A Dynamic Trust Model for Blockchain Network

Neha Mittal
SITE
Vellore Institute of Technology, Vellore
Vellore, Tamil Nadu 632014, India
neha.mittal2016@vitstudent.ac.in

Vani MP
SITE
Vellore Institute of Technology, Vellore
Vellore, Tamil Nadu 632014, India
mpvani@vit.ac.in

Abstract - This paper introduces a dynamic trust model for Blockchain Network. Initially all the nodes connected in the blockchain network will be initialized with trust level. Then, I use several approaches to dynamically update the trust level by the actions performed by nodes in network, such as mining, authenticating, validation, etc. This updating will take place on each node and only the rank will be visible to everyone not the value. These trust ranks will stay synchronized in the network. The decision taken by trust-worthy node need not to be criticized by a less trusty node. Using these trust ranks as a guide, a secure way of validating transaction and later mining over the block takes places which then reduce the chances of Sybil attack and Byzantine Fault Tolerance. This paper demonstrates advantages and concepts for establishing a synchronized, dynamic trust model and for using this as an application in securely storing transactions of supply chain goods in Blockchain.

Keywords: blockchain; trust rank; sybil attack; supply chain; privacy

1. INTRODUCTION

As Blockchain is introduced, the nodes would now been able to participate in the network while maintaining pseudo-anonymity as well as building **decentralized** and distributed infrastructure. Each node acts as master nodes in the network, and hence depreciating need of centralized and default master-slave model. This allows the infrastructure to scale-up and provides approximately 100% uptime.

Blockchain Network, despite of many advantages, also have some security vulnerabilities. Some of the mentioned are: double-spending attack [8], Sybil Attack [7,8], Block with-holding attack, 51% attack [8] etc. As Blockchain always lack central authority to govern, this raises issue whether to replace current system with this system or not.

Since Blockchain involves much of a security threats and vulnerabilities, any method which would be able to evaluate and verify trustworthiness of nodes constantly connected in the network is required to reduce threats for blockchains. In this paper, I propose a trust model to evaluate **trust ranks** for each node and define relationships with other nodes to identify the malicious actors and remove that from network.

This paper is organized as follows, Section 2 presents background study and related surveys, trust model description and implementation in Section 3. Section 4 describes the results and future work of this framework., and Section 5 concludes the research.

2. BACKGROUND STUDY

A dynamic trust model has been developed and maintained for MANETs [1]. The main aim of this paper is to prevent ad-hoc networks from malicious nodes and provide secure routing path for communication and sending data packets. The need of dynamic trust model is to enhance message routing, and reducing existing threats. Evaluation of nodes for choosing the best route path for developing collaborative ad hoc model. They found an approach where there is no need of using time-synchronization and authentication systems, as well as maintaining route and behaviour. And also, integration of current routing protocols which are used in mobile ad hoc networks. This model can be applied to any general application and is not specific.

This paper [2] takes previous history record of nodes to take an account for dynamic and adaptive trust evaluation. This paper focusses majorly on the adaptive condition for wireless and mobile infrastructure. They aim to find the effective approach by looking at the previous record as an evidence to predict future behaviour of the current node which involves mathematical computational. This at last is useful to prevent improper behaviour as well as install new security measures to ensure reliability in environment.

A Bayesian trust model has been introduced [3] that has taken the dynamics of trust calculation and evaluation to the whole new level. The belief of statistical model and symbolic approach are used as complementary. Formation of low-level and high-level layers guides to focus on two different aspects. The basic trust dynamics are taken into account by low-level layer which integrates with the actor by calculating the weightage of components involved in it. Basically, the negative and positive experiences play a major role in making system learn how to build up a dynamic model Whereas the high-level layer taken symbolic approach into account which involves trust components manipulation. The dynamic form discussed here is believed to have dependent on social norms as well. These social norms will make the connection between both the layers.

This paper [4] focusses on dynamic model for WSNs to resist selfish nodes behaviours. Their model uses fuzzy sets and grey theory to calculate and ranked the reputation factor for neighbouring nodes based on their relationship with them. The dynamic nature of model is evaluated into time slices which is used to recover those selfish nodes. These time slices eventually used to predict the time that network has performed negative and positive and based on that giving positive and negative values for itself and the neighbouring nodes.

Self-monitoring and dynamic model for trust [5] is very important when someone is looking to move their architecture to the distributed architecture which lacks our very own central authority-based model. EDTM is such method which solves the problem by efficiently exchanging data and information and also involving only the trusted nodes to prevent leaks in the information. After the simulation has been achieved, this method can be inferred to attack-resistant trust model, but at the same time required some prior assumptions for absolute results. The challenge of selecting true assumption value is still not known and require a deep analysis for working which are going to be out in the next research. This paper describes approach like how to monitor and synchronize the trust level for detection of malicious node in WSNs and also preventing the most common and threatening attack of Byzantine Fault.

The paper which gives the proper and quoted relationship between time and trust value has used Ant-Colony Algorithm [6]. The base theory and argument for this is to provide a real-time trust calculation and updating model using Ant-Colony. After this implementation they have aimed to achieve a relationship between trust, time and inter-operation event. There are certain assumptions which are used to simulate the results that all the inter-operations are successful. And the complexity of this algorithm for updating trust is $O(n^2)$.

3. DYNAMIC TRUST MODEL

I define trust model as reliable, timeliness model for storing transaction on a Blockchain in a secure way and later on preventing malicious attacks from hackers. This integrity is maintained by knowing that which node is used to authenticate the corresponding transaction and which is responsible for writing that over a block. Some assumptions while making this base structure is that nodes are already present to be part of the network, which is synchronized based on their Physical and Logical IP address. Each node has a script which is running continuously in sync as well to dynamically updating the trust ranking for each and every node.

Based on the above assumptions and specifications, I design the trust model as follows. Initially a layout or the base structure of blockchain is developed using NodeJs, which has all the basic functionalities that a blockchain should possess. These include consensus algorithm, mining algorithm, and hash functions. When the node initially joins, they need to copy the first block which is genesis block, and later on all API-endpoints are automated for successful launch of node.

After launching of desired number of nodes for first time, initial trust value would be assigned based on the past activity (if nothing found then by default 0 would be assigned). These script works in synchronization and regular updating phase of 100 seconds, which ensures to eradicate any mismatch between the trust ranking. 100 seconds is by default taken, to bypass or give ample overhead for all the desired steps to happen in single iteration.

When a node does not agree with the majority decisions of authenticating, mining or validating a new transaction and block respectively, then it is treated as it wants to deceive the network and there would be reduction in the trust value which would ultimately lower the reputation factor. If it goes below to the certain point, then respective node is permanently banned from the network and would not be able to become a part again.

On the other hand, if a node behaves positive in the network and is not involve in the malicious activity, will be rewarded with incentives. These will be

added up to the trust value of the node and will eventually increase the rank of node in the network

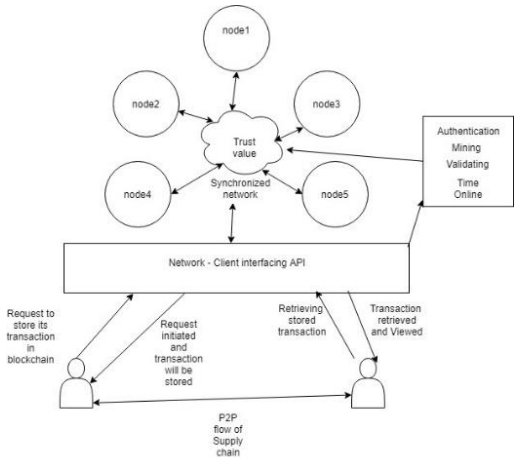

Fig 1: *High-level design of dynamic trust model for Supply Chain*

.And for adding dynamic nature in model, there is time-based incentive. The node which stays longer in the network will be given more points then the node which often comes online in the network for few moments. The reason for this consideration is because they somehow by staying online make 51% attack difficult to execute. Example if there are 7 nodes, then to gain control over the network the attacker needs to change data store on 4 nodes. Whereas, if the number of nodes increase to 11, it takes 6 nodes being attacked to take control of the network. So that's why time-based incentive will be provided which contributes to the trust value of nodes which are connected.

One example of application that could be implemented over this trust model for Blockchain Network is Supply Chain Management [9]. The peer-to-peer transfer of goods would be stored which first authenticates the correct address and then adds the transaction in the block in the blockchain. The node which get request for transaction processing first for authenticating and then later for mining the blocks, if they have high trust value, then decision would be accepted by other nodes. However, if the trust rank is lower, then approval of at least majority of nodes would be needed for future progression.

A. Algorithm

As, we have discussed till now, there are some positive and negative values which are going to decide the ranking of the nodes in the network. Now, if we talk in context of the Blockchain architecture and functionalities which govern seamless transaction processing of applications. Some of the methods which could be use to find the trust values are as follows

1**) Authentication**: Authentication of transaction prior to storing over the permanent blockchain is very important as if we are storing the illegitimate data which cannot be over-ridden later would soon make questioning the integrity and safety of blockchain. The node that is going to authenticate would be provided the incentives.

trust_node ← trust_node +1 (for positive)

trust_node ← trust_node -2 (for negative)

This is self-explanatory that, if the authentication results are positive the node will gain +1 and if the authentication results are negative it will lose 2 points per transaction. To being correct, you need to agree with majority of the nodes i.e. with N+1/2 (if N is odd) and N/2 + 1 (if N is even).

2) **Miner**: Miner defines as the block which is going to mine the block or in the simpler terms we can say, adding new blocks to existing blockchain. The mining function is as complex as it seems like, as mining awards are provided by the network after validation of new block. So, every node will come under race condition and try to solve the cryptographic puzzle, whoever solves that puzzle first will get the reward as well as increase in trust rank if validation is successful. The factors of selection of mining nodes in this case if dependent on the previous records as well as connectivity in the network. So, the node which has low latency tends to have higher connectivity in the network. The choice depends on these factors solely and after the mining is done the trust value will be updated as follows.

trust_node ← trust_node + 8 (for positive)

trust_node ← trust_node -16 (for negative)

If after the validation the block found to be legit would be added in the blockchain, trust value increase and mining rewards would be provided to that node. However, deduction is done if block found out to be selfish and disrupting. If a node has created a block just now, there is a wait time for that node. The wait time is of increase in N/3 length of blockchain, until then that node would not been able to participate in the mining process again. There

could be a DOS attack node there which can stop the service of other nodes and try to mine maximum blocks possible, i.e. if a node A has mined the block of #32 and there are presently 11 connected nodes in the network. Then A has to wait until the length of blockchain reaches #35 then only A can participate in the maximum process.

3) **Time-Connected**: This is most important factor which is the base of implementing time-trust relationship and provide dynamic nature of trust model for blockchain.

For every 100 seconds of nodes given to the network +1 value will be added in the trust value which then reflects in the ranks of nodes.

trust_node ← trust_node + 1(for every 100s).

These mentioned methods and helper functions have been implemented in a script which will run infinitely and continuously update trust ranks for each node gets connected in the network. If a certain node disconnected then, the checkpoint will be stored in that node and every node indicating the last rank of the connected node. Whence it joins again, consensus would synchronize the new length of chain and start calculating trust ranks from that point.

B. Trust Level Calculation

Based on the algorithm that is being discussed above. The procedure of building trust follows like this.

After the synchronization of the nodes, the algorithm starts infinite script which in each iteration give out a trust value for each node. Those values received would be fed in the trust rank function where a pre-defined range is there. A mapping would take place between trust value and its correspondence rank and then the visible rank would be displayed. The values for each role and final value of each node is hidden and they can't view it for security purposes, otherwise the most weightage factor would be chosen by nodes and this greediness would exploit the network flow and compromise everything. It is as similar as calculating ELO ranking in multi-player online gaming.

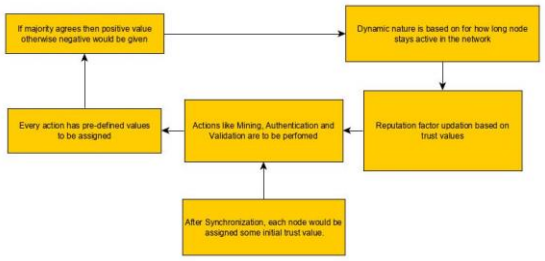

Fig 2: *Flow of trust value calculation for each node*

4. RESULTS AND FUTURE WORK

Several vulnerabilities and threats with blockchain network are discussed in the introduction section. The dynamic trust model is presented in this paper which successfully prevent network from Sybil Attack and Byzantine Fault Tolerance.

Each node needs to maintain ample amount of network connection and have to give computation power to stay in the network and to gain good and respected trust in the network, until they try to forge intentions and perform negative in the network (Sybil Attack). The node has to give more as they get even after successful attack execution. So, the profit margin is not that great to do that.

There is a connection between each node and the decision which is made by majority will be taken into account. And the node which is not agreeing with the decision or providing false information would be given negative values. Hence, making Byzantine Fault Tolerant architecture. Additionally, in the structure of blockchain a simple Proof-of-Work algorithm is implemented in the mining process which adds another prevention layer for the same.

Fig 3 shows the storing of transaction of supply chain application over the blockchain which is done by one peer to another. This also shows the node which is responsible to authenticate the transaction and hashes of previous and current block which ultimately creates cryptographic link between blocks in blockchain. And also, the nonce value, which is a solution of this block.


```
"index": 2,
"timestamp": 1554671551955,
"transactions": [
  {
    "node": "http://192.168.43.117:3002",
    "name": "Silk",
    "buyer": "WERGHNBVFTYHJMNBVFD",
    "seller": "VFRTYUIKMNBVFGHJNBGG",
    "amount": "120",
    "price": "400",
    "transactionId": "30e8d170597911e9b7099bb384a29e08"
  }
],
"nonce": 210096,
"hash": "0000f6c70baa8caf59a41fc394595025d6a155aa7505a3acd15fcb7871887a11",
"previousBlockHash": "6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b"
```


Fig 3: *Sample block which is storing transaction and other related information.*

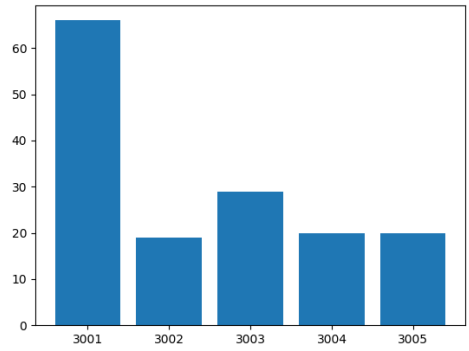

Fig 4: *Trust values of each node after 10 iterations.*

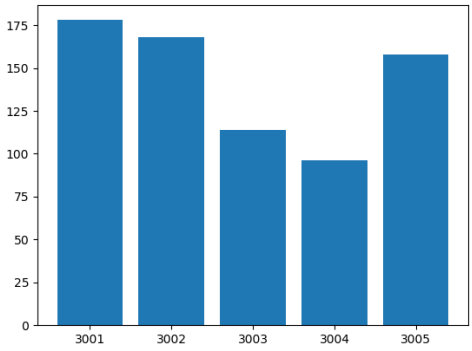

Fig 5: *Trust values of each node after 50 iterations*

Fig 4 and Fig 5 shows the simulation of trust values after 10 and 50 iterations for the network of 5 nodes. First 10 iterations, as specified, does not have any restrictions in which nodes to be selected for transaction and which is to be selected for mining. Hence, we have node 3001 become outlier with maximum trust. But as the algorithm runs, we can see there is not much increase in the 3001-node trust value and infrastructure somewhat becomes normalized. After 50 iterations, we can say the least trusted node is 3004 node and any activity which is done by this node would require a majority-based agreement to process further. That's how the above argument of attack prevention works.

The model I purposed is somewhat linear building model and may require some modifications and enhancement in the algorithm as a future prediction of trust ranking.

The architecture will cope-up with reducing trust factor for DOS attacks but still not prevent DDOS attacks. The node on which Denial-Of-Service attack is going on may not find its way to get connection-based incentive which will not increase the rank of that node and make it vulnerable to sustain in the network.

The maybe possible solution for making this trust model more advanced is to give it a human-like thinking mechanism which again involves Neural Networks and Deep Learning algorithm. This is reserve for another time which then involves new algorithm

5. CONCLUSION

To present this type of dynamic model for enhancing security and involving reputation factor based on actions of nodes is essential. The accuracy and trustable transaction information is at the utmost priority of this model. Again, the goal of this paper is to discuss and develop dynamic trust model for blockchain network that could be used for seamless transaction storing over the blockchain and as well as reducing security threats. The approach discussed doesn't reveal the nodes internal information and doesn't try to alter the information stored by blockchain. The concepts here cannot be govern by a central authority and should only be applied for decentralized network. This is generic concepts and could be applicable to any decentralized application for example in here we applied it to Supply chain.

REFERENCES

[1] Zhaoyu Liu, AnthonyW. Joy, Robert A. Thompson A Dynamic Trust Model for Mobile Ad Hoc Networks.
[2] Azzedine Boukerche, Yonglin Ren, and Richard Werner Nelem Pazzi An Adaptive Computational Trust Model for Mobile Ad hoc Networks.
[3] Dimitri Melaye and Yves Demazeau Bayesian Dynamic Trust Model.
[4] Guowei Wu · Zhuang Du · Yibo Hu ·Taeyoung Jung · Ugo Fiore · Kangbin Yim A dynamic trust model exploiting the time slice in WSNs.
[5] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, and Mohsen Guizani An Efficient Distributed Trust Model for Wireless Sensor Networks
[6] TANG Zhou, LU Zhengding, LI Kai Time-based Dynamic Trust Model Using Ant Colony Algorithm
[7] Zyskind, G., Nathan, O., & Pentland, A. "Sandy." (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops.
[8] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer System
[9] Korpela, Kari, Hallikas, Jukka, Dahlberg, Tomi (2017). Digital Supply Chain Transformation toward Blockchain Integration