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

Mitigation of Sybil Attack in Mobile Ad Hoc Network Using CRYPTO-DSR: A Novel Routing Protocol

Sayan Majumder*[1], Debika Bhattacharyya[2], Subhalaxmi Chakraborty[3]

Submitted: 07/05/2023 **Revised**: 16/07/2023 **Accepted**: 08/08/2023

Abstract: As MANET is ad hoc, dynamic topology is a key function of this network, making MANET prone to different security threats. Although numerous routing protocols and methods exist to find and alleviate Sybil attacks in MANET, the hash function-based DSR protocol is a completely new idea. In this research article, we have introduced a new cryptography-based dynamic source routing protocol, named CRYPTO-DSR. First, we calculated the minimum distance of the route from the origin to the target node using Johnson's algorithm. We then secured the packets full of data inside the nodes using the hash function technique. After decryption, if the packets are found to be accurate, they are forwarded to the subsequent node and so on until they reach the destination. We compared our modified DSR protocol with the normal one and concluded that our crypto-based DSR protocol is much more secure and environmentally friendly than the traditional one in relation to performance, as measured by throughput, end-to-end delay, and the data transfer success rate during a Sybil attack.

Keywords: *DSR, Hash Function, MANET, Sybil, Throughput*

1. Introduction

MANETs are autonomous networks composed of devices that distribute tasks among peers and operate multi-hop, eliminating the need for central base stations or access points [1]. However, MANETs are susceptible to numerous attacks, including the Black hole [2], Wormhole [3], Jellyfish attack [4], DoS [5], where a majority of these attacks are executed by a single compromised node. The Sybil attack [6] poses a serious threat to sensor networks, as it involves an attacker creating multiple forged identities in order to gain unauthorized access. Detecting Sybil attacks, as well as other types of attacks such as sinkhole and wormhole attacks, during multicasting is a challenging task. In a Sybil attack, a malicious node impersonates multiple legitimate nodes, which can lead to data loss and other dangerous consequences for the network if communication is established with the attacker. Raj Kamal Kapur and Sunil Kumar Khatri proved in 2015, that symmetric key cryptography can be a good approach to give extra security to MANET [11]. The encrypted data is conveyed across the network to the intended destination, where the received data and its digital signature are verified using symmetric and asymmetric cryptography. Upon successful validation, the data is accepted, thereby ensuring secure transmission. The proposed technique provides a comprehensive range of security assurances, encompassing confidentiality, integrity, authenticity, and non-repudiation of data.

[1] *The Heritage Academy, Kolkata – 700107, India*
ORCID ID : 0000-0002-8954-2433
[2] *Institute of Engineering & Management, Kolkata – 700091, India*
ORCID ID : 0000-0002-0573-6522
[3] *University of Engineering & Management, Kolkata – 700160, India*
ORCID ID : 0000-0002-6587-6391
** Corresponding Author Email: sayanmajumder90@gmail.com*

2. Related Work

Pranjali Deepak Nikam and Vanita Raut proposed in 2015, Enhanced Adaptive [13] Acknowledgement of the EAACK protocol, employing the Elliptic Curve Algorithm (ECC) specifically designed for MANETs, exhibits notable advantages over other contemporary approaches. EAACK has been shown to achieve higher detection rates for malicious behavior in certain circumstances, without significantly impacting network performance. In the year 2016, Ashis Sharma et. Al proposed a hybrid cryptography technique with SAODV protocol [10] to provide extra security in MANET. Then they also compared the different QoS of MANET like packet delivery ratio, energy, throughput etc. T. Poongodi et. al. presented a resistant Selective Drop Attack (RSDA) scheme, introduced in reference [15], is utilized to provide effective security against selective drop attacks. The scheme proposes a lightweight RSDA protocol designed specifically for detecting malicious nodes in the network during a selective drop attack. This RSDA protocol can be seamlessly integrated with various existing routing protocols for WANETs, such as AODV and DSR. The protocol ensures reliable routing by disabling the link with the highest weight and authenticating nodes using the elliptic curve digital signature algorithm. N Chaitanya Kumar et al. proposed a distributed public key infrastructure (PKI) has been developed using the Shamir secret sharing mechanism [12]. This innovative approach allows nodes within a mobile ad

hoc network (MANET) to collectively hold a fragment of the private key. Unlike traditional PKI protocols that depend on centralized authorities and demand substantial computing resources to handle public and private keys, this approach is better suited for MANETs. Abolfazl Mehbodniya et. al. portrayed in 2021, a study introduced a machine learning-based technique to identify Sybil attacks in IoT-based sensor networks [8]. The research focused on detecting fake identity attacks and evaluating the packet delivery rates of nodes using machine learning algorithms such as Naïve Bayes, Random Forest, and Logistic Regression. The proposed approach demonstrated a significantly higher success rate (92.14% accuracy) in detecting simulated identity attacks compared to conventional methods. In 2021, Charu Sharma and Rohit Vaid proposed the DH-SAM algorithm (Diffie-Hellman Sybil Attack Mitigation) [9] to detect and mitigate Sybil nodes, thereby enhancing network trust and addressing the issue of man-in-the-middle (MITM) attacks. The DH-SAM algorithm uses the Diffie-Hellman algorithm to establish secure keys between two communicating nodes for data transmission. The algorithm's performance is evaluated using various metrics such as detection rate, packet delivery ratio (PDR) [35], throughput, and average end-to-end (AE2E) delay.

Define abbreviations and acronyms the first time they are used in the text, even after they have already been defined in the abstract. Abbreviations such as IEEE, SI, ac, and dc do not have to be defined. Abbreviations that incorporate periods should not have spaces: write “C.N.R.S.,” not “C. N. R. S.” Do not use abbreviations in the title unless they are unavoidable (for example, “IEEE” in the title of this article).

In 2022, Reham Almesaeed and Eman Al-Salem proposed a CPPR (Controlled Pow-er and Packet Rate) mechanism [7] to prevent Sybil attacks in wireless networks. The CPPR mechanism utilizes advancements in the physical layer of sensor nodes to regulate transmission power, effectively preventing many attacks and maintaining a high detection ratio [34]. Furthermore, the CPPR mechanism offers the advantage of minimal operational overhead and energy consumption. Experimental findings demonstrate that the proposed scheme consistently achieves an average detection ratio of 95%, irrespective of the quantity of Sybil nodes in the network. S Muruga-nandam et al. presented a novel method for detecting harmful nodes in conjunction with mobile ad hoc networks (MANETs) and designing intrusion detection and miti-gation schemes [14] to embellish the security of MANETs. The paper proposes a dynamic algorithm for identifying malicious nodes in a MANET environment and conducts experiments to compare the algorithm's efficiency with other existing algo-rithms. In this research paper, we have proved a modified DSR [16] protocol in which cryptography technology [17] with the hash function and encryption both worked well to lock ad hoc networks and impacted a better performance when MANETs face the Sybil attack. The Sybil attack is a highly destructive assault on sensor networks, involving the use of multiple genuine and forged identities to gain unsanctioned en-trance to the network.

A Sybil attack [18] occurs when a node pretends to have a different identity when communicating with other nodes. Interacting with an illegitimate node can result in data loss and pose a significant threat to the network's security. In our work, we have enhanced the Dynamic Source Routing protocol (DSR) [19], which is known for its simplicity and efficiency. DSR is specifically designed for multi-hop wireless ad hoc networks consisting of mobile nodes. After the calculation of distances from one node to another using Johnson’s shortest route technique [20], we stored the shortest path information in a block connected each node with a block and also made a chain connection between them. The data stored inside of the blocks were encrypted using encryption to give extra security [21]. After establishing our CRYPTO-DSR algorithm, we proved this by performance matrices like packet receiving rate, average energy consumption remaining energy after the attack, etc., and compared with nor-mal DSR protocol [22].

The novelties of our proposed algorithm are listed as

1) Introducing a novel ad hoc network routing protocol is described as enriched with the extra dash of security using encryption [23].

2) Our modified algorithm always finds the shortest route to send data packets from source to destination as we have also incorporated Johnson’s algorithm to find this distance.

3. Performance analysis is also completed after Sybil’s [24] attack on the network and this was found to be much more aimed at improving data delivery efficiency of packets or energy consumption, than normal DSR protocol [25].

3. The Proposed CRYPTO-DSR Protocol

Fig. 1. Workflow of Modified CRYPTO-DSR Protocol

From picture 1, we can have a look at that A is the source node from which the data packet is to be dispatched to node I, which is the destination node. After calculating the shortest route using Johnson's algorithm, the data packets are routed along the path. The data is encrypted inside of the nodes using encryption and routed towards the destination. After reaching the goal state, the decryption key must be used to decrypt the packet. Johnson algorithm [26] helps here for multicast routing technique with a negative value. Using this algorithm, we can easily predict the shortest route in a minimum amount of time.

Proposed CRYPTO-DSR Algorithm-

```
Begin CRYPTO-DSR (Character, Blockchain, M, n, |λw)
  if Data= Source then
    a= Packets from n;
    For each packet € a do
      [id number, monitor] = Monitor(pct);
      count_hop=<id number, node_ID, monitor>;
    transactions= Rotate_avg;
    Encryption= Hash (data packets);
    Multicast decryption key to the nodes;
    Receive decryption key from nodes;
  if Data_receive= RREQ then
      Accept packets within n;
      For each a € neighbor do
        calculate Jmin (Johnson's shortest rule);
        Update table entry with min. distance;
      Reaching the terminal node, send RREP ;
End the process.
```

We have used a cryptography-based DSR method which keeps tracking the path of data packets according to their ID no. and monitor. Using the hash function [27], we have encrypted the packets in the node, and accordingly, the decryption key must be sent. If the nodes receive the route request, then the packets are accepted. Using Johnson's shortest route algorithm, the paths are updated between nodes, so that our algorithm can take the minimum amount of time. Using the above-mentioned algorithm, we have secured the routing in MANET and to prove that, we have used our protocol against Sybil attacks. Our proposed algorithm was proved to give a much better performance than the normal dynamic source routing technique. To measure the performance, we have compared some matrices like packet received rate, average energy consumption, throughput, etc. In the case of all the parameters, our algorithm performed much better. We have started with 100 nodes among which 10 nodes are malicious. This number can be changed as per our future choice.

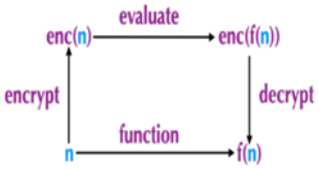

Fig. 2. Encryption Function

Workflow of Cryptography-based DSR routing protocol in MANET:

1. **Initialization**

•Initialize an empty route cache, and set the threshold for node trust as 'T'

•Generate and implement a public-private key pair for each node within the network.

Let's denote:

Route Cache: RC

Threshold for Node Trust: T

RC={} (1)

Let's denote:

N is the set of nodes in the network.

GenKeyPair(n) is a function that generates a public-private key pair for node n.

The key pair generation and implementation can be represented as: For each n in N:

(public keyn, private keyn)= GenKeyPair(n) (2)

2. **Route Discovery**

• When a sender node wants to send a packet to a destination node, it broadcasts

• A route request message containing the public key of the source node and the destination node

• Each intermediate node that receives the request message verifies the signature of the message using the public key of the source node

• If the signature is valid, the node adds its public key to the message and forwards it to its neighbours.

• When a node possesses a cached route to the destination, it responds by sending a route reply message that includes both the cached route and the public key of the destination node.

• When the source node receives a valid route reply message, it verifies the signatures of each intermediate node using their public keys and adding the route to its cache.

MRREQ=BroadcastRouteRequest(S,D) (3)

For each I:

If VerifySignature(MRREQ,S) is valid:

MRREQ=AddPublicKeyToMessage(MRREQ,PI)

ForwardMessageToNeighbors(MRREQ)

- **MRREP=CreateRouteReplyMessage(R,D)** (4)

If VerifyRouteReplySignatures(MRREP,PI1,PI2,…) is valid:

R=ExtractCachedRouteFromMessage(MRREP)R

- AddRouteToCache(R)

3. **Packet Transmission**

• When a sender node wants to send a packet [28] to a destination node, it checks its cache for a route to the destination

• If a route is found, the sender node encrypts the packet using the public key of the next hop node and sends it to the next hop node

• When an intermediate node receives a packet, it decrypts the packet using its private key and forwards it to the next hop node according to the cached route

• When a node intends to transmit a packet to a specific destination, it needs to know the route to reach the destination. If the node does not have the route information in its cache, it needs to initiate a new route-finding technique [29].

The sender node (S) checks its cache for a route to the destination (D).

If a route (R) is found, continue; otherwise, initiate route-finding.

R=CheckCacheForRoute(S,D) (5)

If R is found:

$$\mathbf{C_{encrypted}=Encrypt(C,PNnext)} \quad (6)$$

SendPacketToNextHop(Cencrypted, Nnext). (7)

Cdecrypted=Decrypt(Cencrypted, private keyN) (8)

ForwardPacketToNextHop(Cdecrypted,Nnext) (9)

4. **Security and Trust**

• Every node within the network maintains a table containing the public keys [30] of the nodes it has communicated with and their corresponding trust scores

- When a node accepts a message, it substantiates the signature of the message using the public key of the sender and updates its trust table accordingly.

If a node's trust score falls below the threshold 'T', it is marked as untrusted and its public key is deleted from the route discovery and packet transmission processes.

TrustTable[PKN]=TSN

If VerifySignature(M,PKS) is valid:

• Trust-Ta-ble[PKS] is updated based on some trust calculationTrustTable[PKS] is updated based on some trust calculations.

If TSN<T:

- **UT=UT∪{N}UT=UT∪{N}** (10)

3. Results and Discussions

We have taken a hundred nodes amongst which 10 nodes are malicious however this quantity can be adjusted as per our future requirements. Parameters with their corresponding values are enlisted in Table 1.

Table 1. Parameters Used for Simulation

No.	Parameter	Value
1	Node Number	100
2	Malicious Nodes	10
3	Area	700X700
4	Packet Size	256 bytes
5	Interface Type	Wireless
6	MAC Type	IEEE 802.11
7	Routing Protocol	CRYPTO-DSR
8	Simulation Time	84 Sec.

Performance comparison between normal DSR vs. CRYPTO-DSR for Sybil attack: We have contrasted our algorithm with the everyday one and listed some overall performance matrices with their values, which we have given later in desk two. The measuring components are described as follows-

a) Throughput: Per second, the extent of statistics obtained correctly via the termination node is termed as throughput (bits/sec.).

Throughput= (No. of packets delivered*Packets size)/Total simulation duration.

b) Packet Delivery Ratio: The total quantity of information packets acquired with the aid of the termination node to packets dispatched in complete from the supply node is termed PDR.

c) End-to-End Delay: Extra time taken than every day to attain the vacation spot is termed as a delay.

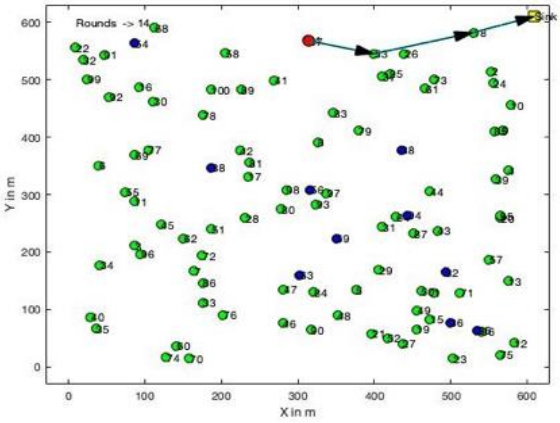

Fig. 3. Node Distribution Scenario in Sybil Attack

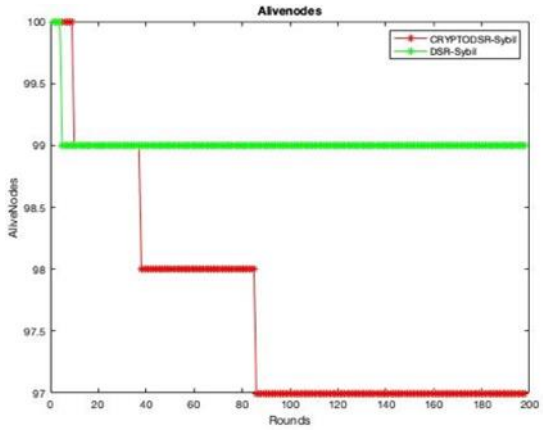

Fig. 4. Comparison of Alive Node after Sybil Attack

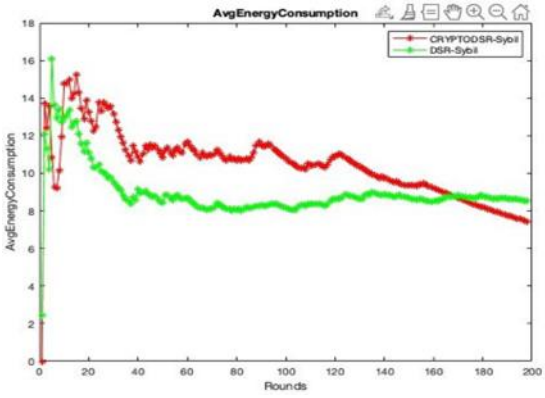

Fig. 5. Comparison of Avg. Energy Consumption After Sybil Attack

We have compiled a Sybil attack in the DSR protocol not red in colour in the graph and green explains the attack scenario in our proposed CRYPTO-DSR protocol. In figure 5, along the X-axis the number of rounds is located whereas the alive nodes are given along the Y-axis. In figure 6, we can observe the avg. energy consumption because of Sybil's attack in the Case of both protocols. The energy consumption is much greater with our modified algorithm as the dead node detection and avoidance take much energy. Figure 4 explains the 100-node distribution scenario at the time of the Sybil attack. Blue-denoted nodes are malicious nodes. The sink node is denoted by a yellow colour, where the packets were delivered.

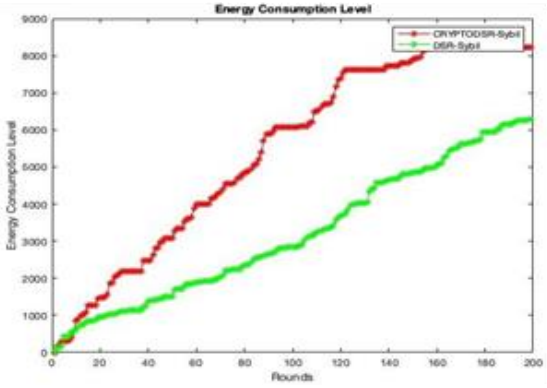

Fig. 6. Comparison of Total Energy Consumption after the Sybil Attack

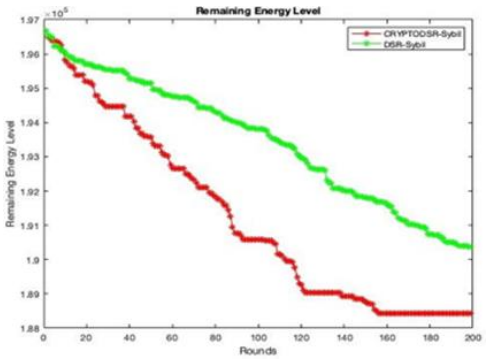

Fig. 7. Comparison of Remaining Energy Consumption after the Sybil Attack

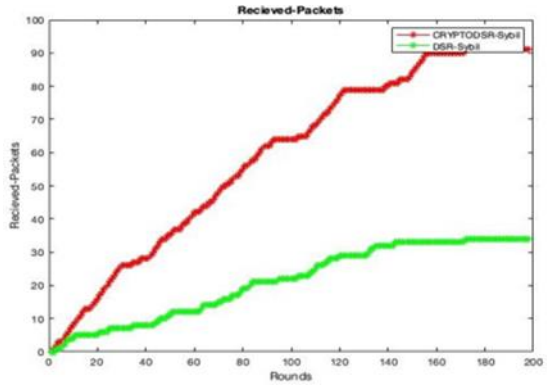

Fig. 8. Comparison of Received Packets Ratio after the Sybil Attack

From figure 8, this conclusion can easily be drawn that the number of received packets is much higher when using our proposed encryption-based DSR protocol than normal DSR. So, our protocol gives better performance in Sybil attack conditions also. We have enlisted the difference in performance parameters generated in the table below.

Table 2. Comparison of Performance Parameters after Sybil attack

DSR Performance Parameters	Values	CRYPTO-DSR Performance Parameters	Values
Number of Nodes	100	Number of Nodes	100
Velocity	5	Velocity	5
Attacking Nodes	10	Attacking Nodes	10
PDR	0.1709	PDR	0.4573
End-to-End Delay	0.0028	End-to-End Delay	0.000739
Throughput	34	Throughput	91

After enlisting our outputs in desk 2, we can say that the packet shipping ratio after the Sybil assault grew to 0.4573 from 0.1709 with the use of our modified algorithm. That ability and enhancement in overall performance have occurred.

Similarly, if we focal point on the end-to-end delay, the value grew to 0.000739 from 0.0028. Throughput was also increased from 34 to 91 after using the CRYPTO-DSR protocol in the Sybil attack scenario. So, we can say the overall performance was increased using a modified cryptography-based DSR routing protocol.

4. Conclusions

In this research work, we present a new secure and encrypted routing protocol named CRYPTO-DSR, which utilizes cryptography and homomorphic encryption. This protocol addresses the problems encountered with the normal dynamic source routing (DSR) protocol in MANET.

The main issues with the DSR protocol include:

1. High simulation time

2. Inability to restore damaged paths

3. Insufficient security

4. Low packet delivery during attacks

5. High delay variance

6. Routing overhead due to packet size and course measurement.

To enhance the security of the protocol, we have modified the DSR protocol and incorporated encryption techniques. Our algorithm works as follows:

1. The shortest route from the source to the end is calculated using Johnson's rule.

2. Data packets are stored within the source node.

3. Encryption is applied to the packets inside the node.

4. If the route discovery is accepted, the data packet is sent to the next node.

5. The subsequent node decrypts the packet and verifies the data's integrity. If the data is valid, it is forwarded.

6. The process continues until the destination is reached.

7. A route reply message is sent.

Table 3. Comparison of DSR Protocol vs. CRYPTO-DSR Protocol

DSR Protocol	CRYPTO-DSR Protocol
Time taken or delay is much higher.	Delay variance is lower.
Throughput is not up to the mark.	Throughput is better than normal.
The packets sent to receive ratio is less.	The packets sent to receive ratio is higher.
Energy consumption is below normal levels.	Energy consumption is higher than a normal level.
Dead node detection capability is poor.	Dead node detection capability is better.
The simulation time taken is 105sec.	The simulation time taken is 82 sec.
No concept of cryptography is included.	Cryptography provides extra security.

References

[1] M. Bharti, S. Rani and P. Singh, "Security Attacks in MANET: A Complete Analysis," 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 2022, pp. 384- 387, doi: 10.1109/ICDCS54290.2022.9780760.

[2] A. Hameed and A. Al-Omary, "Survey of blackhole attack on MANET," 2nd Smart Cities Symposium (SCS 2019), Bahrain, Bahrain, 2019, pp. 1-4, doi: 10.1049/cp.2019.0224.

[3] P. K. Sharma and V. Sharma, "Survey on security issues in MANET: Wormhole detection and prevention," 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 637-640, doi: 10.1109/CCAA.2016.7813799.

[4] S. Kaur, R. Kaur and A. K. Verma, "Jellyfish attack in MANETs: A review," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2015, pp. 1-5, doi: 10.1109/ICECCT.2015.7226168.

[5] Gautam, D., Tokekar, V. (2020). Pattern-Based Detection and Mitigation of DoS Attacks in MANET Using SVM-PSO. In: Pandit, M., Srivastava, L., Venkata Rao, R., Bansal, J. (eds) Intelligent Computing Applications for Sustainable Real-World Systems. ICSISCET 2019. Proceedings in Adaptation, Learning and Optimization, vol 13. Springer, Cham. https://doi.org/10.1007/978-3-030-44758-8_16

[6] Ávila, K., Sanmartin, P., Jabba, D. et al. An analytical Survey of Attack Scenario Parameters on the Techniques of Attack Mitigation in WSN. Wireless Pers Commun 122, 3687–3718 (2022). https://doi.org/10.1007/s11277-021-09107-6

[7] Almesaeed, R., Al-Salem, E. Sybil attack detection scheme based on channel profile and power regulations in wireless sensor networks. Wireless Netw 28, 1361–1374 (2022). https://doi.org/10.1007/s11276-021-02871-0.

[8] Abolfazl Mehbodniya, Julian L. Webber, Mohammad Shabaz, Hamidreza Mohafez & Kusum Yadav (2021)Machine Learning Technique to Detect Sybil Attack on IoT Based Sensor Network, IETE Journal of Research, DOI: 10.1080/03772063.2021.2000509.

[9] C. Sharma and R. Vaid, "A Novel Sybil Attack Detection and Prevention Mechanism for Wireless Sensor Networks," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2021, pp. 340-345, doi: 10.1109/ISPCC53510.2021.9609450.

[10] A. Sharma, D. Bhuriya and U. Singh, "Secure data transmission on MANET by hybrid cryptography technique," 2015 International Conference on Computer, Communication and Control (IC4), Indore, India, 2015, pp. 1-6, doi: 10.1109/IC4.2015.7375688.

[11] R. K. Kapur and S. K. Khatri, "Secure data transfer in MANET using symmetric and asymmetric cryptography," 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, India, 2015, pp. 1-5, doi:10.1109/ICRITO.2015.7359293.

[12] Kumar, Chaitanya & Basit, Abdul & Singh, Priyadarshi & Venkaiah, Vadlamudi. (2018). Lightweight cryptography for distributed PKI-based MANETS. International Journal of Computer Networks and Communications. 10.10.5121/ijcnc.2018.10207.

[13] P. D. Nikam and V. Raut, "Improved MANET Security Using Elliptic Curve Cryptography and EAACK," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, India, 2015, pp. 1125-1129, doi: 10.1109/CICN.2015.221.

[14] Muruganandam, S. , Srinivasan, N. and Sivaprakasam, A. 2022. An Intelligent Method for Intrusion Detection and Prevention in Mobile AdHoc Networks. International Journal of Intelligent Systems and Applications in Engineering. 10, 3 (Oct. 2022), 154–160.

[15] T. Poongodi, M. S. Khan, R. Patan, A. H. Gandomi and B. Balusamy, "Robust Defense Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks," in IEEE Access, vol. 7, pp. 18409-18419, 2019, doi: 10.1109/ACCESS.2019.2896001.

[16] Allahham, Alaa & Mohammed, Muamer. (2017). A MODIFIED ROUTE DISCOVERY APPROACH FOR DYNAMIC SOURCE ROUTING (DSR) PROTOCOL IN MOBILE AD-HOC NETWORKS. International Journal of Software Engineering and Computer Systems. 3. 17-30.10.15282/ijsecs.3.2017.2.0024.

[17] S. S. Jathe and V. Dhamdhere, "Hybrid Cryptography for Malicious Behavior Detection and Prevention System for MANETs," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, India, 2015, pp. 1108-1114, doi: 10.1109/CICN.2015.218.

[18] Bang, A.O., Rao, U.P. A novel decentralized security architecture against Sybil attack in RPL-based IoT networks: a focus on smart home use case. J Supercomput 77, 13703–13738 (2021). https://doi.org/10.1007/s11227-021-03816-2.

[19] Lucindia Dupak and Subhasish Banerjee. 2022. Hybrid trust and weight evaluation-based trust assessment using ECK-ANFIS and AOMDV-REPO-based optimal routing in a MANET environment. J. Supercomput. 78, 15 (Oct 2022), 17074–17094. https://doi.org/10.1007/s11227-022-04530-3.

[20] S. Anitha and B. M. Ramesh, "Network Reconfiguration for Loss Minimization by Using Johnson's Algorithm," 2018 4th International Conference on Electrical Energy Systems (ICEES), Chennai, India, 2018, pp. 680-684, doi: 10.1109/ICEES.2018.8442416.

[21] Shanmuganathan, C, Boopalan, K, Elangovan, G, Sathish Kumar, P. Enabling security in MANETs using an efficient cluster-based group key management with elliptical curve cryptography in consort with sail fish optimization algorithm. Trans Emerging Tel Tech. 2023; 34(3):e4717.doi:10.1002/ett.4717.

[22] Zhang, D, Liu, S, Liu, X, Zhang, T, Cui, Y. Novel dynamic source routing protocol (DSR) based on genetic algorithm-bacterial foraging optimization (GA-BFO). Int J Commun Syst. 2018; 31:e3824. https://doi.org/10.1002/dac.3824

[23] A. Maheswary and S. Baskar, "Letter to shape encryption for securing MANET routing protocols," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, India, 2016, pp. 1-4, doi: 10.1109/ICCIC.2016.7919703.

[24] Vadhana Kumari, S., Paramasivan, B. Defense against Sybil attacks and authentication for anonymous location-based routing in MANET. Wireless Netw 23, 715–726 (2017). https://doi.org/10.1007/s11276-015-1178-7

[25] K. Jayabarathan, J., Avaninathan, S. & Savarimuthu, R. QoS enhancement in MANETs using priority aware mechanism in DSR protocol. J Wireless Com Network 2016, 131 (2016). https://doi.org/10.1186/s13638-016-0629-x

[26] Y. Xia, P. Jiang, G. Agrawal and R. Ramnath, "Scaling and Selecting GPU Methods for All Pairs Shortest Paths (APSP) Computations," 2022 IEEE International Parallel and Distributed Processing Symposium (IPDPS), Lyon, France, 2022, pp. 190-200, doi: 10.1109/IPDPS53621.2022.00027.

[27] M. Riyazuddin, M. J. Sadiq, R. Agrawal, S. K. Shukla, A. Rana and R. Singh, "A Proficient Attack Prediction using Hash Algorithm in Manet," 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2022, pp. 705-710, doi:10.1109/ICTACS56270.2022.9988726.

[28] Rajakumari, K, Punitha, P, Lakshmana Kumar, R, Suresh, C. Improvising packet delivery and reducing delay ratio in mobile ad hoc network using neighbor coverage-based topology control algorithm. Int J Commun Syst. 2022; 35(2):e4260. https://doi.org/10.1002/dac.4260.

[29] B. S. Gouda and C. K. Behera, "A route discovery approach to finding an optimal path in MANET usia ng reverse reactive routing protocol," 2012 NATIONAL CONFERENCE ON COMPUTING AND COMMUNICATION SYSTEMS, Durgapur, India, 2012, pp. 1-5, doi: 10.1109/NCCCS.2012.6413009.

[30] Goyal, A. ., Kanyal, H. S. ., & Sharma, B. . (2023). Analysis of IoT and Blockchain Technology for Agricultural Food Supply Chain Transactions. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 234–241. https://doi.org/10.17762/ijritcc.v11i3.6342

[31] Qureshi, D. I. ., & Patil, M. S. S. . (2022). Secure Sensor Node-Based Fusion by Authentication Protocol Using Internet of Things and Rfid. Research Journal of Computer Systems and Engineering, 3(1), 48–55. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/41

[32] Juneja, V., Singh, S., Jain, V., Pandey, K.K., Dhabliya, D., Gupta, A., Pandey, D. Optimization-based data science for an IoT service applicable in smart cities (2023) Handbook of Research on Data-Driven Mathematical Modeling in Smart Cities, pp. 300-321.