Paper No: SC-08 **Smart Computing**

Blockchain-based distributed reputation model for ensuring trust in mobile adhoc networks

P. P. C. Peiris*
Department of Industrial Management
Faculty of Science,
University of Kelaniya, Sri Lanka
pasan.peiris01@gmail.com

Chathura Rajapakse
Department of Industrial Management
Faculty of Science,
University of Kelaniya, Sri Lanka
chathura@kln.ac.lk

B. Jayawardena
Department of Industrial Management
Faculty of Science,
University of Kelaniya, Sri Lanka
buddhikaj@kln.ac.lk

Abstract: **Mobile ad-hoc networks also known as MANETs have been in global use for numerous applications which are not possible with fixed network topologies. The distributed operation and dynamic topology have encouraged MANETs to be applied for establishing communication in unstable environments. MANET's dynamic topology and mobility have been very advantageous in the fields of military and disaster management. These dynamic characteristics of a MANET also create a major challenge in managing trust between the mobile nodes. Managing the trustworthiness of information that a node provides to the rest of the MANET is very crucial as misinformation spread can lead to erroneous decision making. Although previous studies have been carried out on trust management in MANETs using price-based and reputation systems, the potential of a globally distributed system has not been utilized practically. Therefore, these systems address the trust management issue within a boundary of a single MANET. Above mentioned systems should be re-evaluated when a node from another MANET joins a new MANET as the reputations of the node in the previous MANET cannot be imported to the new MANET. Lack of a possible solution for this gap may result in misinformation spreading by a malicious node before other nodes determine its reputation, which could be very dangerous in sensitive environments. Therefore, a globally distributed reputation model is a timely need in mobile ad-hoc networking. Blockchain technology is one of the most suitable technologies in present for its immutable and distributed properties to build robust systems. Blockchain is a distributed ledger, that has the ability to store feedback from mobile nodes about the accuracy of information provided by other nodes. A trust factor for each node can be calculated using these feedbacks. A mobile node can then decide whether to trust information, based on nodes' trust factors. Adopting a development-oriented research methodology, a blockchain based reputation model prototype has been implemented and validated within the study.**

Keywords: *Blockchain, Mobile ad-hoc networks, Security, Trust management*

I. INTRODUCTION

A. Mobile ad-hoc networks (MANETS)

Mobile ad-hoc networks consist of a set of mobile nodes, wirelessly connected in a self-configured manner. Nodes in the mobile ad-hoc network are free to move as of the frequent changes in the ad-hoc network topology.

The mobile nodes which are within the range of each other can directly communicate, whereas others require the assistance of intermediate nodes to route their data packets. Mobile ad-hoc networks are fully distributed and can operate at any place without the help of any fixed infrastructure as access points or base stations. This feature allows the use of this kind of network in special circumstances such as disastrous events.

Characteristics of MANETS

- Distributed operation - No central authority or control over the network
- Multi hop routing – When a node attempts to send data to other nodes which are out of its radio range, the packets should be forwarded via one or more intermediate nodes in the network.
- Autonomous terminal – Each mobile node in the mobile ad-hoc network is independent and could function as both a host and a router.
- Dynamic topology – Nodes can move freely and [randomly at different speeds. The network topology could change rapidly at an unpredictable time. The nodes in the mobile ad-hoc networks can dynamically establish routing among themselves as they move around, establishing their own network.

B. Trust management in MANETs

These dynamic characteristics of a MANET create a major challenge in managing trust between nodes. There are 2 main aspects of managing trust in MANET as follows.

- Managing the trustworthiness of nodes that act as routers or intermediaries to transfer data packets.
- Managing the trustworthiness of information that a node provides to the rest of the MANET.

Attention to this study will be drawn to the latter aspect of the two trust challenges. As of MANET's dynamic topology, major applications of these networks are used in military and special occurrences such as disastrous events. Therefore, it is crucial that the information a node sends to a destination is accurate and reliable.

Prior studies have been conducted to seek the applicability of Price-based systems and Reward systems in this area. But those systems are limited to the scope of a single MANET.

C. Blockchain

A blockchain is a growing list of records, called 'blocks' that are linked with the use of hashes. Each block contains the previous block's hash which binds the blocks together resulting in a blockchain.

By design, a blockchain is robust to explicit modification of the data in it. It is a distributed ledger that records transactions between two parties. By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new dimension of the internet. Although blockchain was originally devised for the digital currency, Bitcoin, the tech community has now found other potential uses of this technology. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation systems, Internet of Things (IoT), and so on.

When a transaction occurs, it is broadcasted to all the peers in the network. A special group of participating nodes, called miners, collect transactions from a transaction pool and attempt to include them into a lock that satisfies a cryptographic hash function. The process of producing a block which is called a mining process uses considerable computing power and it is probabilistic. Whilst mining a block is hard, verifying a correct block is not [1].

Blockchain's immutable property and distributive property are so useful in creating reputation systems. A reputation system that can be accessed by anyone but is resistant to illegal changes will result in an effective reputation system for many technological fields.

II. LITERATURE REVIEW

A. Trust management in MANETs

Trust management is one of the most important components in the security services of networks. Trust is needed in MANET because wireless networks are more borne to attacks. There are 3 crucial factors in trust management as given below.

- Trust establishment
- Trust update
- Trust revocation

Computing trust is not the only important task but maintaining it, updating and revoking it also becomes crucial factors of a trust management system.

To evaluate the trust of a node, direct monitoring of the node and indirect monitoring of the node can be applied. Direct monitoring is mostly used between immediate neighbouring nodes and also where a trust relationship is formed between two nodes which are new to each other.

Indirect monitoring means receiving secondary information of a particular node's reputation through the form of recommendations as indirect trust. A hybrid approach combining these two trust monitoring methods can be seen in reputation-based trust management applications [2].

Reference [3] discusses a Reliable Trustworthy Approach (RTA) which deals with the prediction of node behaviour. This approach discusses a new node behaviour algorithm which estimates and predicts a behavioural category for the node which is used for node trust management and reliable data transfer in MANET.

In this Reliable Trustworthy Approach, they classify a node into 4 behavioural categories.

- Reliable Category
- Unreliable Category
- Malicious Category
- Selfish Category

The authors have proposed the Semi-Markov process to accurately characterize the node behaviour category predictions. There are 2 other aspects that are affiliated to trust management in Reliable Trustworthy Approach.

- Collective Trust Computation

Node trusts are calculated based on trusts by the other nodes over a period of time in a MANET. Initially, each node is assigned a maximum trust value of 1.

- Trust Recovery

A "Recovery Factor" (RF), also known as a "declining" or "forgetting" factor, allows the nodes that were determined as malicious nodes to have a second opportunity by recovering the trust value.

Reference [4] discusses the challenges in designing Manet protocols.

Due to MANET's high usage in the military, they should support aggressive environments. And also, the variety of nodes and their fluctuating performance constraints often leads the nodes to not to have a predefined trust relationship. Therefore, the authors suggest that the networks should use low complexity distributed network management schemes.

Authors also discuss different attacks on MANETs.

- Eavesdropping – Here, the intruder tries to attack the physical layer of the network for eavesdropping motives.
- Jamming – In this attack, the network traffic is increased and the network comes to a hold.
- Rushing – When a route request is sent, the intruder tries to act as a real source.
- Flooding – Here, the network is flooded with false routing information by malicious nodes and they consume network resources.

Trust management is often implemented in many aspects in MANETs like intrusion detection, access control, key management and identifying misbehaving nodes. Trust management is considered as one of the most important properties when two nodes are communicating with no previous interactions. In this paper, authors emphasize some properties of trust in MANETs.

- Trust should be evaluated in an easy way
- Trust is not static and it often changing
- Trust is subjective
- Trust is context-based

As mentioned in the paper, the authors discuss some currently existing models for trust management in MANETs.

1. CH selection algorithms in MWSN

In reference [5], different attributes of nodes are considered. The parameter or attributes that are taken into account are waiting time, connectivity degree and distance between notes. The selection of the head of clusters is based on the weights of a node. The model has proved optimistic results for avoiding malicious nodes accurately and also for energy efficiency.

2. Objective function

In reference [6], the trust of nodes is calculated by using trust parameter shared between the nodes with the use of objective function, which defines the degree of trust basing on node forwarding behaviour. Direct and indirect method of calculating trust is considered in this paper. In direct method, trust is calculated using the behaviour of neighbour node and in indirect method, the nodes calculate the trust value by observing from its neighbour node. This paper outlines the various trust management mechanisms which operate in MANET environments.

3. Multi parameter metrics method

Reference [7] discusses various parameters that are considered to separate between malicious modes and trusted nodes of the network. The parameters include energy of node, node's motion and energy consumption and have finally given the trust value based on metrics or attributes.

Reference [8] discusses a node-centric trust management method. The goal of any trust reputation-based system is to provide the nodes a method to understand the behaviour of other nodes and provide secure mutual interaction. The trust among the nodes can be built either by direct observance behaviour of node or reputation information provided by other nodes. A central trust management entity is not available in most trust-based frameworks. Therefore, a node must possess decision making capability to revise its strategy of communication and filter indirect information accurately. The node-centric trust refers to the trust that a node has of another node. The following components are available in node centric trust system, where each component can be considered as a step in the trust computation process.

- Information collection
- Information sharing
- Information mapping to trust model
- Decision making

B. Blockchain

Reference [9] discusses an overview of Blockchain technology and the authors emphasize the challenges and the recent advances in blockchain. Blockchain can preserve a certain amount of privacy by using the public key and private key. Users can do transactions with their private public keys without exposing their identities. However, blockchain cannot guarantee transactional privacy since the values of all transactions and balances for each user are publicly visible. According to the authors, a user's Bitcoin transaction can be linked to reveal that particular user's information. A method has also been proposed to map user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. Each user can be uniquely identified by a set of nodes it connects to. As mentioned above, it can be learned and used to find the origin of a transaction. Few methods have been proposed to improve the anonymity of blockchain users. One such proposed method is mixing.

Mixing: In blockchain, users' addresses are stored as pseudonymous. But it is still possible to link addresses to user real identity when many users do transactions using the same cryptocurrency address frequently. Mixing service provides anonymity by transferring funds from multiple input addresses to multiple output addresses.

This method minimizes the risk of identifying users on their transaction behaviours. But dishonest intermediary nodes can keep the funds to themselves without completing the transactions. To avoid such situations, Mixcoins, CoinShuffle methods are proposed by different authors.

Reference [10] discusses how smart contracts work. Nick Szabo introduced smart contract concept as "a computerized transaction protocol that executes the terms of a contract". Smart contracts are scripts that are stored on the blockchain. As they are stored in the chain, they have a unique address. A smart contract can be triggered by addressing a transaction to it. Smart contracts minimize the need for trusted intermediaries between transacting parties as they are embedded into blockchain that can self-enforce itself. When a smart contract is triggered, it then executes the code independently and automatically in a predefined manner on every node in the network. Smart contracts simplify general purpose computations which occur on the train. They are mostly used in data-driven interactions.

C. Trust management using blockchain

Reference [11] discusses a Distributed Management system for Trust and Reward (DMTR). Authors' attention in trust management is focused on detecting uncooperative nodes which drop packets illegally in a MANET. In this paper, the authors discuss the challenges of currently existing incentive systems. Local reputation systems evaluate nodes from their neighbours. They mention that in a MANET, it is a challenge to gather much information from many nodes scattered in the network and share the information among nodes. Therefore, they propose a distributed system based on blockchain technology to overcome that issue.

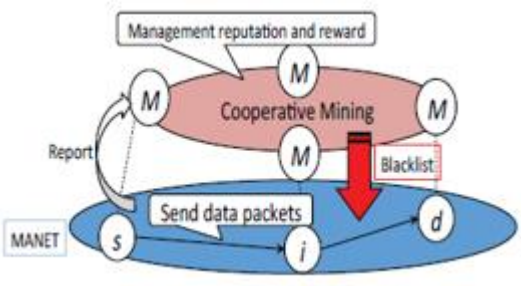

Fig. 1. Proposed DMTR

In this proposed system, cooperative mining has been introduced, which is a concept that aims at accelerating the speed of mining while keeping the total amount of computations requested as proof of work. In DMTR mining, general nodes, the nodes which do not participate in mining

are used to get information about node behaviours periodically. General nodes report the packet ratio that their neighbours really forwarded and the number of packets they are requested to forward.

From the reports, mining nodes create transactions for each report. It contains cost and amount of reward. Cost and reward indicate the amount of points the source node pay and the relay node (which acts as a router to exchange data packets) can obtain, respectively. DMTR allows nodes to have temporary minus balances as malicious nodes in order not to deprive nodes of opportunities to get points as rewards. However, the nodes that have minus balances are included in two blacklists called poor blacklist and malicious blacklist. Mining nodes include the nodes whose reputation values are minus into a poor blacklist, and whose reputation values are less than a threshold value into a malicious blacklist. This reputation is calculated by the packet forwarding ratio of the node.

In DMTR, because of the blockchain size, though mining nodes have the blockchain, they do not broadcast the blockchain to other nodes. Overhead will increase drastically if mining nodes broadcast the blockchain to general nodes. When a new block is generated in the blockchain using the reports, mining nodes update a poor blacklist and a malicious blacklist. Then, general nodes in the MANET receive the blacklist from mining nodes. General nodes then change their behaviours referring to the blacklists. For example, if a node is questioning which nodes to ask to forward packets, the nodes in the malicious blacklist will be ignored.

This proposed a Distributed Management system for Trust and Reward, which motivates the nodes to exchange packets without illegal dropping. But this proposed system's scope is limited to reducing illegal packet dropping in the context of a single MANET. Considerable amounts of communication of data packets are still at risk if a malicious node from another MANET joins this above MANET and starts to drop packets as it takes few rounds of communications to determine the behaviour of the node.

Reference [12] discusses implementing blockchain as an open distributed ledger which enhances the security of authentication infrastructures. They introduced an abstract, graph theoretic model of trust management system for authentication and a matching blockchain model. They have also highlighted five attacks,

1. Stealthy targeted attack
2. Double registration attack
3. Stale information attack
4. Denial of service attack
5. Censorship attack

These can also be avoided by encoding trust information in their blockchain model. It is emphasized that in trust management context, blockchain is a very promising technology to be used to enhance security measures and mitigate security risks in systems. And also, the study reflects the problem of the size of the blockchain becoming larger and causing the blockchain to be bloated with the continuous increase of the capacity need of participating entities. Privacy is another major concern that has to be resolved, as balancing the need for transparency and user privacy is a universal problem. Another key design consideration that has been highlighted is the type of blockchain to be used. Public and open designs, like the ones used by Bitcoin and Ethereum, enable the open participation of all entities that want to contribute to the system. In this case, it will be important to hold the participants accountable for their actions, so that they face repercussions if they misbehave. On the other hand, so-called permissioned or consortium blockchain designs can also offer some advantages regarding accountability. However, they lack the decentralized nature of permissionless public blockchain systems.

III. METHODOLOGY

A. Research approach

According to the analysis of literature, currently, existing models only address the trust management issue between mobile nodes only to a single boundary of a MANET. Therefore, to minimize the gap of misinformation spread between MANETs by malicious nodes, there should be a system that can communicate with all the MANETs. As the MANETs topology is very dynamic, a centralized system is not an appropriate solution. Therefore, a distributed system is the most suitable option for this issue. MANETs usage in sensitive environments like disastrous events and military environments, make its data and node trust highly sensitive. Therefore, the trust value that gets stored in the distributed system cannot be changed by external processes. Therefore, a robust and self-enforcing distributed system is suggested to overcome this issue. Blockchain technology is a leading secure technology that is immutable for external modifications. Its decentralization quality and global accessibility eliminate the barrier of the centralization of a model. Therefore, a blockchain based distributed reputation system is an appropriate recommendation to be researched.

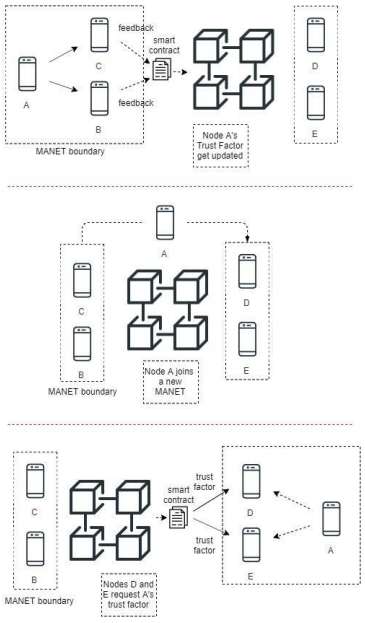

Fig. 2. Overview of Decentralized Application (DApp) Architecture

The research approach was an inductive method where a globally distributed reputation model was introduced to minimize the misinformation spread in MANETs. The use of a distributed system to minimize trust issues between the nodes was experimented. Using blockchain as a distributed

ledger and smart contracts to handle the trust factor calculations was discussed.

As described in figure 2, once a node broadcasts information, other nodes provide feedback about the information provided by that particular node. These feedbacks are then collected by an Ethereum smart contract which calculates a trust value for the transaction and stores it in the blockchain. When another node request for the trust factor of a certain node, the smart contract refers to the blocks and returns the trust factor of that particular node and sends it to the requested node.

Smart contracts are stored in blockchain. Therefore, its instructions and data are immutable and cannot be explicitly modified. Once deployed smart contracts cannot be modified. Every time an update is done to the system, a new block is mined and the latest state in the smart contract is included in it and broadcast to the participating nodes which are located globally. The mobile nodes in the MANETs do not store the blockchain in their storage or memory but communicate with it. The mobile nodes can communicate with the participating nodes in the blockchain which stores a copy of the blockchain.

The smart contract contains 3 main functions.

1. A function to register mobile nodes in the blockchain.
2. A function to update the trust factor of a node
3. A function to return the trust factor of a node

These three functions handle the core processes of the reputation model and mobile nodes can directly communicate with these nodes. The blockchain's latest block contains the latest trust factors of the nodes.

Fig. 3. Preview of Smart Contract Storage

The equation for calculating the latest trust factor of a node is as follows. Trust value received as feedback t, current trust factor TF, number of times feedback is given N

$$TF_{new} = [(TF*N) + t]/(N+1) \quad (1)$$

Trust Factor TF is stored as a big integer data type in Ethereum blockchain. Trust factor should be converted to a number when returning it to requesting nodes.

IV. Implementation

For the development of DApp shown in fig. 3, the following technologies were used.

- Truffle Framework

Truffle is a development environment including a testing framework for Ethereum developers to facilitate easy Ethereum development. It is one of the most used integrative development environments in the Ethereum community.

- Web3.js

Web3.js is a collection of libraries that facilitates the blockchain developers to interact with local or remote Ethereum nodes using an HTTP or IPC connection.

- MetaMask

MetaMask is a browser extension that facilitates DApps to run without becoming a part of the Ethereum network as an Ethereum node. MetaMask also facilitates running smart contracts on Ethereum network. This manages the Ethereum wallet.

- Ganache

Ganache is a blockchain simulator for Ethereum developers to deploy contracts, develop applications and run tests.

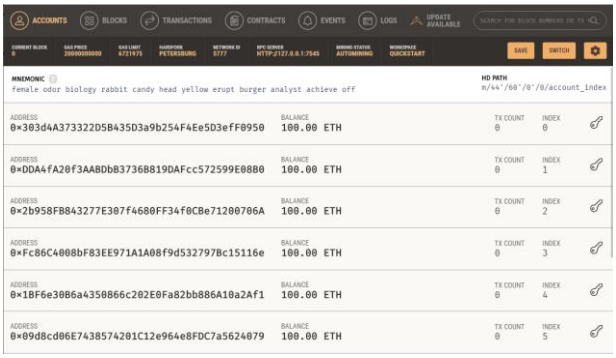

Fig. 4. Unique Addresses Related to Mobile Nodes

In a complete transaction in the DApp shown in figure 2, a smart contract will store the following details in the blockchain.

- Node's ID which broadcast the information
- ID of the node that provides the feedback
- Feedback value

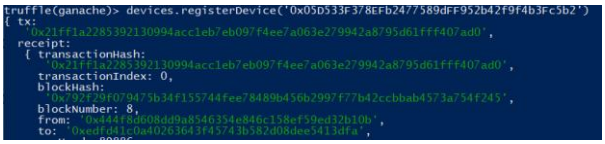

Fig. 5. Example device registration output

A new block in the blockchain is then created with the above data. A mobile node should have a universal identifier named here as ID to be identified uniquely. The prototype was implemented in solidity programming language.

When a new device is registered in the system, it is a transaction which results in the change of the state in the blockchain. The change of state results in a new block getting mined to include the data. Therefore, when a new device is registered in the system a new block is mined by the miners.

V. Prototype Testing and Validation

The study was conducted in three main phases. In the first phase, existing models used for trust management in

MANETs were systematically reviewed, in order to identify the security vulnerabilities, they possess. The second phase focused on developing a model that could minimize security risks. In the third phase, the model was tested.

1. Phase 1: Systematic review

A systematic analysis was done about the currently existing models to find the security vulnerabilities of MANETs. A detailed analysis was done about managing the trust between the mobile nodes when they broadcast and accept the information from other nodes.

2. Phase 2: Building a model

In this phase, minimizing the misinformation spread through malicious nodes in MANETs was focused and to reduce the above risk a globally distributed reputation model was introduced.

3. Phase 3: Testing the model

A prototype was built using the model and tested in simulated environments.

As this study was a development-oriented research, data generated from simulated environments were used to test and validate the blockchain model prototype. The data were generated using ganache blockchain simulator and the truffle framework.

VI. Conclusion

This study is based on managing the trustworthiness of nodes in a MANET and minimizing the spread of misinformation through malicious nodes. Recently, MANETs have been in global use for multiple applications. Most of them are used in real-time autonomous decision-making situations and sensitive environments. Therefore, the trust value of the nodes should be very robust for external modifications. This paper presented a novel approach to use blockchain technology as a globally distributed reputation system to calculate, store and distribute the trust value of the nodes.

The concept of smart contracts in blockchain technology was used effectively, which possesses the ability to communicate with mobile nodes and process the information without human intervention. Registering the nodes, calculating and storing the latest trust value and distribution of a node's trustworthiness on demand is handled by the smart contracts included in the blockchain system. The reputation system stores the trustworthiness of a node in a range of 0 and 1, where 1 depicts that the node is fully trustworthy and 0 depicts that the node is malicious. The initial value for a new node will be 0.5. Therefore, the trust will be defined based on the average trust factor of the nodes.

Consortium blockchain concept which is based on mixed properties of public and private blockchains was used as the basis of the system. Accessibility to the public is a requirement in this system as any node should have the ability to retrieve the trust value of another node. But the action of adding new blocks which contain trust values is only permitted by a governing body with the mining power of the blockchain system. Public blockchain miners are not allowed to participate in this mining process. Governments, military and organizations under the governance of international communities with enough computing power have the ability to mine new blocks and updating the system.

Using the proposed model, the trustworthiness of a node can get migrated from one network to another seamlessly as the trust value is not stored inside a boundary of a MANET but in a distributed reputation system which is accessible globally.

VII. Future Work

The current system processes the feedback from the node in binary. If the information is accurate, the feedback value is 1 and if the information is inaccurate the feedback value is 0. A weighted average score can be introduced to the system, based on the accuracy of the information between 0 and 1 with the integration of machine learning. And also, with the use of 5G technology, the prevailing communication latency can be avoided.

A communication protocol should be researched and implemented to activate efficient communication between the mobile nodes and blockchain model. The effectiveness of MQTT protocols can be tested and validated to build seamless communication between them.

References

[1] Dennis, R. and Owen, G. "*Rep on the block: A next generation reputation system based on the blockchain*". In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). [online] IEEE. Available at: http://10.1109/ICITST.2015.7412073 ,2015, [Accessed 13 Jun. 2019].

[2] Vijayan, R. and Jeyanthi, N. (2006). "*A Survey of Trust Management in Mobile Ad hoc Networks*". International Journal of Applied Engineering Research, 11(4), pp.1-6.

[3] Sridevi, K. and Sridhar, M., "*A Reliable Trustworthy Approach Based on Node Behaviour Prediction for Secure Routing in MANET*". International Journal of Intelligent Engineering and Systems, 2017, 10(6), pp.230-241.

[4] Bindu, G., Karthika, R. and Sridevi, S. "*A study on reliability of Manets using trust management system"*. International Journal of Engineering & Technology, 2018, 7(2.21), p.402.

[5] Rehman E, Sher M, Naqvi SHA, Badar Khan K & Ullah K, *"Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network"*, Journal of Computer Networks and Communications, 2017.

[6] Babu SV & Vijila CKS, *"Survey report on MANETs trust management"*, Advances in Natural and Applied Sciences, Vol.11, No.3, 2017, pp.138-146.

[7] Pradnya MN & Sachin D.B, "Trust System Based Intrusion Detection", Mobile Ad-hoc Network (MANET)", 2012.

[8] Ahmed, A., Abu Bakar, K., Channa, M., Haseeb, K. and Khan, A. "A survey on trust-based detection and isolation of malicious nodes in ad-hoc and sensor networks". Frontiers of Computer Science, 2014, 9(2), pp.280-296.

[9] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. *"An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*". In: 2017 IEEE International Congress on Big Data (BigData Congress), online] IEEE. Available at: http://10.1109/BigDataCongress.2017.85 [Accessed 14 Jun. 2019].

[10] Christidis, K. and Devetsikiotis, M. "Blockchains and Smart Contracts for the Internet of Things", 2016, IEEE Access, 4, pp.2292-2303.

[11] Goka, S. and Shigeno, H. *"Distributed Management System for Trust and Reward in Mobile Ad hoc Networks*". In: 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC). [online] IEEE. 2018.

[12] Alexopoulos, N., Daubert, J., M¨uhlh¨auser, M. and Habib, S. "Beyond the Hype: On Using Blockchains in Trust Management for Authentication",2017 IEEE Trustcom/BigDataSE/ICESS.