International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Hybrid Cryptographic Routing Algorithm for Implementation of Secure Routing in MANET's

Dr. Sangeetha Y. [1], **Dr. Resmi G. Nair** [2]*

Submitted: 22/08/2023 **Revised**: 07/10/2023 **Accepted**: 21/10/2023

Abstract To put it simply, a Mobile Ad Hoc Network (MANET) is a network that has been built out of wireless mobile nodes that does not rely on any preexisting infrastructure. All the nodes of a MANET are able to freely and flexibly exchange data and information with one another. As wireless technology improves and mobile devices become more widely available, MANETs are gaining in popularity. Security in MANET is difficult because of its unique characteristics, such as the random behavior of its nodes, the lack of a centralized authority figure, and the limited availability of resources. One of MANET's most important factors is its energy consumption. As a result, it is crucial to consider the high-velocity MANET environment when building the system that supports energy efficiency. In this work, we present a hybrid routing protocol that combines Digital Certificate authority and SHA-3 authentication with robust route failure detection. To reduce the number of failed communications in Mobile Ad-hoc Networks, the authors of this research propose a new routing strategy based on the SHA-3 cryptographic method. By identifying the attacks and eliminating the malicious node from the network, we suggest a way to help safeguard these systems against this vulnerability. We compared the proposed cryptographic technique SHA-3 along with its peer algorithms in terms of various parameters and evaluated the results.

Keywords: *Cryptographic, Routing, Manet's, Wireless Mobile Nodes, SHA-3.*

1. Introduction

MANETs, or mobile ad hoc networks, are infrastructure-free, self-organizing networks that rely on wireless nodes. Using radio waves, nodes in a MANET can freely and dynamically exchange information with one another [1-3]. When fixed infrastructure is not an option, MANETs bridge the gap between users on the go [4]. It is common for a MANET's routes to malfunction as a result of environmental noise, broadcast interference, and the inherent mobility of the network's nodes. Because of the internet's rapid growth in recent years, MANETs have become increasingly useful for a wide range of mission-critical uses. Recently, MANETs have seen widespread use in the construction of smart networks based on the Internet of Things [5,6]. This calls for a careful reevaluation of the standards for security and uniformity that govern such networks. Due to the limited range of the transmission, nodes must take many hops to connect with one another [7]. Therefore, the availability of each node is crucial. For this reason, a reliable routing protocol is needed to determine the best route in between source and the sink.

Many trust-based routing methods were proposed and analyzed during the development of a MANET. The most reliable management strategies were developed for collaborative routing to identify nodes that destroy themselves due to errors in the network. Researchers have taken into account mobile node reputations and linkages for designing safer route protocols. Additionally, several models of projected routes were developed and used to objectively distinguish between various security breaches. Several experts in the field of research emphasized the main concerns that are inherent to MANETs that rely on the Internet of Things. The design of protocols took into account a wide range of potential security and vulnerability issues [8,9]. There are three main types of routing protocols: reactive, active, and hybrid. Routing table updates are a necessary part of proactive routing algorithms like Destination Sequence Shortest Path (DSDV) [10]. As a result, a flood of control packets is produced. Consequently, it was concluded that these protocols are not appropriate for use in MANETs. Due to this need, adaptive protocols such ad hoc on-demand shortest path routing (AODV) [11] and dynamically destination routing (DSR) [12] were developed. When necessary, a connection is made between the origin and destination.

These protocols consist of two stages: finding routes and keeping them up to date. The routes are calculated by employing a route-discovery algorithm. A route-maintenance step on a source node is used to assess potential topology shifts. Multiple cryptography-based protocols have been developed to ensure the safety of data exchanged between MANET nodes. Popular protocols

[1] *Professor & HOD, Dept. Of Computer Science & Engineering, Rajadhani Institute of Engineering & Technology, Trivandrum, Kerala, India*
hodcs@rietedu.in
[2] *Professor, Department of CSE, SNGIST GROUP OF INSTITUTIONS, North Paravur, Ernakulam, Kerala, India*
reshmignair@sngist.org

include Efficient Network Admission and Certificate-less Secure Communication (ENACSC) [13] Autonomous Location-Aided Route (ALARM) [14], Energy-Efficient Partial Pseudorandom Encryption (EEPPM) [15] and Friend-Based Ad Hoc Networking to Establish Security [16]. (FACES) Non-Interactive Self-Certification (NSC), Statistical Traffic System (STARS) [16], and Anonymous Multi - path routing Protocol (AMRP) [17]. However, these protocols require more power from the nodes and are vulnerable to a number of security risks. In [18], a trust-based strategy with efficient prediction for MANETs on the IoT was proposed. This method takes into account both indirect and direct information assessments and a general feeling of trust in order to arrive at an estimate for the value of the last node. An ant colony optimization-based energy consumption solution was developed for MANETs just on IoT in [19]. The end-to-end delay was reduced by using ant colonies.

These mobility qualities generate protocol independent measurements and show that nodes are dependent on one another in space or time, but they are inadequate to capture some crucial mobility features of scenarios wherein MANETs may be implemented. But in the long run, these protocol-neutral measures have a major impact on how well routing protocols function. The purpose of this article is to make an attempt at classifying and summarizing the routing protocols according to the design factors that affect the performance of mobility.

Trust Aware Safe Energy Efficient Blended Protocol, Fusion Safe Multi - path routing Procedure (HSMRP) , Attribute - based encryption Method , and Chronic Reward-Based Having to learn are just a few examples of the many secure and power multipath routing protocols recently designed for MANETs. When tested against a variety of security risks, these protocols have proven to be extremely effective. The energy requirements of these protocols are lower than those of the current protocols, although further reductions can be made. The Core system Architecture of the MANET is as follows:

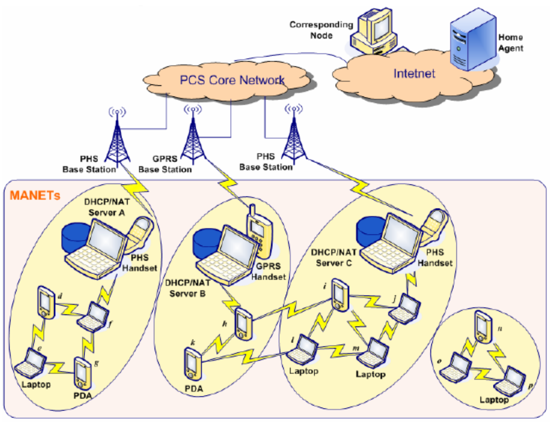

Fig 1. Secure System Architecture for integrated 2-Tier MANET

The rest of the paper is organized as follows. Section 2 Provides the Extensive literature survey on Various Secure routing protocols to be implemented in MANET's.Section3 Provides the Proposed system which uses SHA-3 cryptographic algorithm to be implemented in Routing for secure data transmission. Section4 Provides the evaluated environment and evaluated the proposed System. Finally, section5 concludes the Work

2. Related Works

Due to MANETs' limited resources, developing a reliable routing mechanism is notoriously difficult. To make the most of the available resources while remaining adaptable to changing conditions in the network, such as traffic volume, connection length, and link partitioning, a well-thought-out directing mechanism is necessary. In the meantime, the routing mechanism must provide varying degrees of quality of service (QoS) for various programs. Two major types of MANET are recognized: proactive and reactive. Proactive is also known as "table-driven" protocol. By being proactive, MANET connection points routinely probe all possible routes to every node and strive to maintain accurate, up-to-date navigational information. Accordingly, a vantage point can quickly join a moving track. This causes a significant increase in routing overhead. "On-demand" routing protocols are another name for "reactive" protocols in MANETs. If a situation calls for it, a reactive strategy will investigate alternate paths. An iterative path-finding approach is being requested. Once a path has indeed been started, or if no path has been started after checking out all possible path configurations, we can say that the path discovery procedure has concluded. Proactive routing is not a good fit for highly dynamic, large-scale mobile ad hoc networks [20]. In addition, we elaborate on contemporary routing strategies proposed by other authors[30].

By imagining a protocol called Proactive Source Routing, Zehua Wang et al. [21] made malicious data transmission in MANETs possible. Once in a while, each connection point trades the necessary information with its neighbor to create the spanning tree across the nodes. Thus, we realized that all network nodes provide access to all other network nodes via a path through other network nodes. By using this approach, we can achieve source routing with minimal routing complexity. Then the QoS measurements will be disregarded. It leads to widespread route failures in the highly volatile MANET ecosystem. According to research conducted by Lavanya et al. [22], connection loss is a major factor in halting the functioning of a network. Ad hoc On-Demand Length Vector (AODV) path failure was estimated, and a solution was proposed. A fresh strategy is proposed to lessen the impact of path loss in networks by aggregating the alternative route. The path finding algorithm employed here takes into account intermediate connecting nodes along the route. That's why we've taken such measures to reduce complexity generally. In this method, we just care about the loss of connectivity due to the path [31][33].

During the path-finding phase of MANET communication, connection points are vulnerable to attack. Ad-hoc On Demand Shortest Path (AODV) has been chosen as the routing protocol by Ritu Sharma et al. due to its superior performance in dynamical MANET to integrate route security. By employing an evolutionary algorithm to find the optimal path and to rebuild the path in the event of a detour, we are able to improve upon the AODV and create the Skilled Adhoc On demand Shortest Path Routing (PASODV) [23]. The integrity of PAODV is protected with the help of a digital signature mechanism and a Hash chain [32][38][39].

The issue has been spotted on improved MANETs, as reported by Michal Pioro et al. [24]. When the path changes, so does the connection volume. Path finding that takes into account the state of the connections is used to fix this flaw. In order to reduce the connection rate problem, the authors constructed a model with a path finding method. He also mentioned briefly that low energy between nodes is a possible reason of route failure. The effect of mobility on ad hoc routing protocols was studied by Fan Bai et al. [24] by looking at the distribution of path times. The results of the study supported the authors' hypothesis that, with proper parameterization, exponential distributions provide realistic estimates of path durations for a wide range of mobility models. The estimated path duration does not take into account the channel capacity or the energy level. Enhancement difficulty in network routing was overcome by inferring an active method, as demonstrated by the work of. As the locations in link shift, the route's focal point shifts as well. Each sort of attack on a network layer should be identified and countered, as proposed by Micheal et al., [25]. The precautions detailed in this work can be easily integrated as a supplemental module into any existing automated framework to fully automate the process of preventing attacks. In order to detect a misbehaving node in a MANET, [26] suggested an improved method based on direct reputation[34][36].

An answer describing the confluence of Routing in the IoT was proposed by [27]. Different seniors have been used to test and execute the findings of this paper. It was the intention of jihuai et al., [27] to assess the impact of numerous hops on both bandwidth and delay. Throughput tests clearly favor OLSR over other methods. Babel, on the other hand, has less of a lag and converges more quickly. To solve the problems of Integrated Internet-MANET, Mahaboob. [28] presented a three-pronged approach. Efficient gateway selection process; varying the range of gateway advertisements; and modifying the periodicity of portal advertisements are examples of such concerns[37].

3. Proposed Methodology

For our protocol to perform properly, each node must first receive a digital certificate from the a trusted certificate authority (CA) before joining or constructing a MANET. To ensure successful communication, it is recommended to first authenticate the sending and receiving parties using a shared secret key, which can be achieved using either the Diffie-Hellman protocol for key exchange or the (3, 3) threshold-based Shamir's secrecy scheme. An MST is built based on the MANET graph so as to have a more dependable MANET and to establish routes more quickly. Below, I provide a brief explanation of each of these plans. X.509 data is presented in the way depicted in Figure 2.

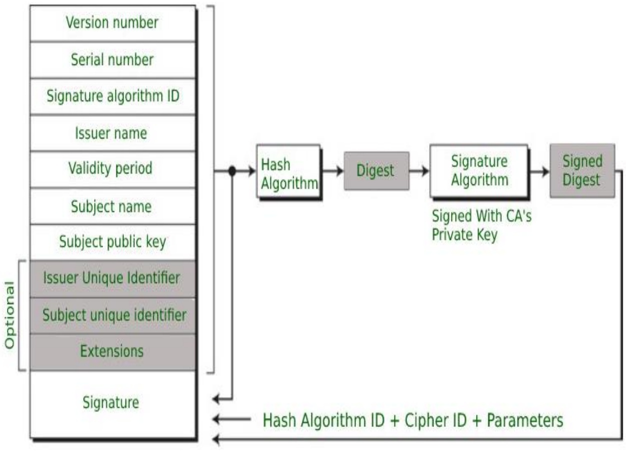

Fig 2. X.509 digital certificate format

The National Institute of Standards and Technology (NIST) kicked up the process to pick a new cryptography hash algorithm with the goal of improving the security and performance of hash functions. The production of digital signatures & message authentication codes are two examples of security-constrained applications that have benefited from SHA-3's evolution as the winner in terms of providing confidentiality [10]. In order to use the Keccak system, the following algorithm is required:

Step 1. There are three equations that define the theta function, and they all use XOR and cyclic shifts of bits.

D[Y] = XOR(B[Y, 0], B[Y,1], B[Y, 2], B[Y, 3], B[Y, 4]) $0 \leq Y \leq 4$ ------- (1).

Step 2: The five input lanes make their first circular movement to the left. Following this procedure, the very last lane will be the very first one. As a result, the lanes undergo a rightward circular shift, with the first lane becoming the last and the second lane becoming the first. At this point, we apply a left circle shift to each lane to reorder the bits within it [29].

A[Y] = ROT (D[Y - 1] , E[Y + 1, 1]), $0 \leq Y \leq 4$ ------- (2)

Step 3: An XOR operation is performed on the input matrix & output lanes generated from (1)(2).

X[A,B] ′= XOR (X[A, B], Z[A]), $0 \le A; B \le 4$ ------ (3)

Step 3: Rho (ρ) and Pi (Π) can be jointly represented, where the latter computes a 5x5 array B from of the cell state A. Rho and Pi operations result in a rotation in a complete circle of the input.

s[A, B].X[A, 2A + 3B] = ROT(X[A, B], T[A, B]), $0 \le A$; $B \le 4$ ------ (4)

Step 4: The lanes have been rotated and relocated within array B. The term "Pi step" is used to describe this process. Modulo 5 is used to calculate the indices.

Step 5: Chi (χ) function controls the lanes. Therefore, 64-bit words replace the status array A with the modified B array acquired from the Rho and Pi step. Chi () is performed by XORing the lanes at address location [A,B] with the logically AND of the channel at address location [A+1,B], and then taking the complement at address location [X+2,Y]. Below is one possible representation of the Chi (χ) function.

X[A, B] = Y[A, B] ((NOT X[A + 1, B]) AND Y[A + 2, B]), $0 \le A, B \le 4$ ------- (5)

Step6: The first stage in the Keccak algorithm, Iota, is the most elementary. Specifically, it takes the lane at position [0,0] of the new state matrix A and performs an XOR operation with the predetermined 64-bit constant BC.

X[0, 0] = XOR (B[0,0], AB) -------- (6)

There are various approaches to implement SHA-3. Here, we've settled on two distinct strategies for implementing SHA-3 encoding: the Step-by-Step Algorithm and the MUX Algorithm. The Keccak structure can be modified further without changing its fundamental functioning.

This is the typical approach to implementing the Keccak algorithm. In this implementation, we hardcode a round length of 28 for the Keccak algorithm. Therefore, the Keccak algorithm's five steps must be performed 28 times. It is state 1 until all five Keccak phases have been completed. The next 27 phases then proceed in a fashion quite similar to that of the initial state. The coding format is also organized in this case to best serve the algorithm's needs. The process is easily illustrated by looking at Figure 2. The 27 procedures are carried out in order, one after the other. Only when one step is finished can the data needed for the following step be gathered. Twenty-seven more stages will be taken in this process. A SHA-3 code is produced at the end of the 28-step process. This encoded result is then used as the basis for the remaining processing steps. Given that each step is repeated in turn, this implementation of the Keccak algorithm is as standard as it gets. Width=283l is the formula that yields SHA-3's round. Sum of digits in a round Equals 14 + 3 l. In this case, l equals 8. Consequently, round= 28 [12]. Figure 3 provides an overview of SHA-3.

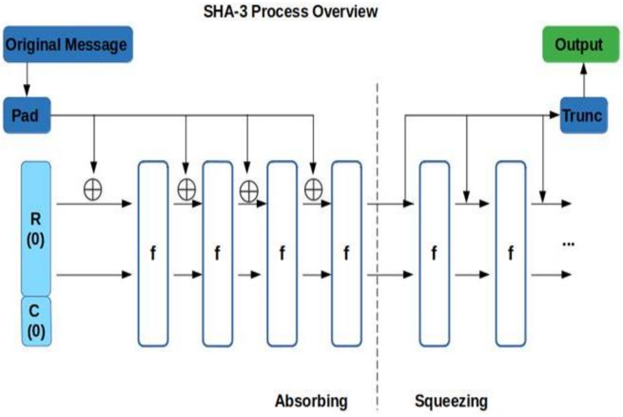

Fig 3. Overview of SHA Algorithm

4. Evaluation of SHA-3

Here, xilinx 14.1 is utilized alongside the programming language Python. Synthesis and implementation are performed on an FPGA from the Spartan-6 family. Spartan-6 LX Field-Programmable Gate Arrays (FPGAs) are designed for uses that demand the lowest possible price. High-end FPGA boards, such as the vertex, can be used to implement the system in its entirety. The results show that the amount of space used by the mux method is drastically less than that required by the standard step-by-step algorithm. The usage of the mux system enables for a consequential decrease in footprint. Keccak structure reduces the number of required blocks from 28 to 4. All that's needed is an extra mux. The results indicate a decrease in the total number of flip flips, slice luts, slice registers, etc.

When compared to the standard method of utilizing the SHA-3 structure, this new implementation significantly reduces the number of blocks used, that is, the number of components. The other approach uses mux, although its delay is much larger than the step-by-step algorithm's. Maximum number of iterations in the step-by-step algorithm has been minimized. The time required by the step algorithm to generate output is drastically reduced when compared to the time required by the mux algorithm. Elements are assigned directly in this sequential process. Since this is the case, we should expect a reduction in the amount of time needed for particular tasks. We evaluate SHA-3 according on the following criteria. In this study, the SHA-3 algorithm's runtime, number of iterations, and delay are compared to those of the SHA-2, SHA-1, and MD-5 algorithms. The results of testing the four algorithms with respect to these three criteria are presented in Table1.

Table 1. Evaluated Results of 4 algorithms

Name of the Algorithm (per 128 bits hash)	Block Size (bits)	Time consumption (ms)	Delay (ms)	Number of Loops
MD-5	512	3.45	1.3	64
SHA-1	512	3.01	1.1	128
SHA-2	1024	2.95	0.9	256
SHA-3	1152	2.06	0.4	512

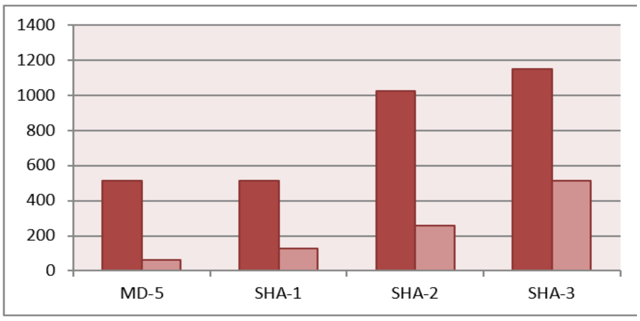

Fig 4. Evaluated Results of Block size and number of Loops

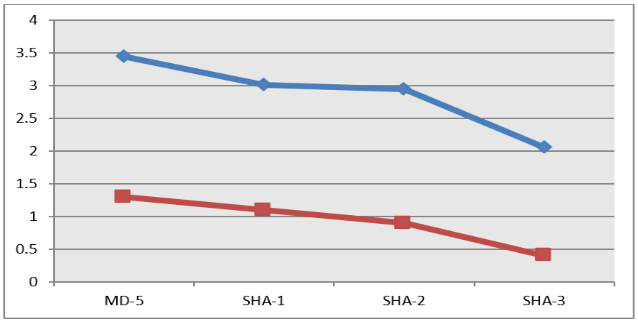

Fig 5. Evaluated Results of Time Consumption and Delay

5. Conclusion

As a solution, we offer a hybrid routing system that combines proactive and reactive measures for security. Proactively developing MANET topology and MST on a periodic basis, the protocol then establishes source-destination routes reactively. A secret-key is formed using the Diffie-Hellman key exchange protocol or the SHA-3 threshold selective encryption technique, and a Security Association is created among a source-destination pair for authentication purposes. Each node in our protocol is digitally certificate-authenticated, and their neighbors are cluster-authenticated by the node in its center. This makes the MANET more trustworthy as a whole. The SA-established secret key is utilized for symmetric encryption/decryption during data transfer. Both the security & performance analyses we provide demonstrate that our protocol is sound and suitable for use in real-world settings.

References

[1] Ben Othman, J.; Mokdad, L. Enhancing data security in ad hoc networks based on multipath routing. J. Parallel Distrib. Comput.2010, 70, 309–316.

[2] Kumar, K.V.; Jayasankar, T.; Eswaramoorthy, V.; Nivedhitha, V. SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks. Int. J. Intell. Netw. 2020, 1, 36–42.

[3] El-Hadidi, M.G.; Azer, M.A. Traffic Analysis for Real Time Applications and its Effect on QoS in MANETs. In Proceedings of the 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 26–27 May 2021; pp. 155–160.

[4] Wu, W.C.; Liaw, H.T. A Study on High Secure and Efficient MANET Routing Scheme. J. Sens. 2015, 2015, e365863.

[5] Devi, V.S.; Hegde, N.P. Multipath Security Aware Routing Protocol for MANET Based on Trust Enhanced Cluster Mechanism for Lossless Multimedia Data Transfer. Wirel. Pers. Commun. Int. J. 2018, 100, 923–940.

[6] Gomathy, V.; Padhy, N.; Samanta, D.; Sivaram, M.; Jain, V.; Amiri, I.S. Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. J. Ambient Intell. Humaniz. Comput. 2020, 11, 4995–5001.

[7] Kousar, R.; Alhaisoni, M.; Akhtar, S.A.; Shah, N.; Qamar, A.; Karim, A. A Secure Data Dissemination in a DHT-Based Routing Paradigm for Wireless Ad Hoc Network. Wirel. Commun. Mob. Comput. 2020, 2020, e2740654.

[8] Maheswari, M.; Geetha, S.; Kumar, S.S.; Karuppiah, M.; Samanta, D.; Park, Y. PEVRM: Probabilistic Evolution Based Version Recommendation Model for Mobile Applications. IEEE Access 2021, 9, 20819–20827.

[9] Funderburg, L.E.; Lee, I.Y. A Privacy-Preserving Key Management Scheme with Support for Sybil Attack Detection in VANETs.Sensors 2021, 21, 1063.

[10] Perkins, C.E.; Bhagwat, P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Comput. Commun. Rev. 1994, 24, 234–244.

[11] Perkins, C. Ad Hoc on Demand Distance Vector

(aodv) Routing Ietf. Internet Draft, draft-ietf-manet-aodv-00.txt. 1997. Available online: https://datatracker.ietf.org/doc/rfc3561/

[12] Broch, J.; Johnson, D.B.; Maltz, D.A. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. draft-ietfmanet-dsr-03. txt. Work-in-Progress. 1998. Available online: https://www.ietf.org/proceedings/42/I-D/draft-ietf-manet-dsr-00.txt

[13] Saxena, N.; Tsudik, G.; Yi, J.H. Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs.IEEE Trans. Parallel Distrib. Syst. 2009, 20, 158–170.

[14] El Defrawy, K.; Tsudik, G. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs. IEEE Trans. Mob. Comput.2011, 10, 1345–1358.

[15] Khan, A.; Sun, Q.T.; Mahmood, Z.; Ghafoor, A.U. Energy efficient partial permutation encryption on network coded MANETs. J. Electr. Comput. Eng. 2017, 2017, 4657831.

[16] Dhurandher, S.K.; Obaidat, M.S.; Verma, K.; Gupta, P.; Dhurandher, P. FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems. IEEE Syst. J. 2011, 5, 176–188.

[17] Chen, S.; Wu, M. Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks. J. Syst. Eng. Electron. 2011, 22, 519–527.

[18] Hammamouche, A.; Omar, M.; Djebari, N.; Tari, A. Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. J. Inf. Secur. Appl. 2018, 43, 12–20.

[19] Subramaniyan, S.; Johnson, W.; Subramaniyan, K. A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique. EURASIP J. Wirel. Commun. Netw. 2014, 2014, 205.

[20] Cong Liu, Jie Wu, “Virtual-Force-Based Geometric Routing Protocol in MANETs”, IEEE, June 2008.

[21] Zehua Wang, Yuanzhu Chen; Cheng Li, “PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks”, IEEE, August 2013.

[22] Lavanya. Poluboyina, Sivakumar Reddy. V, Mallikarjuna Prasad. A, "Evaluation of QoS Support of AODV and its Multicast Extension for Multimedia over MANETs", International Journal of Computer Network and Information Security (IJCNIS),Vol.12, No.1, pp.13-19, 2020. DOI: 10.5815/ijcnis.2020.01.02

[23] Ritu Sharma, “A Secure and Proficient Routing Protocol in Mobile Ad-hoc Networks using Genetic Mechanism”, IJIRCCE,June 2016

[24] Fan Bai , A.Manikandan, S.Pradeep, “Quantitative Analysis of Network Arrangement in Randomized Appropriation in WSN” Journal of Chemical and Pharmaceutical Sciences, pp 181-184, 2017.

[25] Michal Pióro,Dritan NaceYoann and Fouquet, “On Protected Traffic Routing in Wireless Networks with Partial Multiple Link Failures”, IEEE Computer Society Washington, 2013.

[26] Manikandan, A., & Rajarajachozhan, C. (2017). Artificial Bee Colony for Socially Aware Networking. Journal of Chemical and Pharmaceutical Sciences, 2, 299–301.

[27] Jihui Zhang,Qian Zhang,Bo Li,Xiaonan Luo, “Energy-efficient routing in mobile ad hoc networks: mobility-assisted case”, IEEE, Jan 2016.

[28] Mahaboob Sharief Shaik, Fahad Mira, " A Comprehensive Mechanism of MANET Network Layer Based Security Attack Prevention ", International Journal of Wireless and Microwave Technologies (IJWMT), Vol.10, No.1, pp. 38-47, 2020.

[29] M.S Kumar, “Prediction of Heart Attack from Medical Records Using Big Data Mining",International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(4s), pp. 90–99.

[30] M.S Kumar,"Nature-Inspired Optimisation-Based Regression Based Regression to Study the Scope of Professional Growth in Small and Medium Enterprises, International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(4s), pp. 100–108.

[31] Natarajan, V.A., "Improving QoS in Wireless Sensor Network routing using Machine Learning Techniques", Proceedings of the 1st IEEE International Conference on Networking and Communications 2023, ICNWC 2023, 2023.

[32] M.S Kumar, "Chronic Kidney Disease Prediction Using Machine Learning",Journal of Advances in Information Technology, 2023, 14(2), pp. 384–391.

[33] D Ganesh, “Deep Convolution Neural Network Based solution for Detecting Plant Diseases", Journal of Pharmaceutical Negative Results, 2022, 13, pp. 464–471

[34] D ganesh, "Implementation of Novel Machine Learning Methods for Analysis and Detection of Fake Reviews in Social Media", 2nd International Conference on Sustainable Computing and Data

Communication Systems, ICSCDS 2023 - Proceedings, 2023, pp. 243–250

[35] Ganesh, D., Kumar, T. P., & Kumar, M. S. (2021). Optimised Levenshtein centroid cross-layer defence for multi-hop cognitive radio networks. IET Communications, 15(2), 245-256.

[36] Sushama et.al, "Impact of COVID-19 pandemic and the diagnosis of the virus in the human body",World Journal of Engineeringthis link is disabled, 2022, 19(5), pp. 652–657

[37] AnanthaNatarajan, V., Kumar, M. S., & Tamizhazhagan, V. (2020). Forecasting of Wind Power using LSTM Recurrent Neural Network. Journal of Green Engineering, 10.

[38] Sushama et.al, Automated extraction of non-functional requirements from text files: A supervised learning approach", Handbook of Intelligent Computing and Optimization for Sustainable Development, 2022, pp. 149–170

[39] Alia Arshad, Dur-e-Shahwarkundi and ArashReyhaniMasoleh, Compact Implementation of SHA3-512 on FPGA, 2022 Conference on Information Assurance and Cyber Security (CIACS).

[40] Aluka, M. ., Dixit, R. ., & Kumar, P. . (2023). Enhancing and Detecting the Lung Cancer using Deep Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3s), 127–134. https://doi.org/10.17762/ijritcc.v11i3s.6173

[41] Dwarkanath Pande, S. ., & Hasane Ahammad, D. S. . (2022). Cognitive Computing-Based Network Access Control System in Secure Physical Layer. Research Journal of Computer Systems and Engineering, 3(1), 14–20. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/36