A Blockchain-based Approach for Optimal and Secure Routing in Wireless Sensor Networks

Hilmi Lazrag[1], Rachid Saadane[2] and Moulay Dirss Rahmani[1]
[1]*LRIT Lab, FSR, Mohammed 5 University, Rabat, Morocco*
[2]*EHTP, Km 7 Route El Jadida, Oasis, Morocco*

Keywords: WSN; Blockchain; Traffic Load; SINR; Security; Digital Signature

Abstract: The traffic load balance, the interferences reduction, and the security during the routing phase in wireless sensor network (WSN) are investigated in this paper. In our work, we suppose that the network's nodes are sensing some events which generate heavy data that must be carried over several packets. We propose a routing protocol which takes use of the Blockchain technology to offer a shared memory between network's nodes. These nodes are considered as coins which the ownership transacts between the source nodes and the sink. All the transactions are stored in the Blockchain as a mean to share the network's status, in real time. In order to select the optimal path, we introduce a cost function which considers the load density and interferences level at each node. Furthermore, we are taking advantage of the Blockchain security to secure the selected paths in the network. The simulation results have shown that this solution could be applicable and could resolve the issues cited above.

1 INTRODUCTION

Nowadays, wireless sensor networks (WSN) are being wildly used in several domains (Akyildiz et al., 2002), due to their simple implementation and, continuously, improved features (Callaway, 2004), (Limin et al., 2005). This technology gained more importance in the IoT era and had been well investigated. However, WSNs are confronted to many problems. In this paper we are interested in issues related to the traffic load, the interference, and the security in such networks during the routing phase. Indeed, as any distributed wireless system, this type of networks suffer from the absence of a global state and a global clock, which makes it very difficult to predict which path is the most suitable to avoid the traffic load unbalance and to reduce the interferences levels. Furthermore, the WSNs are usually deployed outdoor, in harsh and hostile environments, which makes it hard to maintain high security levels.

In this paper we will introduce the concept of Blockchain introduced by (Satoshi, 2008), which has proved its efficiency in the cryptocurrency and other distributed systems, in order to face the issues cited above. At the first stage of our approach, we consider the network's nodes as coins, all owned by the sink (i.e, the nodes owned by the sink are considered as inactive). Each time a node desires to send a message, it calculates the best path to transmit on. Then it asks the sink to transmit the path's nodes ownership to it. The transaction is stored in the Blockchain and the path's nodes becomes active. In fact, we could check for nodes activity directly in the Blockchain. Though, it seems simple, the path choice requires some advanced logic. Actually, the transmitting node has to find the optimal path based on the traffic load over all the network's nodes and the interference generated by each node that is transmitting in the same time. So, we introduce, also, some cost function, which will help the nodes in selecting the routes. The security of the transaction is supposed to be granted by the blockchain's signatures. In order to validate this approach, we implemented a lightweight blockchain mechanism and we used it to simulate our proposition through an homogeneous static network.

To our best knowledge, our work is the first WSN routing mechanism which considers the Blockchain as a support to share network status in real time in order to enhance the routing process. The main contributions of this paper are as follows:

- Considering nodes as coins and transfer their ownership between each other;
- Use Blockchain as a shared memory to broadcast

Lazrag, H., Saadane, R. and Rahmani, M.
A Blockchain-based Approach for Optimal and Secure Routing in Wireless Sensor Networks.
In *Proceedings of the 1st International Conference of Computer Science and Renewable Energies (ICCSRE 2018)*, pages 175-180
ISBN: 978-989-758-431-2

the status of the network's nodes;

- Use the past nodes' activities to determine the traffic load.

The paper is organized as follows : Section 2 presents the Blockchain technology brefly. Section 3 describes how we attend to introduce the Blockchain in the routing phase and how we use the stored transactions to optimize the routing. Simulation results are illustrated in Section 3. Finally, in Section 4, we give a brief conclusion for this work.

2 THE BLOCKCHAIN

Blockchain appeared, originally, with the cryptocurrency 'Bitcoin' in 2008. Since then Blockchain has gained a strong reputation and had been used in several domains ranging from economy (Swan, 2015) to property acquisition (Peiró and Martinez, 2017) and health care (Kuo et al., 2017).

Blockchain is considered as a distributed ledger of transactions, which plays the role of a database that could be shared over a network of various peers (UK Government, 2015). Blockchain technology was designed to face the digital currencies ownership and the transactions settlement challenges (Satoshi, 2008). It provides, also, a secure mechanism for electronic collaboration which is accomplished without a central trusted party (Satoshi, 2008), (UK Government, 2015). When a transaction from peer A to peer B is made, the information is shared with all the network's peers, underlying the Blockchain. The transaction's credentials are combined in a block, marked with a timestamp and added as a new block to the blockchain. Since all transactions use public-private key cryptography, each transaction could be verified and confirmed by all involved parties. The blocks are appended consecutively, which allows a transparent and total knowledge of all transactions made in the past (Dwyer, 2015), (Böhme et al., 2015).

What one shall retain, is that Blockchain offers a distributed database which keeps track of all transactions made over a network in a secure way. For a better understanding of the Blockchain technology mechanism we refer the reader to (Satoshi, 2008), (Swan, 2015) and (Franco, 2015).

3 SYSTEM MODEL

We consider a static network consisting of n nodes and one sink as shown in Figure 1. Each node is supposed to have a map of the network (number of nodes, their ids, their locations as well as their connectivities). we assume that the nodes are homogeneous in term of transmission power and bandwidth. the sink is supposed to have enough bandwidth and resources to handle all incoming messages. The sensed events arrive randomly at each node. we assume that the events generate some heavy data that will be carried through several packets. These packets have the same size and they are concidered as a single message. Furthermore, we assume that the nodes and the sink have an unlimited source of energy (photo-voltaic ...). So, the routing services could be discussed without being bound in the fetters of the energy shortage constraints.

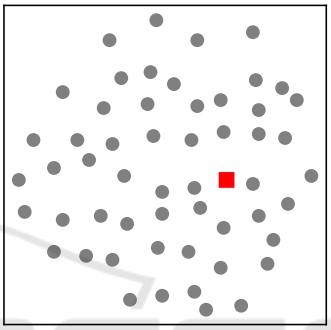

Figure 1: The simulated network: the (gray) dotes represent the sensor nodes and the (red) square represents the Sink.

Even though each node has a good knowledge of the network's distribution, it still can't know the state of the network at a given time. For example, at an instant t a node couldn't tell which nodes are transmitting and which are not. This ignorance is due to the absence of a shared memory. Additionally, a node could not predicts whether its peers have been compromised or not. Hence, the nodes could, naively, send/receive the data to/from some malicious peer, which could offense the integrity and the sanity of the carried data.

In order to make the network's state shareable, we introduce the blockchain mechanism cited above.

3.1 Blockchain as Shared Memory in WSN

As we said before, the Blockchain system is based on a ledger which keeps track of all the transactions circulating in a network. Thus, as we need some way to figure out which nodes are transmitting and through which path, we will store the paths which are active, in real time, as transactions in the Blockchain. To achieve this, we treat the network's nodes as coins.

More precisely, when some nodes are carrying a message from a source node to the sink, their ownership will be affected to the source node. At the first stage all the nodes are owned by the sink. Each node that is owned by the sink is considered to be inactive. Otherwise, all the nodes which are not owned by the sink are considered as active. When a node senses some event, it looks up in the Blockchain and defines a list of all inactive nodes, then it finds among them which ones optimize its path to the sink, we will describe the route choice process in the next subsection. Next, it asks the sink to transfer the path's nodes ownership to it. Once the transaction is registered to the Blockchain the node starts transmitting over the chosen route. When the data is carried successfully to the sink the transmitting node transfers back the ownership of the path's nodes, including itself, to the sink as a way to inform the network's peers that the transmission was finished and these nodes were released.

We assume that a source node could own u nodes while $u \leq n$. We assume also that the nodes transmit over two channels, the first one is dedicated to the paths claiming and to the Blockchain transactions transferring, and the second one is designated to carry the sensed data. We are interested, primarily, in the second channel which is used to transmit the message. We suppose, also, that each intermediate node could be owned, only, by one source node and a source node is owned, only, by itself. When a node senses an event while it is owned by an other node, the latter waits until its ownership is transfered to the sink. In the meantime, the node notifies the sink, through the first channel, in order to be added to a waiting queue. The waiting queue is mainly managed by the sink and it is necessary to apply, a kind of, priorities to the waiting nodes.

As we have seen, this technique allows for a good knowledge of the source nodes as well as the paths which they transmit on, at a given moment. It is necessary, also, to mention that the nodes are represented in the Blockchain by their Ids. Hence, the traffic load could be, easily, determined through the Blockchain. Actually, it suffices to determine, directly from the chain, how many times the status of a node has changed to be active. This changes number is, obviously, the number of messages carried by a node, since a node status changes only when it is in the path on which a message is transmitted. Now, after we defined the traffic load at each node, we have to define the routing determination process of our model.

3.2 Route Determination Process

As each node knows the network's map and as each one can access the Blockchain and find which nodes are transmitting and which nodes are not, it becomes simpler to define the shortest path to the sink through a set of inactive nodes. However, as said previously, our main goal is to balance the traffic load and to reduce the interferences in the routing phase. So, we have to define a cost function which optimizes the path. First of all let us define the signal and interference to noise ratio (SINR) as (Gupta and Kumar, 2000),

$$SINR_{(i,j)} = \left(\frac{p_i}{d_{i,j}^a}\right) / \left(N_0 + \sum_{\substack{k=1 \\ k\neq i}}^{n} \frac{p_k}{d_{k,j}^a}\right) \quad (1)$$

where p_i is the transmission power of the i^{th} node, $d_{i,j}$ is the distance between two nodes i and j, a is the path loss exponent, and N_0 is the power of an additive white Gaussian noise. The equation (1) is used beside the load traffic to determine the routing cost to the next hop. The cost function is defined as follow,

$$Cost_j = SINR_{(i,j)}/(1+\theta_j) \quad (2)$$

where j is the index of the next hop, $SINR_{(i,j)}$ is the signal to interference and noise ratio, and θ_j is the traffic load of the j^{th} node.

When an event is detected and a message is ready to be sent, the source node k starts listing all the inactive nodes, as explained before. Next, it calculates the routing cost, using equation (2), for each of the inactive nodes and determines the optimal path using dijkstra's algorithm (Dijkstra, 1959). Once the path determined, a chain verification is applied to each node of the chosen path. If the chain of all the nodes is verified, the source k claims for the ownership of these nodes and the transaction is registered to the Blockchain. Otherwise, k discards the untrusted nodes and redefines a new optimal path. In case no valid path is found to reach the sink, the source node waits for active nodes to be libereted and notifies the sink, through the first channel, in order to be added to the waiting queue.

3.3 Security in the Routing Phase

We stated in the previous subsection that each source node accomplishes a chain verification, right after it chooses the optimal path, for each node on the chosen route and we highlighted that all untrusted nodes

(those which has not been verified) are discarded. Actually, this kind of filtration guaranties that each selected node, that figures on any path linking all source nodes to the sink, have, necessarily, a clean connexion history, since the nodes that had been on the path of some malicious peer are ignored. Indeed, it is convenient to say that the routing phase has a security layer which lies on the Blockchain's security mechanism shown in (Satoshi, 2008), (Swan, 2015) and (Franco, 2015). Hence, the proposed routing approach has a quiet strong security, especially, with the use of some, trusted, cryptographic algorithms such as ECDSA224 (Johnson et al., 2001) and sha512 (Gueron et al., 2011).

Overall, the proposed routing approach shows that, despite the fact that the process of finding paths is done through some, fairly, complex calculations, it is still secure and optimal, involving multiple cryptographic techniques.

4 RESULTS

To validate our work we simulated a network of 55 nodes which contains one sink. The network is a connected graph and distributed as shown in Figure 1. The simulation was done using Python3, numpy and matplotlib. First of all we created a basic Blockchain mechanism, which responds to the requirements of our work, in term of transactions structure and cryptographic mechanisms. We assumed that the nodes are broadcasting at a transmission power of $1mW$ and we considered that the path loss and the noise are 2 and $5 * 10^{-15}$, respectively. Next, in order to verify the ability of the proposed mechanism to balancing the traffic load, we assumed that only one node is transmitting , several messages, over the network. To evaluate whether there is an enhancement or not, we applied a shortest path routing protocol to the same scenario and we analyzed the returned data.

Figure 2 shows a comparison of the traffic load, when only one node is transmitting, using a shortest path routing protocol against our proposed approach.

As we can see in Figure 2 (a.1), when a shortest path routing protocol is used, the load density is concentrated at a tiny straight region, the brightest area on the illustration (i.e. the brighter a region is the higher the traffic load is). By taking a closer look at Figure 2 (a.2) we could distinguish that the load density is concentrated only around the shortest path between the source node (green dot) and the sink (red square). However, if we take a look at Figure 2 (b.1), when we use our proposed protocol, we could remark that the brightness is concentrated at two points and it fades

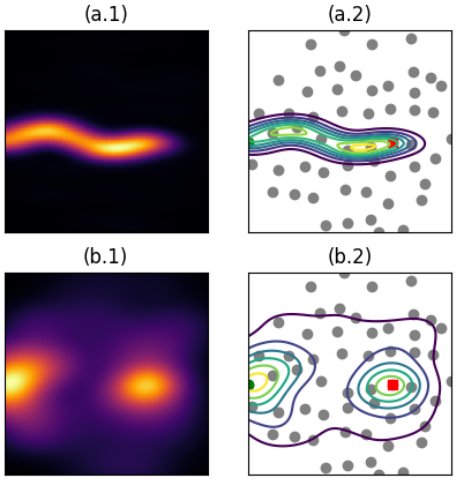

Figure 2: The traffic load when only one node is transmitting: the (green) dot represents the source node. (a.1) shows the density of load and (a.2) shows the implied nodes, while using a shortest path protocol. (b.1) shows the density of load and (b.2) shows the nodes implied in the transmission, while using the proposed approach.

while we move away from them. These two points are the source node and the sink, as we can tell from Figure 2 (b.2). So, rather than be concentrated around a single path, the traffic load is spread over the network, which highlights the efficiency of our system to resolve the load balancing issue.

Now, let's analyze the interferences level for the shortest path routing protocol and our proposed protocol. To do so, three source nodes are considered: the first one senses an event at t_0, the second one senses an event at t_1, and the last one senses an event at t_2. Once, an event is sensed the implicated node selects a path and starts transmitting over it. We assume that when one of, the cited above, source nodes starts sending data it keep transmitting until the simulation ends.

Figure 3 shows the selected routes, when only one source node is transmitting, when two source nodes are transmitting, and when three source nodes are transmitting, simultaneously, while using, both, the shortest path routing protocol and our proposed protocol.

Obviously, when using the shortest path routing protocol and for the three cases, shown in Figure 3: (a.1), (b.1), and (c.1), the source nodes select the shortest paths to the sink. When, using our proposed protocol, we could, clearly, depict that the path choice in the first case, when only one source node is transmitting, mimics the one chosen by the shortest path

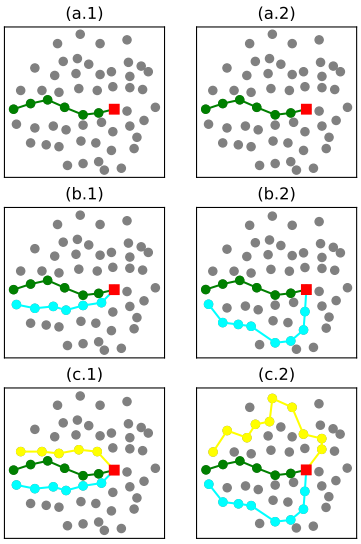

Figure 3: The path choices: the (green) path represents the first route, the (cyan) one represents the second route and the (yellow) represents the third route. The left column is dedicated to the choices made by a shortest path protocol, while the right one shows these made by the proposed protocol.

routing protocol (see Figure 3: (a.2)). This similarity is, totally, comprehensible since the load density is supposed to be equal over the network's nodes and since we are using dijkstra's algorithm to define our paths. However, for the two remained cases we could see, as shown in Figure 3: (b.2) and (c.2), that our proposed mechanism chooses longer routes which are located far from each others. As known, the farther a transmitting node is from its peers the less the interferences are and the nearest it is the higher the interferences became, which means that our approach decreases the interferences between the transmitting nodes.

Finally, after resolving the traffic load balancing and the interference issues, let's run one last simulation where we could evaluate the security of our proposition. First of all we change manually the ownership of some nodes and set it to an unknown owner directly into the block chain which will mess up the blocks signature. These nodes will be considered as corrupted by the system. So, let see how the system will behave to face this issue.

Figure 4 shows the load density when some of the network's nodes are compromised. As shown in Figure 4 (a.1), there are two areas, on the load density illustration, that are darker than the remaind regions.

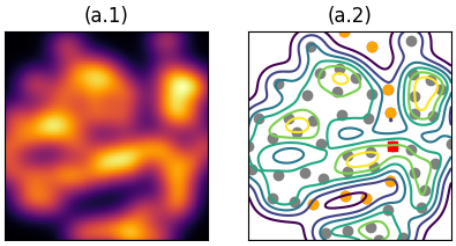

Figure 4: The traffic load when some nodes are compromised: the (orange) dotes represent the compromised nodes. (a.1) shows the load density and (a.2) shows the exact location of the compromised nodes.

The first area is located in the bottom of the figure and moves diagonally to the up right, and the second one starts right in top and continues vertically near to the center. By analyzing the Figure 4 (a.2) we could see that the dark areas correspond to the orange nodes, which we intentionally messed up. And as we said before, the darker an area is the less messages went through it, so we could deduce that the orange nodes have been ignored by the benign nodes of the network during the routes determination processes. Thus, our protocol has shown that it could offer a layer of security in the route determination phase.

5 CONCLUSION

In this paper, optimal routing protocol in wireless sensor networks based on Blockchain has been discussed. To achieve a better solution to the traffic load unbalance, the high interference levels and the security issues, we proposed a protocol which takes advantage of the Blockchain technology benefits. The approach consists of using Blockchain as a shared memory between nodes and storing all the network's activities on it. The nodes are considered as coins which are owned by the sink when they are inactive or owned by the source node if they are carrying some message. Moreover, a cost function is proposed in order to optimize the chosen path. regarding the protocol's security, it is granted by the Blockchain. Simulation results show that the proposed protocol can improve the traffic load balance, decrease the interference levels and guaranty a strong security during the routing phase.

REFERENCES

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, 40:102–114.

Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29.

Callaway, E. H. (2004). Wireless sensor networks architectures and protocols. *Aerbach publishers*.

Dijkstra, E. W. (1959). A note on two problems in connexion with graphs. *Numerische Mathematik*, 1:269–271.

Dwyer, G. (2015). The economics of bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17:81–91.

Franco, P. (2015). *Understanding Bitcoin: Cryptography, Engineering, and Economics*. Wiley.

Gueron, S., Johnson, S., and Walker, J. (2011). Sha-512/256. In *Proceedings of the 2011 Eighth International Conference on Information Technology: New Generations*, pages 354–358. IEEE Computer Society.

Gupta, P. and Kumar, P. R. (2000). The capacity of wireless networks. *IEEE Transactions on Information Theory*, 46:388–404.

Johnson, D., Menezes, A., and Vanstone, S. (2001). The elliptic curve digital signature algorithm (ecdsa). *Int. J. Inf. Secur.*, pages 36–63.

Kuo, T.-T., Kim, H.-E., and Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24:1211–1220.

Limin, S., Jianzhong, L., and Yu, C. (2005). Wireless sensor networks. *Beijing: Tsinghua university press*, pages 1–20.

Peiró, N. and Martinez, García, E. (2017). Blockchain and land registration systems. *European Property Law Journal*, pages 296–320.

Satoshi, N. (2008). Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc., 1st edition.

UK Government, C. S. A. (2015). Distributed ledger technology: Beyond blockchain. *UK Government Office for Science*.