Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

QOS AND DEFENSE ENHANCEMENT USING BLOCK CHAIN FOR FLY WIRELESS NETWORKS

Dr. N. Bhalaji,
Associate Professor,
Department of Information Technology,
SSN College of Engineering,
Chennai, Tamil Nadu, India.
Email: bhalajin@ssn.edu.in

Abstract: The autonomous mobile nodes framing an instantaneous network, utilizing the nearby available device that volunteer in establishing network is coined as the fly wire network. These adhoc type of network framed simultaneously are prone to various vulnerabilities, developing alterations in the information's or hacking of information's or the blocking of services. These security threats causing losses in the information transmitted, makes it necessary for the trust evaluation of the nodes to identify the selfish nodes. So the paper proposes the block chain trust management of nodes to avoid the vulnerabilities in the transmission path, enhancing the performance of the network. The performance of the proposed method is validated in the network simulator –II to ensure its capability in terms of the quality of service and the security (defense).

Keywords: Fly networks, Block chain, Trust management, Vulnerabilities, Quality of service, Defense enhancement

1. Introduction

The self- organizing wireless networks that are formed instantaneously without any infrastructure or the central access point utilizing the nearby available nodes are called the fly wireless network, since the frame the network on the fly without overlaying on any infrastructure or a central body. These fly wireless networks can also be known as an adhoc network which may be further classified into subtypes such as the mobile adhoc network, wireless adhoc network, vehicular adhoc network and the wireless sensor network etc. These are small networks that are designed for a particular purpose or to be part work destined for large purpose. These instantaneous networks formed with the volunteering nearby mobile devices helps in the extending communication from a source node to the destination node, with the other nodes in between behaving like a mediator or the forwarder relaying the information between the sources to the destination if destination is out of sight for the source. The ad hoc networks as whole poses the

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

certain unique characteristics such as dynamically changing network topologies, decentralization, heterogeneity-when the nodes are not of same type, dispersed operation, mobility and energy constraint [12] causing multiple issues in the process of transmitting information's from one end to the other. Form the above listed characteristics of the adhoc or the fly networks, the mobility and the energy constraint of the nodes serve as the prime characteristics that causes issues related to the transmission in the routing of the information paving way for the link failure or the topology change, thus causing failure in the transmission of the information's, the researches proceeded with the aim of envisioning a routing handling the issues of the mobility and energy usage and succeeded in enhancing the network longevity, improving its performance reducing the energy consumption [13] and handling the mobility issues continuing with the same topology throughout the transmission [17], and the routing algorithms based on the evolutionary and the swarm intelligence provided an even enhanced routing, [18], [19], [20] optimizing the energy and the mobility of the network, preventing the dynamic topology changes to a certain extent and enhancing the performance, reducing the link failures.

Though the network performance showed considerable improvement in the process of routing, its decentralized nature made it more prone to the various attacks that cause alteration in the messages, hacking of the information's, block the services, so on, due to their lack of secure boundary and central medium, the presence of the selfish nodes and the usual assumptions made as the nodes are co-operative and invulnerable [12]

To face the above issues related to security in the fly networks, the communication networks were enriched with the intrusion detection system that are single and collaborative [1], so as to enhance the capability of the detection, and introduced secure routing [14] along with the watchdog and path rater [12] to analyze the misbehavior in the network, though the methods sounded to be promising they did not provide maximum traceability. Instead the methods proved to be very costly. But the security threats paved way for more and more loss in the information, so it became essential to evaluate the trust of the nodes, as it plays a vital role in the peer to peer communication that requires, a very high degree of trust, many steps in evaluating the trust of the nodes resulted with more time and energy consumption.

So the paper presents the block chain in the trust management of the nodes, evaluating the trust of the nodes using the statistical inference method based on the Bayes theorem. Since the block chain preserves the originality of the stored data and provides a transparency in the process.

The remaining paper is organized with the section 2 giving the details related to the proposed work based on the block chain, section 3 providing the proposed work that details the block chain based trust management. Section 4

ISSN: 2582-4104 (online)

analysing the QOS enhancements achieved in the fly wireless networks utilizing the trust management with the block chain and 5. Presenting the conclusion holding the overview of the proposed work with the future work to be proceeded with.

2. Related Works

Meng et al [1] the author elaborates the review on the block technology, utilized in enhancing the detection of the intrusions and the also the identification of the open issues in relation to it. Valdeolmillos, et al [2] the paper address the challenges in the different types of the crypto currencies with the highest capitalization in the market and also presents the analysis of the block chain that roots them. Kumar et al [3] the proof of work approach using the expectation maximization algorithm and the polynomial matrix factorization ensures to be more engaging to the cloud and the fog based applications, as they show much efficiency in the terms of the time and energy. Hawlitschek et al [4] development of the trust free systems by designing the trusted interference using the block chain is proposed in this paper. Yaga et al [5] the paper details the overview of the block chain technology in order to help readers in understanding the working of the block chain. Arslanian et al [6] the paper aims in resolving the issues faced by the application of the block chain by exploring several potential resources. Mohsin et al [7] the paper presents the capacities, scopes and the challenges of the block chain technology in varied applications in various fields. Block chain Liu, et al [8], the paper provides the survey considering the state of art physical layer security that can provide a highly secure communication in the wireless networks Zhao et al [9] the adversarial jamming and the eaves dropping in the network is handled by proposing an anti-adversarial jammer, then the AN strategy is employed, to pursue with the further interference in the network, Pathan,et al [10] aims in presenting the challenges incurred in the ad hoc networks usually known as the self-organizing networks in terms of the security. Gudipati et al [11] the Soft RAN is provided to manage with the dense wireless deployment with the mobile nodes and the finite spectrum. Sarika et al [12] the paper presents the variety of the vulnerabilities, attacks and the security issues in the mobile adhoc network compared to the wired networks that holds a quite lot of preventions against the attacks. Das et al [13] the paper provides a better area coverage for the adhoc network, by reducing the number of communications with the help of the triangulation technique, so as to reduce the battery usage to extend the network longevity and connectivity. Kumar et al [14] proposes a trust based security management Balaji, et al [15] the paper presents the dual authentication with the key management to enhance the security of the vehicular adhoc networks that is the subtype of the mobile adhoc network. The above security methods involve the security that does not provide a maximum transparency and traceability, further increasing the cost, so the paper aims in utilizing block chain based trust evaluation for the network, that scopes at providing with the maximum security with the additional features such as the transparency and traceability.

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

3. Proposed Work

The paper details the technology of the block chain in the examining the trust values of the mobile nodes, to identify the nodes that are selfish and liable of being attacked, for separating them from the normal nodes, to prevent the hindrances in the transmission.

Block chain [22] is usually considered as the sequence of the procedures used in the distributed network, to manage the consistency in the database among all the users, the block chain technology does not hold any permanent center nodes, that initializing equal priorities for all the users in it , supplying the copies of the single transaction to all its members. This makes the block chain invulnerable as the information stored could not be altered, just by altering the single copy and must be good enough in altering all the copies recorded in the distributed system. This high reliability and the security of the block chain has made it very prominent in the almost all areas and in the fly wireless network too. The block chain is an organized record that records the assured number of previous done transactions as blocks. The information of the history transactions stored on the individual block is circulated to all the blocks. This forms the chain among the blocks as each block hold the summary of all the transactions handled by the preceding block, in terms of the hash tag. The block also includes certain procedure to determine the miner in the chain by utilizing many miner selection strategy such as the proof of work and the proof of the capacity [3], the nodes superior based on the processing power, capital, capacity of reserve are often selected as the miner and allowed to transmit its block to others in the chain. This ensures the possible way security enhancements and the persistency in the distributed networks. The fig 1 below shows the block chain frame work in the proposed work.

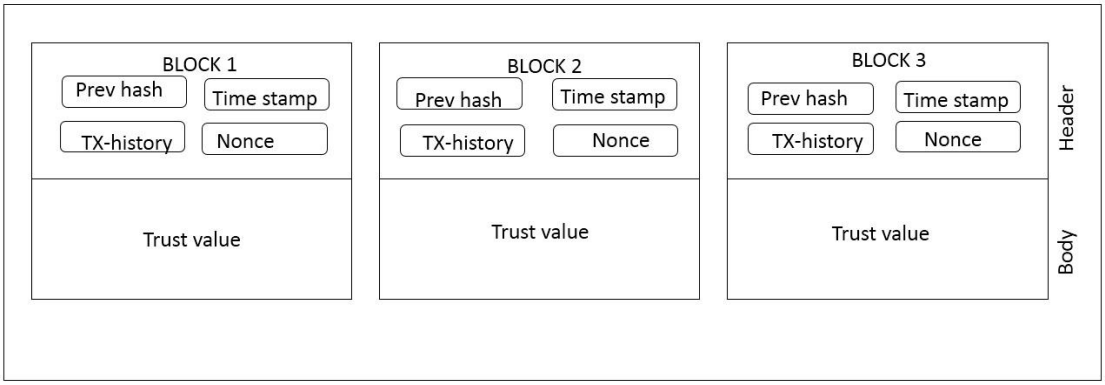


Fig.1Frame Work of Proposed Block Chain

The fig.1 shows the frame work of the block chain, where each block is framed into a chain by holding the information of the previous block in the form of the hash tag, the Nonce is the strategy used in selecting the miner,

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

in the proposed work the nodes with the maximum energy and minimum mobility is selected as the miner for the transmission of the blocks to all the nodes in the network.

3.1. Trust evaluation in the fly wireless network

The trust evaluation of the mobile nodes in the fly wireless network is based on the credits acquired, that involves the number of successful transmission taken place and the number of packet losses incurred along with the energy availability, and the mobility of the each node. The nodes is said to attain a high or low value based on the credits. The values are updated into the nodes that poses a stabilized network topology, containing a maximum processing capabilities in terms of energy and the mobility. The nod estimates the trust values of the each mobile node by calculating all the credit values acquired, and includes the trust information as a block to the block chain once it is been selected as the miner. The strategy proof of stake, proof of work and the proof of capacity, selects the nodes with the maximum stack of trust values, possessing a higher energy and minimum mobility as the miner, in order to provide a timely access of the trust values with the speedy updation of trust values in the block chain, whenever there is a variation in it.

The proposed system utilizes the weighted aggregation in the determining the trust values, between the high and the low value of the credits obtained for each node, the equation (1) is framed in this regard.

$$T_{values} = \frac{w_1 * a - w_2 * b}{a + b} \tag{1}$$

Where the T_{values} is the trust value of the nodes, based on the number of the successful transmission and the failures of the node, w_1 and the w_2 are the weights and the a and b are the high and the low values respectively. Where the credits obtained are evaluated using the statistical interference based on the Bayes theorem. The aggregated credits involves the performance of the nodes in terms of the successful transmissions and the failures, of the each node the equation (2) shows the estimation of the credits using the statistical inference based on the Bayes theorem.

$$prob_{E/C} = prob_E \prod_{N=1}^{n} prob\left(\frac{C_N}{E}\right) \Big/ prob_E \prod_{N=1}^{n} prob\left(\frac{C_N}{E}\right) + prob_{\acute{E}} \prod_{N=1}^{n} prob\left(\frac{C_N}{E}\right) \tag{2}$$

ISSN: 2582-4104 (online)

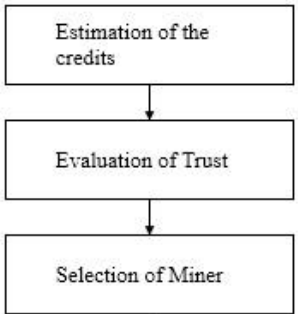
Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

Where the E represents the events, that included the successful completion and the failures occurred, the E/C is the credits gained on the occurrence of the events, $prob_{E/C}$ is the probability of the credits that could be gained on the occurrence of the event, whenever the $prob_{E/C}$ surpasses the threshold value that is previously set, the credits are remarked as high and else generates the credits with the low values. This enables the nodes to periodically update the credit values to the node with the stabilized processing capabilities that is liable of being selected as the miner.

3.2. Trust Management with Block chain in Fly wireless network

The trust management for the fly wireless network utilizing the block chain ensures many benefits, that improves the quality of service and the defense mechanism of the network,

The block chain behaving like a distributed ledger, facilitates cooperativeness' among each node to retain the reliableness of the stored information. It ensures the enhancement in the scalability of the system to a large extent, reducing the severity of the single point failures, as it always maintains the copy of all it's happening (transmissions) in every member (node) in the fly network , with the ability of performing certain operations over the stored information's. The frame work that depicts the chain of blocks eludes the interference caused in terms of the malicious attacks and adversary jamming, as the alteration in one block in the chain would develop the need to reconstruct all the entire blocks, which would be result with the exponential increase of the time of alteration. Thus enabling a consistency in the information stored. In case of the fly wireless network, the mobile nodes involved bestows to the block chain and retrieves data from it. So as to supply with the valuable trust values once being inquired by the other nodes in the network. The block chain assures timeliness in the data recorded, as the updated trust values are reflected



Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

in a higher speed due to the miner selection that is based on the strategies like the proof of the stake, proof of work and the proof of the capacity. The fig 2 gives the flow involved in the proposed process for the trust management in the fly wireless network with the block chain The data recorded in the block chain enables a node to gain knowledge on the trustworthiness of the nodes, the miner usually gather the trust information and once the nodes request for the trust details of the other neighboring nodes, the miner checks for the identification of the requesting nodes and forwards the details to it. So the block chain improves the trust management providing a better consistency, availability and timeliness with the protection. The following steps explains the trust management offered by the block chain for the fly wireless network.

All the mobile nodes that have volunteered in framing the network, are subjected to the following process to identify the malicious attacks that causes alteration of the information creating losses in the transmission of the packets and blocking of services. To handle the security threats the trust evaluation of the node is done and managed with the help of the block chain.

(i)For all nodes $\{M_1, M_2, \dots \dots M_m\}$ the credits values are evaluated based on the successful transmission and the failures in the transmission with the $prob_{E/C} = prob_E \prod_{N=1}^{n} prob(\frac{C_N}{E}) \Big/ prob_E \prod_{N=1}^{n} prob(\frac{C_N}{E}) + prob_{\acute{E}} \prod_{N=1}^{n} prob(\frac{C_N}{E})$ and estimated as high or low based on the threshold value,

(ii) Based on the credits generated, the weight aggregation is performed to evaluate the trust of the nodes using the equation$T_{values} = \frac{w_1 * a - w_2 * b}{a+b}$, and the trust values evaluated are stacked into the node with the stable processing

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

capabilities identified using the particle swarm optimization that evaluates the nodes to select the nodes with the maximum energy and the minimum mobility, applying the foraging behavior of the swarms.

(iii) The nodes determined to be stable are filled with the trust values of the nodes and nonce helps in determining the miner using the strategies, such as the proof of work, proof of stake and the proof of processing capacity, the node with the maximum stake is selected as the miner, so that it helps in the speedy updation of the periodical trust values. The miner selection in the proposed is done involving the $hash\ value(M_{id,}\ time_{stamp}, previous\ _{hash}, nonce\ )$ all the stable nodes simultaneously alters the nonce and estimates the hash values, the node with the $hash_{values} \leq Threshold_{values}$ is selected as the miner. The miner enables the periodic updation of the information recorded in the chain of blocks.

(iv) The trust values from the miner are formed as the blocks and the added to the existing block chain. In the proposed work the nodes with the maximum stake and the processing capacities are selected as the miner, where the relationship between the mode of the selection (S_m) and the $Threshold_{values}$ is given as$Threshold_{values} = 2^{N_n - N_m} - 1$, where the N_m represents the continuous low values in the $Threshold_{values}$ and N_m gives the bits in the $hash_{values}$, and the $N_m = \int e^{-(\varphi * Threshold_{values} * \mu)}$

(v) The trust values stacked are framed into blocks with the dual parts, one holding the identity of the block along with the node identity ($M_{id,}$), previous hash and the, time stamp and the nonce is termed as the header, and the one containing the information of the trust value is coined as the body of the block, the block chain uses the secure hashing algorithm-256 in the proposed work to generate the hash values and the information are recorded into the block chain using the merle tree, in a secure and the efficient manner.

(vi) Each time a trust block is added to the chain by the miner the nonce is verified and then inserted into the chain, it further utilizes the distributed consensus protocols to determine the blocks to be added and discarded under circumstances were multiple number of blocks are received. The distributed consensus considers the block of the particular miner to be inserted, discarding the other blocks, it is to be noted that the other eliminated blocks also has to be gathered by the miner in order to insert them into the chain. This process enables the miners to record the same type of block chain that retaining the persistency of the network.

(vii) For each mobile nodes a minimum threshold for the trust value (min_{Tv}) is maintained, for any $M_n < min_{Tv}$ is considered to be the selfish node and liable of malicious attack. This detail is broadcasted to all the other nodes, to further prevent the node from taking part in the transmission, thus ensuring a reliable and a secure transmission.

ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

So the proposed system using the block chain in the trust management enables the identification of the mobile nodes prone to the malicious attack, thus improving the security enhancement of the transmission, along with the quality of service.

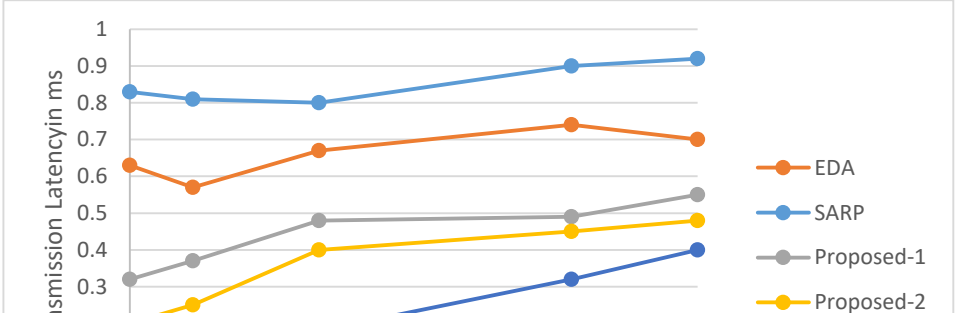
4. Results and Discussion

The proposed method of block chain in fly wireless network to ensure secure and reliable transmission to improve the quality of the service is evaluated using the network simulator -2 to validate its performance over varying number of nodes ranging from 100 to 200, over a simulation area of 1000*1000 sq. Units, with the simulation time of 100 seconds and the initial energy of 100 joules. The packet size is defined to be 1024 bytes, the table.1 below gives the detail of the parameters used in the simulation.

Parameter	Values
Number of Mobile Nodes	100-200
Simulation Area	1000*1000sq.Units
Simulation Time	100 seconds
Initial Energy	100 joules
Threshold value	.5
Packet size	1024 bytes
Hash algorithm	Secure Hash algorithm-256

Table.1 Simulation Parameters

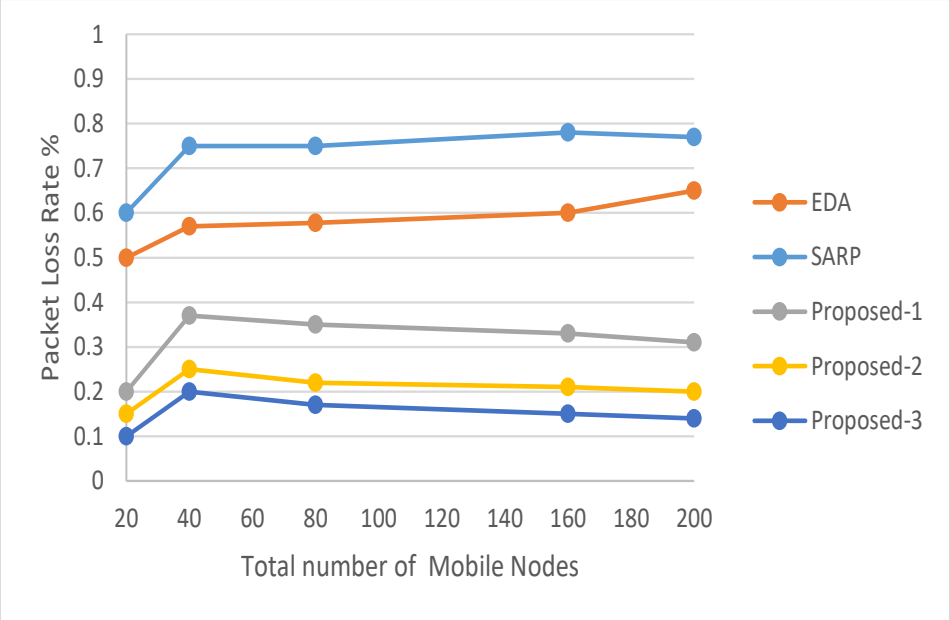
The evaluation the performance improvement achieved in the fly wireless network, using the block chain services in terms of security and the reliable transmission is compared with the prevailing methods SARP[14] and the EDA [15], to ensure the consistency in the network using the proposed system. The Fig.3 shows the transmission latency of the proposed method and its comparison with the prevailing methods that provide secure transmission.



ISSN:

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

The simulation result obtained in the Fig.3 for the transmission latency of the proposed method, shows a considerable improvement in the latency compared to the other methods of security aware protocol and enhanced dual authentication. The Fig. 4 is the simulation result of the packet loss rate that determines the percentage of failure in the process of transmission in the network the packet loss rate obtained for the proposed method shows the improvement achieved in terms of the successful transmissions as the packet loss rate of the proposed method using block chain methodology providing a defense mechanism against the spoofing attacks, black hole, warm hole and the ballot stuffing attacks etc. enables a reliable transmission that is highly secured, improving the number of successful transmissions and reducing the packet losses.



ISSN: 2582-4104 (online)

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 01
Pages: 1-13
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.1.001

Fig .4 Packet Loss Rate

The fig.4 gives packet loss rate of the proposed and the prevailing methods for different number nodes ranging from 100 to 200, the packet loss rate of the proposed method attains a considerable reduction, compared to the SARP and the EDA.

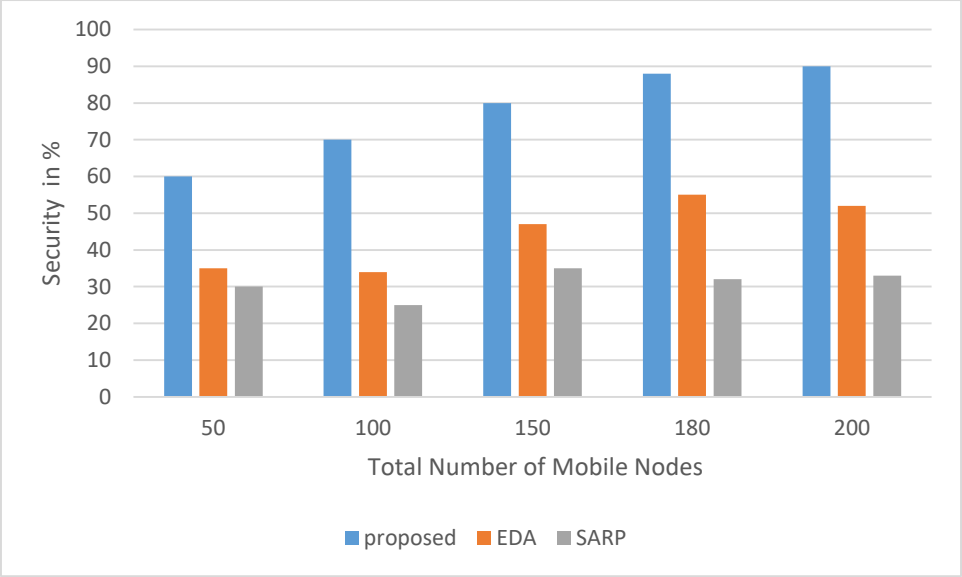


Fig .5 Defense Enhancement

The Fig .5 shows the percentage of the defense enhancement achieved in the proposed method compared to the security aware protocol and the enhanced dual authentication protocol. The proposed system with the block chain in the trust management ensures 40% of heightened security than the security aware protocol and the 23.7% security enhancement than the enhanced dual authentication.

5. Conclusion

ISSN: 2582-4104 (online)

The paper proposes a defense mechanism for the fly wireless networks against the security threats that either hack the information's or alter the information's. The defense mechanism includes the block chain in the trust management of the fly wireless networks, by generating the credit values based on the performance of the nodes using the statistical inference based on the Bayes theorem and trust evaluation using the weight aggregation method and framing the blocks the trust to form a chain to avoid the malicious activities, further the proposed system is validated and compared with the prevailing security aware and the dual authentication schemes to, ensure the quality of service and the defense enhancement rendered by the proffered system. In future the paper is to proceed with the network virtualization extending the coverage and the performance of the network with the block chain mechanism providing the security in allocating the frequency slices in the network, eluding the double spending in the resources of the wireless network.

References

[1] Meng, Weizhi, Elmar Wolfgang Tischhauser, Qingju Wang, Yu Wang, and Jinguang Han. "When intrusion detection meets blockchain technology: a review." *Ieee Access* 6 (2018): 10179-10188.

[2] Valdeolmillos, Diego, Yeray Mezquita, Alfonso González-Briones, Javier Prieto, and Juan Manuel Corchado. "Blockchain Technology: A Review of the Current Challenges of Cryptocurrency." In *International Congress on Blockchain and Applications*, pp. 153-160. Springer, Cham, 2019.

[3] Kumar, Gulshan, Rahul Saha, Mritunjay Kumar Rai, Reji Thomas, and Tai-Hoon Kim. "Proof-of-Work consensus approach in Blockchain Technology for Cloud and Fog Computing using Maximization-Factorization Statistics." *IEEE Internet of Things Journal* (2019).

[4] Hawlitschek, Florian, Benedikt Notheisen, and Timm Teubner. "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy." *Electronic commerce research and applications* 29 (2018): 50-63.

[5] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019).

[6] Arslanian, Henri, and Fabrice Fischer. "Blockchain As an Enabling Technology." In *The Future of Finance*, pp. 113-121. Palgrave Macmillan, Cham, 2019.

[7] Mohsin, A. H., A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, and K. I. Mohammed. "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions." *Computer Standards & Interfaces* (2018).

ISSN: 2582-4104 (online)

[8] Liu, Yiliang, Hsiao-Hwa Chen, and Liangmin Wang. "Physical layer security for next generation wireless networks: Theories, technologies, and challenges." *IEEE Communications Surveys & Tutorials* 19, no. 1 (2016): 347-376.

[9] Zhao, Nan, F. Richard Yu, Ming Li, Qiao Yan, and Victor CM Leung. "Physical layer security issues in interference-alignment-based wireless networks." *IEEE Communications Magazine* 54, no. 8 (2016): 162-168.

[10] Pathan, Al-Sakib Khan, ed. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[11] Gudipati, Aditya, Daniel Perry, Li Erran Li, and Sachin Katti. "SoftRAN: Software defined radio access network." In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 25-30. ACM, 2013.

[12] Sarika, S., A. Pravin, A. Vijayakumar, and K. Selvamani. "Security issues in mobile ad hoc networks." *Procedia Computer Science* 92 (2016): 329-335.

[13] Das, Sanjoy, Subrata Sahana, and Indrani Das. "Energy Efficient Area Coverage Mechanisms for Mobile Ad Hoc Networks." *Wireless Personal Communications* (2019): 1-14.

[14] Kumar, A. Vinodh, and S. Kaja Mohideen. "Security aware routing protocol for hybrid wireless network (SARP-HWNs) via trust enhanced mechanism." *International Journal of Business Data Communications and Networking (IJBDCN)* 15, no. 1 (2019): 34-57.

[15] Balaji, N. Alangudi, R. Sukumar, and M. Parvathy. "Enhanced dual authentication and key management scheme for data authentication in vehicular ad hoc network." *Computers & Electrical Engineering* 76 (2019): 94-110.

[16] Saudi, Nur Amirah Mohd, Mohamad Asrol Arshad, Alya Geogiana Buja, Ahmad Firdaus Ahmad Fadzil, and Raihana Md Saidi. "Mobile Ad-Hoc Network (MANET) Routing Protocols: A Performance Assessment." In *Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017)*, pp. 53-59. Springer, Singapore, 2019.

[17] Arumugham, Kowshika, and Vivekanandan Chenniappan. "Least Mobility High Power (LMHP) Dynamic Routing for QoS Development in Manet." *Wireless Personal Communications*105, no. 1 (2019): 355-368.

[18] Kumari, Priyanka, and Sudip Kumar Sahana. "An Efficient Swarm-Based Multicast Routing Technique." In *Computational Intelligence in Data Mining*, pp. 123-134. Springer, Singapore, 2019.

[19] Sharma, Anju, and Madhavi Sinha. "A differential evolution-based routing algorithm for multi-path environment in mobile ad hoc network." *International Journal of Hybrid Intelligence* 1, no. 1 (2019): 23-40.

[20] Joshua, Christy Jackson, and Vijayakumar Varadarajan. "An optimization framework for routing protocols in VANETs: a multi-objective firefly algorithm approach." *Wireless Networks* (2019): 1-10.

ISSN: 2582-4104 (online)

[21] Kochovski, Petar, Sandi Gec, Vlado Stankovski, Marko Bajec, and Pavel D. Drobintsev. "Trust management in a blockchain based fog computing platform with trustless smart oracles." *Future Generation Computer Systems* 101 (2019): 747-759.

[22] Tschorsch, Florian, and Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." *IEEE Communications Surveys & Tutorials* 18, no. 3 (2016): 2084-2123.

ISSN: 2582-4104 (online)