A Chaotic Map-based Approach to Reduce Black Hole Attacks and Authentication Computational Time in MANETs

Ahsan Saud Qadri Syed
Sheikh Abdullah Technical Institute, Ministry of Education, Bahrain
syedahsanqadri@gmail.com

C. Atheeq
GITAM University, Hyderabad, Telangana, India
atheeq.prof@gmail.com (corresponding author)

Layak Ali
Central University of Karnataka, Karnataka, India
layakali@cuk.ac.in

Mohammad Tabrez Quasim
Department of Computer Science and Artificial Intelligence, College of Computing and Information Technology, University of Bisha, P.O. Box 551, Bisha, Saudi Arabia
tabrezquasim@gmail.com

Received: 24 February 2024 | Revised: 18 March 2024 | Accepted: 19 March 2024

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.7073

ABSTRACT

The need for Mobile Ad hoc Networks (MANETs) has expanded with the development of mobile computing and wireless sensor network technologies. However, this increase has also led to a rise of the attacks on these networks. In order to ensure high Quality of Service (QoS) and maintain connectivity, MANETs require careful consideration of factors, such as power, connectivity, secure transmissions, authentication, and handovers. Handovers are necessary for seamless network connectivity and require quick authentication to ensure uninterrupted service. Although RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography) algorithms are commonly used for authentication due to their fast asymmetric key encryption-decryption and exchange, they are less effective against black hole attacks. Chaos algorithms provide a faster authentication process and are efficient against false behavior black hole attacks. This study demonstrates that the chaos algorithm is a viable option for providing fast authentication and preventing malicious nodes from disrupting the network.

Keywords-MANETs; authentication; computational time; black hole attack; chaos

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) have received a lot attention since the emergence of wireless networks. Mobile nodes keep moving and keep temporary connections with many of the other mobile nodes in the same MANET. The nodes frequently change the entire network's topology as they move randomly and connect to any of the other nodes residing in the network [1]. MANET nodes usually can act as both routers and hosts [2]. Mobile nodes that randomly surf the network automatically connect to other mobile stations, requiring little human intervention. Data must be safeguarded and securely exchanged between interacting entities because the network is subject to assaults. User data from untrusted nodes are mostly protected through authentication [3]. To securely send and receive data, communication parties authenticate each other during mutual authentication [4]. Due to cellular networks and handovers, MANETs occasionally follow the latter procedure. Many techniques have been developed for mutual authentication to protect data [5]. To provide authentication, keys must be generated by size. How securely communication parties share secret keys determines the authentication strength [6]. Before connecting to a new node in a MANET, a mobile node must quickly and securely authenticate the data exchanged to ensure continued mobile services.

Most studies use Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) [7, 8]. Asymmetric key-based techniques like the RSA algorithm convert string characters into integers and adopt a private-public key method. While authenticating employing the RSA algorithm [9], the receiver sends a transfer request along with a public key to the sender. Then the sender encrypts the message to be transferred utilizing the same public key and sends it. The latter forwards this encrypted data back to the receiver. The receiver, on reception decrypts the data and views the original transfer content. The ECC encryption algorithm is an asymmetric key based mechanism that deploys anew public and private keys. Here, a number is selected in a certain range value. To generate the public key, a point on the curve is taken. For encrypting a message "m" using ECC approach, a point "X" is used on the curve and two cipher-texts get generated. For decrypting the two cipher-texts in order to obtain the original message, the private key is utilized.

External attacks on MANETs include black hole attacks. An external attack occurs when the attacker snoops and reacts to requests and data. Black hole attack nodes may deceive the requesting node without knowing the destination [10]. They falsely reply ACK to RouteReq without knowing the destination's in-force route. After accepting the route request, the attacker becomes a network active element. The attacker may potentially tunnel messages outside the MANET. Many nodes may collaborate to launch a black hole attack.

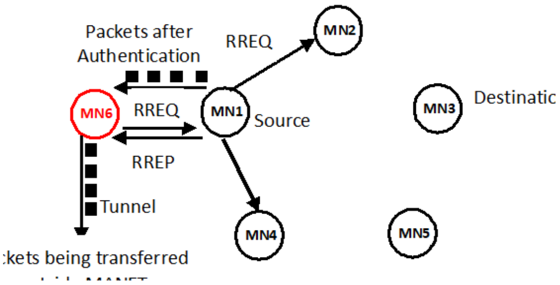

Fig. 1. Black hole attack in MANETs.

All the nodes with malicious intent work with intrigue, which initially creates routing-loops and then such malicious nodes forward packets through inappropriate routes or selectively disrupt the sender’s packets. This leads to hampering or retardation of routing services and trust between the nodes in a MANET.

II. LITERATURE REVIEW

Authors in [11] mention the use of the novel chaotic algorithm and the security it provides. This approach was efficient enough to put aside the consumption of modular exponent and scalar product that was employed by the elliptic algorithm. Various ways to deal with routing attacks in MANETs were described in [12]. The authors discussed the wormhole attack in detail. They described MANET short-circuiting and various prevention measures like Superman methodology and dynamic connectivity factor. Regarding the security aspects and the importance of security in wireless mobile networks, in [13, 14] various vulnerabilities and disadvantages of MANETs were listed down.

With the aim of reducing the computational time of authentication in MANETs and thereby providing fast connectivity and secure authentication, many studies have proposed the implementation of the RSA and ECC algorithms. Authors in [15] focused on the trustworthiness of software and network hardware. Their research was mainly dependent on fault-based attacks that usually appear in mobile networks. They developed a fault-based attack and exploited a severe flaw of RSA algorithm. Authors in [16] applied a message digest algorithm named MD5 along with RSA. It had a 128 bit message digest and output generated by a 512 bit grouping. No computational time parameters and safety elements had been taken into consideration. Also, the loss of the digest message would result in loss of many acknowledgments. Authors in [17] proposed securing MANETs engaging AES and RSA. Message digesting was again used in this study and AES, RSA, and Secure Hash Algorithm (SHA) V-12 were implemented. In conclusion, AES was found to be the best for both fixed length and variable length encryptions. SHA-12, being a combination of the AES and RSA does not give as good results as the ECC's. Also, there is no consideration of the fact of the existing black hole attacks in this research.

A MANET calls for stable information transmission among its nodes post authentication. In [18], the authors followed the approach of Hybrid-RSA (H-RSA) algorithm for enabling a secure data transmission in MANETs. Authors in [19] gave a detailed study on authentication and security in Wireless Sensor Networks (WSNs) using the ECC algorithm. Secure authentication in wireless mobile and sensor utilizing networks was built employing elliptic curves having 161 curve points instead of 320 points. They deployed the Diffie-Hellman key exchange algorithm with ECC that required two scalar multiplications. Also, Diffie-Hellman algorithm suffers from man-in-the-middle attacks as public keys cannot be directly authenticated.

The ECC-based approach in [20] enhanced the legitimacy of session key by implementing a single-way hash function. This means that only a single party would hash the secret key by using the XOR function. Mutual authentication and security from sensor node replication and Sybil attacks was the main contribution of this study. ECC offers less computational time but the problem of false behavior and black hole still persists. Also, a one-way hash would be easily decrypted if a data breach occurs [21]. Authors in [22] described secure handovers in MANETs. The work utilized a new way named ES-HAS: ECC that paved the way for secure authentication between roaming mobile users. Authors briefed on various attacks by false behavior of malicious nodes out of which the byzantine attack was taken care by the chaos algorithm.

The importance of security in MANETs and its direct proportionality to the survivability of the established network was explained in [23]. The authors describe the emerging trends for MANETs and explain the need of authentication and authorization to keep a MANET alive. They suggest multi-layer implementation for MANETs to prevent various updated attacks.

III. MATERIALS AND METHODS

Chaos refers to complex, difficult to predict non-linear systems, which are influenced by entities named control parameters. A minute change in those values will result in the appearance of large diversity in the system. Even though chaotic map-based models are already used, they are employed as an improved theory to develop new control and synchronization algorithms for systems that are inherently chaotic or exhibit chaotic behavior, which is included in the proposed model. These algorithms can be implemented to stabilize or synchronize chaotic systems, making them more predictable and easier to control [24]. The response of a chaotic system to inputs creates is unpredictable. No correlation exists between the provided value and the output. Chaos behaves like non-linear systems. A non-linear system usually acts randomly. This randomness has no stochastic origin, making it so unpredictable that a black hole attacker will find it hard to authenticate. Chaos algorithms have the ability to generate many map-based keys [25], select one, and instantaneously verify it if the receiver knows the control parameters and the model, which is its most essential characteristic for MANET authentication. Chaos algorithms have been applied to tackle issues like inter-connecting stability, geometrical parameters, digital signatures, and byzantine falsifications [26-28]. Their authentication mechanism is shown in Figure 2. To deploy chaos at its best, chaotic maps are to be developed in such a way that the entropy produced by the map results in the required chaotic situation. Chaotic map-based Chebyshev polynomials make use of a discrete logarithmic problem which is defined as:

$$\cos(n\theta) = T_n \cos(\theta) \qquad (1)$$

The Chaotic map-based Diffie Hellman problem states that in (2), it is impossible to compute the value of $T_{nm}(X)$, given the values of $T_n(x)$, X, N, and $T_m(X)$.

$$T_m(T_n(X)) \;=\; T_n(T_m(X)) = T_{mn}(X)(\text{mod } N) \qquad (2)$$

with $n \geq 2$.

The entropy is evaluated by:

$$mHI = -\sum P(R = i)\log 2P(R = i) \qquad (3)$$

A logistic map illustrates a variety of behaviors and it has transitions between these behaviors as the random key parameter is altered. The logistic map of the proposed scenario is illustrated in (4):

$$N = KX(1 - X)\left(\frac{1}{W}\sum_{i=1}^{n}\frac{Y_i}{Z_i}\right) \qquad (4)$$

where N represents the new calculated value, K is the control parameter, X is the current value, Y is an intermediate variable, Z is a transformation function, and W is another auxiliary variable.

Chaos-based cryptosystems are preferred over symmetric cyphers like AES because the key generation map is harder to understand. AES offers high-level picture encryption. The attacker node will be confused by producing random keys at varied control settings, machine state, and input values, allowing them to guess or identify the key for decrypting the stolen communications. Digested acknowledgment reduces black hole attacks. The source delivers n packets and the destination keeps and acknowledges them by digesting with its key. With this digested ACK, the source confirms whether it received the ACK from the desired destination or from an attack. If the digested value is matched at the source, then it forwards packets, otherwise, it considers the intermediate node as a black hole.

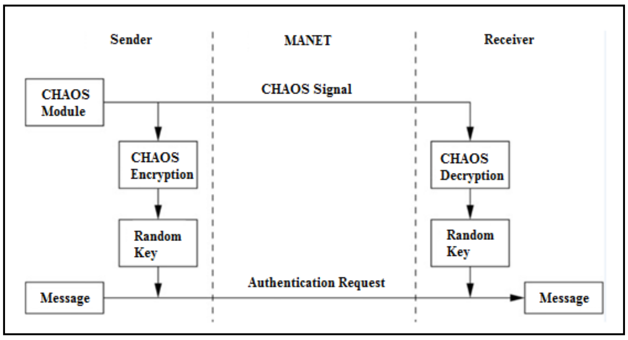

Fig. 2. Authentication and encryption in MANETs using random key.

A. *Algorithm for Chaos-based Encryption*

1) *Initialization*

Chaotic map function: F(x), control parameters: $\alpha,\beta,\gamma,\delta$ (specific to the chosen chaotic map), length of chaotic key: n, length of plaintext: L, the plaintext message is initialized as M.

2) *Key Generation*

- Generate a chaotic key K using the chosen chaotic map and control parameters.
- Initialize x_0 to a random value between 0 and 1.
- For i = 0 to n−1:

$$x_i + 1 = F(x_i;\ \alpha, \beta, \gamma, \delta) \qquad (5)$$

$$K_i = \text{fractional part of } (x_i + 1.\,L) \qquad (6)$$

3) *Image Encryption*

- Break the plaintext message M into blocks or elements, depending on the chosen encryption approach.
- For each element M_i, encrypt using a complex operation E based on the chaotic key:

$$E_i = E(M_i, K_{i \bmod n}) \qquad (7)$$

4) *Packet Transmission*

If data are sent over a network, the encrypted message is divided into packets and is transmitted to the destination. Let P be the set of packets, P={P_1, P_2,…,P_m}, where m is the number of packets. The packets can be created using a function that takes the encrypted message, packet size s, and an index j as input:

$$P_j = \text{CreatePacket}(E, s, j) \qquad (8)$$

where P_j represents the jth packet created from the encrypted message E with size s.

5) Black Hole Attack Mitigation

During data transmission, the source node maintains a count of sent packets and expects acknowledgments (ACKs) from the destination. Let A be the set of the received ACKs, $A=\{A_1,A_2,\ldots,A_m\}$, where m is the number of packets. The Packet Loss Rate (PLR) for the received ACKs is calculated by:

$$\mathrm{PLR} = \frac{\mathrm{Packets\_Sent} - \mathrm{Packets\_Acknowledged}}{\mathrm{Packets\_Sent}} \qquad (9)$$

If PLR exceeds a predefined threshold, it indicates a potential black hole attack.

$$\mathrm{Threshold} = \mu + k \cdot \sigma \qquad (10)$$

where μ is the mean (average) of the historical PLR values, σ is the standard deviation of the historical PLR values, and k is a constant multiplier for the threshold margin.

The mean (μ) and standard deviation (σ) of historical PLR data, along with a constant multiplier (k) for the threshold margin, are used to determine the threshold value. When the current PLR exceeds the threshold, a potential black hole attack is indicated.

6) Authentication and Black Hole Detection

- M_i: The received message element.
- MAC_i: The received MAC value for element M_i.
- K_i: The chaotic key component used for the encryption of element M_i.
- $MAC_i^{expected}$: The expected MAC value for element M_i calculated at the receiver.
- n: The length of the chaotic key.
- $E(M_i, K_i)$: The encryption function that encrypts the element M_i using the key K_i.
- $V(MAC, K_i)$: The verification function that checks the authenticity of MAC using key K_i.

B. Authentication Steps

1) Receiving Messages

Receive a set of encrypted message elements and their corresponding MAC values: $\{(M_1,MAC_1), (M_2,MAC_2), \ldots,(M_m,MAC_m)\}$.

2) Authentication Verification

For each received element M_i and its corresponding MAC (MAC_i):

- Calculate the expected MAC value ($MAC_i^{expected}$) at the receiver using the same chaotic key K_i that was deployed for encryption: $MAC_i^{expected}$=Calculate MAC(M_i, K_i)
- Verify the authenticity of the received MAC value MACi utilizing the key K_i and the verification function V: $Authenticated_i=V(MAC_i, K_i)$
- If $Authenticated_i$ is TRUE, the element M_i is considered authenticated. The opposite indicates data tampering.

3) Repeat Authentication

Repeat the authentication process for all the received message elements $M_1,M_2,\ldots,M_m$.

4) Action on Authentication Status

- Based on the authentication status of each element, we can accept, reject, or take specific actions, e.g. if all elements are authenticated, accept the entire message. If any element fails authentication, consider taking security measures, such as reporting or rejecting the message.

In this authentication process, more notations, including $Authenticated_i$, have been introduced to represent the authentication status of each element. The verification function V checks whether the received MAC value matches the expected MAC value calculated applying the corresponding chaotic key K_i. The proposed approach secures network data transmission, especially against black hole attacks. Key generation utilizes map and control parameters to generate a chaotic key. This key breaks the plaintext message into pieces and performs a sophisticated encryption procedure. The encrypted message is packetized for network transmission using a specified function. The technique mitigates black hole attacks to protect data. It calculates PLR and compares it to a threshold to detect assaults. The program also verifies data authenticity putting into service Message Authentication Codes (MACs). Each message element's MAC is calculated and compared to the receiver's predicted MAC. Verified elements are valid; unverified ones may indicate data tampering. In brief, the introduced method deploys chaotic cryptography and authentication to protect transmitted data from black hole attacks and secure networked communication.

IV. RESULTS AND DISCUSSION

Top numbers in RAS, ECC, and chaos algorithms made public key authentication perform. Tables I-III illustrate the computational time for authentication implementing public information and input values from RSA, ECC, and Chaotic maps. In primitive authentication, senders and receivers use secret keys based on the method. The average RSA computation time is 7.671 ms. ECC authentication took 5.032 ms, less than RSA, and chaotic maps authentication took 2.8775 ms, less than RSA and ECC.

TABLE I. AUTHENTICATION USING RSA ALGORITHM

Sender Public Key (Prime no.)	Receiver Public Key (Prime no.)	Rounds of exp. fun.	Password	Computational Time (ms)
7	11	1(e)	12345678	2.10
3	5	1(e)	72891203	0.89
5	7	1(e)	33774911	1.50
11	13	2(e)	78678678	3.30
37	41	3(e)	18710126	11.10
17	59	2(e)	97586444	5.10
23	29	2(e)	72892343	8.24
29	31	2(e)	34174911	9.71
17	23	1(e)	47278678	4.87
59	67	3(e)	73917626	14.72
53	73	3(e)	37826492	13.24
79	83	3(e)	47629436	17.29
Average Computational Time				7.671

The time complexities were calculated employing similar prime numbers and the same authentication password. A graph comparing computational times for RSA, ECC, and chaos authentication shows that the latter nicely fits this scenario. After utilizing similar inputs and passwords for authentication, the results were identical. The impact of black hole attack was also decreased. Since pseudo random numbers make chaos authentication highly randomized, hostile nodes cannot guess the key, making it secure.

TABLE II. AUTHENTICATION USING ECC ALGORITHM

Curve Pt.1	Curve Pt.2	Curve Pt.3	Curve Pt.4	Sender Public Key (Prime no.)	Receiver Public Key (Prime no.)	Password	Computational Time (ms)
10	20	30	40	7	11	12345678	1.40
10	20	30	40	3	5	72891203	0.60
10	20	30	40	5	7	33774911	1.00
10	20	30	40	11	13	78678678	2.20
10	20	30	40	37	41	18710126	7.40
10	20	30	40	17	59	97586444	3.40
10	20	30	40	23	29	72892343	4.34
10	20	30	40	29	31	34174911	5.80
10	20	30	40	17	23	47278678	3.98
10	20	30	40	59	67	73917626	9.32
10	20	30	40	53	73	37826492	9.45
10	20	30	40	79	83	47629436	11.5
Average Computational Time							5.032

TABLE III. AUTHENTICATION USING CHAOS ALGORITHM

Sender's Public Key (Prime no.)	Receiver's Public Key (Prime no.)	Password	Computational Time (msec)
7	11	12345678	1.11
3	5	72891203	0.50
5	7	33774911	0.77
11	13	78678678	1.30
37	41	18710126	4.10
17	59	97586444	2.90
23	29	72892343	3.12
29	31	34174911	3.45
17	23	47278678	2.31
59	67	73917626	4.89
53	73	37826492	4.43
79	83	47629436	5.65
Average Computational Time			2.8775

Figure 3 indicates that reactive routing methods like AODV have less packet loss than proactive routing protocols. AODV involve only source-to-destination routes when needed. The route must be maintained until communication ends, and then terminated. The graph indicates that reactive routing protocols have lower packet loss than proactive routing protocols. Packet loss increases with node count in proactive routing approaches although it is significantly lower in the proposed strategy. The graph reveals that the proposed technique has less packet loss than the present one. Figure 4 presents the packet delivery ratio of the proposed mechanism and existing methods with and without a black hole node. The proposed method provides maximum PDR even in the presence of a black hole attack. A primary constraint of communicating entities is that they need to maintain data integrity. Authentication plays a vital role in protecting the data from unauthorized nodes. Traditional methods provide authentication with a lack of minimum time computation. The proposed mechanism consumes minimum time for mutual authentication. Its graphical comparison for various key sizes is presented in Figure 5.

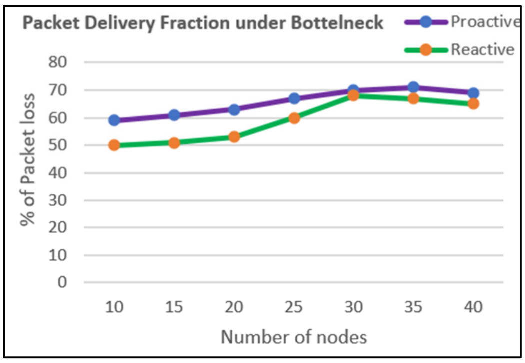

Fig. 3. Comparing routing protocols used for packet transmission.

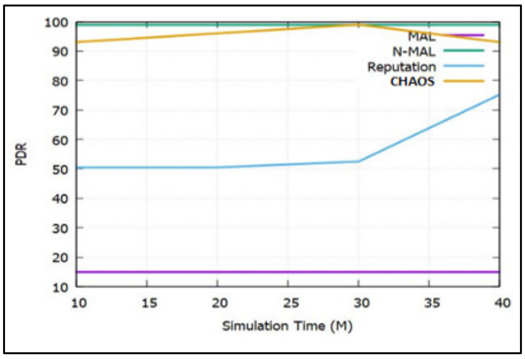

Fig. 4. Comparison of packet delivery ratio with respect to simulation time.

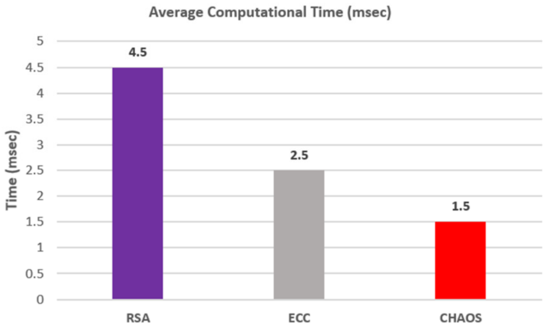

Fig. 5. Comparing the evaluated computational times of RSA, ECC, and chaos authentication.

The novelty of the presented work lies in the utilization of the chaos algorithm for enhancing the authentication in MANETs. This approach sharply contrasts with the traditional RSA and ECC algorithms, which, despite their fast asymmetric key encryption-decryption capabilities, fall short in defending against black hole attacks. The chaos algorithm not only provides a more rapid authentication process compared to its predecessors, but also demonstrates robustness against these types of network breaches.

Compared to the existing mechanisms, the proposed method significantly reduces the overhead associated with data communication, which, in turn, ameliorates the performance of MANETs. In contrast to RSA and ECC, which typically require an average computational time of 4.5 ms and 2.5 ms, respectively, the chaos algorithm significantly eliminates this time to just 1.5 ms. This improvement speeds up authentication while simultaneously reducing the risk of false behavior black hole attacks, which have been a persistent challenge for network security.

V. CONCLUSION

An authentication solution that is cost-effective and also displays higher performance than RSA and ECC is proposed, representing a significant improvement in the field of MANET security. This solution dramatically reduces the communication overhead that is involved with authentication protocols. The former accomplishes this reduction by addressing the widespread problem of black hole attacks in a more effective manner. A significant improvement in MANET performance has been achieved as a consequence, which guarantees that the network will continue to be robust without the weight of excessive computational costs.

A look into the future will show that the field of research is going to broaden, making it possible to investigate more subtle factors that influence network vulnerability. Attention will be devoted towards understanding how the energy consumption patterns of mobile nodes and their buffer utilization techniques contribute to the network's susceptibility to attacks. The purpose of this investigation is to establish more comprehensive security measures that address both purposeful and unintentional threats to the integrity of the network. This will be achieved by investigating these unintentional, yet influential factors.

REFERENCES

[1] A. K. S. Ali and D. U. V. Kulkarni, "Characteristics, Applications and Challenges in Mobile Ad-Hoc Networks (MANET): Overview," *I nternational Journal of Electronics & Communication*, vol. 3, no. 12, pp. 6–12, 2015.

[2] N. Raza, M. U. Aftab, M. Q. Akbar, O. Ashraf, and M. Irfan, "Mobile Ad-Hoc Networks Applications and Its Challenges," *Communications and Network*, vol. 8, no. 3, pp. 131–136, Jul. 2016, https://doi.org/10.4236/cn.2016.83013.

[3] A. A. K. Mohammad, A. Mirza, and S. Vemuru, "Cluster Based Mutual authenticated key agreement based on Chaotic Maps for Mobile Ad Hoc Networks," *Indian Journal of Science and Technology*, vol. 9, no. 26, pp. 1–11, Jul. 2016, https://doi.org/10.17485/ijst/2016/v9i26/95137.

[4] A. Alomari, "Mutual Authentication and Updating the Authentication Key in MANETS," *Wireless Personal Communications*, vol. 81, no. 3, pp. 1031–1043, Apr. 2015, https://doi.org/10.1007/s11277-014-2169-1.

[5] M. S. A. Razak, S. P. A. Gothandapani, N. Kamal, and K. Chellappan, "Presenting the Secure Collapsible Makerspace with Biometric Authentication," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12880–12886, Feb. 2024, https://doi.org/10.48084/etasr.6400.

[6] G. Vidhya Lakshmi and P. Vaishnavi, "An Efficient Security Framework for Trusted and Secure Routing in MANET: A Comprehensive Solution," *Wireless Personal Communications*, vol. 124, no. 1, pp. 333–348, May 2022, https://doi.org/10.1007/s11277-021-09359-2.

[7] V. Kumar *et al.*, "Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme," *Journal of Scientific & Industrial Research*, vol. 81, no. 10, pp. 1061–1072, Oct. 2022, https://doi.org/10.56042/jsir.v81i10.57471.

[8] S. Kanthimathi and P. Jhansi Rani, "An efficient packet dropping attack detection mechanism in wireless ad-hoc networks using ECC based AODV-ACO protocol," *Wireless Networks*, Oct. 2022, https://doi.org/10.1007/s11276-022-03156-w.

[9] A. A. Mohammed, S. A. Razak, A. Hanan, I. Mohammed, and Y. Abdella, "A Review on Blackhole Attack in Mobile Ad Hoc Networks," in *International Conference on Wireless Networks*, Las Vegas, NV, USA, Jul. 2010, pp. 116–121.

[10] A. O. Aljahdali, F. Thabit, H. Aldissi, and W. Nagro, "Dynamic Keystroke Technique for a Secure Authentication System based on Deep Belief Nets," *Engineering, Technology & Applied Science Research*, vol. 13, no. 3, pp. 10906–10915, Jun. 2023, https://doi.org/10.48084/etasr.5841.

[11] C. K. Nagpal, C. Kumar, B. Bhushan, and S. Gupta, "A Study of Black Hole Attack on MANET Performance," *International Journal of Modern Education and Computer Science*, vol. 4, no. 8, pp. 47–53, Aug. 2012, https://doi.org/10.5815/ijmecs.2012.08.07.

[12] C. Guo, C. C. Chang, and C. Y. Sun, "Chaotic maps-based mutual authentication and key agreement using smart cards for wireless communications," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 2, pp. 99–109, 2013.

[13] R. K. Singh and P. Nand, "Literature review of routing attacks in MANET," in *International Conference on Computing, Communication and Automation*, Greater Noida, India, Apr. 2016, pp. 525–530, https://doi.org/10.1109/CCAA.2016.7813776.

[14] Z. U. R. Khan and A. Sharma, "Security Aspects of MANETs: A Review," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 7, pp. 40–44, 2019.

[15] A. Pellegrini, V. Bertacco, and T. Austin, "Fault-based attack of RSA authentication," in *Design, Automation & Test in Europe Conference & Exhibition*, Dresden, Germany, Mar. 2010, pp. 855–860, https://doi.org/10.1109/DATE.2010.5456933.

[16] Z. L. Ping, S. Q. Liang, and L. X. Liang, "RSA Encryption and Digital Signature," in *International Conference on Computational and Information Sciences*, Chengdu, China, Oct. 2011, pp. 369–372, https://doi.org/10.1109/ICCIS.2011.245.

[17] R. Mohan, G. Prabakaran, and T. Priyaradhikadevi, "Seagull Optimization Algorithm with Share Creation with an Image Encryption Scheme for Secure Vehicular Ad Hoc Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 13000–13005, Feb. 2024, https://doi.org/10.48084/etasr.6786.

[18] P. Papadimitratos and Z. J. Haas, "Secure data transmission in mobile ad hoc networks," in *2nd ACM workshop on Wireless security*, San Diego, CA, USA, Sep. 2003, pp. 41–50, https://doi.org/10.1145/941311.941318.

[19] E. H. Teguig, Y. Touati, and A. Ali-Cherif, "ECC Based-Approach for Keys Authentication and Security in WSN," in *9th IEEE-GCC Conference and Exhibition*, Manama, Bahrain, Dec. 2017, pp. 1–4, https://doi.org/10.1109/IEEEGCC.2017.8447901.

[20] I. Temirlan and Y. Li, "ECC-based User Authentication Scheme for Wireless Sensor Networks," *International Journal of Engineering Research & Science*, vol. 3, no. 6, pp. 21–28, Jun. 2017, https://doi.org/10.25125/engineering-journal-IJOER-JUN-2017-5.

[21] C. Atheeq and M. M. A. Rabbani, "Mutually authenticated key agreement protocol based on chaos theory in integration of internet and MANET," *International Journal of Computer Applications in Technology*, vol. 56, no. 4, pp. 309–318, Jan. 2017, https://doi.org/10.1504/IJCAT.2017.089088.

[22] S. K. S., J. Rangasamy, S. S. Kamath, and C.-C. Lee, "ES-HAS: ECC-Based Secure Handover Authentication Scheme for Roaming Mobile User in Global Mobility Networks," *Cryptography*, vol. 5, no. 4, Dec. 2021, Art. no. 35, https://doi.org/10.3390/cryptography5040035.

[23] M. N. Lima, A. L. dos Santos, and G. Pujolle, "A survey of survivability in mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 66–77, 2009, https://doi.org/10.1109/SURV.2009.090106.

[24] J. Ryu, D. Kang, and D. Won, "Improved Secure and Efficient Chebyshev Chaotic Map-Based User Authentication Scheme," *IEEE ACCESS*, vol. 10, pp. 15891–15910, 2022, https://doi.org/10.1109/ACCESS.2022.3149315.

[25] M. A. Lateef, C. Atheeq, M. A. Rahman, and M. A. Faizan, "Data Aegis Using Chebyshev Chaotic Map-Based Key Authentication Protocol," in *Intelligent Manufacturing and Energy Sustainability*, A. R. Manchuri, D. Marla, and V. V. Rao, Eds. New York, NY, USA: Springer, 2023, pp. 187–195.

[26] C. Atheeq and M. M. A. Rabbani, "CACK—A Counter Based Authenticated ACK to Mitigate Misbehaving Nodes from MANETs," *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, vol. 14, no. 3, pp. 837–847, Apr. 2021, https://doi.org/10.2174/2213275912666190809104054.

[27] R. B. Naik and U. Singh, "A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption," *Annals of Data Science*, vol. 11, no. 1, pp. 25–50, Feb. 2024, https://doi.org/10.1007/s40745-021-00364-7.

[28] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, "Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home," *Electronics*, vol. 11, no. 7, Jan. 2022, Art. no. 1083, https://doi.org/10.3390/electronics11071083.