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

Mitigation of Wormhole attack in MANET Using Cryptic-AODV: A Modified Routing Protocol

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

Submitted: 27/08/2023 **Revised**: 18/10/2023 **Accepted**: 30/10/2023

Abstract: Mobile Ad-hoc Networks (MANETs) inherently possess dynamic topologies, so their vulnerability to various security threats is a critical concern. While a variety of routing protocols and strategies have been developed to detect and mitigate Wormhole attacks in MANETs, a novel approach is presented in the form of the hash function-based AODV protocol within this research study. We introduce a new cryptographic Ad-Hoc on Demand Distance Vector (AODV) routing protocol known as CRYPTIC-AODV. To establish routes from source to destination, we utilize Dijkstra's algorithm to calculate the shortest path. The data packets are then safeguarded within the network nodes using a hash function technique. Upon decryption, if the data packets are validated, they are subsequently forwarded from one node to the next until they reach the destination. In our comparative analysis, we assessed the performance of our modified AODV protocol against existing protocols, namely, DSR, DSDV, and ZRP. Our findings demonstrate that the crypto-based AODV protocol offers enhanced security and efficiency while being environmentally conscious, as evidenced by improved throughput, reduced end-to-end delay, and increased data transfer success rates, especially in the presence of Wormhole attacks.

Keywords: *AODV, PDR, Throughput, Wormhole.*

1. Introduction

Mobile Ad Hoc Networks (MANETs) represent self-organizing networks comprised of interconnected devices that collaboratively distribute tasks among their peers, utilizing multi-hop connections for communication. Unlike traditional networks, MANETs operate without the need for centralized base stations or access points [1]. However, MANETs are susceptible to a variety of security threats, including the Black hole [2], Wormhole [3], Jellyfish attack [4], and Denial of Service (DoS) [5], with a significant number of these attacks being orchestrated by a single compromised node. In specific contexts, such as sensor networks, the Sybil attack [6] is a critical concern where malicious actors create multiple fraudulent identities to gain unauthorized access. The detection of Sybil attacks and other malicious activities, such as sinkhole and wormhole attacks, during multicast communication, poses a considerable challenge.

During a Sybil attack, a malicious node assumes the identity of multiple legitimate nodes, potentially leading to data loss and other adverse consequences for the network when communication is established with the imposter. A breakthrough in 2015 by Raj Kamal Kapur and Sunil Kumar Khatri demonstrated the effectiveness of symmetric key cryptography in enhancing MANET security [11]. This approach involves encrypting data before transmission, ensuring that it remains confidential during its journey across the network. Upon reaching the intended destination, the received data and its digital signature undergo verification, utilizing both symmetric and asymmetric cryptography techniques. Successful validation ensures the secure acceptance of the data, offering a comprehensive set of security guarantees, including data confidentiality, integrity, authenticity, and non-repudiation.

A Mobile Ad Hoc Network (MANET) comprises a diverse range of mobile nodes that create network connections on-demand. In the context of MANET, every packet within the network functions as a router [36]. This adaptability has resulted in the extensive adoption of MANET in a multitude of applications, including disaster management, military operations, personal area networks, and various other domains. MANET thrives in dynamic and mobile environments, necessitating the identification of potential points of failure within this ad-hoc framework [37].

Efficient protocol design is crucial for transmitting packets in a dynamic environment, ensuring seamless communication between senders and receivers within the network topology. MANET environments can be categorized into reactive, proactive, and hybrid types. These environments offer connection-less, serverless, and decentralized models, facilitating dynamic data access in remote-control scenarios and enhancing security measures

[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
3University of Engineering & Management, Kolkata–700160, India
ORCID ID : 0000-0002-6587-6391
** Corresponding Author Email: sayanmajumder90@gmail.com*

[38].

The functionality of a MANET encompasses addressing data blockages and communication latency. MANET networks provide a versatile framework suitable for a wide range of social networking scenarios. Data transmission in MANET networks relies on a combination of reactions and queries, ensuring responsive and efficient information exchange [39].

2. Related Work

Mobile Ad Hoc Networks (MANETs) offer a decentralized approach where each device collectively holds a fragment of the private key, contrasting with traditional PKI protocols reliant on centralized authorities and significant computing resources. This approach is particularly well-suited for the dynamic nature of MANETs. In a 2021 research conducted by Abolfazl Mehbodniya and colleagues, a machine learning-driven approach was introduced for the detection of Sybil attacks in sensor networks based on the Internet of Things (IoT) [8]. The primary focus of this research was on the detection of counterfeit identity attacks and the assessment of node packet delivery rates, achieved through the application of machine learning algorithms such as Naïve Bayes, Random Forest, and Logistic Regression. The proposed methodology demonstrated a significant improvement in success rates, achieving an impressive accuracy of 92.14% in the identification of simulated identity attacks when compared to conventional methods. In a separate effort during the same year, Charu Sharma and Rohit Vaid introduced the DH-SAM algorithm (Diffie-Hellman Sybil Attack Mitigation) [9]. This algorithm was designed to identify and mitigate Sybil nodes, thereby enhancing network trust and effectively addressing the issue of man-in-the-middle (MITM) attacks. The DH-SAM algorithm achieves this by utilizing the Diffie-Hellman algorithm to establish secure keys between communicating nodes, ensuring the secure transmission of data. The algorithm's performance was assessed using various metrics, including the detection rate, packet delivery ratio (PDR) [35], throughput, and average end-to-end (AE2E) delay.

In 2022, Reham Almesaeed and Eman Al-Salem introduced a mechanism called CPPR (Controlled Power and Packet Rate) [7], which was specifically developed to combat Sybil attacks within wireless networks. The CPPR mechanism takes advantage of advancements in the physical layer of sensor nodes, enabling the regulation of transmission power to effectively thwart various attacks while maintaining a high detection rate [34]. Moreover, this mechanism is distinguished by its minimal operational overhead and low energy consumption. Empirical results consistently demonstrated an average detection rate of 95% using the proposed approach, regardless of the number of Sybil nodes within the network.

In a separate work, S. Muruganandom and collaborators presented an innovative approach aimed at detecting malicious nodes in the context of mobile ad hoc networks (MANETs) and the design of intrusion detection and mitigation schemes [14] to enhance the security of MANETs. The paper introduces a dynamic algorithm for the identification of malicious nodes within a MANET environment and conducts comparative experiments to assess its efficiency when compared to existing algorithms.

In this research, we have demonstrated the effectiveness of a modified AdHoc on Demand Distance Vector [16] enriched with cryptographic technology [17], employing hash functions and encryption to bolster security when MANETs face Sybil attacks. Sybil attacks involve the use of multiple genuine and forged identities to gain unauthorized access to sensor networks [18], posing a grave security risk. In our research, we have improved upon the AODV protocol [19], which is well-known for its simplicity and efficiency. AODV is a protocol designed for multi-hop wireless ad hoc networks that consist of mobile nodes. Our approach involved calculating distances between nodes using Johnson's shortest route technique [20] and then storing this shortest path information in blocks to establish connections between nodes. The data contained within these blocks were secured through the application of advanced encryption techniques [21].

Following the introduction of our CRYPTIC-AODV algorithm, we substantiated its efficacy through performance metrics such as packet reception rates, average energy consumption, remaining energy after an attack, and more, comparing it with the standard DSR, DSDV, and ZRP protocols [22].

Notable innovations in our proposed algorithm include:

1. The introduction of a modified ad hoc routing algorithm fortified with additional security through encryption [23].

2. Consistent determination of the shortest route for data packet transmission from source to destination, incorporating Johnson's algorithm to calculate these distances.

3. Comprehensive performance analysis post-WormHole attack on the network, indicated marked improvements in data delivery efficiency, packet reception, and energy consumption, compared to the conventional AODV protocol [25].

3. Proposed Cryptic-AODV Protocol

In Figure 1, we can observe that 'A' serves as the source node responsible for transmitting a data packet to 'I,' which functions as the designated destination node. The process commences by determining the shortest route through the application of Johnson's algorithm. Once the optimal path is computed, the data packets follow this route. Within each

node along the way, the data is safeguarded through encryption before being directed towards its final destination. Upon reaching the destination node, the decryption key becomes imperative for unpacking the contents of the packet. Johnson's algorithm [26] plays a vital role in facilitating multicast routing techniques, even handling scenarios involving negative values. Leveraging this algorithm ensures efficient prediction of the shortest route in minimal time.

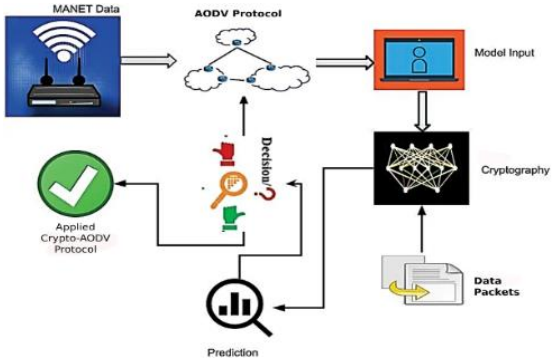

Fig. 1. Cryptic-AODV Architecture

We have implemented a cryptography-based AdHoc On-Demand Distance Vector Routing (AODV) method designed to trace the path of data packets based on their unique identification numbers while closely monitoring their progress. Employing a hash function [27], we have applied encryption to these packets within the nodes, necessitating the secure transmission of decryption keys. When nodes receive route requests, they validate and accept the packets accordingly. Johnson's shortest route algorithm has been instrumental in dynamically updating the paths between nodes, ensuring our algorithm operates with minimal time delay.

Algorithm 1: Steps: Encryption with Cryptic-AODV

Input: Data Packets from source to destination

Output: H and T Key generation

Within the AODV of MANET

1. Elliptical curve coefficients detection, y3 = x3 + ax + b over Fn (Finite space).

2. Based point selection G = (x0 ,y0) with a large order r and G' = E

3. and m < r, where m is an integer.

Encryption in MANET

1. Ksecret_key generation at random.

2. Computes H = Gk | n | and T = Bk w |n.

3. Produces the ciphertext (H, T)."

4. AODV attribute values, A 1 , A2 ,• • • An."

5. An (H , T) = (An H , An T).

6. Sends (An H , An T) to data nodes

Decryption

Input: Encryption variables An H and An T.

Output: Decryption of W.

Decryption of the ciphertext (An H , An T)

Computes R = A0 Hm |n|; R-Encrypted

By employing the aforementioned approach, we have effectively enhanced the security of routing within Mobile Ad Hoc Networks (MANETs). To substantiate the effectiveness of our protocol, we subjected it to rigorous testing against Sybil attacks. Our proposed algorithm demonstrated significantly superior performance when compared to the conventional Dynamic Source Routing technique. To evaluate its performance, we conducted an analysis involving various metrics, including packet reception rates, average energy consumption, throughput, and more. In all these parameters, our algorithm outperformed the standard method. The system's public keys, denoted as (G, B), are openly accessible through a public channel, whereas the private key is represented as 'm.' Encrypted data is stored centrally within the AODV. To gain access to nodes within the network, individuals must obtain permission during the network's revocation phase. This revocation process involves the application of advanced deep learning techniques, such as the AdaBoost integrated regression model, which assesses whether a specific node is a potential attacker or a legitimate user.

Algorithm 2 provides the estimation of WormHole attack situation in the AdHoc network.

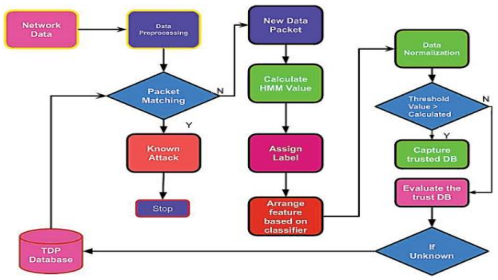

Fig. 2. Flow Diagram of Cryptic-AODV Protocol

Algorithm 2: Parameter Estimation

---

input: WormHole Attack sequence = {(al1 , al2 • • •) (al3 , al4 • • •) • • • }"

Output: λn+1

Start

For n = 0 generate λi0.

For aij0 = λi0 set bj (k)0.

For WormHole attack n = 0, 1, 2 . . . do

End for

End for

Set values

Set $value_{comparison}$.

If P (Zi = 1| i; = 1) > $Value_{trust}$

then

Compare T1 and T2 with $Value_{estimated}$

End if

for value (Z;) compare WormHole attack

End if End for

End for

Algorithm 3:WormHole Attack Estimation

Input: Target Node computation

Output: d dimension WormHole attack matrix

Construct the data node matrix Z

1. Compute matrix Wk for distances between nodes as Wk (i, j) = e-|| -xi ||

2. Use the Laplace transform to find the similarity index.

3. Compute WormHole attack node.

4. Compute eigenvector dimensionality.

5. Latent dimension target nodes calculated.

The Cryptic-AODV proposal primarily addresses the classification of WormHole attacks in the MANET environment. In order to evaluate the effectiveness of attack detection and classification, this study leverages the CICICS 2020 dataset. The AODV mechanism is specifically designed to enhance the network's ability to classify and detect attacks. To achieve efficient data processing, the proposed approach employs the SVM classification model for attack detection. However, to ensure optimal processing and maintain computational efficiency and accuracy, the scheme involves the selection of a subset of relevant features while eliminating irrelevant ones. Figure 3 illustrates the attack classification model for MANET.

For the training and testing of attack scenarios, the developed Algorithm utilizes the CICIDS dataset. Attack instances within the MANET are computed based on the dataset's attributes. The division of the dataset into training and testing subsets is detailed in Table 2.

The dataset is divided to facilitate the computation of attacks within the MANET network. Specifically, 70% of the data is allocated for training purposes, aiming to attain the desired accuracy for the system. The remaining 30% of the data is then reserved for testing, allowing for an evaluation of the network's performance.

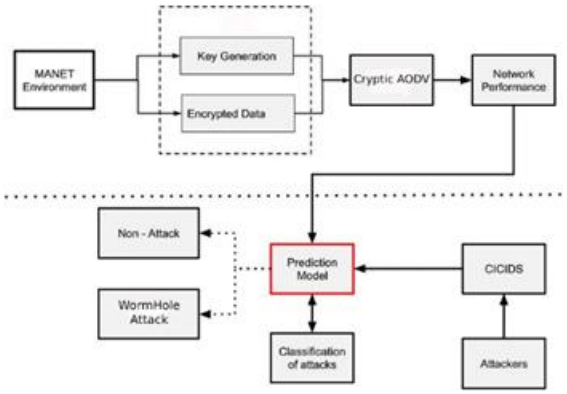

Fig. 3. Cryptic AODV Attack Classification Model

The dataset is divided to facilitate the computation of attacks within the MANET network. Specifically, 70% of the data is allocated for training purposes, aiming to attain the desired accuracy for the system. The remaining 30% of the data is then reserved for testing, allowing for an evaluation of the network's performance.

Table 1: Dataset Distribution

Data Distribution	Count	Training Count Testing
Normal Activity	69070	9930
Anomaly	56640	13150
Wormhole Attack	2989	989

4. Results and Discussions

Table 2: Simulation Settings

Simulation Parameters	Values
Software Used	Python
Mobility of Nodes	5ms/s,7ms/s 10ms/s
No. of Nodes	10,20,30,40,50
Channel	Multipath

The performance characteristics of the Cryptic-AODV proposal are evaluated across various parameters, including Delay, Jitter, End-to-End delay, Packet Delivery Rate (PDR), and Throughput.

To assess the performance of the modified scheme, mobility patterns of nodes are adjusted, specifically varying between 5, 7, and 10 (ms/s). Additionally, the mobility aspect is further explored by altering the number of nodes, ranging from 10, 20, 30, 40, to 50. Table 4 provides a comprehensive overview of network performance under different node mobility scenarios.

Furthermore, the performance of the modified AODV scheme is subjected to a comparative analysis with existing techniques such as Dynamic Source Routing (DSR) [19], Destination Sequenced Distance Vector (DSDV) [20], and Zone Routing Protocol (ZRP) [17]. This evaluation includes aspects related to the encryption and decryption of MANET data for analysis. The performance comparison takes into consideration variations in the number of nodes and the presence of attack nodes within the MANET environment.

Table 3: Performance of MANET without Attackers

Delay (s)

No. of Nodes	DSR	DSDV	ZRP	Cryptic-AODV
10	23	19	15	9
20	29	22	20	11
30	36	27	25	12
40	38	30	29	15
50	44	33	30	21

Loss %

No. of Nodes	DSR	DSDV	ZRP	Cryptic-AODV
10	24	18	20	10
20	31	23	21	12
30	37	28	26	14
40	39	31	31	17
50	45	34	32	24

PDR %

No. of Nodes	DSR	DSDV	ZRP	Cryptic-AODV
10	44	59	75	99
20	43	51	68	98
30	37	44	66	97
40	39	43	67	99
50	31	42	68	98

Throughput (kbps)

No. of Nodes	DSR	DSDV	ZRP	Cryptic-AODV
10	43	52	48	65
20	41	43	52	66
30	37	42	55	65
40	36	43	47	68
50	27	42	43	69

In Fig. 4, a graphical representation of the delay characteristics of the Cryptic-AODV is presented in comparison to DSR, DSDV, and ZRP protocols. The simulation results clearly indicate that the proposed method exhibits minimal delay, particularly within the range of 10 to 50 nodes. This suggests that our proposed modified protocol outperforms the other methods in terms of minimizing delay under these conditions.

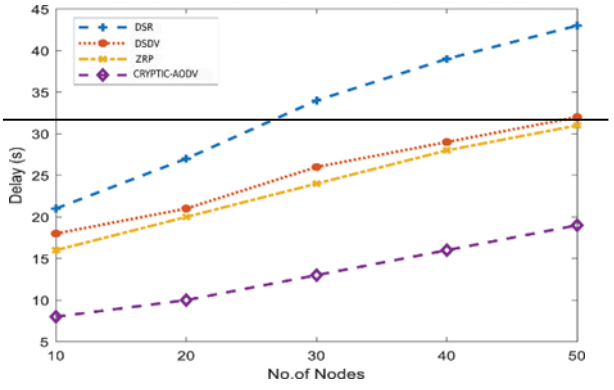

Fig. 4. Comparison of Delay

In Fig. 5, the graph illustrates the loss characteristics of the Cryptic-AODV in comparison to DSR, DSDV, and ZRP. According to the simulation results, the proposed method exhibits minimal loss, particularly within the range of 10 to 50 nodes. This indicates that our modified algorithm is

effective in minimizing data loss under these conditions. Moving on to Fig. 6, it depicts the packet delivery ratio of the Cryptic-AODV as compared to DSR, DSDV, and ZRP. The simulation results reveal that the proposed method achieves a maximum packet delivery ratio, especially when the node count falls within the range of 10 to 50 nodes. This suggests that Cryptic-AODV excels in ensuring a higher rate of successful packet delivery under these circumstances.

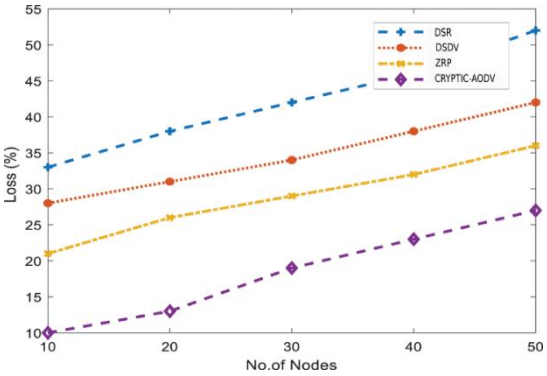

Fig. 5. Comparison of Packet Loss

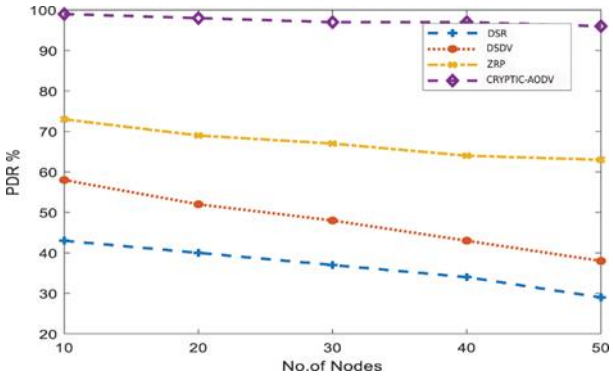

Fig.6. Packet Delivery Ratio

In Fig. 7, the graph illustrates the throughput performance of the Cryptic-AODV in comparison to DSR, DSDV and ZRP. The simulation results clearly demonstrate that the proposed method achieves a maximum throughput when the number of nodes falls within the range of 10 to 50 nodes. This indicates that our proposed algorithm is particularly effective at maximizing data transfer rates under these conditions.

However, it's important to note that as the number of nodes increases beyond this range, there is a notable increase in both loss and delay. Additionally, the Packet Delivery Ratio (PDR) and throughput of the MANET network show a decline when compared to existing techniques. This suggests that while Cryptic-AODV excels in certain scenarios, its performance may be less favorable when dealing with larger numbers of nodes, leading to increased data loss and delays.

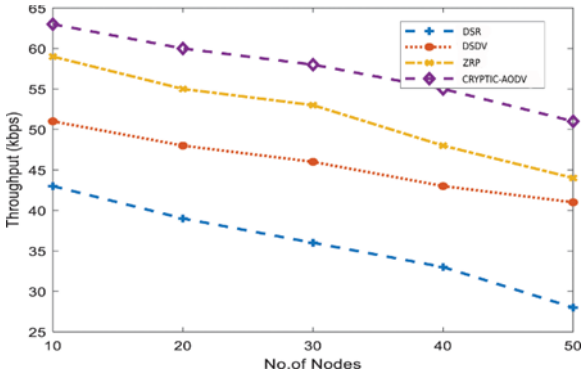

Fig. 7. Packet Delivery Ratio

5. Conclusions

The MANET network faces a multitude of security challenges due to its high node mobility environment. This paper introduces a security scheme designed to address attack prevention and classification within the MANET network, employing a modified AODV architecture. The Cryptic-AODV scheme we have introduced makes use of ECC-based (Elliptic Curve Cryptography) data encryption and decryption within the AODV network. In the subsequent phase, a dual approach is employed to both prevent and detect attacks. This approach is rooted in a model based on transductive learning, which includes the computation of k-centroids and hyper-alerts.

To thoroughly evaluate the effectiveness of the Cryptic-AODV scheme, we conducted an extensive performance assessment focused on attack detection and classification. The classification process within the Cryptic-AODV model utilizes a dedicated classifier designed specifically for categorizing attacks. Remarkably, our proposed model demonstrates an impressive overall accuracy rate of 98% within the context of this cryptography-based approach implemented within the Software-Defined Networking (SDN) framework.

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 forIntrusion 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 neighbour 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] V. R. Ghorpade, Y. V. Joshi, and R. R. Manthalkar. 2009. Efficient public key authentication in MANET. In Proceedings of the International Conference on Advances in Computing, Communication and Control (ICAC3 '09). Association for Computing Machinery, New York, NY, USA, 106–112. https://doi.org/10.1145/1523103.1523126

[31] S. Majumder and D. Bhattacharyya, "Mitigating wormhole attack in MANET using absolute deviation statistical approach," 2018 IEEE 8th Annual Computing and Communication Workshop and 49 Conference (CCWC), Las Vegas, NV, USA, 2018, pp. 317-320, doi: 10.1109/CCWC.2018.8301780. 50

[32] Majumder, S., Bhattacharyya, D. (2020). Improvement of Packet Delivery Fraction Due to Discrete Attacks in MANET Using MAD Statistical Approach. In: Mandal, J., Mukhopadhyay, S. (eds) Proceedings of the Global AI Congress 2019. Advances in Intelligent Systems and Computing, vol 1112. Springer, Singapore. https://doi.org/10.1007/978-981-15-2188-1_15

[33] Majumder, S. (2020). Improvement of Packet Delivery Fraction Due to Wormhole Attack by Modified DSR and AODV Algorithm. In: Mandal, J., Mukhopadhyay, S. (eds) Proceedings of the Global AI Congress 2019. Advances in Intelligent Systems and Computing, vol 1112. Springer, Singapore. https://doi.org/10.1007/978-981-15-2188-1_7

[34] A. Kushwaha and H. Sharma, "Enhancing Selective Encryption Algorithm for Secured MANET," 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation, Kuantan, Malaysia, 2012, pp. 326-329, doi: 10.1109/CIMSim.2012.16.

[35] Majumder, S., Bhattacharyya, D. (2020). Relation Estimation of Packets Dropped by Wormhole Attack to Packets Sent Using Regression Analysis. In: Mandal, J., Bhattacharya, D. (eds) Emerging Technology in Modelling and Graphics. Advances in Intelligent Systems and Computing, vol 937. Springer, Singapore. https://doi.org/10.1007/978-981-13-7403-6_49.

[36] K. N. Dattatraya and K. Raghava Rao, “Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN,” Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 3, pp. 716–726, 2022.

[37] N. V. Patil, C. R. Krishna, K. Kumar and S. Behal, “E-Had: A distributed and collaborative detection framework for early detection of DDoS attacks,”

Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 4, pp. 1373–1387, 202

[38] N. Veeraiah and B. T. Krishna, "Trust-aware FuzzyClus-fuzzy NB: Intrusion detection scheme based on fuzzy clustering and Bayesian rule," Wireless Networks, vol. 25, pp. 4021–4035, 2019.

[39] M. S. Shaik and F. Mira, "A comprehensive mechanism of manet network layer based security attack prevention," International Journal of Wireless and Microwave Technologies, vol. 10, no. 1, pp. 38–47, 2020.