International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V70I2P2238

Volume 70 Issue 2, 328-342, February, 2022
© 2022 Seventh Sense Research Group®

Original Article

Energy Efficient Optimal Transaction Selection and Elimination for Energy Efficient Secure Blockchain Transaction

Michel Rwibasira[1], Suchithra R [2]

[1]*PhD Scholar in Computer Science and Information Technology Jain University Bangalore, Karnataka, India*

[2]*Head of Department of Computer Science and Information Technology Jain University Bangalore, Karnataka, India*

[1]kananura25@gmail.com, [2]suchithra.suriya@gmail.com

Abstract *- Blockchain is a secure, shared, and distributed registry that makes recording and tracking resources easier without the use of a trusted third party. It enables both sides to communicate and share resources within a network of partners, rather than a single central body, where distribution decisions are determined by a majority. In general, what is valuable can be tracked in a blockchain network to reduce security risks and save on security check costs for all stakeholders. Ledger technology distributed in blockchain has emerged in recent years as a successful platform for machine-to-machine commerce. When writing a blockchain ledger requires a high memory of almost 395 GB in the system without permission. Therefore, any activity accepted by any participant is likely to increase the book size. On the other hand, the authorized system assumes that the registration is copied only in a closed group of known participants. This can lead to smaller registrations, but it can also mean that multiple ledgers are stored at the same time. To overcome these shortcomings, this paper has developed a proposed method for reducing the size of common notebooks in a blockchain system based on Energy Efficient Optimal Transaction Selection and Elimination (EEOTSE). EEOTSE approach reduces power and optimizes blockchain framework. In addition, multiple attacks such as 51% attacks, double costs, and selfish attacks affect the security of the blockchain. To prevent these attacks, the proposed method presented in this article is called the BLCMAShield method. BLCMAShield provides high security with low execution time compared to other existing methods. Attack detection rate, error rate, execution time, power consumption is used to analyse the performance of the BLCMAShield & EEOTSE method and are compared with the existing method. Experimental results show that BLCMAShield & EEOTSE provides the best results from existing methods.*

Keywords – *Blockchain, 51% attacks, double costs, selfish attacks, BLCMA Shield and EEOTSE.*

I. INTRODUCTION

Bitcoin was the world's first truly decentralised global currency. Its primary goal, as with other currencies, is to facilitate the exchange of goods and services through creating a shared commodity. It is not, however, issued by the government or even a single organisation, as is the case with traditional currencies. Bitcoin has shown tremendous growth in both value and quantity of transactions since its launch in late 2008. Its success stems from the creative use of a peer network to track all parts of a currency's life cycle, from creation to transfer between users. This is in contrast to prior research [1], [2], [3] or consumer credit generation [9] that focused on developing systems that relied on intermediaries. Users must trust the original issuer, which is still employed to clean up operations, in order to use these systems.

Bitcoin is commonly compared to currency since transactions are almost instantaneous and irreversible. Bitcoin, on the other hand, is beyond the reach of currency, allowing global transactions to keep up with local items. It has a history of public transactions as well as a number of new and creative applications, including smart real estate, micropayments, contracts, and escrow transactions for dispute settlement. Bitcoin is gradually becoming a viable alternative to the US dollar or the euro as more businesses accept bitcoins for their products and services. Bitcoin's continued existence demonstrates that the underlying concepts are sound. However, there is room for improvement. Blockchain is a new technology that allows you to execute digital transactions in a matter of seconds. Blockchain is a secure, shared, and distributed registry that makes recording and tracking resources easier without relying on a trusted third party. It allows both sides to communicate and share resources within a network of partners, rather than a single central body, where distribution decisions are determined by a majority. It is proved to be safe from attackers attempting to take control of the system through connecting the central controller. Money, houses, automobiles, and land are all examples of tangible resources. In general, valuables can be tracked in a blockchain network to reduce security concerns and save all stakeholders money on security checks. Ledger technology distributed in blockchain has emerged in recent years as a successful platform for machine-to-machine commerce.

Although distributed registers can be a key factor in emerging technologies such as machine-to-machine automation, the storage space typically required for registry setup can be large prohibitive for many types of devices. When writing a blockchain ledger requires a very high memory of almost 395 GB in an unauthorized system (open to the public). Therefore, any activity accepted by any participant is likely to increase the ledger size. On the other hand, the authorized system assumes that the registration is copied only in a closed group of known participants. This can lead to smaller registrations but can also mean that multiple ledgers are stored at the same time. To overcome these shortcomings, this paper has developed a proposed method for reducing the size of the common ledger in a blockchain system based on Energy Efficient Optimal Transaction Selection and Elimination (EEOTSE). This proposed method allows each network participant to independently select and exclude any operations that have already been performed. The EEOTSE method reduces the execution time of the blockchain method by reducing the size of the book. By reducing the computational time, energy is also stored within the framework we provide. The proposed method has the ability to extract unmodified status data structures after eliminating some common registry operations from other operations. However, blockchain is introduced into the Network. Unfortunately, the difficulty with blockchain knowledge in large networks is that a few nodes will not be proficient at controlling the neighbours when it crashes. When you turn on the live function, it reasons an extended circuit, not a small circuit. In fact, the idea is that each novel block contains the hash approach of the preceding chain, and under certain situations, if the node does not succeed, there will be no data update during the failure. He (who is he) then discovers that not all nodes in the blockchain system have similar information, yet if he employs circulated registrations, which becomes a major confront that requests to be attended to in the blockchain. In addition, 51% of assaults have the ability to build two chains, one public and one private, implying that the public blockchain can be shared with others in the blockchain network, but the private blockchain keeps previous transactions and expenses private. The attacker then launches a private chain, which was acceptable in the Network due to the blockchain notion of long-chain imitation. At the same time, double expenses will display. Furthermore, because it is a node with 51 percent power, the assault can stop some actions because it is a node that is faster than others in the Network and can select to close each operation from a specific address. Even if no blockchain includes any blocks, such as those with 51 percent, it can sometimes be a mining monopoly, causing other miners to abandon the Network because it can mine all of the blocks as well as all future blogs and prizes (incomplete sentence). The government may prove that the attack can double the cost and ban particular IP addresses on the Network to deter people from using the blockchain because it is a highly costly attack to implement. To prevent these attacks, the proposed method in this work is called BLCMAShield Approach. This new approach improves blockchain security and prevents 51% attacks, double costs, and selfish excavations.

The main contributions of this paper are summarised as follows:

(i) To develop a novel security mechanism BLCMAShield for blockchain framework to prevent 51% attack, double-spend and selfish mining attack

(ii) To develop a novel energy-efficient, high-performance blockchain framework.

(iii) To develop an Energy Efficient Optimal Transaction Selection and Elimination (EEOTSE) for reducing the memory and execution time of blockchain.

(iv) To achieve high security with low execution time than the other existing approaches

(v) To minimise the energy using EEOTSE and maximise the efficiency of the blockchain framework.

The manuscript of this document is organized as follows: Section 2 discusses some of the relevant contemporary literature. Section 3 presents a detailed description of the proposed architecture. Section 4 presents the experimental results, which include the general operating results of comparing the performance of EEOTSE and other compression methods previously published. Conclusion and Conclusions and future work are provided in Section 5.

II. BACKGROUND

In bitcoin, a peer-to-peer electronic money system, blockchain guarantees the eradication of double-spending. When comparing blockchain to banking institutions, it appears that decentralised systems are more protected against attacks and damage. However, many assaults continue to occur in the blockchain, posing a severe threat to user security. In blockchain networks, DDoS assaults are fairly common.

Vasek et al. [5] demonstrate a practical investigation into the occurrence and impact of distributed denial of service (DDos) attacks on bitcoin operators. They discovered that currency exchange, mining, and gaming businesses are more likely to be targeted than other businesses. DDos is more prevalent in larger water tanks than in smaller ones. Danny [6] discusses and shows bitcoin vulnerabilities such as 51 percent assaults, double fees, dust operations, and code-based attacks. All of these attacks make it easy to create personal networks. Herrmann [7] analyze bitcoin systems, particularly double-cost prevention mechanisms, for the possibility of double-spending attacks and find weaknesses in certain usage scenarios. People expect to examine attributes to handle or prevent numerous threats when they are recognised. Decker et al. [8] examine how bitcoin distributes transactions and blogs throughout the Network to update copies of books using multi-hop broadcasts. All of this blockchain research is critical and beneficial to its security. Many applications based on blockchain have emerged as a result of its development. Watanabe et al. [9] New blockchain delivery mechanisms for contract administration, such as digital rights management, are included. Digital contracts lower user prices and make it impossible for anyone to reject or amend the content.

Because of the unequal knowledge and the opaque supply chain, there is an imbalance. By studying the potential of blockchain technology in logistics, Badzar el at. [10] hopes to contribute to research in the fields of logistics management and supply. They employ blockchain to boost supply chain transparency for both suppliers and consumers, enhancing the security and standardisation of online commerce.

Wilkinson and colleagues [11] are developing open-source software projects to demonstrate the concept of decentralised, secure, and efficient cloud storage. Some people are even using blockchain to connect their applications. Xu et al. [12] are a group of researchers who have come up with a novel way to solve. Proposing new approaches based on new types of distributed software architecture can assist individuals in agreeing on shared states without the use of centralised integration points or specific participatory components. With the usage of blockchain technology in software engineering, the application development process will be expedited, and the success rate of application development will improve. According to Alibaba's projections for the top ten technologies of the future, blockchain is a feasible and critical technology. As a result, further blockchain research is needed.

Bitcoin, while being a young system, has sparked a lot of research in a variety of fields. The legislation [1], economics [4], and technological aspects of bitcoin are all explored. In the original Nakamoto document, the problem of double costs is addressed, albeit only in principle. Karame et al. [16], in numerous scenarios, has examined the probability of a successful double value attack. We introduce the idea of information hiding, which produces this problem, notwithstanding the potential of double costs that cannot be discovered by a longer detection period. In a quick payment situation, Bamert et al. [3] provide some relief from the problem of multiple charges. The incentives for nodes to relay information to all networks were found to be insufficient by Babaioff et al. [2]. Miners perform fees-related activities and request them by being able to produce blocks that include transactions, which is the present system's dominating technique. Bitcoin mining frequently necessitates specialised equipment and consumes excessive energy. Becker et al. [4] compare the environmental impact of bitcoin to traditional currencies. Their conclusion is that while bitcoin transaction costs are modest, maintaining and securing the Network against attack is costly. The quantity of computing power in a network, as we've seen, is likely to fluctuate. The anonymity of bitcoin transactions is another point that has sparked heated debate. The fact that all transactions are recorded in a copybook and the transaction's details are visible to all network participants indicates that confidentiality is impossible. However, Nakamoto says that confidentiality is an alias because the account holder's identity and the identity of the account are kept separate. [15] Reid et al. analysed the claim and concluded that the owner's details might be obtained by reconciling the confidentiality of multiple accounts involved in a transaction. Shamir et al. [17] used a number of worldwide statistics to examine the transaction chart, including an estimate of 78 percent of outbound bitcoins and an in-depth examination of the busiest places in the transaction chart. Elias [18] explored the legal and ethical implications of bitcoin's lack of anonymity. ZeroCoin [13], which permitted the launch of a decentralised coin mixing service based on zero-knowledge, later addressed the issue of anonymity in Bitcoin. Hanke et al. [14] has previously introduced payment mechanisms for bitcoin contracts and provided transactions between dealers and their clients. Another method based on the commitment from blockchain to carbon dating is CommitCoin [19].

Mwittende et al. [22] proposed a keyless, uncertified approach based on signature ring matching. In the early stages of communication, it creates session keys that allow users to store and access sensitive data. In the second stage, the protocol uses an uncertified ring signature to verify the user's identity, reducing calculation costs while maintaining user anonymity. A previous article [23] showed the ring signature system based on the elliptical curve algorithm. This approach creates a privacy storage protocol that protects the privacy of users' data and identities in the blockchain application, using the complete anonymity of the ring signature.

The security of existing signatures and the confidentiality of user identities are not guaranteed, as the Public Key Infrastructure (PKI) architecture uses registration keys for ringtone signatures. Once the attacker receives the registration key, the security of the existing signature and the confidentiality of the user's identity is not guaranteed. In light of the above, one study [24] found a powerful, secure ring signing system based on the Rivest-Shamir-Adleman algorithm. This approach ensures the anonymity of the signatories while providing mutual security. The security provided ensures that even if an attacker obtains a user's current key, he or she will not be able to reset the key from the previous step.

Even if an attacker gets the user's current key, backward security ensures that they will not be able to calculate the user's key in the future. The user's private key is updated in phases, and the signature cycle is divided into several times. As a result, even if the attacker gets the user's private key at this point, he or she will be unable to obtain the prior stage's private key or compute the later time, necessitating the usage of the strong forward secure ring signature mechanism.

However, there are not many statements about double-spending and 51% attacks on bitcoin, and we cannot find any conversion. This issue is addressed in the bitcoin wiki as a warning that states, "To avoid double costs, transactions should not be considered valid until a certain number of blocks in the blockchain confirm or confirm the transaction [sic]". [20]. There are a number of requests for companies that cannot wait for confirmation that is not very useful or has not yet been implemented [21].

III. MATERIALS AND METHODS

A blockchain is a collection of operations that are organised into blocks. Every transaction defines a state change in any type of data structure, such as a cash account statement or cache storage value. Every block has a header with enough information to identify all previous blocks and decide whether or not they have been updated. The sign of the previous block, as well as the sign of the operation included in the block itself, might be provided in the header.

This document presents a new approach called EEOTSEShield to ensure secure, energy-efficient blockchain operation. This is shown in Fig.1. There are two newly developed approaches: Energy Efficient Optimal Transaction Selection and Elimination (EEOTSE) and BLCMAShield. A detailed diagram of the proposed method is shown in Fig.2.

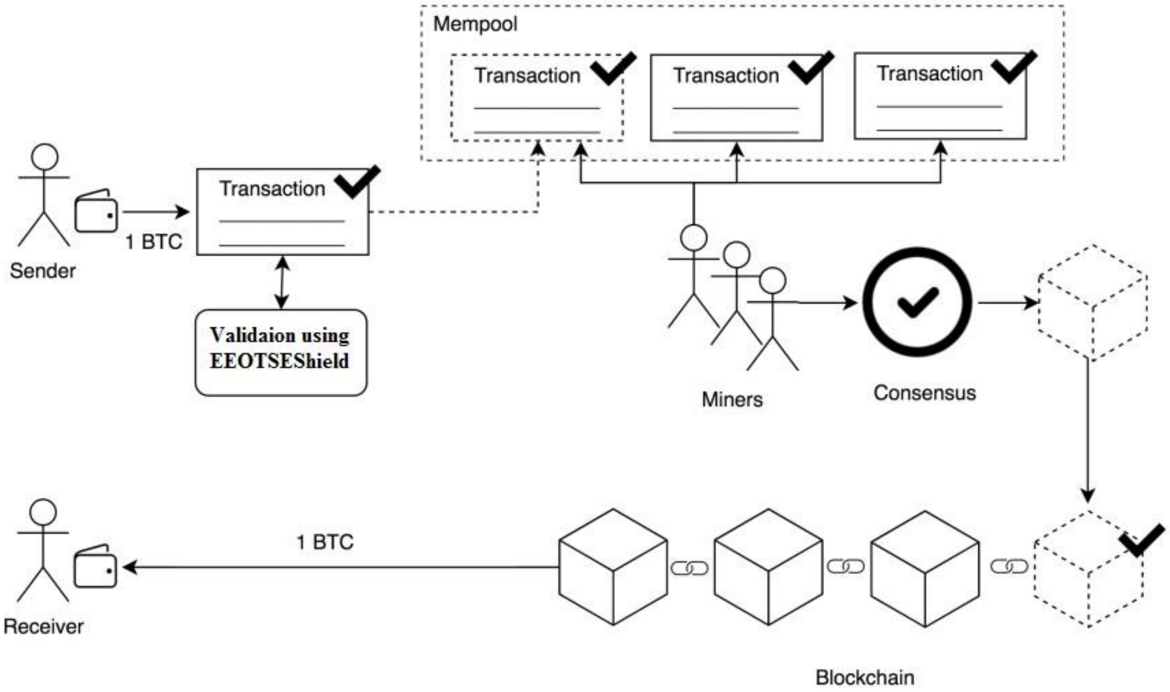


Fig.1 Detailed diagram of EEOTSEShield

The block is validated using EEOTSE. This should be interpreted as blockchain network participants' habit of omitting operations that do not contribute to important system features and are not very interesting. The system's protection against the loss of local units after reorganisation could be a method is similar to restoring disc space, with the exception that the process of interest can be left

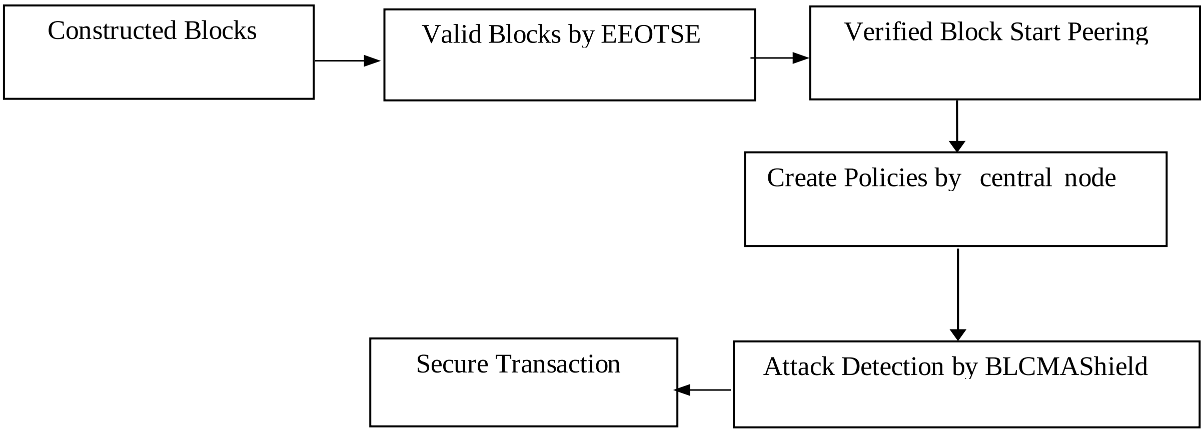

Constructed Blocks
Valid Blocks by EEOTSE
Verified Block Start Peering
Create Policies by central node
Attack Detection by BLCMAShield
Secure Transaction

Fig.2 Overall flow diagram of EEOTSEShield

Network's participants' information demands. This key feature, while the interest is determined by the unattended while the ability to restore the data structure to its original condition is preserved. If certain circumstances are met, you should leave. The arbitrary prediction functions, which can be set to remove only transactions that cancel each other or are totally replaced by later processes, is used to control elimination

This work also provides security in the blockchain against 51% attacks, double spend and self-attack by introducing the BLCMAShield Approach. In BLCMAShield, attackers start to enter the Network because their privately constructed blocks interfere with the initial location policy and the long position principle. The general algorithm for the EEOTSEShield method is presented in Algorithm 1.

1. Initialise Network with normal node and a central node
2. Wallet creation for all nodes with public and private id
3. After wallet creation, the next step is to create a block
   - Block is created with (Block Id, timestamp, data, nonce, hash, previous hash)
4. An electronic ledger is created after a block is created by a node
   - Ledger is created with (Node Id, Block Id, Time Stamp, Previous Hash, Block Transaction)
5. And then Block Validation process is started using EEOTSE
   - Randomly Select Nodes for Mining
   - Before mining Blocks are validated using four conditions
     i. New Block hash == 0
     ii. previous block id +1 == Block Id iii. previous hash == new block hash
     iv. new block hash == hash value calculated for new black at t hash is time
6. If a new block satisfies the above four conditions, then this verified block starts Peering to Network
7. To start peering to Network, verified Block Signs with Private Key
8. This verified block is added to the blockchain
   - Calculate hash for a block
   - Add hash parameter to block
   - Add a block to the chain
9. After that central node created a policy
10. Central Node Send Identical Copy of the ledger to all nodes in Network
11. If a new block does not satisfy the above four conditions, it is considered an Invalid block
12. So Central Node delete hash from Ledger
13. After completing this process, the attack model is generated
14. In this process, one node is randomly selected as an attacker
15. This attacker node generates a private chain by creating blocks
16. And then Attacker Start Peering to Network

In this stage, the Attacker is detected using Block Initial spot & Long Spot Detection Process

A. BLOCK CONSTRUCTION : A block is the basic structure of a blockchain, which is a sequence of blocks creating a blockchain, as shown in the figure. 3. The first blockchain is called a building block that does not have a block before. Each block has a sign of the previous block. A block contains a set of operations that are visible online. The operation is performed by a unit called diggers that calculates the hash value using the public key of the recipient on the Network. Also, each block has a timestamp, nonce - helps to calculate the sign, the main block sign, the block version. A logbook is created after creating a block of nodes. The logbook is created with a Node ID, Block Id, Time Stamp, Previous Hash, Block Transaction.

B. BLOCK VALIDATION USING EEOTSE

In this step, the Block Validation process is started using EEOTSE. Flow diagram of EEOTSE shown in Fig. 4.

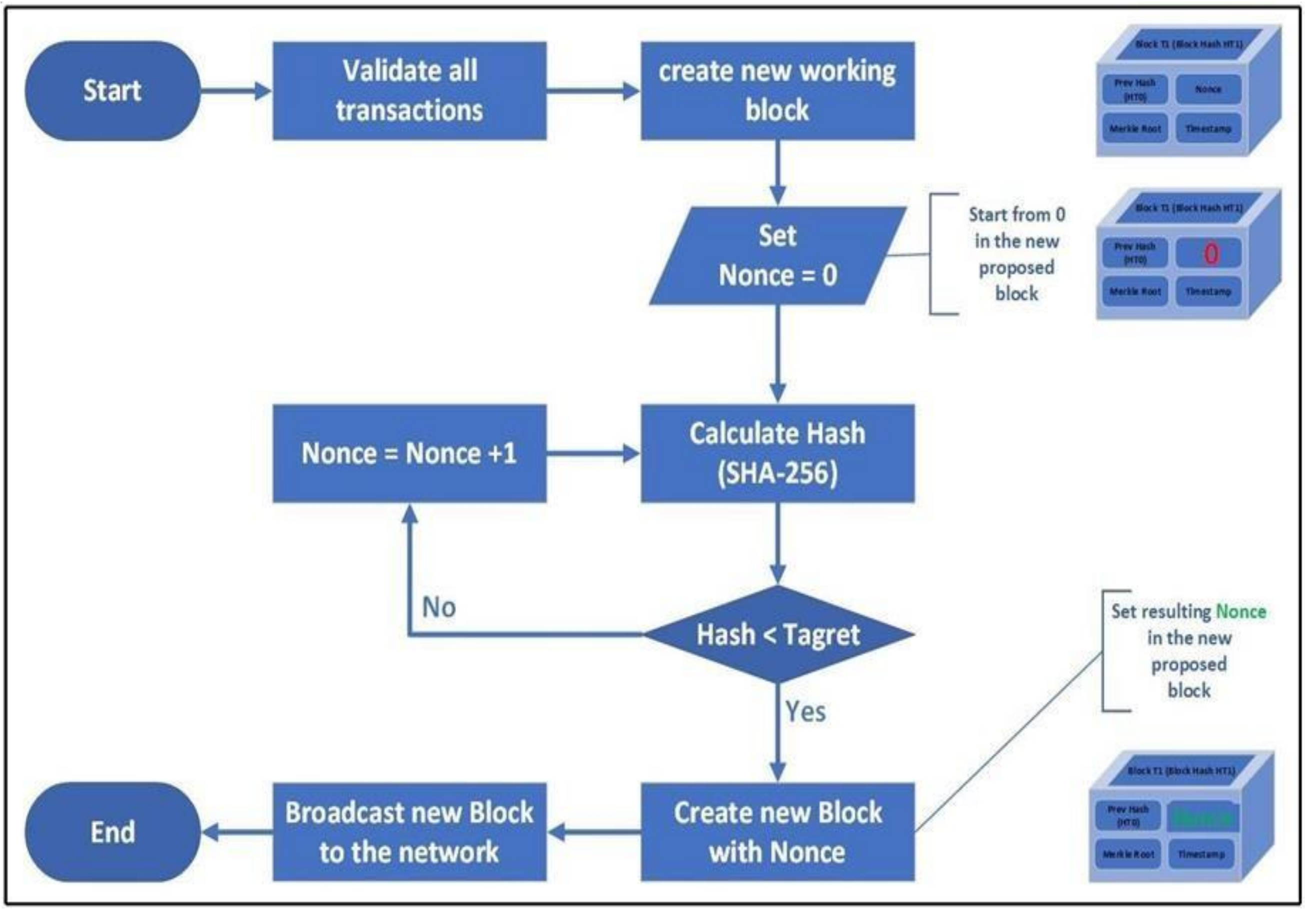

Start
Validate all transactions
create new working block
Block T1 (Block Hash HT1)
Prev Hash (HT0)
Nonce
Merkle Root
Timestamp
Set Nonce = 0
Start from 0 in the new proposed block
Block T1 (Block Hash HT1)
Prev Hash (HT0)
0
Merkle Root
Timestamp
Nonce = Nonce +1
Calculate Hash (SHA-256)
No
Hash < Tagret
Yes
Set resulting Nonce in the new proposed block
End
Broadcast new Block to the network
Create new Block with Nonce
Block T1 (Block Hash HT1)
Prev Hash (HT0)
Merkle Root
Timestamp

Fig.3 Structure diagram of a blockchain

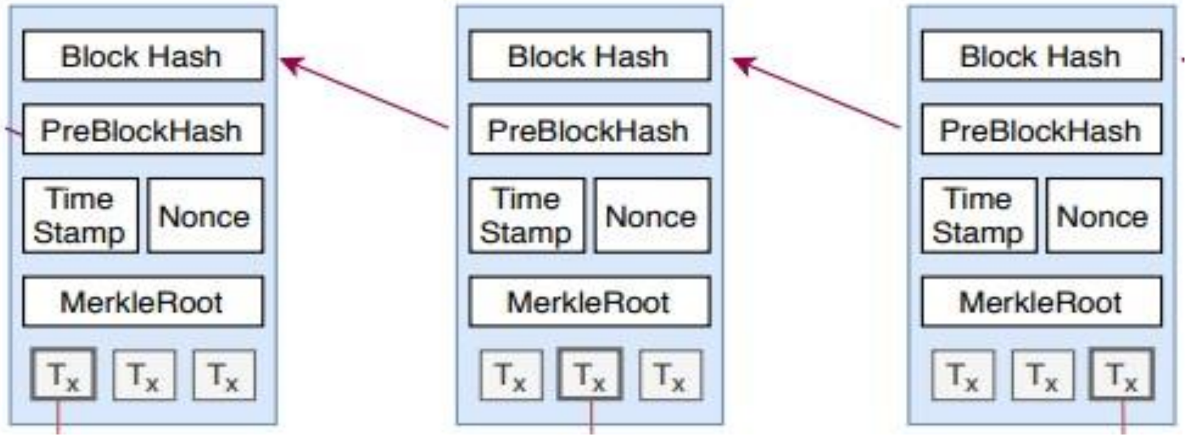


Fig.4 Overall Flow Diagram of EEOTSE

Blocks are validated using four conditions

1. New Block hash == 0
2. previous block id +1 == Block Id
3. previous hash == new block hash
4. new block hash == hash value calculated for new black at t hash is time

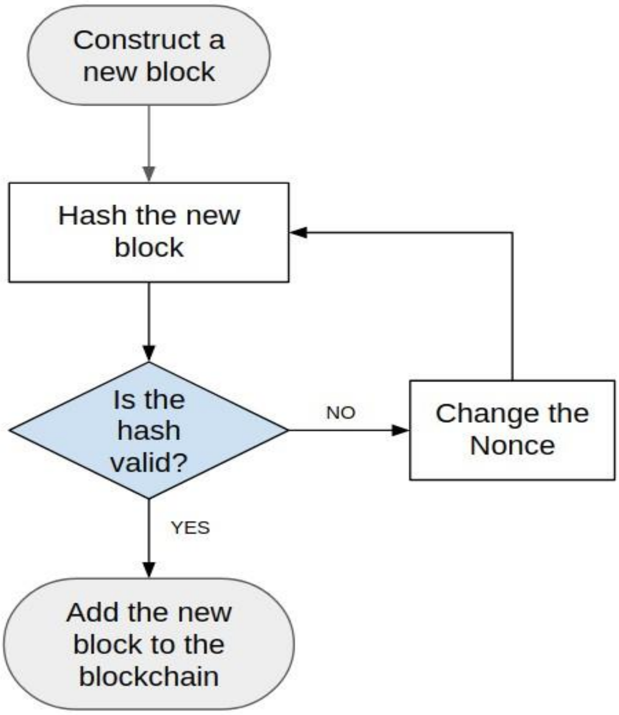


Fig.5 New block Creation Process of EEOTSE

If new block satisfies above four conditions, Block Signs with Private Key. This verified then this verified block starts Peering to block is added to blockchain. After that, hash is Network. To start peering to Network, verified calculated for block shown in Fig. 4.

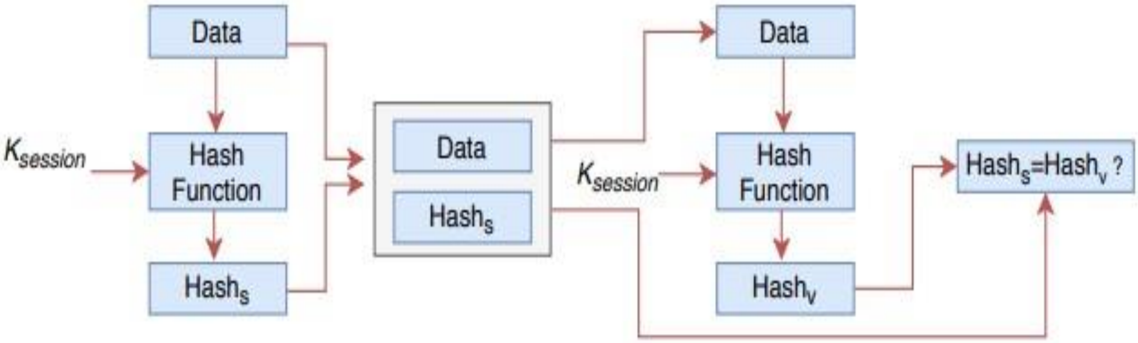


Fig.6 Hash Parameter Creation Process of EEOTSE

Then the hash parameter is added to the block. The most recent valid block is uploaded to the blockchain, which can now be viewed. A data block is added to the chain of blocks when it is checked. These blocks are linked by hashing, and data interchange is nearly impossible due to the usage of hash and cryptographic signatures. This data chain is known as a blockchain, and copies of it are maintained in multiple locations, making it accessible to anybody on the globe. The Network's activities and other information, such as the blog title and Merkle root, are contained in each block (see Figure 4). A hash is written to the header of each block in the blockchain to identify it. The Genesis block is the first link in the chain. Our main goal in integrating blockchain with IoT devices is to build scalable distribution networks with high bandwidth.

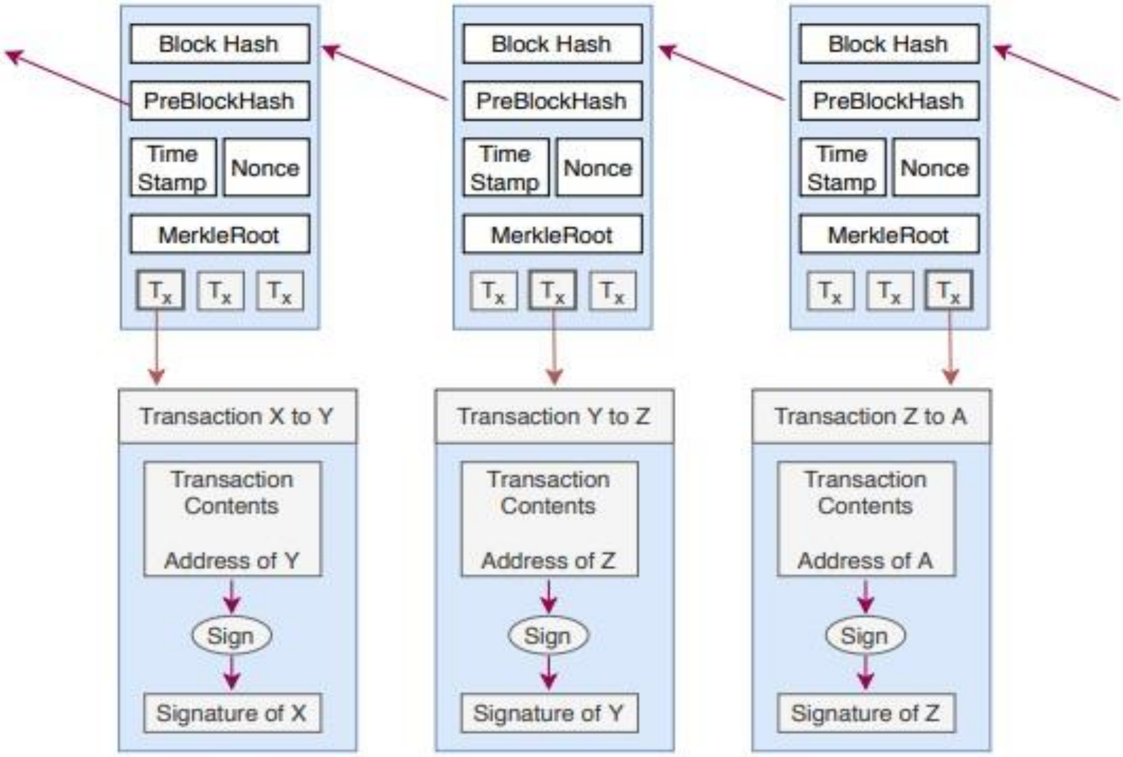
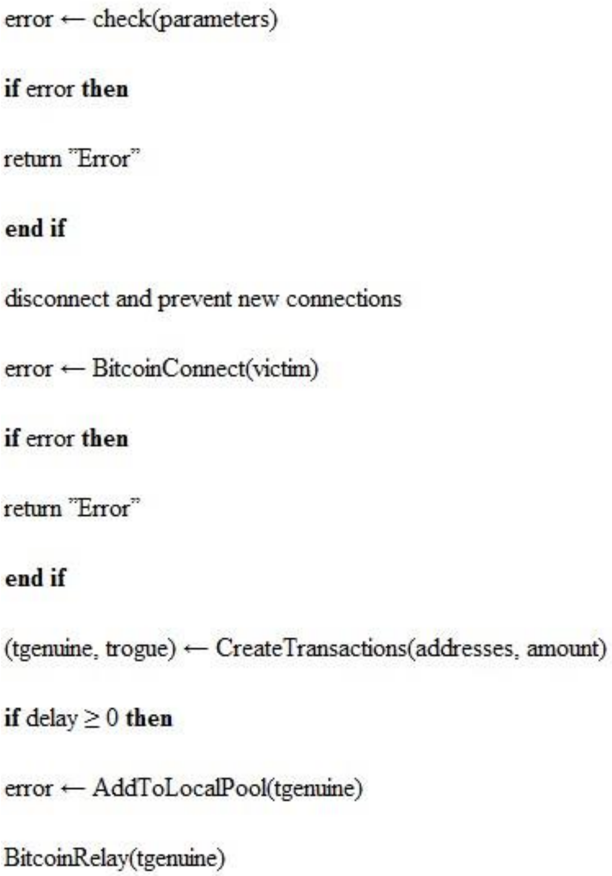


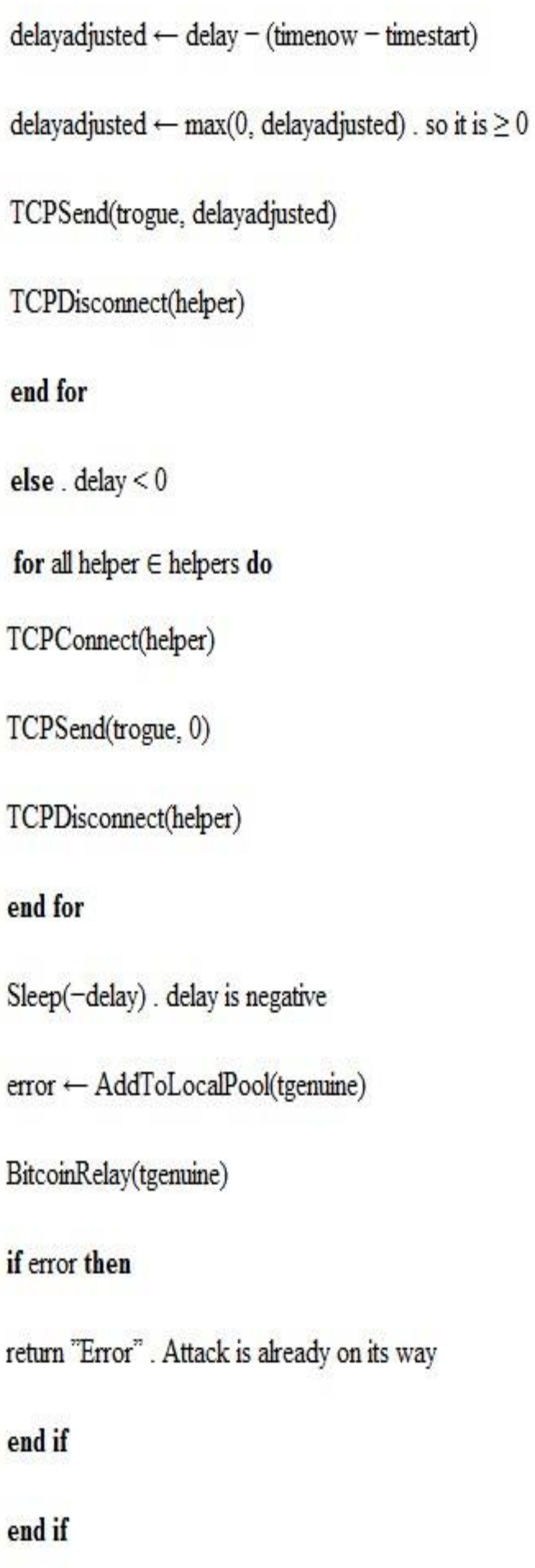
Fig.7 Blockchain Peering Process of EEOTSE

C. ATTACK DETECTION BY BLCMASHIELD

This work also provides security to blockchain against 51% attack, double-spend and selfish mining attacks by introducing BLCMAShield Approach. In BLCMAShield, an attacker starts peering with the Network by privately building blocks, thereby preventing initial spot and long spot policy. These two policies are created and managed by a various number of central nodes. Each created block is approved by these central nodes first. This approval process is done by a majority selection process. Each participant must sign the marked block in order for the active chain to expand. Most participants check each block and set up the same host to a hello message to notify all other nodes in the Network about the event. A message cannot be created if it is not responded to by enough members. The message contains a valid authentication signature and can be authenticated by all nodes in the Network. So, this step avoids the double-spend attack. Following this approval process, it aborts the peer immediately by penalization to mine the number of blocks. The number of penalized blocks is decided by the number of blocks the adversary manages to mine in secret. This two-step checking process prevents attackers and avoids the 51% attack, double-spend and self-mining attacks.



```
error ← check(parameters)
if error then
    return "Error"
end if
disconnect and prevent new connections
error ← BitcoinConnect(victim)
if error then
    return "Error"
end if
(tgenuine, trogue) ← CreateTransactions(addresses, amount)
if delay ≥ 0 then
    error ← AddToLocalPool(tgenuine)
    BitcoinRelay(tgenuine)
```

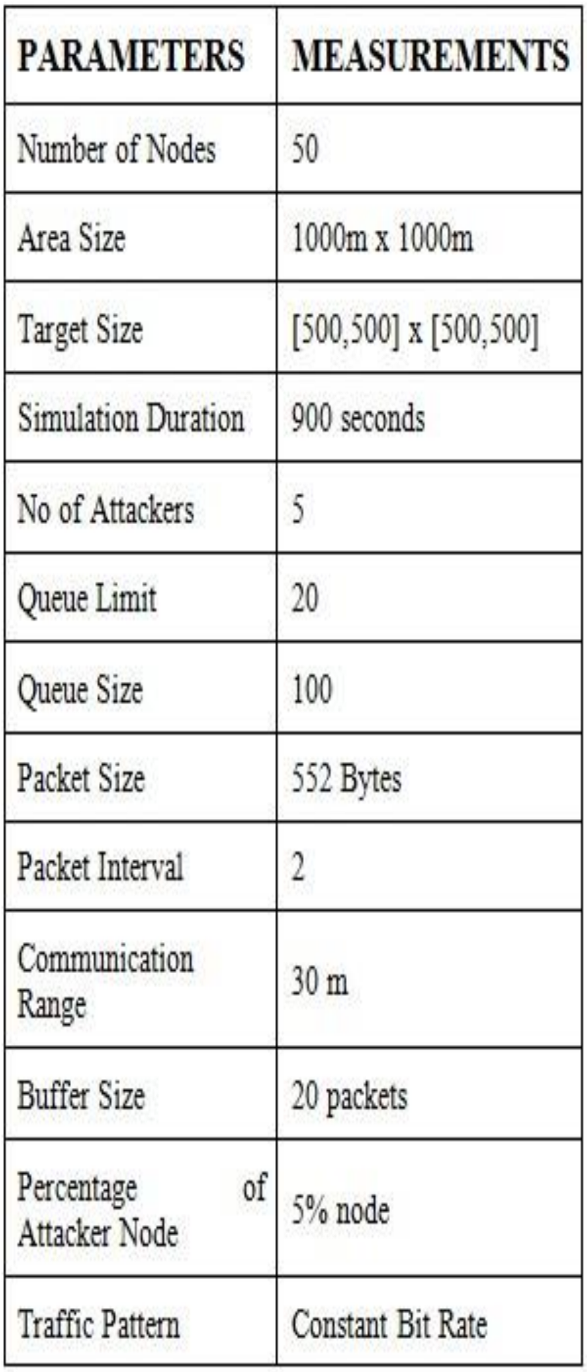


```
        delayadjusted $\leftarrow$ delay $-$ (timenow $-$ timestart)
        delayadjusted $\leftarrow$ max(0, delayadjusted) . so it is $\geq 0$
        TCPSend(trogue, delayadjusted)
        TCPDisconnect(helper)
    end for
else . delay $< 0$
    for all helper $\in$ helpers do
        TCPConnect(helper)
        TCPSend(trogue, 0)
        TCPDisconnect(helper)
    end for
    Sleep($-$delay) . delay is negative
    error $\leftarrow$ AddToLocalPool(tgenuine)
    BitcoinRelay(tgenuine)
    if error then
        return "Error" . Attack is already on its way
    end if
end if
```

IV. EXPERIMENTAL RESULTS

A. SIMULATION ENVIRONMENT

NS2 was used to implement the presented system. Table 1 lists numerous parameters used in the simulation.



PARAMETERS	MEASUREMENTS
Number of Nodes	50
Area Size	1000m x 1000m
Target Size	[500,500] x [500,500]
Simulation Duration	900 seconds
No of Attackers	5
Queue Limit	20
Queue Size	100
Packet Size	552 Bytes
Packet Interval	2
Communication Range	30 m
Buffer Size	20 packets
Percentage of Attacker Node	5% node
Traffic Pattern	Constant Bit Rate

B. EXPERIMENTAL ANALYSIS

Varying Number of Attacker Nodes

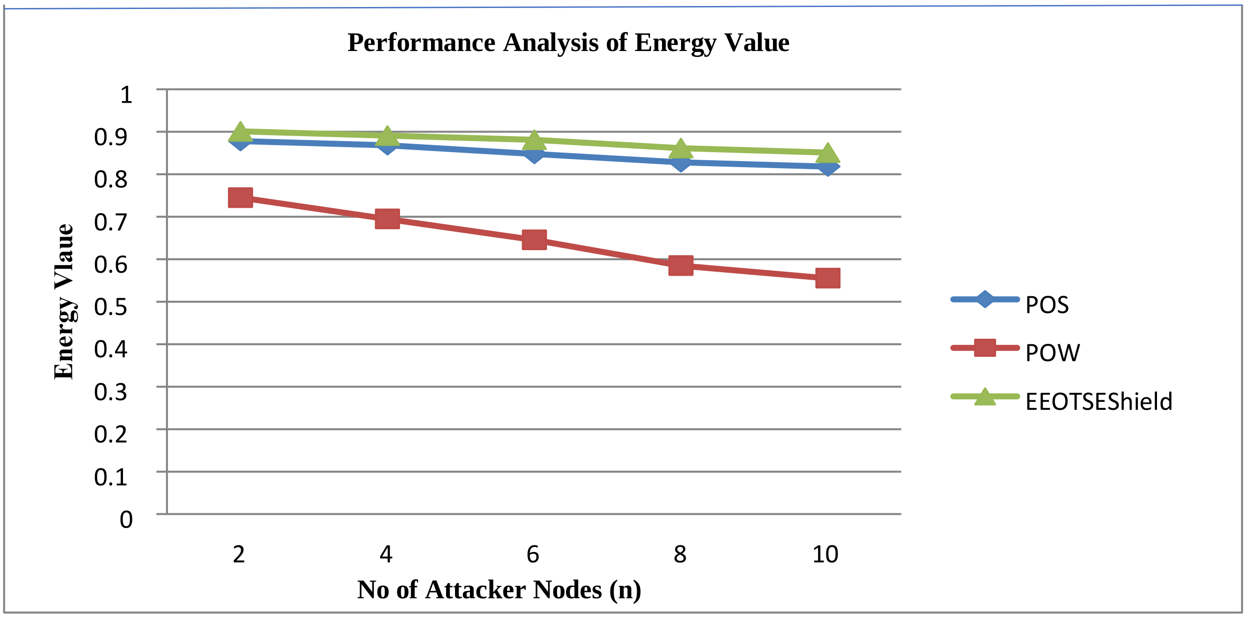


Figure 7.1 Comparison of Energy values of POS, POW, and EEOTSESHIELD for DSR Protocol

The following section discusses and illustrates the energy value of the POS, POW and EEOTSESHIELD. Figure 7.1 illustrates the acquired results for the various numbers of the nodes. The overall percent of the malicious node in the Network is chosen consciously from 0 to 10 in percentage. The maximum mobility speed of the nodes is given as 20 m/s. In the next step, the threshold for the energy metric is 35% - 75%. Figure 7.1 indicates that the EEOTSESHIELD scheme expresses a higher energy value related to conventional POS. It can be understood that EEOTSESHIELD prevails 92% of energy is preserved while detecting the harmful nodes.

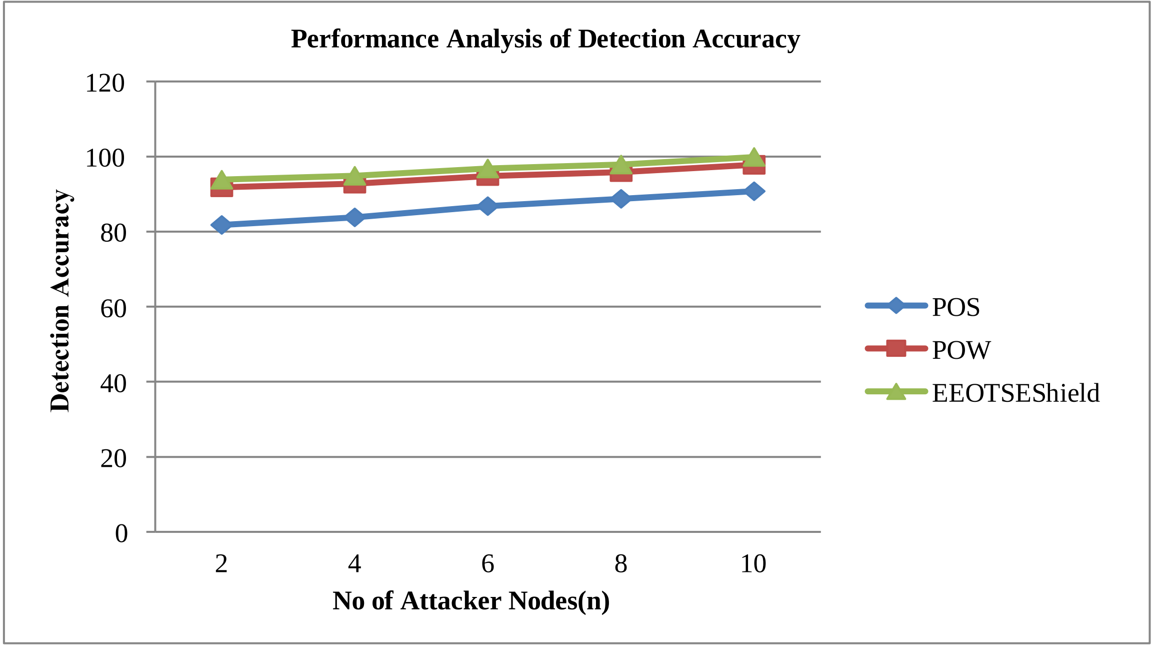


Figure 7.2 Comparison of Detection Accuracy of POS, POW, and EEOTSESHIELD for DSR Protocol

This detection accuracy rate of POS, EEOTSESHIELD and POW for DSR protocol results are compared and shown in Figure 7.2. The threshold for energy metrics is 35% - 75%. Figure 7.2 clearly shows that the proposed EEOTSESHIELD provides an efficient result. POS provides 95% accuracy. The detection accuracy of EEOTSESHIELD is 97.8% which is efficient than other schemes.

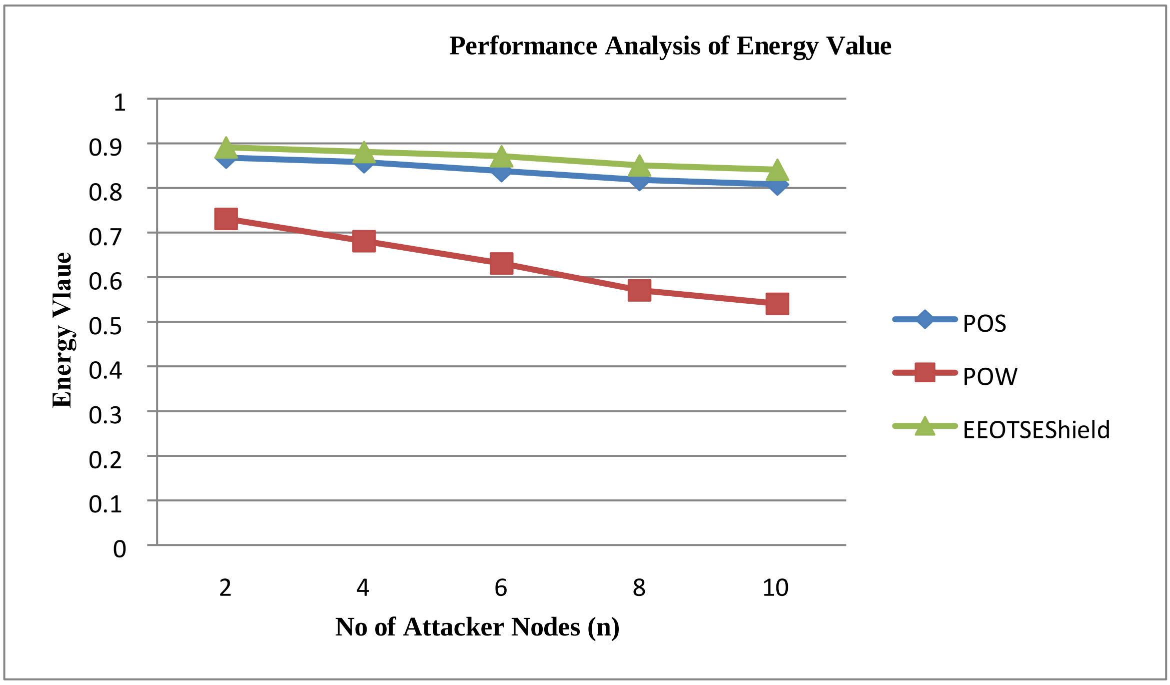


Figure 7.3 Comparison of the Energy value of POS, POW and EEOTSESHIELD for double threshold

Varying Number of Nodes with a Different

Threshold.

The energy value of the POS, POW and EEOTSESHIELD for double threshold results are compared and shown in figure 7.3. The threshold for energy metric is 35 and 75. POW and EEOTSESHIELD are calculated, and it is found to be within the threshold value, which has been derived from the packet delivery ratio. On observation, it has been noted that the threshold value, when at 75 (I have changed the sentence. please check whether this is correct), displays a higher energy value related to the other mechanisms. A threshold value is outperformed in the observation that 93 percent of its energy process of finding the attacker node. Here the total value is calculated, and the threshold value is calculated, which helps in finding the total number of nodes that are under threat. The great disadvantage of this scheme comes with a rate that there is a clear 10 percentage exposure to the detection of the packet delivery ratio. It clearly shows that when EEOTSESHIELD threshold is 75% provides 93% of energy process of finding attacker helps to find the dip in the POW and EEOTSESHIELD value which are calculated with the given factors affecting the threshold value.

This detection accuracy rate of POS, POW and EEOTSESHIELD for double threshold results are compared and shown in figure 7.4. A threshold value of 75 is observed when an overall percentage of a malicious node in the Network is chosen consciously from 0 to 10 in percentage. The mobility speed of the node is given as 20 m/s, and the threshold value is also noted 35% - 75% is a corresponding energy-efficient value of EEOTSESHIELD. Figure 7.4 clearly shows that the proposed EEOTSESHIELD provides an efficient result. EEOTSESHIELD provides 97% accuracy.

This PPV rate of POS, POW and Figure 7.6 Comparison of Detection Prevalence Value of POS, POW and EEOTSESHIELD for double threshold results are compared and shown in figure 7.5. A threshold value of 75 is observed when an overall percentage of a malicious node in the Network is chosen consciously from 0 to 10 in percentage. The mobility speed of the node is given as 20 m/s, and the threshold value is also noted 80% - 98% is a corresponding energy-efficient value of EEOTSESHIELD. Figure 7.5 clearly shows that the proposed EEOTSESHIELD provides an efficient result. EEOTSESHIELD provides 98% PPV.

This detection prevalence rate of POS, POW and EEOTSESHIELD for double threshold results are compared and shown in figure 7.6. A threshold value of 75 is observed when an overall percentage of a malicious node in the Network is chosen consciously from 0 to 10 in percentage. The mobility speed of the node is given as 20 m/s.

The threshold value is also noted 80% - 90% is a corresponding detection prevalence value of EEOTSESHIELD. Figure 7.6 clearly shows that the proposed EEOTSESHIELD provides an efficient result. EEOTSESHIELD provides 98% detection prevalence.

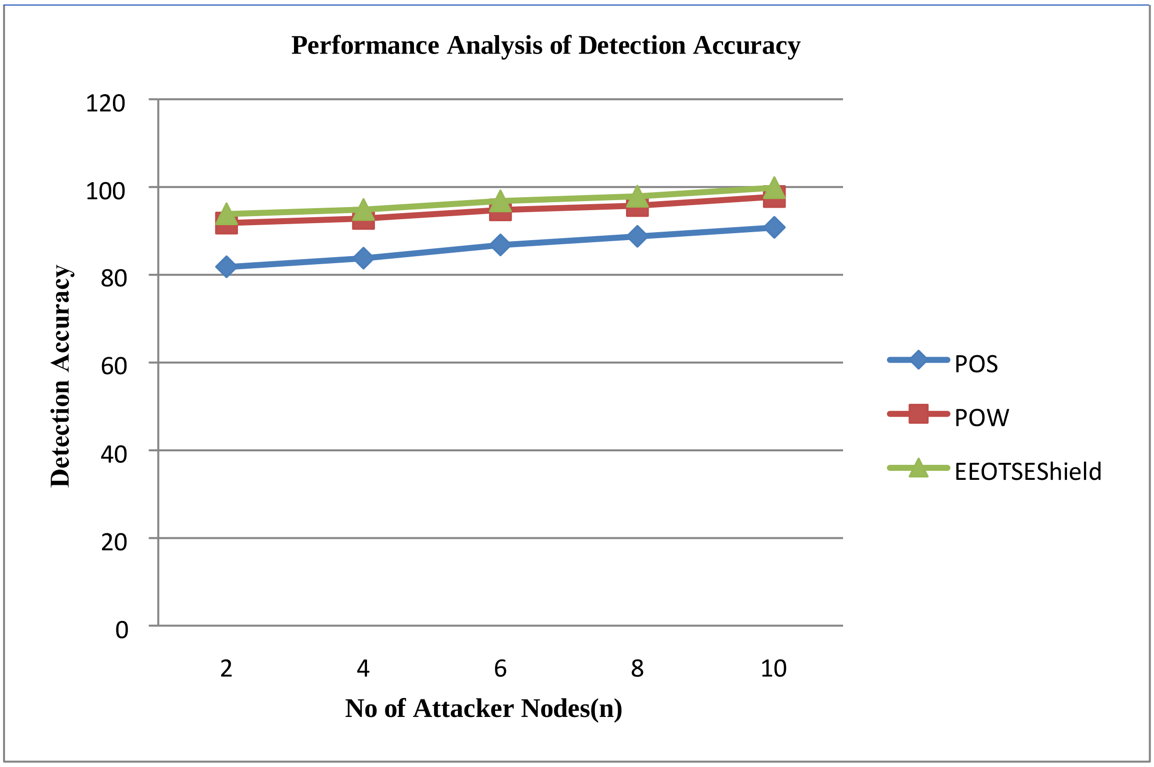


Figure 7.4 Comparison of Detection Accuracy of POS, POW and EEOTSESHIELD for double threshold

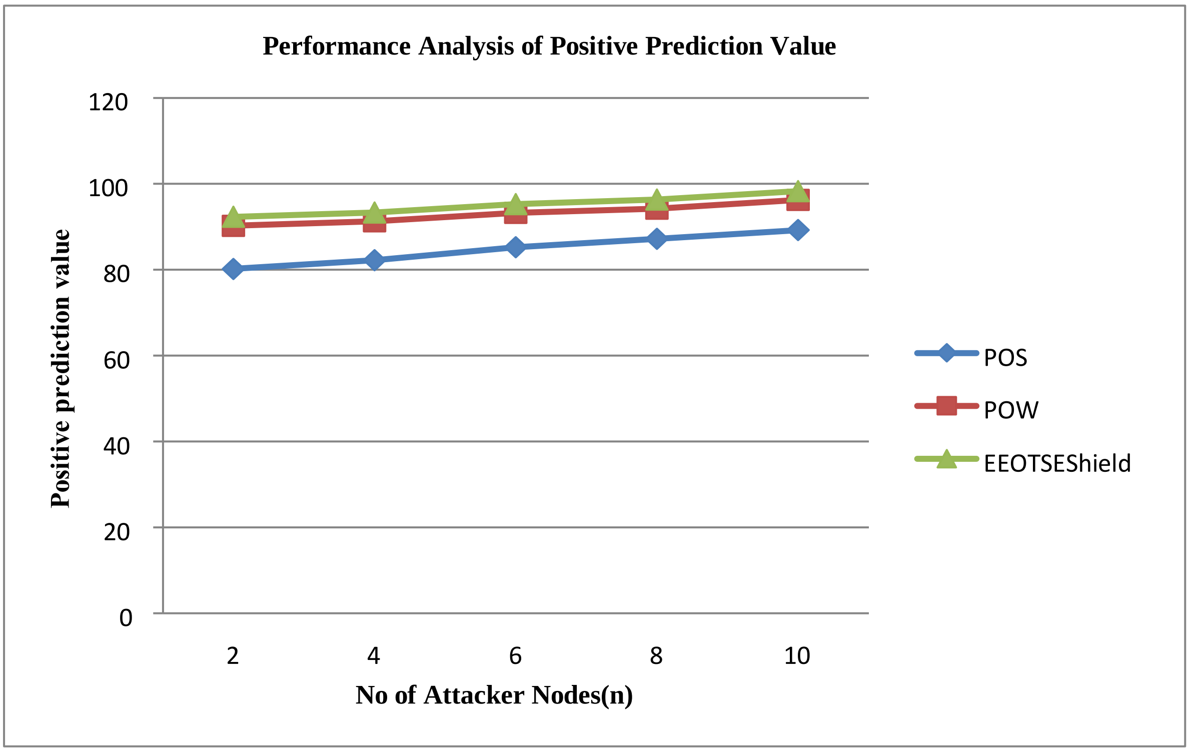


Figure 7.5 Comparison of Positive Prediction Value of POS, POW and EEOTSESHIELD for double

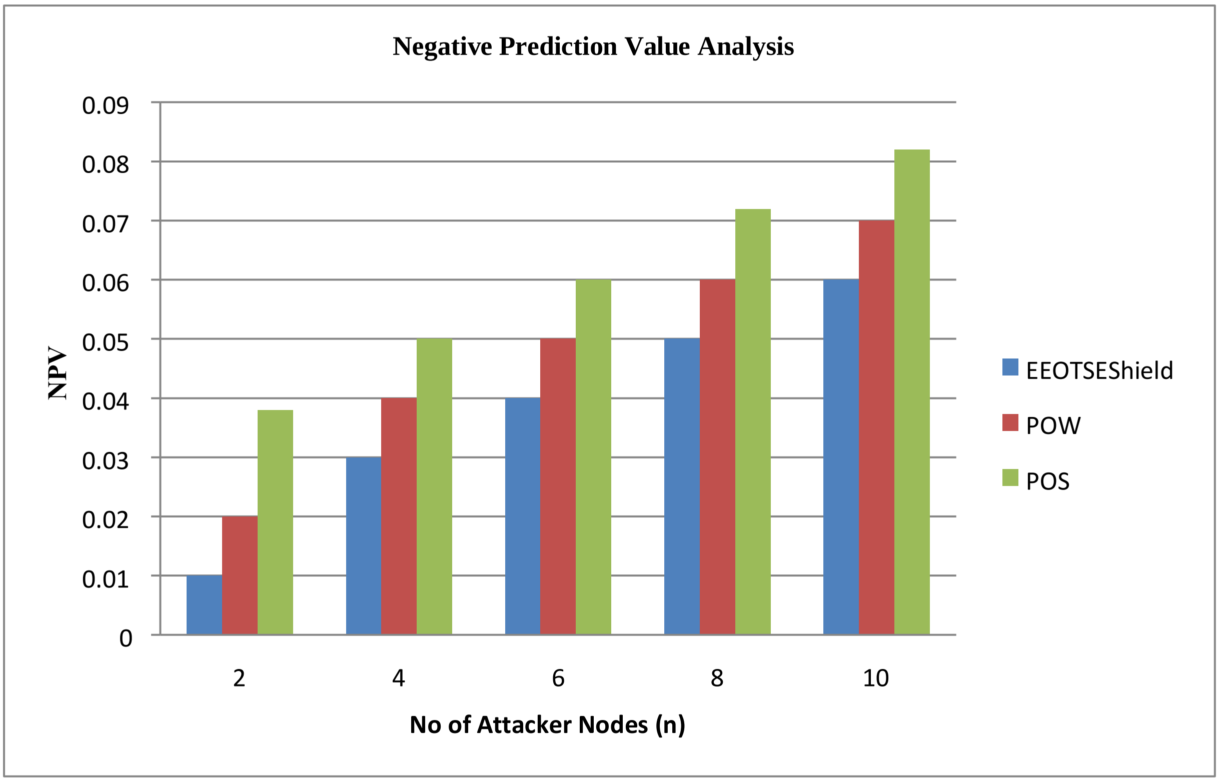


Figure 7.6 Comparison of Detection Prevalence Value of POS, POW and EEOTSESHIELD for double threshold

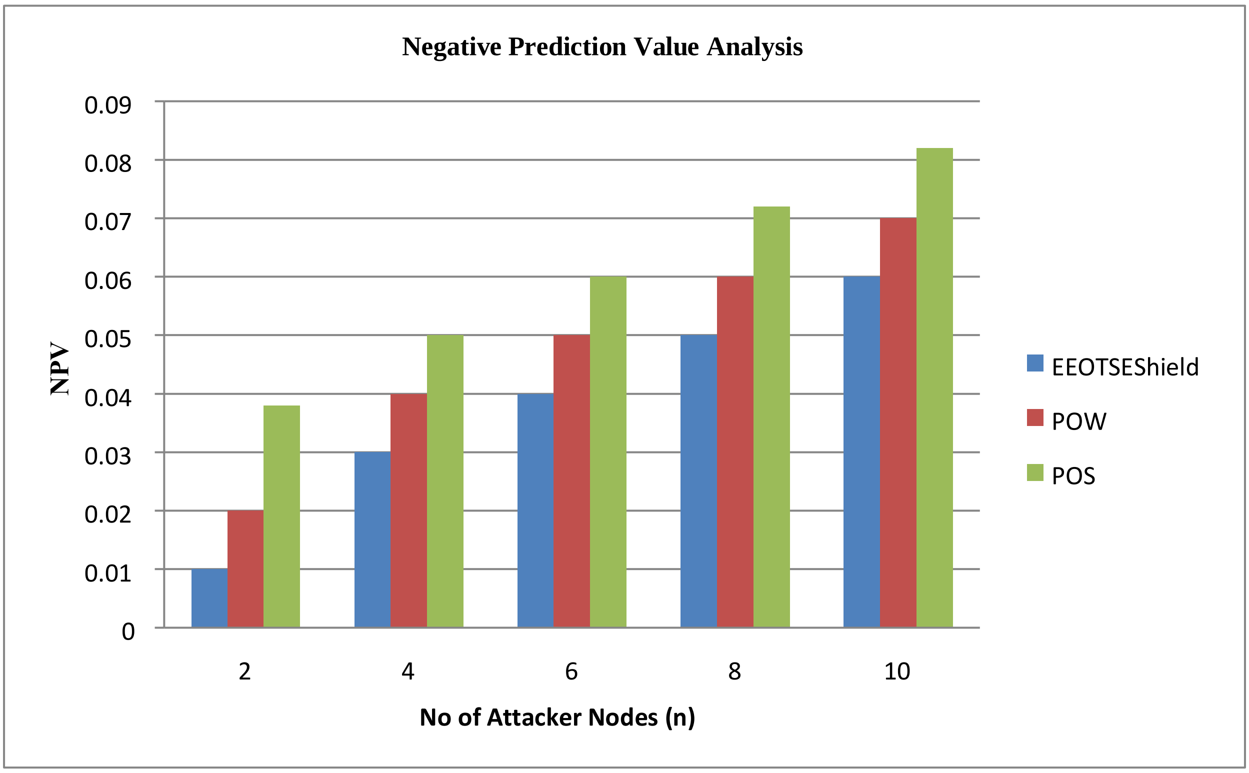


Figure 7.7 Comparison of negative prediction value of POS, POW and EEOTSESHIELD

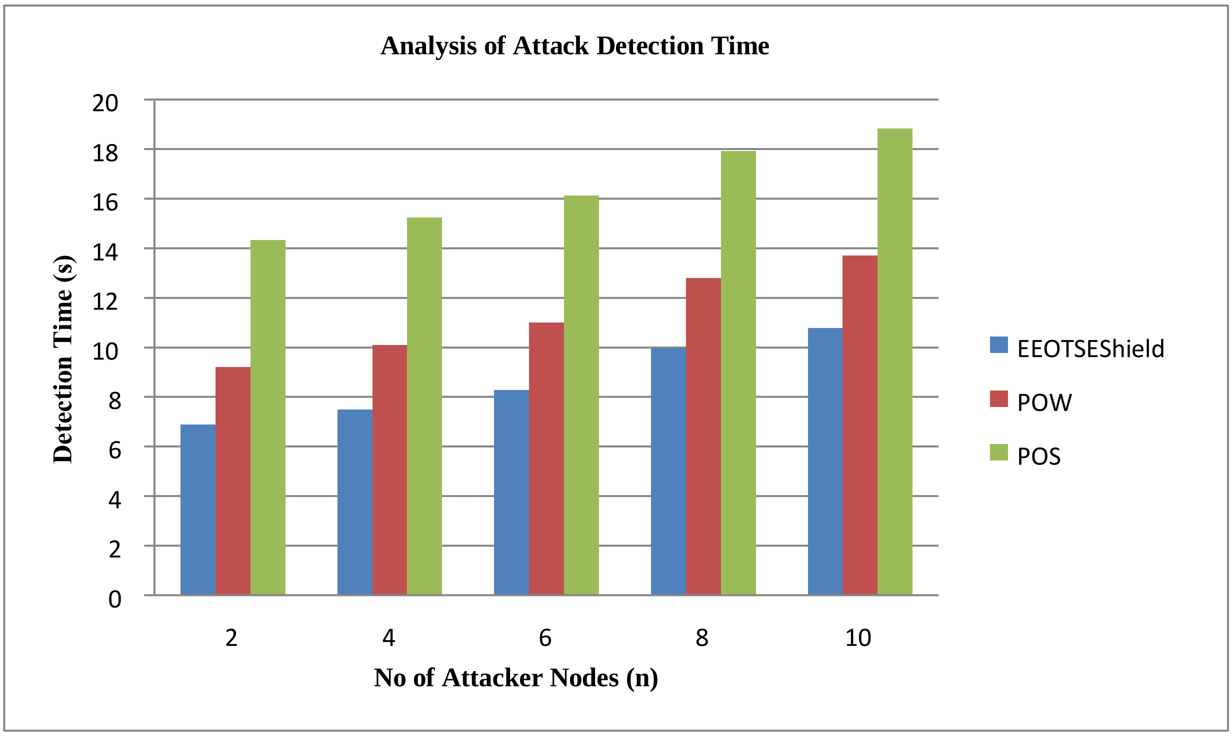


Figure 7.8 Comparison of attack detection time of POS, POW and EEOTSESHIELD for double threshold

Double threshold
This NPV rate of POS, POW and EEOTSESHIELD for double threshold results are compared and shown in figure 7.7. A threshold value of 75 is observed when an overall percentage of a malicious node in the Network is chosen consciously from 0 to 10 in percentage. The mobility speed of the node is given as 20 m/s, and the threshold value is also noted 0.01% - 0.06% is a corresponding NPV value of EEOTSESHIELD. Figure 7.7 clearly shows that the proposed EEOTSESHIELD provides an efficient result. EEOTSESHIELD provides 0.06% NPV.

Figure 7.8 Comparison of attack detection time of POS, POW and EEOTSESHIELD for double threshold
This attack detection time of POS, POW and EEOTSESHIELD for double threshold results are compared and shown in figure 7.8. A threshold value of 75 is observed when an overall percentage of a malicious node in the Network is chosen consciously from 0 to 10 in percentage. The mobility speed of the node is given as 20 m/s, and the threshold value is also noted 6s- 10s is a corresponding attack detection time of EEOTSESHIELD. Figure 7.8 clearly shows that the proposed EEOTSESHIELD provides an efficient result. EEOTSESHIELD provides 10s attack detection time.

V. CONCLUSION

In this article, we have outlined the mechanisms for secure blockchain operations in the blockchain, reducing the risk of attacks by 51%, double costs, and selfish attacks. The proposed mechanism prevents attempts to double the cost by generating a special type of output that requires the display of a private key in the event of an attempt to double the cost. Every bitcoin user can act as an observer and be rewarded by detecting 51% attacks, double spending and selfish mining attempts. The reward the observer receives is equal to the value the attacker pays as a penalty for attempting to double the transaction. To prevent these attacks, the proposed method presented in this article is called the BLCMAShield method.

BLCMAShield provides high security with low execution time compared to other existing methods. Attack detection rate, error rate, execution time, power consumption is used to analyze the performance of BLCMAShield & EEOTSE method and are compared with the existing method. Experimental results show that BLCMAShield & EEOTSE provides the best results from existing methods.

REFERENCES

[1] Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity. Technical report, Federal Bureau of Investigation, (2012).

[2] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On bitcoin and red balloons. In Proc. of Electronic Commerce, (2012).

[3] Tobias Bamert, Christian Decker. Lennart Elsen, Samuel Welten, and Roger Wattenhofer. Have a snack, pay with bitcoin. In IEEE 1nternation Conference on Peer-to-Peer Computing (P2P), Trento, Italy, (2013).

[4] Jorg Becker, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer, and Rainer Bohme. Geld stinkt, bitcoin auch - eine Okobilanz der bitcoin block chain. In BTC (2012). Workshop Bitcoin.

[5] M. Vasek, M. Thornton, and T. Moore, Empirical analysis of denial-of-service attacks in the bitcoin ecosystem, in International

Conference on Financial Cryptography and Data Security. Springer, (2014) 57–71.

[6] D. Bradbury, The problem with bitcoin, Computer Fraud & Security, 2013(11) (2013) 5–8.

[7] M. Herrmann, Implementation, evaluation and detection of a double spend-attack on bitcoin,(2012).

[8] C. Decker and R. Wattenhofer, Information propagation in the bitcoin network, in Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on. IEEE, (2013) 1– 10.

[9] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, Blockchain contract: Securing a blockchain applied to smart contracts, in Consumer Electronics (ICCE), 2016 IEEE International Conference on. IEEE, (2016) 467–468.

[10] A. Badzar, Blockchain for securing sustainable transport contracts and supply chain transparency-an explorative study of blockchain technology in logistics, (2016).

[11] S. Wilkinson, J. Lowry, and T. Boshevski, Metadisk a blockchain-based decentralized file storage application, Technical Report. http://metadisk. org/metadisk. Pdf, Tech. Rep., (2014).

[12] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, The blockchain as a software connector, in Software Architecture (WICSA), 2016 13th Working IEEE/IFIP Conference on. IEEE, (2016)182–191.

[13] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. ZeroCoin: Anonymous distributed e-cash from bitcoin.(2013) .

[14] I1ja Gerhardt and Timo Hanke. Homomorphic payment addresses and the pay-to-contract protocol. CoRR, abs/1212.3257, (2012).

[15] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In Proc. of the Conference on Social Computing (social com), (2011).

[16] G.O. Karame, E. Androulaki, and S. Capkun. Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin. In Proc. of Conference on Computer and Communication Security, (2012).

[17] Dorit. Ron and Adi Shamir. Quantitative analysis of the full bitcoin transaction graph.

[18] Matthew Elias. Bitcoin: Tempering the digital ring of gyges or implausible pecuniary privacy. Available at SSRN 1937769, (2011).

[19] Jeremy Clark and Aleksander Essex. Commitcoin: Carbon dating commitments with bitcoin. In Financial Cryptography and Data Security. (2012).

[20] Bitcoin wiki. https://en.bitcoin.it/wiki/Confirmation. Confirmation looked at on 2012-04-18.

[21] Bitcoin wiki. https://en.bitcoin.it/wiki/Myths#Point_of_sale_ with_bitcoins_isn.27t_possible_because_of_the_10_minute_wai t_ for_confirmation. Myths, looked at on 2012-04-18.

[22] G. Mwitende, Y. Ye, I. Ali, F. Li, Certificateless authenticated key agreement for blockchain-based wbans, J. Syst. Archit. 110 (11) (2020) 1–31.

[23] X. Li, Y. Mei, J. Gong, F. Xiang, Z. Sun, A blockchain privacy protection scheme based on ring signature, IEEE Access 8 (8) (2020) 76765–76772.

[24] F. Li, Z. Liu, T. Li, H. Ju, H. Wang, H. Zhou, Privacy-aware PKI model with strong forward security, Int. J. Intell. Syst. 8 (8) (2020) 1–17.