: Set this field to the primary MAC address of this B.A.T.M.A.N. node.
- TVLV length: Length of the TLVL data appended to the OGM
- Throughput: Throughput metric value in 100 kbit/s. Initialize with BATADV_THROUGHPUT_MAX_VALUE
- TVLV data: Appended TVLV data for the originator.



(a) A wireless mesh network

Node	O_1	$N_1^{O_1}$	$N_2^{O_1}$	$N_3^{O_1}$	$N_1^{O_n}$	$N_2^{O_n}$	$N_3^{O_n}$
Broadcasted OGMs	100	-	-	-	-	-	-
Rebroadcasted OGMs	-	100	100	100	-	-	-
Received OGMs	-	-	-	-	90	**97**	94

(b) Transmission of an OGM generated by O_1

Originator	Next-hop	Potential next-hop
O_1	$N_2^{O_n}$	$N_3^{O_n}$

(c) Routing table from O_n

Fig. 1. B.A.T.M.A.N. diffusion diagram [26]

By its design, a B.A.T.M.A.N. adv node does not know the whole network topology. The topological view of a node is limited to a horizon of one hop. It receives packets from arbitrary sources and builds its routing table by analyzing the statistics of the messages received from the sender. It is susceptible to various poisoning attacks, as the network is made up of a mesh of non-authenticated and unreliable peers [26] [27]. A malicious host could send OGMs that announce the existence of nonexistent nodes, which could cause a routing overflow because it is the Originator that destroys the OGM and thus creates a denial of service [27]. An attacker can also manufacture OGM messages with the address of another existing node, such as Originator (here, the malicious node impersonates an existing node to generate an OGM), with valid sequence numbers that it has not actually received to manipulate the routing of other hosts and redirect the route to the destination to itself. In this way, a node can impersonate another node and thus usurp its identity [27].

The B.A.T.M.A. N protocol is therefore vulnerable to DoS, identity theft and route manipulation attacks. The solutions that are generally proposed for these attacks in WMNs are intrusion detection systems (IDSs) [22]. Their disadvantages are as follows: (1) they require memory and a powerful computing capacity to analyse the behaviour of neighbours [24], (2) they cannot trace the origin of an attack after detecting it (e.g., attacks by manufacturing fake OGMs), and (3) they cannot detect a poisoning attack due to a node in the network reporting false information on the behaviour of neighbouring nodes.

2.4 Blockchain technology: its security system

A blockchain is a registry where transactions carried out by members of a network are secured by cryptographic methods. They are recorded one after the other, and all users each have a copy with identical content; this makes it possible to reach a consensus between them for any exchange of messages [27] [28] [29]. This mode of operation gives them the confidence needed to carry out new transactions without the need for a third party to supervise them.

Blockchains can be classified into three types: public, private (authorized) and hybrid. (1) Public blockchains are open, distributed, and decentralized and allow anyone to view and confirm transactions [28] [29] [30]; (2) authorized blockchains are accessible only to preapproved parties, and all participants know each other [28] [29] [30]; and (3) hybrid blockchains are a combination of the first two types [30] [31].

Operation of a **blockchain**. As its name suggests, a blockchain is a chain of blocks, each containing several transactions, which will be entered into the blockchain by the nodes of the network. The implementation may differ from one blockchain to another, depending on the consensus algorithm. The main elements of a block comprise (1) an index to inform the position of the block in the chain; (2) a date to record the date the block was created; (3) the data to be stored in the block; (4) a hash to identify the block; and (5) the previousHash, which is the hash of the previous block.

A block to be valid must validate the following rules: (i) the index of the block must follow the index of the previous block; (ii) the previousHash matches the hash of the previous block; and (iii) the hash of the block is valid. If the result satisfies the

consensus, the block is added to the blockchain, and the miner is remunerated according to the network's remuneration policy.

Case of integration **of the blockchain in WMNs**. *The RightMesh platform* is a WMN platform using blockchain technology and tokens called RMESH. This platform provides each node with an Ethereum portfolio. Each participant in the network is paid in tokens for all the activities they perform on the network (data transfer, block mining, etc.). Nodes are thus encouraged to participate in network activities [3]. The blockchain on this platform is not used as a means of securing the network but as a means of securing payment transactions for services offered to other nodes (as a server) and for the purchase of services offered by other nodes (as a client). Payments are made by tokens [3].

The SmartMesh platform. SmartMesh is an Internet of Things protocol based on a blockchain. It extends the functionalities of network protocols to make micropayment in cryptography without the internet possible. [32].

We have noticed that most cases of blockchain integration in WMNs are made in the sense of developing online payment platforms. This is not in line with our goal of providing a blockchain integration model that offers better security against DoS and identity theft attacks. As WMNs are an open and decentralized type of network, the public blockchain model, which is also open and decentralized, is the most appropriate model for integration in a WMN.

3 Proposal of BlockWMN: a model for integrating a blockchain in a WMN

In this section, we propose BlockWMN, a model for a self-managed decentralized security system by integrating public blockchain technology into a WMN, to provide security as effectively as the IDS solutions presented in section 2.3 against DoS and identity theft attacks. To do this, we need to build a consensus algorithm that will allow us to validate the block data before integrating it into the blockchain (see section 2.4)

3.1 Blockchain Consensus Algorithm

A consensus algorithm is a function performed by a blockchain network to reach a consensus. The most common implementations are proof of participation (PoP) and proof of work (PoW), which are used by Bitcoin. The protocol prescribes the main rules of the system, and it is the consensus algorithm that defines how these rules will be followed to achieve consensus when verifying and validating the data blocks of the blockchain [17].

In the following, we describe BlockWMN, our consensus algorithm for integrating blockchain technology in a wireless mesh network.

3.2 Proposal of BlockWMN: a model that integrates blockchain technology.

In this subsection, we present different principles of BlockWMN. We model a WMN as a valued and oriented graph in which we deploy a public blockchain platform that will record the image of the WMN.

Modeling of the WMN. Let G= (X, U) be the graph representing a WMN, where "X" is the set of vertices of the graph representing network nodes and "U" is the set of arcs of the graph representing the wired or wireless links existing between network nodes. Let "u" belong to U; if u= (a, b) is an arc of G, then "a" and "b" are the start (source) and end (destination) points of "u", respectively. The arcs can be provided with a cost, capacity, etc. [33],[34]. Figure 2 graphically illustrates our modelling.

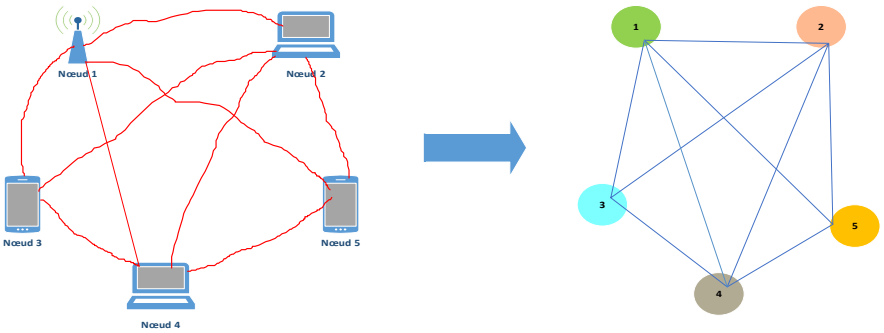


Figure 1**.** A wireless mesh network and its modelling

The role of the blockchain platform here in the model is to keep the graph image to secure the information exchanged in the network. Thus, we will record in our blockchain (1) all the WMN nodes, their types (router, gateway, computer, etc.) and the services they offer and (2) all the pairs of interconnected nodes (arc) with both the quality and the cost of the connection.

Main rules of BlockWMN. When integrating a new node:

Rule #1: When a new node is integrated, its MAC address and its public data encryption key provided by the node are recorded in the blockchain with the different services offered by this node in the list of network nodes (graph). Thus, if a node wants to communicate with another node, it can have access to the MAC address, the public key and all the information it needs about that node in the blockchain. Asymmetric cryptography allows a user to sign a transaction carried out on the public register of the blockchain and thus to certify that he is the author of the transaction. The term "asymmetric" comes from the nature of the information needed to encrypt the data: one part is private (the private key or decryption key, known only to the user), and another part is public (the public key or encryption key, known to the entire network). Each user has a private key and a public key [35].

Rule #2: Arcs from the new node to adjacent nodes must be included in the network arc list in the blockchain. The reverse arc is not automatically added.

Rule #3 (the addition of a new arc): the addition of a new arc (n_1, n_2) in the list of network arcs contained in the blockchain is done on the declaration of a node n_1 (source node) that declares to have direct access from another node n_2 (target node). This declaration is made on a trust basis, and it will be verified by each network node thanks to the consensus algorithm known by all nodes.

In case of withdrawal, suspension or exclusion of a node:

Rule #4 (withdrawal): If node n_1 (source node) declares that it no longer has direct access to another node n_2 (target node) to which it recently had access, upon declaration of n_1, arc (n_1, n_2) is removed from the set of network arcs contained in the blockchain after validation by the consensus algorithm.

Rule #5 (suspension): If a node n_1 is suspended from the network for any reason, this information will simply be added to the node information in all nodes of the network registered in the network block.

Rule #6 (Exclusion): If a node n_1 is excluded from the network for any reason, (1) this information will be added to the node information in the list, and (2) all arcs with node n_1 as the source or target will be removed from the network arc list.

BlockWMN Consensus algorithm. In the context of a blockchain, reaching a consensus ensures that all the nodes in the network agree on the same state of the blockchain and the data stored in it. In our case, we consider that the nodes' declarations are made based on trust ascertainable by this consensus algorithm. When a node n_1 declares that it can directly access node n_2:

```
If
   Node n2 exists in the list of network nodes registered in the
   blockchain and is not under suspension or exclusion
Then,
   Create the arc (n1, n2) and include it in the list of arcs in
   the graph representing the WMN contained in the blockchain
End if
```

Analysis of the **security flaws of the proposed model.** We compare the security flaws of our model in relation to identity theft and DoS attacks. The BlockWMN model allows us to observe our WMN as an oriented graph. Thus, we can take advantage of the mathematical calculations of graph theory to analyze our solution.

Illustration of an identity theft attack in the context of our model:

Step 1: A malicious node n_x has impersonated node n_1 and wants to carry out an attack on a neighboring node n_v.

Step 2: It sends a message to a neighboring node n_v with the identity of node n_1.

Step 3: The neighboring node n_v receives the message from the malicious node n_x.

Step 4: Node nv uses the oriented graph of the network in the blockchain to calculate the shortest path (n_1, n_v).

Step 5: The n_v node will check:

```
If
   The node nx that sent the message belongs to the path
   calculated in step 4.
Then,
```

n_v takes into account the message.
Else
n_v destroys the message.
End if

The conclusion of the simulation of an identity theft attack is that the attack cannot therefore thrive unless the node whose identity is being stolen has trusted the malicious node by declaring it to be a trusted node, resulting in the creation of the path (n_1, n_x).

Illustration of a DoS attack in the context of our model

Let n_x be a corrupted node in our WMN that wants to carry out a DoS attack. There are three possible scenarios:

(1) n_x is the server node and refuses to render the service: in this case, it is declared inaccessible in the graph and will be considered withdrawn; therefore, Rule 4 of our model, which deals with cases of withdrawal from the network, is applied to it. In this case, it will be considered withdrawn from the network and therefore will no longer be solicited, and the nodes will look for another server in the network that can provide the same service in the blockchain. The graph will be updated, and node n_x will no longer be part of it (see fig. 3.);

(2) n_x is not the server node and refuses to route messages: same treatment as in case (1);

(3) n_x is not the server node but wants to corrupt the information before routing it: it will not be able to do so because the information is encrypted with the receiver's public key that the sender may have had directly in the blockchain in the receiver node's information.

In conclusion, this DoS attack in our model cannot thrive because, as soon as a node is unavailable, it is declared withdrawn, and the other nodes will stop communicating with it.

We can conclude from the above analysis that our system offers security against identity theft and DoS attacks, to which ordinary WMNs are vulnerable because their operation is based on trust between nodes [27].

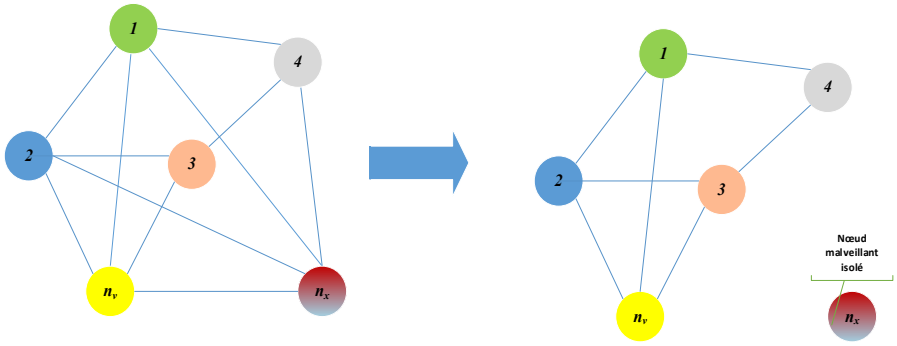


Figure 1**.** Isolating a node after a Denial of Service (DoS)

4 Application of the BlockWMN model to a wireless community network

In this section, we present the implementation of our model in a wireless community network. To this end, we use the B.A.T.M.A.N.adv routing protocol in which we applied the BlockWMN model as described above. We then analyze our model in relation to DoS and identity theft attacks.

4.1 Presentation of BATMAN Blkc: the proposed model.

Our model proposes to extend the B.A.T.M.A. N adv. Protocol to BATMAN blkc. by modifying the original format of the OGM based on the BlockWMN model. As we presented in section 2.3, to signal its presence, each network node that implements the B.A.T.M.A.N., protocol floods the network at a defined frequency with OGMs that allow other network nodes to define the best path to nodes that emitted the OGMs.

With the integration of the blockchain in the protocol, we will modify the behavior of B.A.T.M.A. N in OGM processing, at their creation, during their transmission and at their reception. As we presented above, nodes will no longer transmit OGMs by flooding after a certain fixed period. Instead, only each time there is an event (arrival of a new one, departure or suspension of an old adjacent node, etc.) or a variation (deterioration or improvement of the quality of the connection with adjacent nodes, new service proposed by a node, stop or suspension of a service proposed by a node, etc.) of its predefined environment.

During the production of an OGM, B.A.T.M.A. N only gives the address of the Originator (the one who created it). With our modification, the sequence number that informs about the number of OMGs already issued by the Originator is no longer necessary. We are going to replace it by the address of the second node (the arc target), which can be according to the case: the new node, the one that has left, was suspended or the one with which the connection rate with the arc source has varied. The flow rate filled in by the OGM is that of the last two nodes to have exchanged a given OGM. In the proposed model, the flow rate will inform about the quality of the connection between the new node and the Originator and will not be modified during the diffusion of the OGM. The flags that are not used by B.A.T.M.A. N will be used to inform the type of information (addition, deletion and suspension of a node; variation of a flow rate between two nodes, etc.

Thus, the OGM format of BATMAN blkc will take into account the arc that links the new node and the node to which it is connected (see fig. 4.

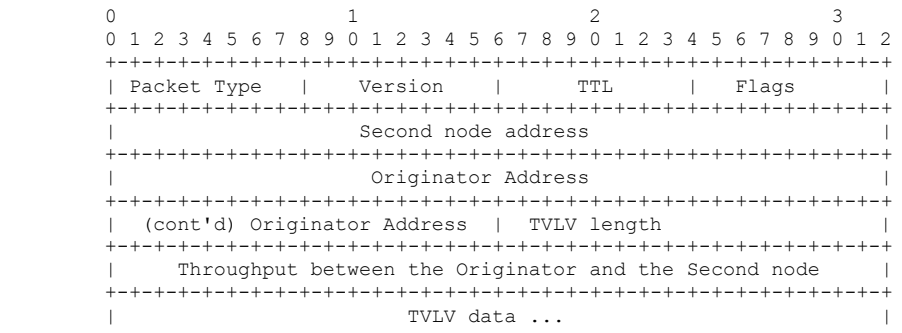


Fig. 1. Format of the modified OGM of BATMAN blkc.

On the reception of an OGM that announces the appearance of a new node or a new arc, the node to which the second node has connected sends the OGM to signal the arrival of a new node or the creation of a new arc in the network for which it vouches. The node that receives it will check in the blockchain

```
IF The second node is in the node list Then
    IF the reported arc is in the list of arcs Then
       it destroys the OGM
    Else
       the arc is added to the list of arcs
  End IF
Else
    the new node is added in the node list
    the new arc is added to the list of arcs
End IF
```

On receipt of an OGM announcing the suspension/deletion of a node, each node in contact with this node will issue an OGM to signal the suspension/deletion of its relationship with the suspended or gone node. The node receiving this OGM will check in the blockchain

```
IF The second node is in the node list Then
    IF the reported arc is in the list of arcs Then
           it deletes this arc in the list of arcs of the
    blockchain
    Else
        it destroys the OGM
    End IF
Else
    it destroys the OGM
End IF
```

On receipt of an OGM that signals the variation in quality/cost of the connection between two nodes, i.e. on an arc; an arc having a well-defined direction, in this case, it is the source node that will signal the variation of the flow rate in the direction of the arc. The node that receives this OGM will check in the blockchain

```
IF The second node is in the node list Then
```

```
    IF the reported arc is in the list of arcs Then
        It changes the value of the flow rate in the blockchain
        at the level of this bow
    Else
        It destroys the OGM
    End IF
Else
    It destroys the OGM
End IF
```

The OGM is transmitted to all the nodes of the network to update the network blockchain after validation by the other nodes.

4.2 Discussion and Analysis of BATMAN Blkc the proposed model.

The image of the network that can be calculated by all nodes from their copies of the network blockchain allows checking the existence of a node or an arc in the network and calculating the best path between two nodes. From the analysis of the security holes made in section 3.2, we can deduce that our model is not vulnerable to DoS and identity theft attacks, which are some of the weaknesses identified in WMNs running with the B.A.T.M.A. N protocol [4].

In addition, we can also see that our model produces OGMs just to signal events whereas in the B.A.T.M.A. N protocol, each node produces by a fixed period (by default every second) an OGM that floods the network and consumes the bandwidth [27].

The quality of the link between two nodes being recorded in the blockchain allows the node to calculate the cheapest path to another node in the network. This is not the case for the B.A.T.M.A. N protocol, which only knows the best neighbor for one to reach a remote node [26].

Despite all these advantages that our model offers, maintaining a blockchain requires considerable energy for the calculation of the proof of work [28][30] and storage space to save data for the network nodes [28], which is not the case for the B.A.T.M.A.N. protocol nodes [21][26].

5 Conclusion and future works

In this paper, we have proposed BlockWMN, a model for integrating blockchain into WMNs. We illustrate its relevance by focusing on securing the network, especially against DoS and identity theft attacks. The description of our model allowed us to show that with the help of a blockchain, we can make WMNs less vulnerable to DoS and identity theft attacks.

Our model uses the blockchain as a secure database to save in real time the network graph and the credentials of all the network nodes. In BlockWMN, each node has the possibility to check in the blockchain all the signaling information received from other network nodes. Unlike other approaches, our model is decentralized, open and flexible.

We applied BlockWMN to the B.A.T.M.A.N.adv routing protocol to build a secure wireless community network, which resulted in the proposition BATMAN Blkc,

which manipulates a modified OGM format to protect the network from DoS and identity theft attacks.

The implementation of BlockWMN can help to bring WMNs to the attention of telecom operators to extend their network coverage in remote, poor and sparsely populated areas at a reduced cost. However, one problem remains: network participation requires nodes to have high computing power and data storage capacity to be able to use the WMN blockchain.

From this perspective, we plan to propose a security model for WMNs based on blockchains with an optimization of its consensus algorithm coupled with the Software Defined Network (SDN) paradigm to (1) monitor and (2) reduce its energy and memory capacity consumption.

Compliance with Ethical Standards:

Disclosure of potential conflicts of interest

Conflict of Interest: The authors declare that they have no conflicts of interest.

Research involving Human Participants and/or Animals

Ethical approval: This article does not contain any studies with human participants performed by any of the authors.

Informed consent

Informed consent: Not applicable

Declarations

Authors' contributions

Not applicable

Funding

Not applicable

Availability of data and materials

Not applicable

References

1. MeshBox : MeshBox va créer un nouveau standard d'appareil de routage/stockage distribué, White Paper, January 2017, V3.0.0, (2018).
2. Manuel Joao Sampaio Martins: Wireless Mesh Network Application, (2013).

3. Dr. Jason Ernst and al: A Decentralized Mobile Mesh Networking Platform Powered by Blockchain Technology and Tokenization, white book, (2018).
4. Abdelaziz Amara Korba : Détection d'Intrusion et Sécurisation du Routage dans les Réseaux Ad hoc, Postgraduate Thesis, (2016).
5. Comprendre la blockchain : Anticiper le potentiel de disruption de la blockchain sur les organisations, White Paper, (2016).
6. Ngouaha Mbikakeu Ronald : Implémentation de la blockchain pour la sécurité et la traçabilité des transactions financières : cas de l'application mobile « DirectCash » d'ALLIANCE FINANCIAL S.A., (2018).
7. Ian F. AKYILDIZ and X. WANG: 'Wireless Mesh Network'. John wiley et sons Ltd (2009).
8. A. OUNI, H. RIVANO, F. VALOIS : 'Ordonnancement du trafic dans un réseau maillé sans fil'. INRIA2010 research report (2010).
9. A. A. FERHAT et BENMOHRA Amel RAMDINI : "Réseaux Mesh (Maillés) sans fil « WMNS »", (2014).
10. U. ASHRAF : 'Qualité de Service et Routage dans les Réseaux Maillés Sans Fil', 2010.
11. https://fr.wikipedia.org/wiki/Topologie_mesh. last accessed 2019/04/25.
12. Prof-Dr Eng Thomas Djotio N. : Sécurité de Services Réseaux, (2019) ;
13. Dmittriy Kuptsov, Oscar Garcia-Morchon, Klaus W. and Andrei Gurtov: On Application of Cooperative Security in Distributed Networks, (2007).
14. J. DROMARD : Vers une solution de contrôle des admissions sécurisé dans les réseaux mesh sans fil, Ph.D. thesis, Troye University of Technology, (2013).
15. www.businessdictionary.com/definition/free-rider.html. last accessed 2019/02/14.
16. https://blog.nameshield.com/fr/2017/09/06/3-attaques-dns-plus-communes-combattre/. last accessed 2019/02/14.
17. Binace Academy, (2019), La tolérance aux 'pannes byzantines' https://www.binance.vision/fr/blockchain/byzantine-fault-tolerance-explained, last accessed 2019/08/13.
18. Thesis Abdelmajid HAJAMI: Sécurité du routage dans les réseaux sans fil spontanés: cas du protocole OLSR, Ph.D. Thesis, Mohamed V University, Morocco, (2011).
19. Stanislas de Quénetain : « Algorithme des Généraux Byzantins : le mode de consensus des blockchains privées », (2017).
20. Https: //en.m. wikipedia.org /wiki/Freifunk, last accessed 2019/12/29.
21. Benjamin Sliwa, Stefan Falten and Christian Wietfeld: Performance Evaluation and Optimization of B.A.T.M.A.N. V Routing for Aerial and Ground-based Mobile Ad-hoc Networks, (2019).
22. Anderson Morais: Distributed and cooperative intrusion detection in wireless mesh networks. Ph.D. Thesis, University of EVRY VAL D'ESSONNE, (2012).
23. RAHMOUNE Amer : Simulation d'un protocole de surveillance des interfaces d'un routeur, Thèse de M.S., Université A/MIRA de Bejaïa, Algérie, (2015).
24. GEORIS Antoine : « Evaluation de protocoles de routage ad hoc », Master's thesis is computer science, University of Mons, (2012).
25. https://www.open-mesh.org/projects/batman-adv/wiki/Ogmv2, last accessed 2020/08/25.
26. Axel Neumann, Corinna Aichele, Marek Lindner & Simon Wunderlich (2008): Better approach to mobilead-hoc networking (B.A.T.M.A.N.). (2008).
27. DOBE Abel : « Problématique d'intégration des technologies Blockchain aux réseaux maillés sans fil : application aux réseaux communautaires sans fil. », (2018).
28. Stéphane Loignon : Big Bang Blockchain - La seconde révolution d'internet, (2017).
29. Deloite : Blockchain : A technical primer, (2018).

30. B. CHOULI, F GOUJON, Yves-M LEPORCHER : Les Blockchains : de la théorie à la pratique, de l'idée à l'implémentation, PP 141-146, Epsilon, (2017).
31. Tom Zilavy : Hybrid Blockchain, What Is a Hybrid Blockchain and Why You Need to Know about It. Altcoin magazine, (2018).
32. Livre Blanc SmartMesh, SmartMesh Foundation Pte. Ltd, (2017).
33. Jean-Charles Régin, Arnaud Malapert : Théorie des Graphes, (2016).
34. Amir Qayum : Théorie des Graphes, Université de Paris Sud 11, (2006).
35. https://www.cryptoencyclopedie.com/single-post/Quest-ce-que-la-cryptographie-asymetrique-, 2017/07/10, last accessed 2019/08/27.
36. Maxime Eglem : Blockchain – Qu'est-ce que le consensus Proof-of-Work? (2018), last accessed 2019/08/13.