Performance comparison of different algorithms to secure the information for Wireless sensor Network

Oumayma El Gatte [1*], *Ahmed* El Abbassi [2], *Omar* Mouhib[1] *Amine* Tilioua[3]

[1] Laboratory of Electronics Systems, Information Processing, Mechanics and energetic, faculty of sciences, Ibn Tofail University, Campus Universitaire, BP 13, Kenitra, Morocco

[2]Team Renewable Energies, Information Processing and Transmission Laboratory, Department of Engineering Sciences, Faculty of Sciences and Techniques Errachidia, Moulay Ismaïl University of Meknès, B.P. 509, Boutalamine, Errachidia, Morocco

[3]Research Team in Thermal and Applied Thermodynamics (2.T.A.), Mechanics, Energy Efficiency and Renewable Energies Laboratory, (L.M.3.E.R.). Department of Engineering Sciences, Faculty of Sciences and Techniques Errachidia, , B.P. 509, Boutalamine, Errachidia, Morocco

Abstract. In WSNs "Wireless Sensor Network" and ad hoc networks, efficient and secure routing protocols are essential to ensure reliable communication and optimal resource utilization. Cluster-based routing is organizing the network into clusters, a designated cluster head manages each cluster, which improves scalability and reduces routing overhead. This approach is highly effective in balancing energy consumption and extending network lifetime, particularly in large-scale networks. Conversely, trust-based routing protocols establishing trust metrics for each node, which are used to make routing decisions in order to prioritize security. This method mitigates the risk of attacks by identifying and isolating malicious nodes, thereby ensuring the integrity and confidentiality of data transmission. The integration of blockchain technology with convolutional neural networks (CNNs) represents a promising frontier in decentralized artificial intelligence (AI). However, this fusion has led to considerable security within both the blockchain and AI communities. Through a detailed comparison of these methodologies, this paper highlights their respective advantages, limitations, and potential applications in term of security and energy. The findings suggest that while cluster-based routing is well-suited for energy-efficient networks with stable topologies, trust-based routing offers superior security features, making it ideal for environments with higher risks of node compromise, and the blockchain associated to the CNN ensure a high security.

Keywords— Wireless Sensor Network (WSN), Convolutional Neural Network (CNN), Cluster-based routing, Trust-based routing, Blockchain.

1 Introduction

To be able to make right decisions and take the best actions, it necessary to be situation aware in public safety operations. The purpose of those operation is to protect humans. The rapid advancement of technology has led to the proliferation of wireless sensor networks (WSNs) and ad hoc networks, which are increasingly relied upon for a variety of applications, from environmental monitoring to military communications. In these networks, the design of efficient and secure routing protocols is critical to ensuring reliable data transmission, optimal resource utilization, and network longevity. Among the diverse approaches developed to address these challenges, so the most prominent methodologies are the cluster-based routing and trust-based routing. Cluster-based routing protocols enhance network scalability and energy efficiency by organizing nodes into clusters, with cluster heads managing intra- and inter-cluster communication. This approach is particularly advantageous in large-scale networks where minimizing energy consumption is crucial. On the other hand, trust-based routing protocols focus on security, using trust metrics to evaluate and select routing paths, thereby protecting the network from malicious nodes and ensuring the integrity of data transmission. Parallel to developments in network protocols, the AI has viewed significant interest in decentralized learning frameworks, particularly through the integration of blockchain technology with convolutional neural networks (CNNs). Blockchain, known for its decentralized and secure ledger capabilities, has been proposed as a means to enable collaborative, secure training of CNNs across distributed networks. However, the application of blockchain in CNNs has sparked confusion within the AI and blockchain communities. Questions regarding the necessity of blockchain for decentralized Artificial Intelligence, the impact of blockchain's consensus mechanisms on CNN training speed and scalability, and the feasibility of such integrations have led to a growing need for clarity in this emerging area.

This paper aims to address these two distinct yet related areas by providing a comparative analysis of cluster-based and trust-based routing protocols in WSNs and ad hoc networks, as well as clarifying the role of blockchain in CNN-based decentralized AI. By examining the advantages, limitations, and potential applications of these approaches, this study seeks to offer insights that will enhance the understanding and

* Corresponding author: oumayma.elgatte@uit.ac.ma

development of both secure, efficient network protocols and decentralized AI systems.

2 Cluster Based Routing

Cluster-based routing is designed for mobile ad hoc networks (MANETs), where the nodes of the network are organized into disjoint clusters in a distributed manner. Each cluster is composed of a cluster head (CH) and several cluster members. In this hierarchical structure, the high-level clusters have as members the Cluster head of the lower level Network, with the highest-level cluster heads communicating directly with the base station (BS). The base station is responsible for selecting the cluster heads through a two-stage process. In the first stage, potential cluster head candidates are identified based on factors such as their relative distance to the base station, remaining energy levels, potential neighboring sensor nodes, and the frequency with which they have previously served as cluster heads. Once selected, the cluster heads manage the cluster by generating two types of schedules for the members: one for sleep mode and another for TDMA-based data transmission. Data is transmitted within the cluster and from the cluster head to the base station using a multi-hop communication method [1].

2.1 Routing specification

One key can specify a Cluster, which represents to max of the distance allowed for a cluster:

- Intra Cluster: Proactive Routing
- Inter Cluster: Reactive Routing

2.2 Key factor routing

The maximum number of hops allowed to reach any node from the cluster head within a single cluster is uniform across all nodes. This key factor helps divide the entire network into overlapping sub-networks. It is influenced by the total number of nodes in the network, making its determination a crucial aspect of the proposed protocol. The key factor will be balanced, so if it is too large, the cluster size will be too big, leading to increased proactive routing overhead. Conversely, if it is too small, the cluster size must be reduced, in order to have more clusters and an increase in reactive routing overhead [1].
Fig. 1 illustrates a typical hierarchy of the Clustering protocol which is detailed in the paragraph below:

- The role of Cluster head is collecting the data from the cluster members and forward it to the other clusters head, and the Base Station is the considered as the final destination.

- Thanks to the ability of CH to require more energy, the Cluster Head rotate among clusters members in order to distribute the energy consumption.

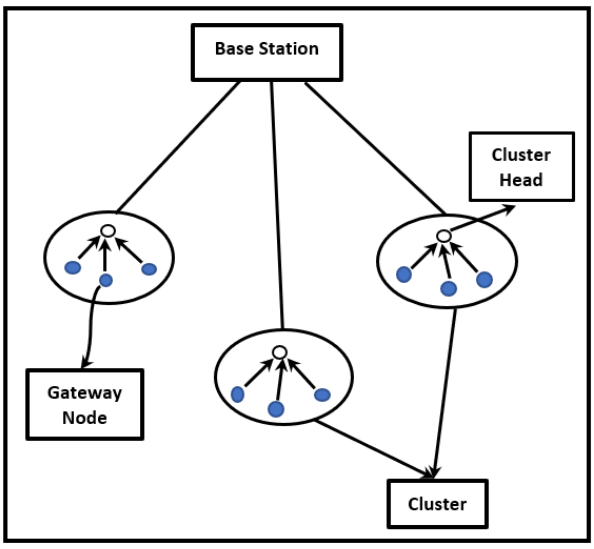

Fig. 1. Hierarchical Cluster Based Routing

- Every Gateway node transmit sensor data only to the CH, to value the number of transmissions to longer distances.
- The same data aggregated at the CH is present to the cluster members in close vicinity.
- To reduce the complexity of the routing protocol, only the cluster head are required to know the methodology of forwarding to the next level CH or BS [2].

3 Trust Based Routing

3.1 Definition

The Trust-based routing is to involve the selecting nodes for routing based on their participation and reliability. Thanks to the node's history of cooperation and reputation, trust is determined, and it built basing on such factors availability, success rate in packet delivery preservation of packet priority. The creation of reliable path for packet forwarding is enabled by each node assigned a trust. The current trust-based routing protocols lack safeguards to protect the evaluation process. To prevent malicious nodes from undermining the system, it is necessary to conceal the criteria used for assessing trustworthiness [3].

3.2 Trust Mechanism

Trust is a judgment formed based on the existing data, making it a subjective interaction between entities. The calculation of trust degree is a quantitative process that evaluates the trust relationship.

3.2.1 Degree of Trust

The size of the trust degree is determinate by the routing information and node behavior. Basing on the behavior of the routing information the trust degree will be calculated

$$Rs = TMS / (TMS + TMF) \quad (1)$$

TMS represents the number of successfully transmitted packets.

TMF represents the number of failures.

We set Rs=0, if a node has no routing information forwarding behavior [4].

3.2.2 The calculation of the overall trust degree

In various specific applications, network nodes have differing expectations regarding the services provided by other nodes. Consequently, the overall trust degree is determined as the weighted sum of individual trust degrees. Let α represent the weight of Rs and β the weight of Rn. The overall trust degree is calculated :

$$R=\alpha \times Rs + \beta \times Rn \ (0 \leq \alpha, \beta \leq 1 \text{ and } \alpha+\beta=1) \quad (2)$$

When R = 0, the node is entirely untrusted; when $0 < R < 0.5$, the node is considered untrusted; when $0.5 \leq R < 1$, the node is trusted; and when R = 1, the node is fully trusted [4].

4 Blockchain and CNN:

4.1 Blockchain:

4.1.1 Generality

A blockchain operates as a collaborative digital ledger, where data is not stored on a single computer but distributed across multiple computers within a network. In other words, a blockchain is a decentralized system typically implemented as a distributed ledger. A blockchain serves as a shared digital ledger, where data is not housed on a single machine but spread across multiple computers within a network. In essence, a blockchain is a decentralized system, usually functioning as a distributed ledger [5].

4.1.2 Data Storage Security

Blockchain relies on a decentralized data storage mechanism that minimizes the risk of failures while enhancing security and reliability. Due to the large volume of data and the associated storage and power requirements, optimizing efficiency is crucial to accelerating data processing and reducing storage space. Achieving efficient and secure storage is key to maintaining the integrity of blockchain systems. Additionally, ensuring trust and transparency among participants is a primary goal to foster trustworthiness throughout the system [7].

4.1.3 Decentralized Storage

To verify and store data, a blockchain ecosystem uses a chain of encrypted blocks, with distributed nodes playing a key role in generating and updating the ledger, ensuring the decentralization of stored information. Blockchain is crucial for managing storage and decentralizing grid energy operations. However, frequency fluctuations may increase due to the uncertainty in integrating distributed energy into the grid [7].

4.2 Convolutional Neural Network

4.2.1 Definition

A Convolutional Neural Network (CNN) processes input data by applying a set of filters through convolution. This operation is loosely analogous to the use of receptive fields in the retina, as seen in Fukushima's original recognition network. For simplicity, consider a CNN with a single hidden convolutional layer [6].

4.2.2 Typical format

The architecture of a Convolutional Neural Network has purpose designed to learn spatial hierarchies of features from input data, typically images automatically and adaptively. A CNN is composed of several key layers that each play a specific role in processing the input. The main components of CNN architecture are :

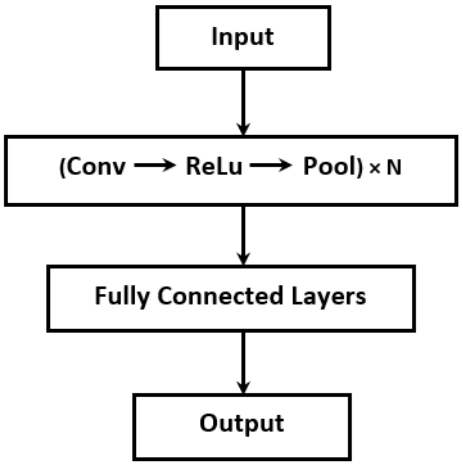

Fig. 2. CNN Component

- **Input Layer**:

Usually, an image in 3D matrix represented the input to a CNN is, where the depth corresponds to color channels (RGB).

- **Convolutional Layer (Conv Layer)**:

This is the core building block of a CNN. A set of filters (also called kernels) that convolve across the input image to detect features such as edges, textures, or patterns applied by the convolutional layer.

- **Activation Function (ReLU):**

An activation function, typically a Rectified Linear Unit (ReLU), is applied in order to introduce non-linearity to the model after each convolutional operation. This helps the network to learn complex patterns.

- **Fully Connected Layer (FC Layer)**:

The output is flattened into a 1D vector and passed through one or more fully connected layers after several convolutional and pooling layers, where every neuron is connected to every neuron in the previous layer. It's help to make a high level of decision.

- **Output Layer:**

The final layer is typically a fully connected layer with an activation function like Softmax or Sigmoid, depending on whether it's a multi-class or binary classification problem. This layer produces the final predictions or probabilities.

5 Combining Blockchain with CNN

The integration of Blockchain and Convolutional Neural Networks (CNNs) offers numerous advantages by leveraging the strengths of both technologies. Blockchain provides a decentralized, secure, and transparent framework for storing and sharing data. while CNNs excel at extracting meaningful features from data, particularly in tasks like image and pattern recognition. Combining these two technologies can result in enhanced security, efficiency, and trustworthiness in various applications.

Blockchain can be used to securely store and manage the massive amounts of data required for training CNNs, ensuring data integrity and preventing tampering. This decentralized approach reduces the risk of single-point failures, promotes transparency, and enhances collaboration in environments where multiple entities contribute to data collection and model training.

6 Results and experiment

Security is considered a major challenge in the development and deployment of Wireless Sensor Networks (WSNs) due to several inherent vulnerabilities and limitations of these Security remains a significant challenge in the development and deployment of Wireless Sensor Networks (WSNs) due to the inherent vulnerabilities and limitations of these networks. WSNs are composed of spatially distributed sensor nodes that are resource-constrained, with limited computational power, memory, and battery life. These nodes are deployed to monitor environmental conditions, collect data, and transmit it for various applications, such as fire detection, environmental monitoring, healthcare, and industrial automation. Due to their wireless nature and limited resources, WSNs are highly susceptible to various security threats, including eavesdropping, data tampering, denial-of-service (DoS) attacks, and node compromise.

The challenge becomes particularly acute when the WSN is deployed in critical or sensitive applications, such as fire detection in remote areas, where the data collected by sensor nodes is crucial for timely decision-making and emergency response. Once an alert is triggered, such as the detection of a fire, the data is transmitted through the network to a central system for further analysis and action. However, during this transmission process, the risk of an attack significantly increases, as malicious actors may attempt to intercept, manipulate, or disrupt the data flow. Therefore, ensuring secure and reliable data transmission in WSNs is critical for the effective functioning of these systems.

In our proposed method, we explore the integration of Convolutional Neural Networks (CNNs) with Blockchain technology to enhance the security of WSNs. CNNs are highly effective at analyzing and recognizing patterns in data, and in this context, they can be used to analyze sensor data and identify potential threats or anomalies within the network. Blockchain, on the other hand, provides a decentralized and tamper-proof framework for securely storing and transmitting data. By combining the capabilities of CNNs and Blockchain, we aim to create a secure and efficient system for monitoring and transmitting sensor data in WSNs.

The proposed method will be compared with traditional routing algorithms used in WSNs, specifically cluster-based routing and trust-based routing algorithms. Cluster-based routing is a popular approach that groups sensor nodes into clusters to optimize energy consumption and extend the network's lifespan. Trust-based routing, on the other hand, relies on the concept of trust to establish secure communication paths between nodes, based on their behavior and reliability. Both algorithms offer different advantages in terms of energy efficiency and security, but they also have limitations, particularly in dealing with sophisticated attacks.

To evaluate the effectiveness of the proposed CNN-Blockchain integration, we will use a fire detection scenario as a case study. In this scenario, once a fire is detected, the sensor nodes in the WSN will collect data related to the event, such as temperature, smoke levels, and location. The data is then transmitted through the network for further analysis and alerting relevant authorities.

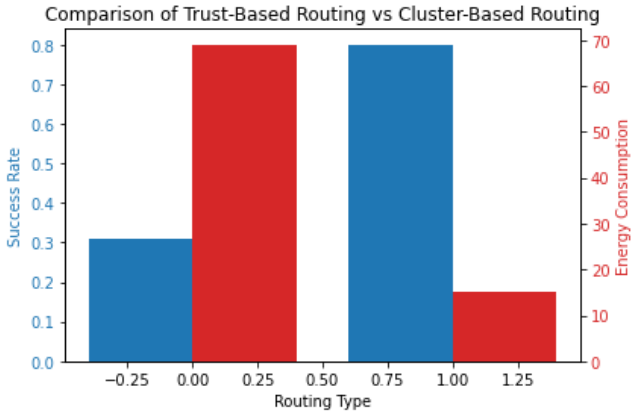

Fig. 3. The comparison between the routing Protocol

During this data transmission phase, the risk of attacks on the network is greatly increased, as attackers may attempt to intercept or alter the sensor data. Our study aims to compare the performance of the CNN-Blockchain approach with traditional routing algorithms in terms of both energy consumption and security.

Specifically, we will examine how each method handles the secure transmission of data under attack conditions, as well as the energy efficiency of each approach, given the limited resources of the sensor nodes.

Trust-Based Routing so the trust values are generated randomly for each node. The success rate is based on how many nodes exceed the trust threshold, and energy consumption increases with untrusted nodes. Cluster-Based Routing the nodes are grouped into clusters, and the success rate is assumed to be 80% if clusters are balanced. Energy consumption depends on the number of clusters. Now we try to optimize the delay of the security of the Network so a little comparison between the cluster-based routing, trust-based routing and the blockchain associated to the CNN is established in the following table:

Table 1. The time delay comparison

Cluster-based routing (Time in s)	0.0870	0.0868	0.0815
Trust-based routing (Time in s)	0.1500	0.1564	0.1438
CNN and blockchain (Time in s)	0.3972	0.4187	0.4003

So, we can see that the cluster-based routing is the best one on the term of the delay to secure the Network.

7 Conclusion

In this paper, we conducted two types of comparisons to evaluate the performance of different routing techniques. The first comparison focused on cluster-based routing and trust-based routing, specifically analysing their energy consumption efficiency. Efficient energy usage is critical in wireless networks, where energy constraints often limit network lifespan. Our analysis showed that cluster-based routing outperformed trust-based routing in terms of energy consumption, making it more suitable for energy-sensitive environments. The second comparison extended the analysis by incorporating blockchain technology associated with Convolutional Neural Networks in order to evaluate its potential benefits. We examined these algorithms in terms of delay, a key performance indicator for real-time applications. Although the integration of blockchain with CNNs gives advantages in decentralization and security, it introduces certain latency issues. Consequently, when considering both energy efficiency and delay, cluster-based routing emerged as the best overall solution. However, despite its advantages, cluster-based routing does have some significant limitations. One of the primary drawbacks is its complexity, which can make it difficult to implement and manage in large-scale networks. Additionally, cluster-based systems can struggle with database corruption and lack robust recovery mechanisms, leading to potential data loss or performance degradation.

These challenges, push us to our next objective to refine the existing algorithm to address these shortcomings.

References

1. D. K. Sharma, C. Kumar, S. Mandal, An efficient cluster based routing protocol for MANET. Proc. 2013 3rd IEEE Int. Adv. Comput. Conf. IACC 2013 224–229 (2013) https://doi.org/10.1109/IAdCC.2013.6514225

2. K. Chennakesava Rao, M., Vissa, M., Mrudula, S. & Dikshit, A. K. Energy Efficient Cluster Based Routing Protocol for wireless sensor networks. 2015 Int. Conf. Control Instrum. Commun. Comput. Technol. ICCICCT 2015 813–817 (2016) https://doi.org/10.1109/ICCICCT.2015.7475390.

3. Y. Gahi , M. Guennoun, Z. Guennoun, K. El-Khatib, An encrypted trust-based routing protocol. 2012 IEEE Conf. Open Syst. ICOS 2012 (2012) . https://doi.org/10.1109/ICOS.2012.6417643

4. Z. Yu, H. Zhou, Z. Wu, A trust-based secure routing protocol for multi-layered satellite networks. Proc. 2012 IEEE Int. Conf. Inf. Sci. Technol. ICIST 2012 313–317 (2012) https://doi.org/10.1109/ICIST.2012.6221658

5. E. Elrom, The Blockchain Developer. The Blockchain Developer (2019). https://doi.org/10.1007/978-1-4842-4847-8

6. K. Audhkhasi, O. Osoba, B. Kosko, Noise-enhanced convolutional neural networks. Neural Networks 78, 15–23 (2016). https://doi.org/10.1016/j.neunet.2015.09.014

7. Y. He, Z. Zhou, Y. Pan, F. Chong, B. Wu, K. Xiao, H. Li. Review of data security within energy blockchain: A comprehensive analysis of storage, management, and utilization. High-Confidence Comput. 100233 (2024). https://doi.org/10.1016/j.hcc.2024.100233

8. Z. Shi, Y. Ye, Y. Wu. Rank-based pooling for deep convolutional neural networks. Neural Networks 83, 21–31 (2016). https://doi.org/10.1016/j.neunet.2016.07.003