A Blockchain Based Framework for Reputation Management and Node Misbehaviour Detection in Wireless Sensor Networks

1st Kartik Bhatia
Faculty of Computer Science
Dalhousie University
Halifax, Canada
kr330412@dal.ca

2nd Srinivas Sampalli
Faculty of Computer Science
Dalhousie University
Halifax, Canada
srini@cs.dal.ca

***Abstract*—With the growth of smart applications such as smart cities and smart farming, the importance of Wireless Sensor Networks (WSNs) is gradually being realized by many industrial enterprises. In particular, WSNs have shown enormous potential for being an interesting research area and in this decade, it is expected to grow manifold both in terms of applications as well as business revenues. WSNs consist of resource constrained devices which are present in an open and unsecured environment, and this makes them vulnerable to both internal as well as external attacks. Internal attacks can affect the network's performance by increased energy consumption and introducing transmission delays. Consequently, this represents a critical security challenge for the deployment of WSNs. Many researchers have proposed solutions based on trust management systems that proves to be an efficient way for detecting such attacks by enhancing trust relationships and data routing reliability.**

In this paper, we extend the trust management system to include a distributed consensus mechanism based on blockchain which validates data packets originating from various source nodes. Additionally, a new algorithm is developed to estimate a node's reputation based on its historical energy consumption data. Reputation and trust are both crucial factors that characterize malicious behaviour in the network. We have evaluated our proposed work with another existing trust model named Belief-based Trust Evaluation Mechanism (BTEM) and compared our results in terms of performance metrics after performing various simulation runs. The results show that there is a significant improvement in the detection rate and accuracy. Furthermore, we have shown that our framework fulfils important security requirements such as integrity, authenticity and confidentiality by analyzing it for various security attacks.

***Index Terms*—WSN, Blockchain, Routing attacks, Reputation management**

I. Introduction

With the emergence of wireless communications, Wireless Sensor Networks (WSNs) are becoming a growing field in computer science research. They are being used in several application areas, ranging from defence to commercial businesses. Due to sensors deployed in hostile environments and using wireless medium to communicate between them, these devices are susceptible to different attacks and can get easily compromised by adversaries. These adversaries can launch insider attacks using the compromised nodes making security a challenging issue. To implement security mechanisms, several researchers have modified and developed various security techniques including trust and reputation based security systems to ensure the WSN is secure against any malicious attack. However, many security challenges still need to be considered before proceeding ahead with developing various security models.

In this paper, our main objective is to design a unique framework that detects malicious nodes present in the network by integrating decentralised blockchain technology and trust management systems to overcome the shortcomings of other existing work. Firstly, we consider two critical node parameters, namely, energy consumption and packet forwarding rate, to mitigate the lack of trust. These parameters are recorded periodically and utilised to compute the trustworthiness and reputation of each node. Secondly, the data packets are validated by a decentralised blockchain that contains records of identity, key and reputation maintained by several base stations in a distributed manner. Our work examines the potential for a combination of a trust model and the blockchain-based reputation that expects to make more accurate decisions about malicious nodes present in the communication network by working with the blockchain model to validate the data packets.

II. Related Work

During our literature review, we found that few papers [1] [2] [5] have addressed the mitigation of routing attacks either trust-based or blockchain-based security mechanisms. The review has shown a lack of trust between the sensor nodes related to the exchange of information, which has led some researchers [3] [4] to propose trust and reputation-based security systems for detecting any anomalous behaviour of a node.

In some cases, both techniques have been used, however, most papers that use blockchain-based mechanisms rely on the Proof of Work (PoW) consensus mechanism that is extremely resource-intensive for low battery devices such as wireless

sensors. It is also notable that some papers using blockchain-based techniques only use blockchain as a storage mechanism while there is no effort to extend the scope of blockchain usage. Therefore in this work, we have designed a new framework that uses both the techniques and the Proof of authority (PoA) consensus mechanism.

III. Methodology

In this paper, we address the issue of malicious nodes present in WSNs disrupting routing activities. The objective is to identify these malicious nodes and minimise the likelihood of selecting them as a next-hop node by prohibiting them from routing activities. Figure 1 shows the architecture for the WSN topology considered for our proposed framework. The proposed model consists of cluster-based WSN with blockchain consortium and static sensor nodes deployed in the sensing environment. With higher memory and processing capabilities, the base station acts as a trusted entity and gateway for blockchain. It carries out functionalities like managing blockchain and transaction data.

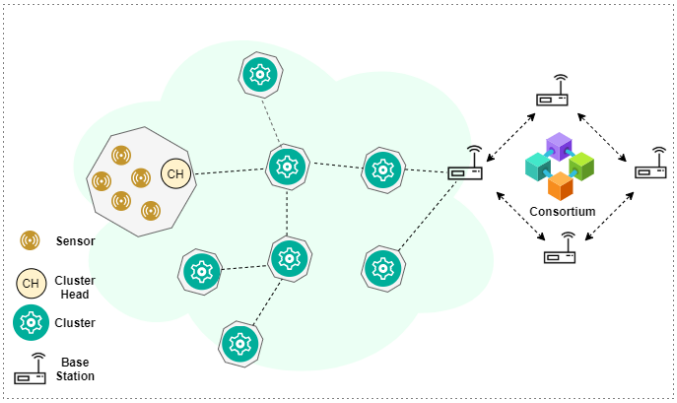

Fig. 1. Network Setup for Proposed work

We propose a solution by developing a framework that has two parametric components namely trust and reputation. Trust component uses communication trust as a parameter to identify whether the packets are forwarded successfully or dropped. Whereas, blockchain based reputation system uses energy as the core component for estimating the reputation of the node. This involves two phases confidence score calculation and reputation estimation. We also develop an algorithm that calculates the confidence score using the energy consumption of nodes and uses blockchain to store and validate the information of the data packets. The framework also calculates the reputation based on historical confidence values. Furthermore, we find that there has been no effort to solve the malicious node detection using a PoA consensus algorithm, which requires less computational resources and makes it suitable for WSN.

The malicious nodes in the computed paths are identified during the detection phase at sink node, which requires every node to append its id, residual energy and trust on its relay node to the data packets as encrypted tags and send them to the relay node with the packet. The tags are added sequentially by intermediate nodes until the packet reaches the sink node. The decryption process begins at the sink node, where all the tags are decrypted using the sink node's private key, which allows the sink node to gather all the trust values and energy levels of each intermediate node. Later, the sink node estimates the reputation of the intermediate node based on historical confidence scores. Also, it determines the average trustworthiness by aggregating the trust scores received from various child nodes. Both trust and reputation are verified against the predefined threshold to decide on its maliciousness.

IV. Evaluation and Results

This section will describe the experimental evaluation for our proposed framework. We evaluate the performance using the Network simulation tool (NS3) after performing various simulations. Additionally, we have compared our proposed framework with an existing security model BTEM. Several parameters such as detection rate and trustworthiness of nodes are studied while varying the number of malicious nodes present in the network

A. Discussion of results

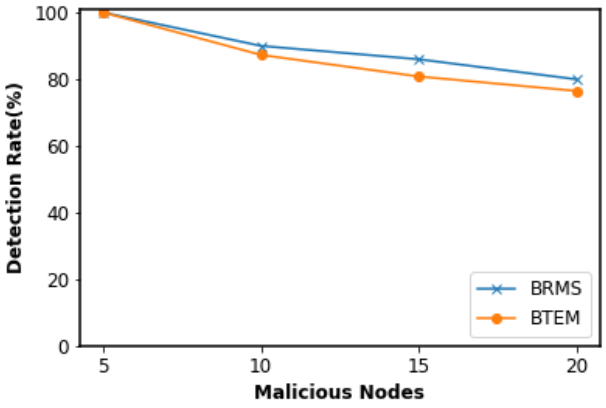

Fig. 2. Comparison with BTEM model: Detection Percentage

From Figure 2, we observe that the detection rate of our framework is better than that of BTEM. The detection rate for both the frameworks is dropping as we increase the number of malicious nodes but still, our framework outperforms BTEM by some margin. The reason behind this performance trend is attributed to our two parameters trust and blockchain-based historical reputation. Contrarily, the BTEM paper only uses one factor to detect the malicious nature of a node, which often results in false positives. Our framework avoids false positives by using historical reputation calculated using blockchain.

Figure 3 shows malicious node detection over different dropping rates. We see that the performance for 30% and 50% drop rate has a similar number of detection rates. The difference is with respect to the time taken to detect these malicious nodes, it is observed that as the packet dropping rate increases, the framework requires more time to detect

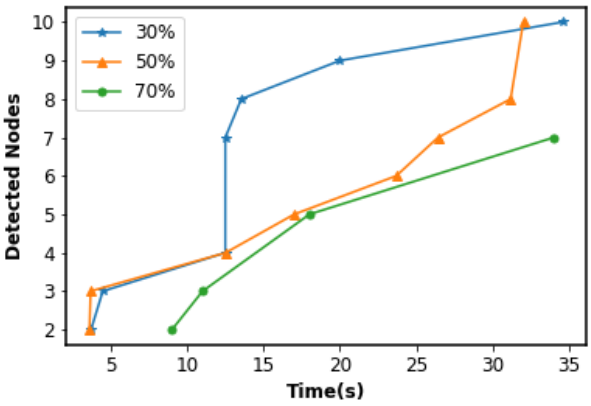

Fig. 3. Node detection variation over different dropping rate

the malicious nodes. The underlying cause of this trend is the inability of packets to reach the sink node as the packet drop rate increases.Due to the loss of packets, there are few historical records that permit us to detect whether a node is malicious or not. For the drop rate of 70%, the detection starts slightly late due to the same reason mentioned above and it detects fewer malicious node compared to 30% and 50% drop rates.

B. Security Analysis

In our framework, the majority of the attacks are detected during or after the decryption phase at the sink node. Based on our simulated network, we have performed an analysis for our framework. In this analysis, we demonstrate our framework's usefulness in detecting various kind of malicious attacks.

- **Selective forwarding attack** The selfish behaviour is shown by node by dropping a packet. For every packet drop, the nodes trust would decrease and eventually only consume a small amount of energy in receiving the packet. Our model is designed in such a way that if there is a packet drop, energy consumption will decrease, which will lead to a decrease in reputation over a period. When the reputation is below the predefined threshold, we can say that the node is malicious.
- **Node insertion attack** The framework requires all sensor nodes to get registered first before deployment. These nodes are allocated with the keys and enrollment certificates stored on the blockchain. If a node's identity is not matched with any node certificate present in the registration list, then the sink node detects malicious node insertion in the network.

V. Conclusion

Wireless sensor networks face many security threats during data transmission leading to the disruption of data availability. To counter this problem, we have proposed a decentralized framework for reputation management and malicious node detection. The nodes which hamper the data routing through selective forwarding of data packets are discovered by estimating their reputation through blockchain and trust from child nodes.

In this work, we assign a reputation to each node as the data routing progresses. The reputation for malicious nodes allows us to determine the malicious activity carried by a node. The reputation of a node is calculated using a nonlinear function which over a while falls rapidly for node showing selfish behaviour. Besides, using a Proof of authority consensus mechanism between validators rather than traditional consensus like Proof of work proved to be beneficial for low-powered sensor devices where transactions are validated by fewer validators before committing to the blockchain. The proposed model has been simulated on NS3 and compared with an existing model to evaluate its performance metrics like detection rate and detection accuracy. The security analysis represents an enhancement in recognizing the malicious behaviour and the reason behind it is using two parameters that prevent any false positives. The results reveal the effectiveness of our proposed framework

References

[1] W. She, Q. Liu, Z. Tian, J. -S. Chen, B. Wang and W. Liu, "Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 38947-38956, 2019.

[2] V. Dedeoglu, J. Raja, D. Guntur , D. Ali , "A trust architecture for blockchain in IoT, "Computing, Networking and Services, pp. 190-199. 2019.

[3] U. Prathap, P. D. Shenoy and K. R. Venugopal, "CMNTS: Catching malicious nodes with trust support in wireless sensor networks," 2016 IEEE Region 10 Symposium (TENSYMP), 2016, pp. 77-82.

[4] R.W.Anwar, Z. Anazida, O. Fatma , I. Saleem ,"BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks." Future Generation Computer Systems 96 ,2019.

[5] M. A. A. Careem and A. Dutta,"SenseChain: Blockchain based Reputation System for Distributed Spectrum Enforcement," 2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), 2019, pp. 1-10.