International Journal of Safety and Security Engineering
Vol. 10, No. 4, August, 2020, pp. 567-572
Journal homepage: http://iieta.org/journals/ijsse

Secure Data Transfer in Manet with Key Calculator and Key Distributer Using Cryptography Methods

Yaswanth Kumar Alapati*, Suban Ravichandran

Department of Information Technology, Annamalai University, Annamalai Nagar-608002, Tamil Nadu, India

Corresponding Author Email: aykumar@rvrjc.ac.in

https://doi.org/10.18280/ijsse.100417

Received: 13 January 2020
Accepted: 10 June 2020

Keywords:
MANET, security, data loss, cryptography methods, key generation, key distribution, packet delivery rate, malicious nodes, secure data communication

ABSTRACT

A Mobile Ad Hoc Network (MANET) is combined with number of versatile nodes that can communicate with one another without having any predefined foundation. These versatile nodes in the MANET go about as routers to transfer the information from source to destination. Since there is an expansion in number of portable clients and its applications, the versatile nodes security assumes a significant job in it. Even there are many methods for providing security to MANET, there are still several attacks causing in MANET. Secure data transfer in MANET can be achieved by introducing strong cryptographic methods and key exchange techniques. The reason for key generation and key maintenance is to give secure techniques for avoiding malicious activities in the MANET and to increase system performance. In this paper a strong cryptographic method is proposed, which generates and maintains keys and distribute keys safely to trusted nodes avoiding malicious nodes. The proposed method detects the malicious nodes and avoids them to participate in communication to improve packet delivery rate and to reduce delay in the network. The proposed method considers a node as a MANET Key Calculator (MKC) which generates keys and selects another node as MANET Key Distributer (MKD) for providing secure data transfer in MANET by applying cryptography methods. The proposed method is compared with traditional methods and the results show that the proposed method is exhibiting better performance.

1. INTRODUCTION

MANETs are made out of self-sorted remote gadgets that participate to control the system and forward one another messages [1]. The arrangement of secure routing to these systems faces explicit vulnerabilities because of the absence of fixed framework and the non-dependable clients that need to utilize the system [2]. MANETs are mainly used for establishing communication during a wired system fails and during natural disasters. Nodes in a MANET can enter/leave the network dynamically [3].

Because of dynamic topology, and due to random node availability in MANET, it frequently undergoes attacks. To overcome the security attacks the essential cryptographic procedures are helpful [4]. The qualities of MANET bear the two difficulties and openings in accomplishing security objectives, for example, secrecy, validation, trustworthiness, accessibility, and non repudiation [5]. The countermeasures can be considered as features that decrease security vulnerabilities and attacks [6]. The MANET framework is depicted in Figure 1.

In MANETs there is no central administrator to deal with nodes and the communication problems [7]. In this manner nodes need to coordinate for the successful data transmission. In general, nodes may decline to participate in communication by not sending data packets to others and performing malicious actions in the network [8]. The proposed method selects two nodes as key calculator and key distributor and based on them the data is transferred securely from source to destination [9]. The cryptographic methods are applied on the data for avoiding malicious nodes to modify the contents of the data [10].

Cryptography is a significant and integral method for secure data interchanges. It changes plaintext into cipher text. Cryptography has two predominant classes, specifically symmetric-key and Asymmetric Key approaches [11]. In symmetric-key cryptography, a similar key is utilized to encrypt and decrypt the messages, while in the asymmetric methodology, various keys are utilized to change over the data [12]. Despite the fact that the deviated cryptography approaches are adaptable and are less difficult for key distribution than the symmetric methodologies, symmetric-key calculations are commonly more calculation effective than the other cryptographic calculations [13]. In MANETs, the computational process for key administration is firmly dependent upon node's accessible methods and the dynamic system topology [14]. Key management manages key generation, key maintenance, key distribution for securing the data. The process of Asymmetric cryptographic is illustrated in Figure 2.

Figure 3 illustrates the usage of Key Calculator and Key Distributor. In a MANETs, dependable transportation of data to the destination is of significant interest to clients sending data over that system [15]. The data on the system probably won't be communicated to the destination because of various malicious actions in the network [16]. These reasons can be categorized into two classifications, network failures and security attacks [17]. The fundamental issue is to recognize

anomalous changes in the system and sort them. Security attacks can be reduced by cryptography methods [18]. The MANET is a portable network and can be formed wherever necessary and because of its dynamic nature, MANETs frequently undergo several attacks [19]. The proposed method needs to improve security for the data in the network to improve packet delivery rate and the throughput of the system [20].

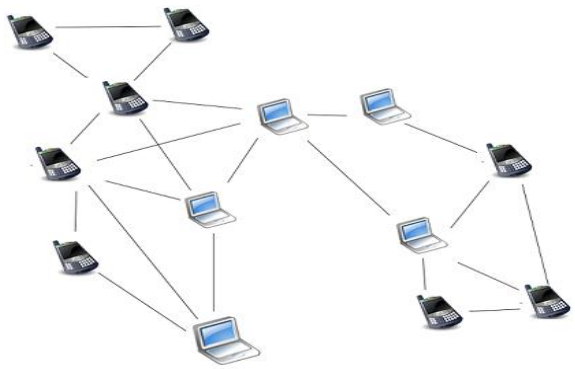

Figure 1. MANET framework

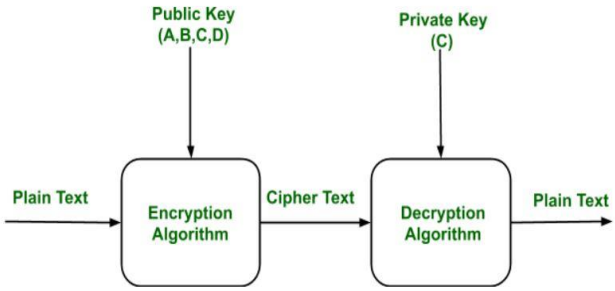

Figure 2. Asymmetric cryptography method

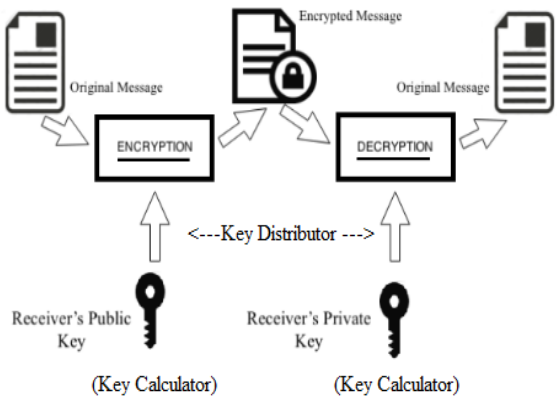

Figure 3. Key calculator and key distributor in communication

2. LITERATURE SURVEY

Saudi et al. [1] have proposed a protected on-request specially appointed routing convention dependent on DSR that forestalls attacks utilizing the symmetric cryptography. To influence the objective of the authenticity of each field in a route request, the initiator essentially incorporates a message verification code. The objective can without much of a stretch confirm the trust of the route utilizing the common key. Single direction hash capacities are utilized to confirm that no data packet was discarded which is called per-jump hashing.

Mandhare et al. [2] proposed Secure Routing Protocol (SRP) that utilizes symmetric cryptography to give start to end validation. The convention depends on route requesting technique and it requires a Security Association (SA) among source and destination node. The security association is acquired by means of the information on the partner's open key. SRP makes no supposition in regards to the neighbor nodes, which displays optional and malicious behavior. Nodes utilize secure message transmission (SMT) to guarantee successful data transmission. The Authenticated Routing for Ad hoc Networks depends on AODV and it is an independent convention that uses cryptographic key support, which relates its IP address with an open key so as to accomplish the security objectives of verification and non-revocation. The method utilizes cryptographic endorsements to bring verification, message-trustworthiness and non-renouncement to the route disclosure process. The source node communicates a marked data packet to its neighbors for a route to the goal.

Cai et al. [3] proposed a plan for data transmission in remote networks. The nature of administration levels for each end to end stream was communicated utilizing a resource utility capacity, and their calculations. The common channel was displayed as a transmission capacity characterized by maximal factions of shared intrusive connections.

Mwangi et al. [4] have displayed Metric Based Clustering (MBC) method which utilizes the host availability and host portability mutually to choose cluster heads. MBC was a quick focalized and load adjusting cluster approach that had the option to offer critical enhancement for versatility for enormous scale systems. Versatility has been considered as far as the normal connection drop time; the clusters developed by MBC are more steady than numerous different plans. The control overheads for group development utilizing the MBC method are kept generally low whenever contrasted with other plans. The proposed plan expanded the cluster head life time, yet more energy utilization happens for grouping. This will reduce the general system dependability in MANETs.

Garikipati et al. [5] proposed a Wormhole attacks location in specially appointed systems which is a measurable investigation. A Secure Routing Protocol against Byzantine Attacks for MANETs in Adverse circumstances gives a strategy to beat byzantine attacks utilizing open key cryptographic calculation for secure interactive communication in MANETS.

Narayanan et al. [6] proposed a methodology which uses improved security components so it fulfills the primary security prerequisite and ensures the revelation of a right and secured route. Gurung et al. [7] have proposed to build up an energy proficient secure routing method. Sirisala et al. [8] have presented the on-request routing conventions AODV, DSR on IEEE 802.11 and the trademark of these routing methodologies are displayed.

Musale et al. [9] have given the logical outcomes for the likelihood of achievement of information transmission over the systems taking the likelihood of accomplishment or failure of individual ways. Das et al. [10] have tended to

overcome secrecy and trust issues for a remote system containing malicious nodes.

Doss et al. [11] projected a protected key administration method for various leveled energy systems to improve both adaptability and survivability of gathering key administration for huge scale remote systems. This plan proposed a staggered security model, and a decentralized gathering key administration foundation to accomplish a security model. These methodologies limited the key administration overhead and improved strength to any single point failure issue. With the increments in the quantity of gatherings and the stature of the progressive structure, the overhead and the key supporting nature will increase.

El Houssaini et al. [12] introduced a nonexclusive development of dynamic key consideration by consolidating a regular verified key, an open key encryption and a multi-signature. In the wake of registering a common private key, a relating open key was distributed. A multi signature was joined as a trust for open key. This convention was utilized in cluster communication, group key shared by all individuals. In this way, the security between each gathering is low in a specially appointed system.

3. PROPOSED METHOD

In the proposed work, when a MANET is established and a secure route is identified and the routing table is updated with the source and destination address with routing information. To perform data communication among the secured route identified, source node will identify two nodes in the routing table as Key Calculator and Key Distributor. Cryptographic calculations are utilized for validation, privacy, trust. Most cryptographic frameworks require a fundamental secure, dynamic, and effective key management framework. Key management is a focal piece of any protected communication. The proposed method utilizes strong cryptography methods for secure data transmission.

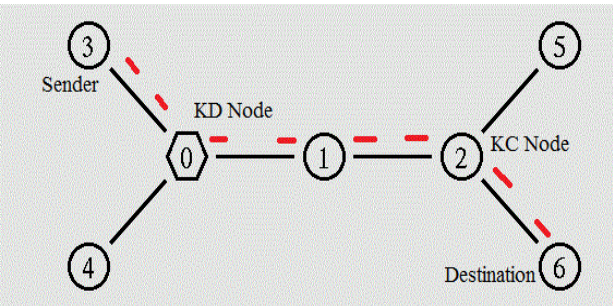

Figure 4. KC and KD node selection

3.1 Selecting nodes as KC and KD

When a network is established and a route is identified, the process of selecting key calculator and key distributor is initiated. The network initially allocates energy levels to the nodes in the network [21]. After route discovery, based on the remaining energy levels and the nodes which are in central location of the route are considered as the KC node and KD node. The node KC generates the keys as pairs i.e. public key and private key and send the pair set to KD node. The KC node task is to generate the key pair values and then transmit the key set only one time for KD node in a transaction. All the nodes in the network who involved in communication has to register with the KD node as it verifies the node authenticity before distributing the keys.

The test cases are executed and Figure 4 and Figure 5 Indicates the simulation results for the manet in which communication is initiated.

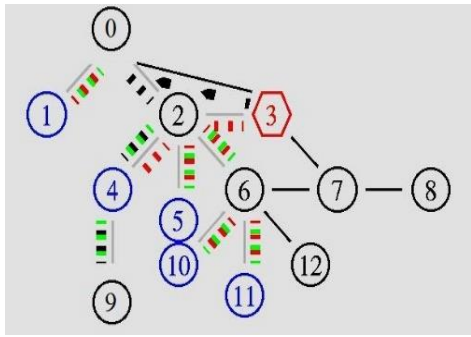

Figure 5. Simulation model

3.2 Secure key generation

After establishing a MANET and selecting the KC and KD nodes then the KC node initially has to generate a Key pair set and distribute it to KD node which distributes the keys to the nodes involved in communication. The process of generating key pair that contains public key and private key is done using the algorithm explained below.

Public key generation
Consider two prime numbers x and y.
PUK=x*y.
$\Theta(K) = (x-1)(y-1)+x+y$.
$H(k) = \Theta(K) + (x \,\&\, y)$
$PUB(K_i) = H(K) \,\&\, x \,\&\, y + PUK$

Private Key generation

KC Node considers integer numbers v1,v2 ….,v_n such that the GCD of first and last numbers are 1.
Consider a new set of integer numbers m1,m2,…..,m_n
$K \equiv m1 \pmod{v1}$
$K \equiv m2 \pmod{v2}$ . . . . . $K \equiv m_n \pmod{v_n}$
$K = m1p1K1 + m2p2K2 + \ldots\ldots\ldots + m_n p_n K_n$
$T_i = V_i/m_i$, $p_i = T_i\text{-}1 \pmod{m_i}$.
$PRK(K_i) = T_i * PUB(K_i) –x\text{-}y\text{-} PUK$.
Key Pair (KP) = set { $PUB(K_i)$: $PRK(K_i)$}

After key pairs are generated, they are transferred to the Key Distributor. When communication is initiated, then based on the routing information source node will request public key from KD node.

The KD verifies the routing table and then sends the public key to source node for encryption. The cipher text is then divided into data packets and then transferred to neighbor nodes based on routing table information [22, 23]. When data is received by the destination, it requests the private key by sending source node id as a request. The KD node verifies the destination is a valid one or not and then distributes the private key to the destination node for decryption of data. The proposed method framework is depicted in Figure 6.

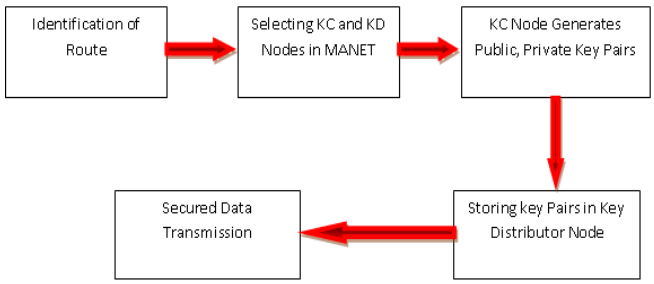

Figure 6. Data communication framework

4. RESULTS

The proposed method is implemented using NS2 simulator which establishes a MANET and the key generation process and distribution process is used for successful data transmission. The parameters used in the implementation are illustrated in Table 1.

Table 1. Parameters used

MANET Parameter	Value
Value x	800
Value y	600
Simulation time	150s
Speed	(0-3)m/s
Routing Protocol	AODV,DSDV
Mobility	Random
Maximum Connections	8
Number of nodes	20,40,60,80
Packet size	1460
Data Rate	1Mbps
Traffic Type	Constant Bit Rate(CBR)
MAC Protocol	Mac/802_11

The packet delivery ratio of the proposed method using KC and KD nodes is high when compared to traditional methods. The proposed method strictly verifies the nodes that involved in communication. The comparison levels are depicted in Figure 7.

The average delay of the proposed method is low when compared to the existing method. The data is successfully transmitted to the destination without any delay. The Average delay of the proposed and existing methods is depicted in Figure 8.

The security for the data in the proposed method are high when compared to the traditional method. The security for the data is improved by utilizing KC node and Key Distributor nodes in the network. The KC node generates the keys and send to the only nodes involved in communication with the help of key distributor node [24]. Here there is no chance for malicious nodes to access the keys and to participate in data communication. If keys are not accessed, then there is no chance for malicious nodes to access sensitive data in the network. In this way the security of the proposed method is high as the existing methods do not use KC and KD nodes as a part of their network. The metrics considering the security for the data are packet delivery rate, and the delay levels as indicated that if the packet delivery rate is high, it indicates that malicious activities are reduced in the network. The security for the data levels are depicted in Figure 9.

The throughput level of the proposed method is high when compared to traditional method. The throughput level is depicted in Figure 10. The proposed method in the real time environment also exhibits better results than the traditional methods. Selecting KC and KD nodes may be time consuming and these nodes are performing complex operations that results in power consumption but the security is considered as the key point and the performance will be improved even number of the nodes in the MANET is increased.

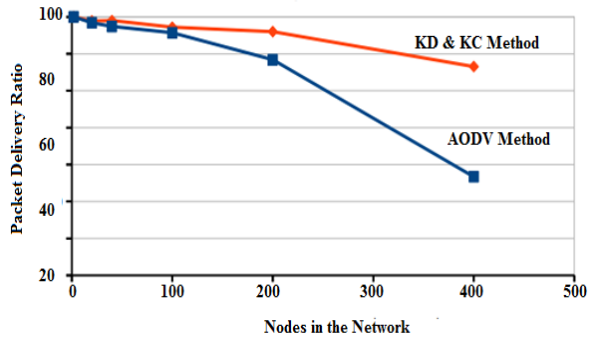

Figure 7. Packet delivery ratio

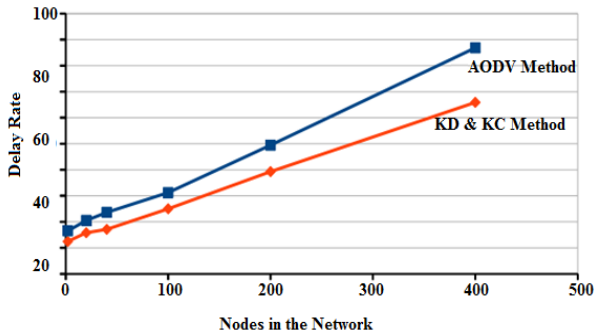

Figure 8. Delay levels

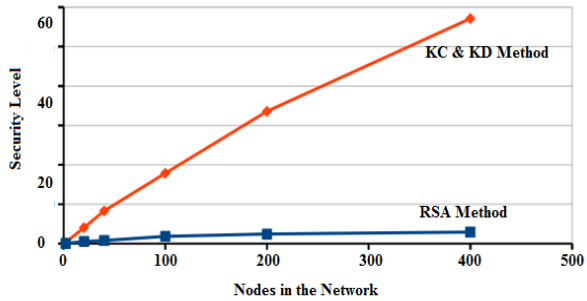

Figure 9. Security for the data levels

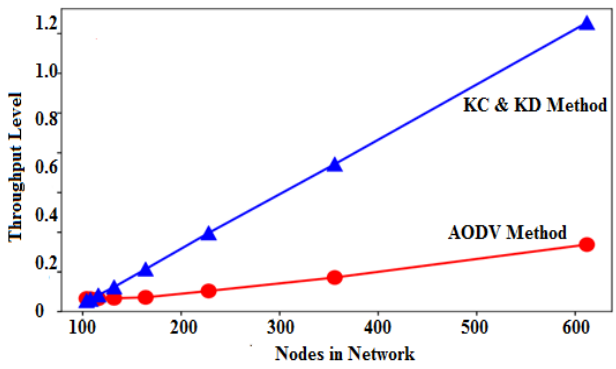

Figure 10. Throughput level

5. CONCLUSION

The security in network prevails as the major concept in wireless communication. The existing algorithms analyze the faults, link failures and breaks for providing an efficient communication system. But it is unable to provide high security in a network against attacks. Moreover, addressing the security issues to provide a good quality of service in MANET is a complex, critical and essential task. Portable Ad hoc Networks comprise of versatile nodes with no Controller Authority. Here the node might be influenced by a few sorts of attacks. It might cause the packet dropping and misrouting the data to another node. In the proposed work, cryptography methods are used for secure data transmission between the source and the destination. The proposed method uses Key Generator which generates the public and private keys for data encryption and decryption. The keys are distributed to intermediate nodes using the Key Distributor as malicious nodes are avoided to involve in communication. Even Cryptographic methods in the proposed method are complex, security is improved which strictly considers only trusted nodes during data communication. The proposed method exhibits better results when compared to traditional methods. The proposed method achieves 96% accuracy in data transmission with less packet drop ratio.

REFERENCES

[1] Saudi, N.A.M., Arshad, M.A., Buja, A.G., Fadzil, A.F.A., Saidi, R.M. (2019). Mobile Ad-Hoc Network (MANET) routing protocols: A performance assessment. The Third International Conference on Computing Mathematics and Statistics, pp. 53-59. https://doi.org/10.1007/978-981-13-7279-7_7

[2] Mandhare, A., Kadam, S. (2019). Performance analysis of trust-based routing protocol for MANET. Computing, Communication and Signal Processing, pp. 389-397. https://doi.org/10.1007/978-981-13-1513-8_41

[3] Cai, R.J., Li, X.J., Han, P., Chong, J. (2019). An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. IEEE Transactions on Mobile Computing, 18(1): 42-55. https://doi.org/10.1109/TMC.2018.2828814

[4] Mwangi, E.G., Muketha, G.M., Ndungu, G.K. (2019). A review of security techniques against black hole attacks in mobile ad hoc networks. 2019 IST-Africa Week Conference (IST-Africa), Nairobi, Kenya, pp. 1-8. https://doi.org/10.23919/ISTAFRICA.2019.8764862

[5] Garikipati, V., Naga, N., Rao, M. (2019). Secured cluster-based distributed fault diagnosis routing for MANET. Soft Computing and Signal Processing, 900: 35-51. https://doi.org/10.1007/978-981-13-3600-3_4

[6] Narayanan, M. (2019). Secured key management with trusted certificate revocation in MANET. Information Systems Design and Intelligent Applications, 862: 159-168. https://doi.org/10.1007/978-981-13-3329-3_15

[7] Gurung, S., Chauhan, S. (2019). A survey of black-hole attack mitigation techniques in MANET: Merits drawbacks and suitability. Wireless Networks, 26: 1981-2011. https://doi.org/10.1007/s11276-019-01966-z

[8] Sirisala, S., Ramakrishna, S. (2019). Survey: Enhanced trust management for improving QoS in MANETs. First International Conference on Artificial Intelligence and Cognitive Computing, Hyderabad, India, pp. 255-263. https://doi.org/10.1007/978-981-13-1580-0_25

[9] Musale, S.S., Dhende, S., Shirbahadurkar, S.D., Najan, A.S. (2019). Gray hole and cooperative attack prevention protocol for MANETs. Emerging Technologies in Data Mining and Information Security, 814: 559-566. https://doi.org/0.1007/978-981-13-1501-5_49

[10] Das, I., Shaw, R.N., Das, S. (2020) Analysis of energy consumption in dynamic mobile Ad Hoc Networks. Data Communication and Networks, 1049: 235-243. https://doi.org/10.1007/978-981-15-0132-6_15

[11] Doss, S., Nayya, A., Suseendran, G., Tanwar, S., Khanna, A., Le, H.S., Pham, H.T. (2018). APD-JFAD: Accurate prevention and detection of jelly fish attack in MANET. IEEE Access, 6: 56954-56965. https://doi.org/10.1109/ACCESS.2018.2868544

[12] El Houssaini, M.A., Aaroud, A., El Hore, A., Ben-Othman, J. (2016). Detection of jamming attacks in mobile Ad Hoc Networks using statistical process control. Procedia Computer Science, 83: 26-33. https://doi.org/10.1016/j.procs.2016.04.095

[13] Tiwari, S., Jain, A., Chowhan, G.S. (2011). Migrating packet dropping in Ad hoc Network based on modified ACK-based scheme using FSA. International Journal on Emerging Technologies, 2(2): 102-105.

[14] Kaur, J., Singh, T. (2014). A secured data transmission method using enhanced proactive secret sharing scheme to prevent black hole attacks in MANETs-a review. International Journal of Computer Applications, 119(10): 20-28. https://doi.org/10.5120/21104-3827

[15] Naresh, A., Pavani, V., Chowdary, M.M., Narayana, V.L. (2020). Energy consumption reduction in cloud environment by balancing cloud user load. Journal of Critical Reviews, 7(7): 1003-1010. https://doi.org/10.31838/jcr.07.07.184

[16] Sarada, K., Narayana, V.L., Gopi, P., Pavani, V. (2020). An iterative group based anomaly detection method for secure data communication in networks. Journal of Critical Reviews, 7(6): 208-212. https://doi.org/10.31838/jcr.07.06.39

[17] Mounika, B., Anusha, P., Narayana, V.L., Lakshmi, G.V. (2020). Use of blockchain technology in providing security during data sharing. Journal of Critical Reviews, 7(6): 338-343. https://doi.org/10.31838/jcr.07.06.59

[18] Narayana, V.L., Sudheer, B.N., Maddumala, V.R., Anusha, P. (2020). Fuzzy base artificial neural network model for text extraction from images. Journal of Critical Reviews, 7(6): 350-354. https://doi.org/10.31838/jcr.07.06.61

[19] Narayana, V.L., Gopi, A.P., Khadherbhi, S.R., Pavani, V. (2020). Accurate identification and detection of outliers in networks using group random forest methodoly. Journal of Critical Reviews, 7(6): 381-384. https://doi.org/10.31838/jcr.07.06.67

[20] Pasala, S. (2020). Identification of attackers using blockchain transactions using cryptography methods. Journal of Critical Reviews, 7(6): 368-375. https://doi.org/10.31838/jcr.07.06.65

[21] Ullah, I., Rehman, S.U. (2010). Analysis of black hole attack on MANETs using different MANET routing protocols. Master Thesis. School of Computing, Blekinge Institute of Technology, Blekinge, Sweden.

[22] Wei, C., Long, X., Bai, Y.B., Gao, X.P. (2007). A new

solution for resisting gray hole attack in mobile Ad-Hoc Networks. Second International Conference on Communications and Networking in China, Shanghai, China, pp. 366-370. https://doi.org/10.1109/CHINACOM.2007.4469403

[23] Narayana, L.V., Gopi, A.P., Lakshmi, D.V.V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4): 391-397. https://doi.org/10.1504/ijwmc.2020.108539

[24] Li, W.J., Joshi, A. Security issues in mobile ad hoc network-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore, USA.