Proceedings of the Second International Conference on Inventive Research in Computing Applications (ICIRCA-2020)
DVD Part Number: CFP20N67-DVD; ISBN: 978-1-7281-5373-5

A Time Interval based Blockchain Model for Detection of Malicious Nodes in Manet Using Network Block Monitoring Node

Dr.V.Lakshman Narayana[1]
[1] Postdoctoral Research Fellow, Lincoln University College, Malaysia. & Assoc. Professor, Vignan's Nirula Institute of Technology and Science for Women, Peda Palakaluru, Guntur, Andhra Pradesh, India
lakshmanv58@gmail.com

Dr.Divya Midhunchakkaravarthy[2]
[2] Associate Professor, Lincoln University College, Malaysia.
divya@lincoln.edu.my

Abstract— **Mobile Ad Hoc Networks (MANETs) are infrastructure-less networks that are mainly used for establishing communication during the situation where wired network fails. Security related information collection is a fundamental part of the identification of attacks in Mobile Ad Hoc Networks (MANETs). A node should find accessible routes to remaining nodes for information assortment and gather security related information during route discovery for choosing secured routes. During data communication, malicious nodes enter the network and cause disturbances during data transmission and reduce the performance of the system. In this manuscript, a Time Interval Based Blockchain Model (TIBBM) for security related information assortment that identifies malicious nodes in the MANET is proposed. The proposed model builds the Blockchain information structure which is utilized to distinguish malicious nodes at specified time intervals. To perform a malicious node identification process, a Network Block Monitoring Node (NBMN) is selected after route selection and this node will monitor the blocks created by the nodes in the routing table. At long last, NBMN node understands the location of malicious nodes by utilizing the Blocks created. The proposed model is compared with the traditional malicious node identification model and the results show that the proposed model exhibits better performance in malicious node detection.**

Keywords— Routing table, Time Interval Based Blockchain Model, Malicious Node Detection, Network Block Monitoring Node, Block Analysis.

I. INTRODUCTION

MANETs are persistently self-arranging, infrastructure less systems made of an assortment of cell phones with no central administration. In such systems, every node can assume a job as a host or a switch helping out different nodes during data transmission [1]. As the essential objective of MANETs routing, secure routing intends to set up a right and productive way by the dispersed nodes themselves and can transmit the information quickly and accurately. An ordinary case is that the single node attacker or the group attackers will bargain the system by direct attack or indirect attack in the wake of misdirecting the route for communication. The MANET structure is depicted in Figure 1.

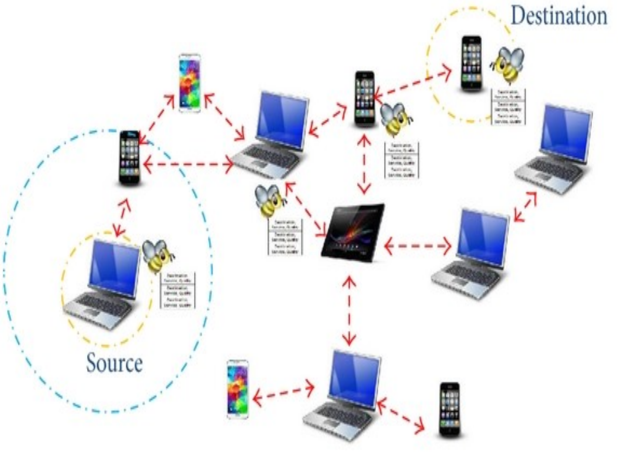


Fig 1: MANET Structure

Blockchain as a potential answer for establishing trust among the network as it has been effectively inquired about in different fields, including ad hoc networks [2] [3]. To exploit the decentralized idea of blockchain innovation, one must think about the restricted assets of MANETs when structuring a trust framework [4]. For instance, actualizing a blockchain executing a blockchain is a complex computational agreement even it provides strong security to the nodes with no central administration [5]. The process of how a block is created is illustrated in Figure 2.

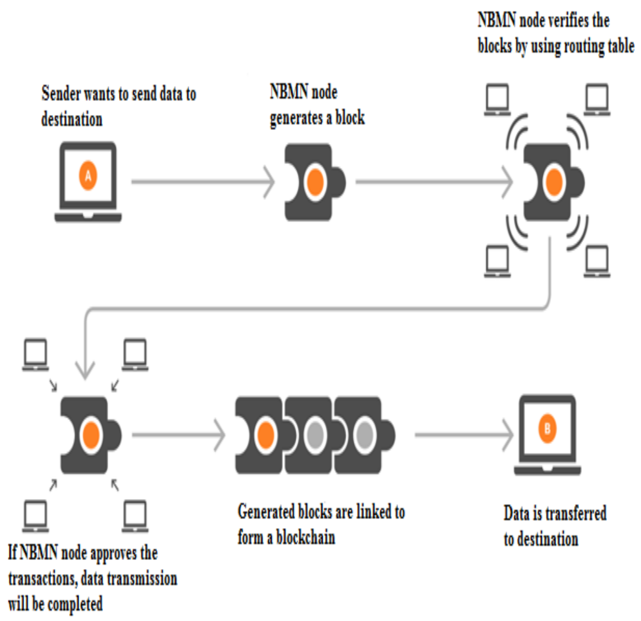

Sender wants to send data to destination
NBMN node generates a block
NBMN node verifies the blocks by using routing table
If NBMN node approves the transactions, data transmission will be completed
Generated blocks are linked to form a blockchain
Data is transferred to destination
A
B

Fig 2: Transaction Locking Process

In the event that a routing log section is distinguished to be bogus on the destination node, NBMN would then be able to follow the routing log back to the previous node, where another fake routing log may likewise be found. It can keep on following the deficiency to another node and afterwards it may at long last find that the fake log section that was brought about by the malicious node [15]. The provenance of NBMN node is clear as it plays a major role in the detection of malicious nodes based on the generated blocks verification.

The principle goal of the proposed work is excessively identified and disposes of the malicious nodes in MANET. The proposed strategy comprises the identification of a malicious node that reduces the system performance by dropping the data packets intentionally, establishing a fake route and causing data communication with it. The generated blocks at specific time intervals are analyzed by the NBMN node and such malicious behavior nodes are avoided and removed from the routing table to involve in communication.

II. LITERATURE SURVEY

MANETs are defenseless against numerous sorts of attacks, for example, Man in the Middle attack, DoS etc [16] [17]. As of late, numerous plans have been proposed to forestall various attacks like; a cryptographic mechanism to confirm members inside the system [18].

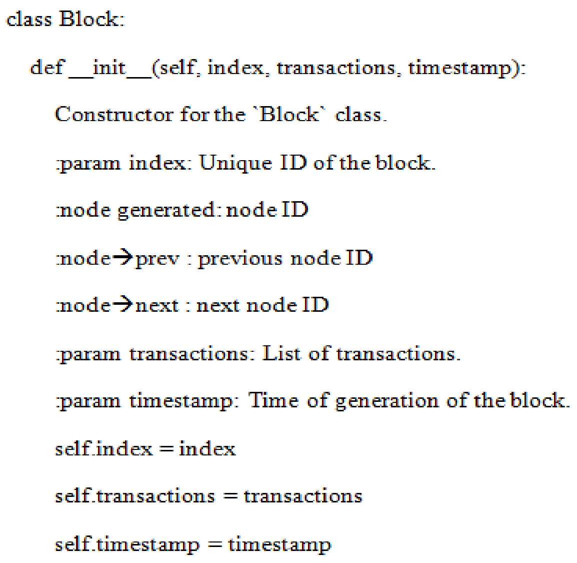
B. David el at [1] proposed a hybrid framework that is used to recognize outside intruder by utilizing intruder hypothesis in MANET. Group head for each cluster is chosen by one ideal answer for lessening the asset utilization of recognition outside interloper, which gives interruption administration to different nodes in its group [19]. These nodes are called typical nodes [20]. To forestall inside interruption neighboring nodes take an interest in the diversion and every node watches and treat neighbors at that point evaluates a trust as an incentive for them [21]. In the event that the evaluated trust estimation of a node may not exactly an edge, at that point it is recognized as a getting out of hand node [22].

E. Androulaki et al [3] proposed cluster-based wormhole interruption discovery calculation for MANET that eases these disadvantages and effectively mitigates the wormhole attack in MANET. In multi-jump remote frameworks, the requirement for participation among nodes to transfer each other's packets opens them to a wide scope of security dangers incorporating the wormhole attack

G. Glissa et al [6] proposed a Light Weight Trust-Based Routing (LWTBR) convention for MANETs. In this, trust esteem is kept up by each neighbor and it will assist with improving versatility. This model takes a shot at the double output where 1 speaks to full trust while 0 speaks to no trust. Another information structure has been added to the convention for the estimation of packets that will be going to convey.

III. PROPOSED METHOD

The proposed method efficiently identifies the malicious nodes in the MANET. When a MANET is established and routing process is completed, a node is selected from the MANET called Network Block Monitoring Node (NBMN) that is used for monitoring and analyzing the blocks generated after every transaction done by a node. The transactions done by every node is locked and a block is created that links with other blocks forming a blockchain. The block is created with the module depicted in Figure 3.



```
class Block:
  def __init__(self, index, transactions, timestamp):
    Constructor for the `Block` class.
    :param index: Unique ID of the block.
    :node generated: node ID
    :node→prev : previous node ID
    :node→next : next node ID
    :param transactions: List of transactions.
    :param timestamp: Time of generation of the block.
    self.index = index
    self.transactions = transactions
    self.timestamp = timestamp
```

Fig 3: Block Creating Module

The proposed model selects NBMN node and creates a block when communication is initiated and nodes start transferring data packets to neighbor nodes based on the routing table. A node when transfers data to the next node send 'CMP' message, node ID and neighbor ID to the NBMN node. The NBMN node verifies the routing table and validates the transaction if both the nodes are genuine and generates a block. This process is continued until all the data packets are transferred successfully. The node which intentionally drops the packets is accurately identified in the proposed model.

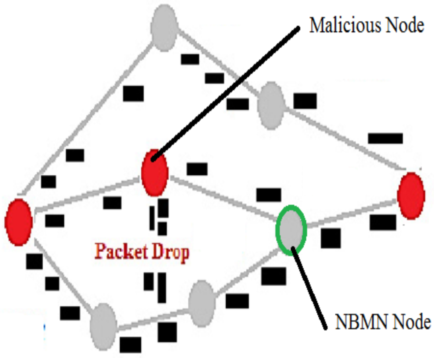


Fig 4: Packet Droppings in MANET

The framework of the proposed model is depicted in Figure 5. The blocks generated by NBMN node forms a blockchain after completing the data transmission successfully. The TIBBM model framework locks the data transmissions done by node and malicious nodes are easily identified and removed from the network.

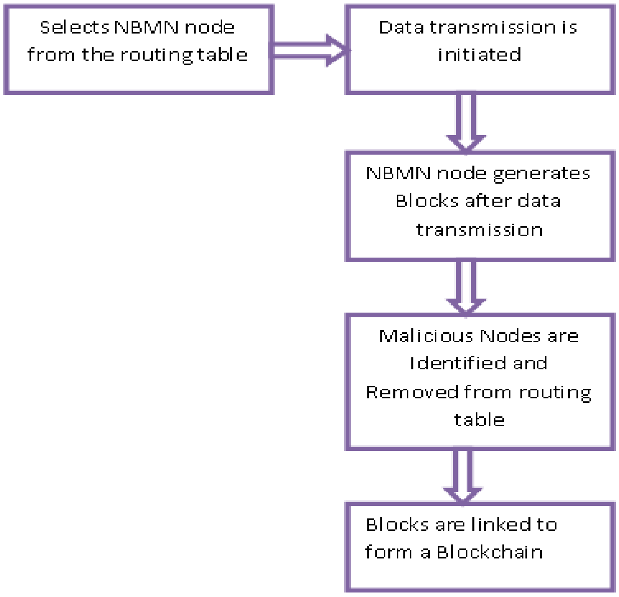

Selects NBMN node from the routing table
Data transmission is initiated
NBMN node generates Blocks after data transmission
Malicious Nodes are Identified and Removed from routing table
Blocks are linked to form a Blockchain

Fig 5: TIBBM Framework

The TIBBM model selects the NBMN node that generates the blocks after every transaction and finally, a blockchain is generated which is very helpful for analyzing all transactions done and it becomes easy to identify malicious nodes. The NS2 simulation of the data transfer is depicted in Figure 6.

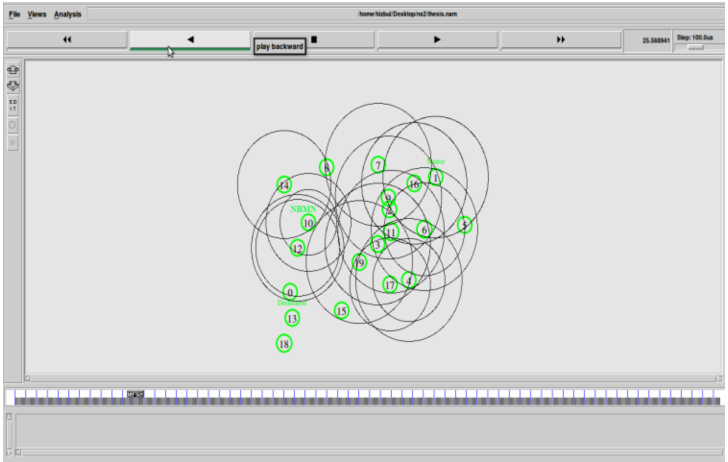
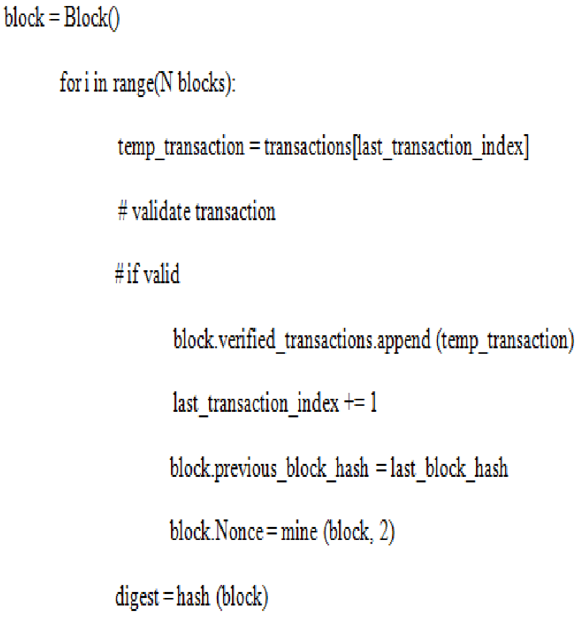


Fig 6: NS2 simulation Data Communication

After completing the data transmission, the blocks are linked and form a blockchain for locking all the transactions done that would become easy to identify the malicious nodes in the network or to identify malicious actions in the network to improve the network performance. The blockchain is generated and represented in Figure 7.



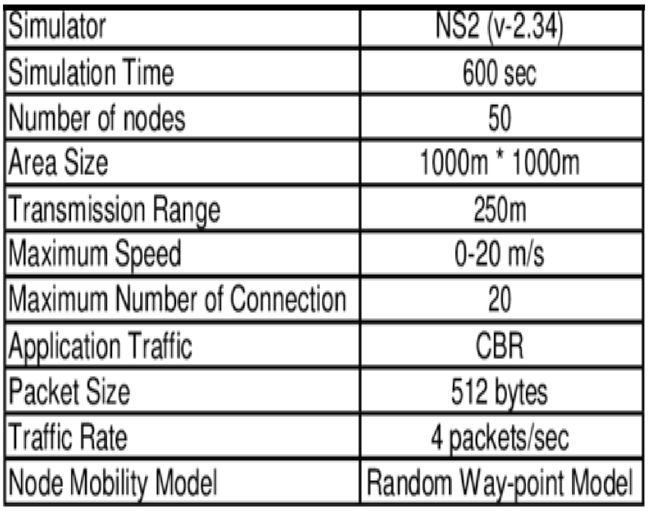
```
block = Block()
    for i in range(N blocks):
        temp_transaction = transactions[last_transaction_index]
        # validate transaction
        # if valid
            block.verified_transactions.append (temp_transaction)
            last_transaction_index += 1
            block.previous_block_hash = last_block_hash
            block.Nonce = mine (block, 2)
        digest = hash (block)
```

Fig 7: Blockchain generation

IV. Results

The proposed Time Interval Based Blockchain Model for MANET is simulated in NS2 that represents nodes mobility and for designing blockchain for analyzing the nodes behavior implemented using ANACONDA SPYDER representing generation of block [23]. The parameters used for creating NS2 simulation is represented in Table 1.

Table 1: MANET Parameters.



Simulator	NS2 (v-2.34)
Simulation Time	600 sec
Number of nodes	50
Area Size	1000m * 1000m
Transmission Range	250m
Maximum Speed	0-20 m/s
Maximum Number of Connection	20
Application Traffic	CBR
Packet Size	512 bytes
Traffic Rate	4 packets/sec
Node Mobility Model	Random Way-point Model

The proposed model generates a blockchain for analyzing the security to identify the malicious nodes in the network. The nodes which cause malicious tasks in the network are eliminated from the routing process and not allowed to involve in data transmission. The structure for creating a blockchain is represented in Figure 8.

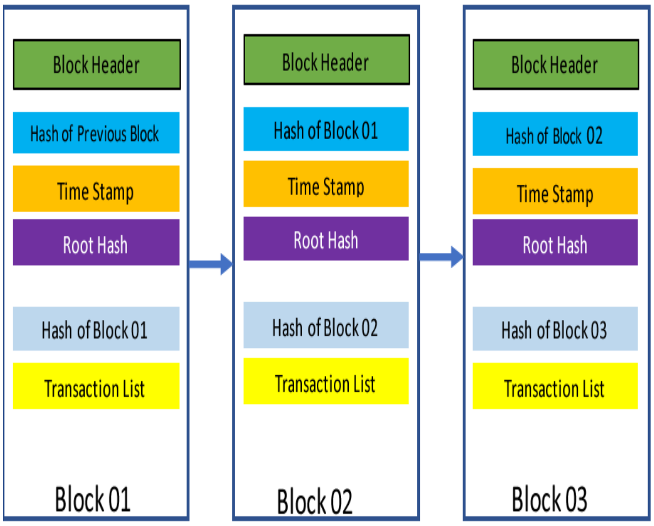


Fig 8: Blockchain block structure

The proposed TIBBM method is compared with the traditional Blockchain-Based Contractual Routing (BCR) routing method and the results show that the proposed method takes less time in the identification of malicious node. The malicious node identification time levels are depicted in Figure 9.

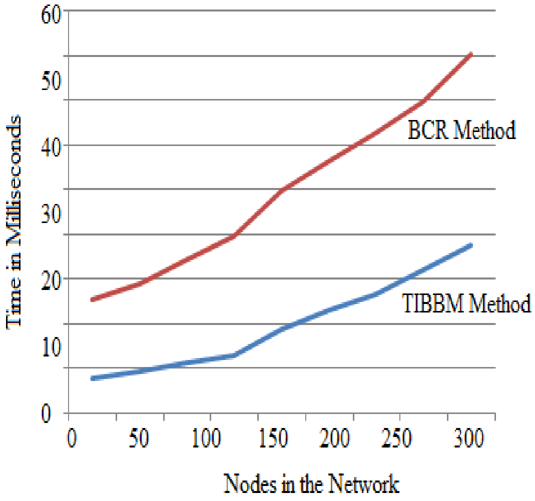


Fig 9: malicious node identification time

The proposed TIBBM method is compared with the traditional Blockchain-Based Contractual Routing (BCR) routing method in creating blocks after a transaction is done and the results show that the proposed method takes less time in block creating time. The block creating time levels are depicted in Figure 10.

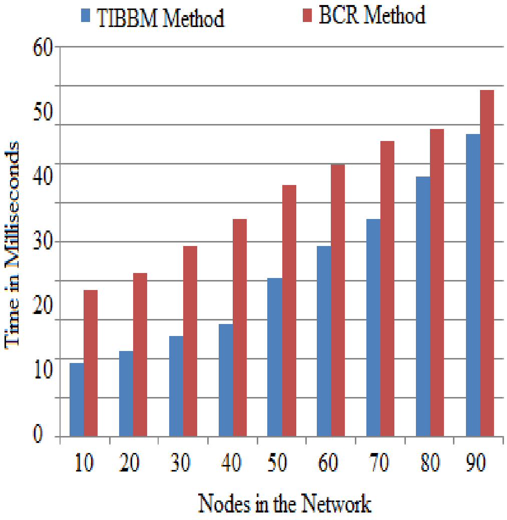


Fig 10: Block creating time interval

The proposed method effectively identifies the malicious nodes in the network by analyzing the blocks generated and removes the nodes causing malicious actions on the network. The proposed TIBBM method is compared with the traditional BCR method and the packet drop rate is depicted in Figure 11.

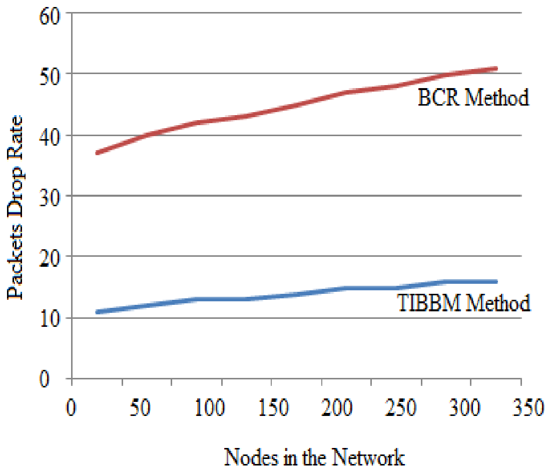


Fig 11: Packet drop Rate

The proposed method accurately identifies the malicious nodes in the network by analyzing the blocks generated and forms a blockchain with all the transactions done. The NBMN removes the nodes causing malicious actions on the network. The proposed TIBBM method is compared with the traditional BCR method and the accuracy rate is depicted in Figure 12.

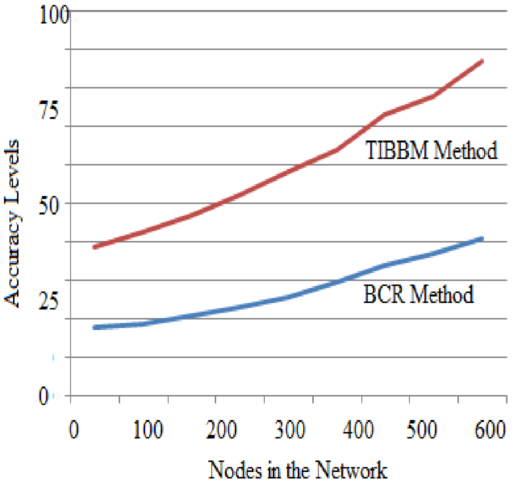


Fig 12: Accuracy in Malicious node detection

V. Conclusion

MANEs are used to establish communication whenever required without the need for any fixed infrastructure. Providing security to the route identified, and for the data being transmitted in the network is a challenging task. A malicious node detection model based on trust evaluation and block analysis in a MANET is introduced. The main aim of this manuscript is to detect nodes that are malicious in the network by analyzing the blocks generated by each and every node after transmitting the data. In the existing works, different malicious node identification techniques and methodologies are proposed, but they have some disadvantages, including high misdetection rates, inefficiency, and high communication cost. To overcome all these issues, Time Interval Based Blockchain Model is introduced that uses a Network Block Monitoring Node for analyzing the blocks generated by the nodes at a specific time interval. The proposed model exhibits better accuracy in identification of malicious nodes in the network thereby reducing the packet droppings in the network. The performance of the proposed method is better as the network eliminates the malicious nodes to involve in data transmission.

References

[1]. B. David, R. Dowsley, and M. Larangeira, "MARS: Monetized Ad-hoc Routing System (A Position Paper)," in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 82–86, Munich, Germany, June 2018.

[2]. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in Proceedings of the Annual International Cryptology Conference (CRYPTO'17), vol. 10401 of Lecture Notes in Computer Science, pp. 357–388, Springer, Cham, 2017.

[3]. E. Androulaki, A. Barger, V. Bortnikov et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in Proceedings of the the Thirteenth EuroSys Conference (EuroSys '18), pp. 1–15, Porto, Portugal, April 2018.

[4]. Deepa and B. Latha, "HHSRP: A cluster based hybrid hierarchical secure routing protocol for wireless sensor networks," Cluster Computing, pp. 1–17, 2017.

[5]. Jain and B. Buksh, "Solutions for secure routing in mobile ad hoc network (MANET): A survey," Imperial Journal of Interdisciplinary Research, vol. 2, no. 4, pp. 5–8, 2016.

[6]. G. Glissa, A. Rachedi, and A. Meddeb, "A secure routing protocol based on RPL for internet of things," in Proceedings of the 59th IEEE Global Communications Conference, GLOBECOM 2016, pp. 1–7, USA, December 2016.View at: Google Scholar

[7]. M. Bouaziz and A. Rachedi, "A survey on mobility management protocols in Wireless Sensor Networks based on 6LoWPAN technology," Computer Communications, vol. 74, pp. 3–15, 2016.

[8]. Da Silva, E.; dos Santos, A.L.; Albini, L.C.P.; Lima, M.N. Identitybased key management in mobile ad hoc networks: Techniques and applications. IEEE Wirel. Commun. 2008, 15, 46–52.

[9]. Wu, B.; Wu, J.; Fernandez, E.B.; Magliveras, S. Secure and efficient key management in mobile ad hoc networks. In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, Washington, DC, USA, 4–8 April 2005.

[10]. Huhtonen, A. Comparing AODV and OLSR routing protocols. Telecommun. Softw. Multimed. 2004, 26, 1–9.

[11]. Yang, J.; He, S.; Xu, Y.; Chen, L.; Ren, J. A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks. Sensors 2019, 19, 970.

[12]. Zhang, Y.; Lazos, L.; Kozma, W. Amd: Audit-based misbehavior detection in wireless ad hoc networks. IEEE Trans. Mob. Comput. 2012, 15, 1893–1907.

[13]. Raja, L.; Baboo, S.S. An overview of MANET: Applications, attacks and challenges. Int. J. Comput. Sci. Mob. Comput. 2014, 3, 408–417.

[14]. Sivakami, R.; Nawaz, G.K. Secured communication for MANETS in military. In Proceedings of the 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), Tirunelveli, Tamilnadu, India, 18–19 March 2011; pp. 146–151.

[15]. Bakar, A.A.; Ghapar, A.A.; Ismail, R. Access control and privacy in MANET emergency environment. In Proceedings of the 2014 International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 3–5 June 2014; pp. 1–6.

[16]. Cho, J.-H.; Swami, A.; Chen, R. A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv. Tutor. 2010, 13, 562–583.

[17]. Plesse, T.; Adjih, C.; Minet, P.; Laouiti, A.; Plakoo, A.; Badel, M.; Muhlethaler, P.; Jacquet, P.; Lecomte, J. Olsr performance measurement in a military mobile ad hoc network. Ad Hoc Netw. 2005, 3, 575–588.

[18]. Kartha, G.K.; Neeba, E.A. Trust Establishment in Mobile Ad Hoc Networks. In Proceedings of the 2014 3rd International Conference on Eco-Friendly Computing and Communication Systems, Mangalore, India, 18–21 December 2014; pp. 133–137. Omar, M.; Challal, Y.; Bouabdallah, A. Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. J. Netw. Comput. Appl. 2012, 35, 268–286.

[19]. Eschenauer, L.; Gligor, V.D.; Baras, J. On trust establishment in mobile ad-hoc networks. In Proceedings of the International Workshop on Security Protocols, Cambridge, UK, 17–19 April 2002; pp. 47–66.

[20]. P. Anusha, Aala Ravikiran,(2020), "Energy Priority With Link Aware Mechanism For On-Demand Multipath Routing In Manets", International Journal of Advanced Science and Technology, Vol. 29, No. 03, (2020), pp. 8979 - 8991.

[21]. Venkata Rao Maddumala, (2020), "Enhanced Morphological Operations for Improving the Pixel Intensity Level", International Journal of Advanced Science and Technology, Vol. 29, No. 03, (2020), pp. 9191 - 9201.

[22]. B. Tarakeswara Rao,(2020), "Use of Blockchain in Malicious Activity Detection for Improving Security", International Journal of Advanced Science and Technology, Vol. 29, No. 03, (2020), pp. 9135 - 9146.

[23]. C.R.Bharathi (2020), "Unlimited Bandwidth for RF Applications Using Design and Examination of CMOS LNA", International Journal of Advanced Science and Technology, Vol. 29, No. 03, (2020), pp. 9056 - 9062.

[24]. Naresh, (2020)," Energy Consumption Reduction in Cloud Environment by Balancing Cloud User Load", Journal of Critical Reviews, Vol 7, Issue 7, 2020, pp:1003-1010. doi: 10.31838/jcr.07.07.184

[25]. K. S, V.LN(2020), "Improving Relevant Text Extraction Accuracy using Clustering Methods", TEST Engineering and Management, Volume 83, Page Number: 15212 – 15219.

[26]. K. S (2020)," An Iterative Group Based Anomaly Detection Method For Secure Data Communication in Networks", Journal of Critical Reviews, Vol 7, Issue 6, pp:208-212. doi: 10.31838/jcr.07.06.39.

[27]. Banavathu Mounika, (2020)," Use of BlockChain Technology In Providing Security During Data Sharing", Journal of Critical Reviews, Vol 7, Issue 6, pp:338-343. doi: 10.31838/jcr.07.06.59.

[28]. V.L.N, BNS,(2020)," Fuzzy Base Artificial Neural Network Model For Text Extraction From Images", Journal of Critical Reviews, Vol 7, Issue 6,pp:350-354, doi: 10.31838/jcr.07.06.61.

[29]. VLN,APG (2020)," Accurate Identification And Detection Of Outliers In Networks Using Group Random Forest Methodoly", Journal of Critical Reviews, Vol 7, Issue 6,pp:381-384, doi: 10.31838/jcr.07.06.67.

[30]. Sandhya Pasala, (2020)," Identification Of Attackers Using Blockchain Transactions Using Cryptography Methods", Journal of Critical Reviews, Vol 7, Issue 6,pp:368-375, doi: 10.31838/jcr.07.06.65

[31]. C.R.Bharathi, L.V. Ramesh, (2020)," Secure Data Communication Using Internet of Things", International Journal of Scientific & Technology Research, Volume 9, Issue 04,pp:3516-3520.

[32]. Bharathi C R ,(2018),"Multi-mode Routing Algorithm with Cryptographic Techniques and Reduction of Packet Drop using 2ACK scheme in MANETs", Smart Intelligent Computing and Applications, Vo1.1, pp.649-658. DOI: 10.1007/978-981-13-1921-1_63

[33]. Schweitzer, N.; Stulman, A.; Shabtai, A.; Margalit, R.D. Mitigating denial of service attacks in olsr protocol using fictitious nodes. IEEE Trans. Mob. Comput. 2015, 15, 163–172.