SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I7P103

Volume 10 Issue 7, 23-32, July 2023
©2023 Seventh Sense Research Group®

Original Article

Enhanced Chaotic Map Based Key Agreement to Mitigate Packet Dropping Attack from MANETs

S. Syed Abdul Syed[1], C. Atheeq[2], A. Abdul Azeez Khan[3], K. Javubar Sathick[4], E. Syed Mohamed[5], C. Altaf [6]

[1,3,4,5]B.S Abdur Rahman Institute of Science and Technology, India.
[2]GITAM Deemed to be University, India.
[6]Lords Institute of Science and Technology, Telangana, India

[2]Corresponding Author : atheeq.prof@gmail.com

Received: 19 April 2023 Revised: 20 June 2023 Accepted: 12 July 2023 Published: 31 July 2023

Abstract *- MANET is a self-organized wireless network with no infrastructure. Especially data transfer from one system to another needs to be done securely. To provide data integrity, authentication plays a vital role in data communication. RSA and ECC are widely used algorithms in the real world, but authentication using these algorithms is time-consuming. Towards this, various algorithms came into existence with different security primitives. However, studying the critical agreement process among these security mechanisms is important. We have studied the patents related to secure end-to-end communication in MANET. Therefore, we aim to design a chaos-based mutual authentication algorithm that takes less time than these existing algorithms and evaluate concerning attack Resilience, packet delivery fraction, delay, throughput, and overhead. Simulation results show the result of the proposed mechanism and give better performance in terms of the said parameters. Comparison of the proposed system presents better results when compared to RSA ECC in terms of key generation mechanism.*

Keywords *- MANET, Security, Authentication, Chaos, Hash, Key, RSA, ECC.*

1. Introduction

A mobile ad hoc network is a unique network that does not rely on a fixed infrastructure but instead uses a self-configuring and self-forming mobile device network that communicates wirelessly. These devices can establish communication links through wireless connections such as Wi-Fi, cellular, or satellite. Some MANETs can be restricted to a small area of wireless devices, while others can be connected to the Internet. Since wireless connections in MANETs are susceptible to bit rate errors, data transmission may occur over multiple hops if the destination is out of range of the source mobile node. The network's control and management are distributed, and communication links between nodes are symmetric. In contrast to traditional networks, mobile ad hoc networks are unique in that they lack a fixed infrastructure and have dynamic topology due to the autonomous mobility of their nodes[1]. These nodes are end hosts, serve as routers, and have limited energy and computing resources.

Mobile ad hoc networks (MANETs) present several challenges due to their unique characteristics. One of these challenges is flat addressing, which is difficult to maintain in a network without a hierarchy[2]. Mobility is also a significant challenge, as the network topology changes frequently, making it challenging to adapt and react quickly. Heterogeneity is another issue, as not all nodes are the same, affecting the network's performance. Network-to-network connectivity, such as internet access, is another challenge that needs to be addressed.

MANETs have dynamic topology, meaning that multi-hop connections change quickly, resulting in half-or full-duplex connections[3-5]. The transmission rate of radio is higher than the wireless communication throughput, and each node in a MANET serves as both a router and a host, which makes the network autonomous[6, 7]. However, the nodes in MANETs have limited battery life and memory space, which can affect their performance. MANETs apply in scenarios such as Vehicular Ad hoc networks and spontaneous conferences[8].

In addition to the characteristics mentioned above, MANETs offer various advantages, such as self-configuration of every node, separation from central network administration, robustness due to decentralization, flexibility, and cost-effectiveness compared to wired networks. MANETs can also accommodate the addition of more nodes in the network. They can be set up anywhere and time, making them suitable for various applications, including military battlefields, personal area networks, Bluetooth, and collaborative work.

However, security is a significant concern in MANETs due to their dynamic nature and autonomous property. Although previous research has focused on achieving maximum security, it has resulted in network overhead in the routing process, and the assumption that mobile nodes undergoing communication are trustworthy has led to misbehaviour and Chaos in the network, ultimately degrading network performance.

This paper continues: Section II surveys, Section III describes the proposed work, Section IV evaluates performance, and Section V concludes the paper. Finally, Section VI briefly discusses current and future enhancements.

2. Literature Survey

The RSA cryptosystem is a type of public key cryptography that uses the factorization of two big prime numbers. The name RSA is derived from the surnames of Rivest-Shamir-Adleman. This system is the first to have a separate method for encryption and decryption.

RSA uses public and private keys[9]. The private key is hidden, but the public key is accessible. RSA uses public and private keys. The private key is hidden, but the public key is accessible. The process involves critical generation, key encryption, and key decryption. Figure 1 demonstrates that messages are encrypted using the public key but are decrypted using the private key.

ECC generate a key in less time than RSA [10]. To ensure better data security, larger key sizes are required, which results in overhead on computing systems. ECC has lower overheads than RSA, making it more efficient [11]. ECC offers the same level of security as RSA but outperforms RSA in operational efficiency and security [12, 13]. ECC also has the advantage of using shorter keys to provide security.

Previous work has demonstrated that establishing a secure path from source to destination through REQ and REP messages and sharing a secret key for authentication results in higher computational costs for authentication between the source and destination [14-17]. The work also shows more possible attacks in the network due to its dynamic nature [18]. ECC generates keys using elliptic curve properties instead of large prime numbers. Elliptic curves are points that satisfy a cubic equation and the point at infinity.

ECC cryptosystem users receive public and private keys. The public key generates ciphertext and verifies digital signatures, while the private key reconstructs plaintext and generates them. Figure 2 shows this. ECC keys are smaller, reducing storage and transmission needs. Elliptic curve groups offer RSA-like security with a smaller modulus. Also, 'b' and 'd' are assumed to be different. RSA has been found to have slow signing and decryption processes, which makes it less efficient. Therefore, it is being replaced by ECC, which is much faster in these processes. ECC provides more secure signatures that can be computed in two stages, unlike RSA, which is vulnerable to attacks. ECC also offers excellent key exchange protocols, while RSA is more susceptible to attacks. Moreover, binary curves used in ECC are quick to implement in hardware. Although both RSA and ECC offer security, they come with computational overhead. However, the proposed system provides enhanced security and addresses these issues.

3. Materials and Methods

ECC outperforms RSA by using small fundamental size values, fast computing, less power utilisation, and memory usage for MANETs, which improves the network's overall performance. The research studies comparing RSA and ECC came to this conclusion. Therefore, the time required to generate a key using ECC is significantly longer than chaos theory, even though this time is significantly shorter than RSA. The traditional cryptosystems are, therefore, inferior to chaos theory, which is superior.

The Chebyshev polynomial can explain the proposed system:

Mason and Handscomb present Chebyshev's polynomial composition property. The two-element critical agreement theory allows imparted elements to trade open keys via unprotected channels and create a common secret key.

They accept that the distribution of private data is via some safe medium; however, it is constrained to MANET.

Chebyshev polynomial t n(x):[–1,1] → [–1,1] is defined as

$T_n (x) = \cos(n\cos^{-1}(x))$.

This polynomial maps T_n: R->R of degree n is defined using recurrence relation as

T_n*x=2x $T_{n-1}(x)$- $T_{n-2}(x)$, where $n\geq 2$, $T_0(x)=1$,and $T_1(x)=x$.

Hash function is used in the authentication process of the proposed system that uses Chebyshev polynomials to generate the session key. Many fundamental agreement mechanisms that use Chebyshev polynomials are subjected to intensive scrutiny due to the rapid development of the chaotic concept associated with cryptography.

Mechanisms that use the Chebyshev polynomials can be broken down into three categories according to the number of users: key agreement, authentication protocols with various architectures, and multi-tier chaos protocols[20-24]. The essential management technique for authentication based on a password for three-tier architecture that utilises modular exponentiation on an elliptic curve has recently been widely presented. This technique was developed in recent times. In any event, these plans call for a considerable amount of calculation weight, and even the most recent exploration is still focusing on the key management scheme for authentication on a three-tier architecture.

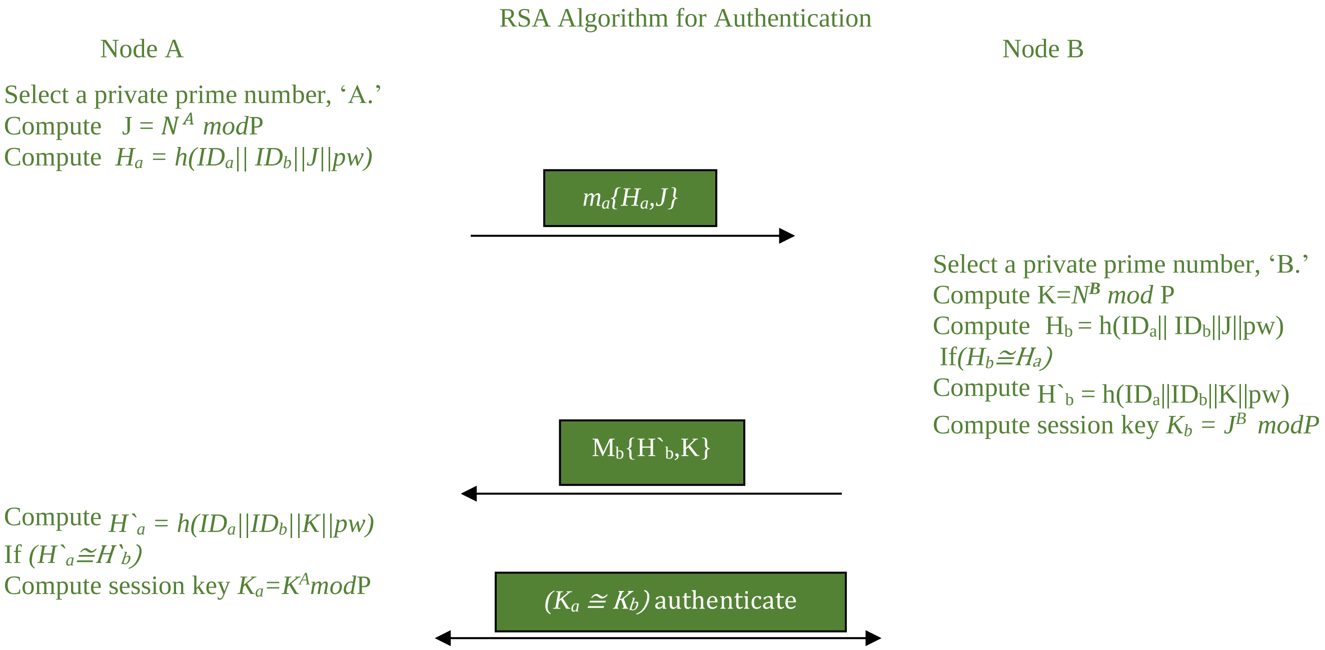
RSA Algorithm for Authentication
Node A
Node B
Select a private prime number, 'A.'
Compute $J = N^A \; mod P$
Compute $H_a = h(ID_a || ID_b || J || pw)$
$m_a\{H_a, J\}$
Select a private prime number, 'B.'
Compute $K = N^B \; mod \; P$
Compute $H_b = h(ID_a || ID_b || J || pw)$
If $(H_b \cong H_a)$
Compute $H`_b = h(ID_a || ID_b || K || pw)$
Compute session key $K_b = J^B \; modP$
$M_b\{H`_b, K\}$
Compute $H`_a = h(ID_a || ID_b || K || pw)$
If $(H`_a \cong H`_b)$
Compute session key $K_a = K^A modP$
$(K_a \cong K_b)$ authenticate

Fig. 1 Authentication using RSA

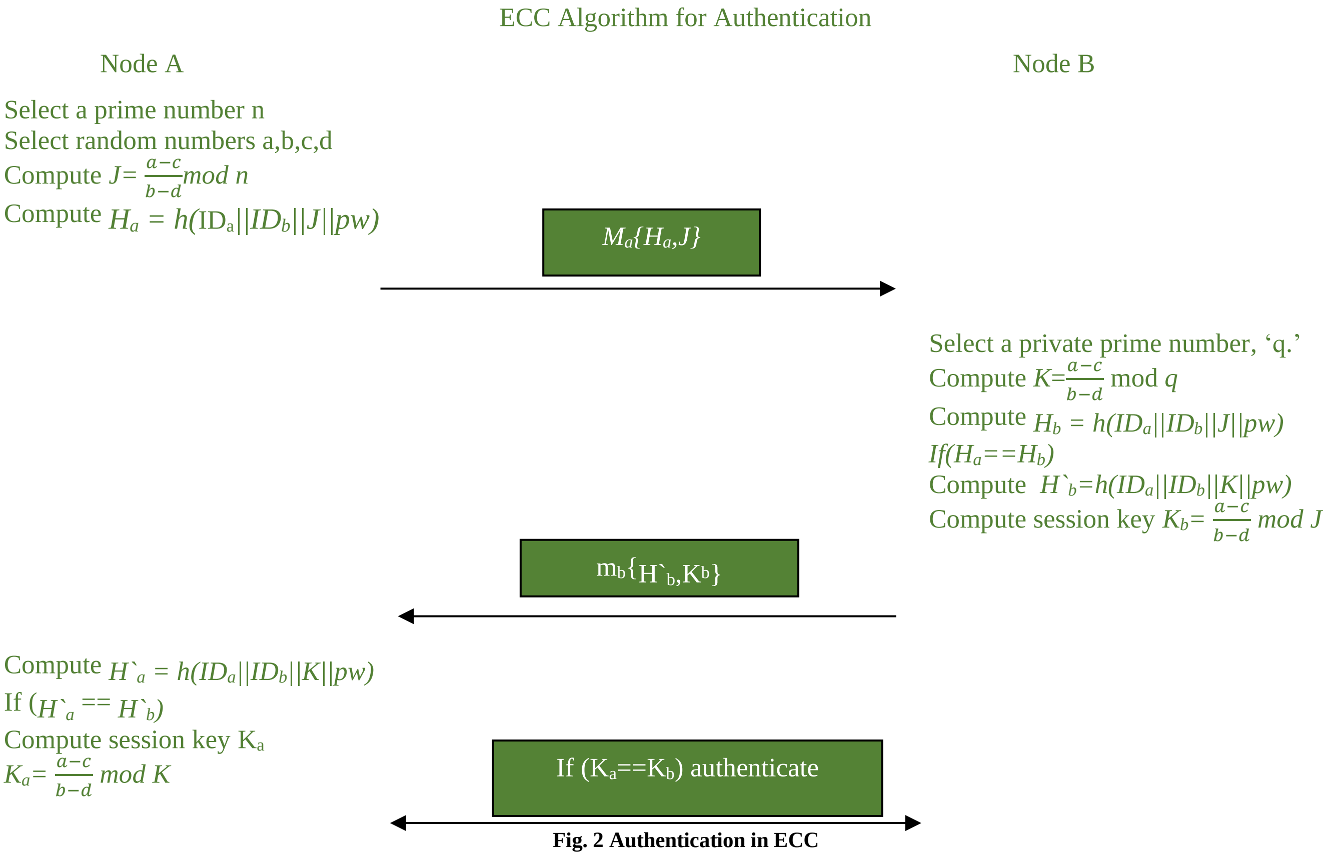
ECC Algorithm for Authentication
Node A
Node B
Select a prime number n
Select random numbers a,b,c,d
Compute $J = \frac{a-c}{b-d} mod \; n$
Compute $H_a = h(ID_a || ID_b || J || pw)$
$M_a\{H_a, J\}$
Select a private prime number, 'q.'
Compute $K = \frac{a-c}{b-d}$ mod q
Compute $H_b = h(ID_a || ID_b || J || pw)$
$If(H_a == H_b)$
Compute $H`_b = h(ID_a || ID_b || K || pw)$
Compute session key $K_b = \frac{a-c}{b-d} \; mod \; J$
$m_b\{H`_b, K_b\}$
Compute $H`_a = h(ID_a || ID_b || K || pw)$
If $(H`_a == H`_b)$
Compute session key K_a
$K_a = \frac{a-c}{b-d} \; mod \; K$
If $(K_a == K_b)$ authenticate

Fig. 2 Authentication in ECC

4. Chaotic Maps

A subfield of mathematics known as chaos theory studies the behaviour of dynamical systems that are extremely sensitive to their initial conditions. According to the interdisciplinary chaos theory, despite chaotic complex systems appearing to be random, there are underlying patterns, ongoing feedback loops, repetition, self-similarity, fractals, self-organization, and reliance on initial programming.

Turbulence, weather, the stock market, our mental states, and other nonlinear phenomena that are practically impossible to predict or control are dealt with by chaos theory.

4.1. Chaos Algorithm

Suppose the source is node A, and the destination is node B.

Node A is the source.

Step 1:Select a private prime number, i.e. ’m’
Step 2:Compute $(x)= cos(m\ cos^{-1}(x))$
$H_a=H(ID_s||ID_d||T_m(x)||pw)$
Now considering node B, i.e., the destination
Step 3: Select a prime no ‘f’
Step 4: compute $T_f(x)=cos(f,cos^{-1}(x))$
$H_b{}^1=H(ID_s||ID_d||T_m(x)||pw)$
Step 5: the values of m_b are sent to the source.
Now, the values at the source
Compute $H_a{}^1=H(ID_s||ID_d||T_m(x)||pw)$
If $(H_a{}^1==H_b{}^1)$
Now computing $T_m\,(T_f\,(\mathrm{x}))$ on the source and computing $T_f\,(T_m(\mathrm{x}))$
Both the source and destination agree on a session key.
Therefore,
$T_m\,\left(T_f\,(\mathrm{x})\right) = T_f\,(T_m(\mathrm{x}))$
Hence, this the algorithm for Chaos.

Fig. 3 Authentication using CHAOS

The work presented here details the secure authentication procedure for MANETs, as shown in figure 3. The algorithm demonstrates significantly improved performance compared to the currently used RSA-based mutual authenticated key agreement protocol. The proposed method's computational overhead is significantly lower than other approaches already in use[27].

As a result, generating keys using Chaos takes significantly less time than using RSA or ECC. Our work goal is to achieve protective communication with security objective authentication. We believe this to be the most effective method for achieving trustworthiness and nondenial in the information correspondence between the source and the destination.

5. Results and Discussions

We analyze the results of the above algorithms using the Network Simulator tool (NS2) version NS2.34. The performance is analyzed using the parameters such as delay, throughput, overhead, and packet delivery ratio. The simulation parameters are presented in Table 1, and the results are represented in the graphs.

Table 1. Simulation parameters

Simulation Parameters	Values
Simulation Time	120 seconds
Number of nodes	50
Medium	Wireless medium
MAC	802.11
Mobility Model	Random way point
Routing Protocol	AODV
Radio Communication	Random way point
Packet Size	512 bytes
Data	CBR
Simulation Area	900m x 900m

Delay: Delay is the interval between the time the sender generates a packet and the time the recipient receives it. Delay is the interval between the time the sender generates a packet and the time the recipient receives it[25, 26]. Delay is the interval between the time the sender generates a packet and the time the recipient receives it.

As shown in Table 2, it is evident that the performance in terms of End -to-End delay is presented for RSA, ECC, and Chaos algorithms. At various simulation time steps, the results are observed. The simulation time is taken into account between 0 and 9.5 seconds. We can observe that Chaos has less delay compared to other algorithms.

The average time a data packet needs to travel from beginning to End. We display the end-to-end delay of various algorithms in Figure 4. The horizontal axis plots the simulation time in seconds, and the vertical axis displays the end-to-end delay. We differentiate end-to-end delay using RSA, ECC, and Chaos algorithms. Our proposed chaos algorithm has less delay than RSA and ECC algorithms.

Overhead: Overhead defines how many packets are being used in data communication. The overhead values of three different mechanisms are presented in Table 3.

Table 2. Values of delay of RSA, ECC and CHAOS

Time	CHAOS	ECC	RSA
0	0	0	0
0.5	0	0	0
1	0	0	0
1.5	0.056460	0.112192	0.112467
2	0.038234	0.076099	0.076238
2.5	0.032155	0.064065	0.064158
3	0.029121	0.058055	0.058127
3.5	0.027292	0.054443	0.054495
4	0.026078	0.052036	0.052079
4.5	0.025208	0.050316	0.050353
5	0.024560	0.049027	0.049059
5.5	0.024053	0.048024	0.048053
6	0.023645	0.047219	0.047245
6.5	0.023316	0.046566	0.046589
7	0.023040	0.046017	0.046038
7.5	0.022805	0.045918	0.045575
8	0.022604	0.045918	0.045174
8.5	0.022430	0.045918	0.044829
9	0.022280	0.045918	0.044528
9.5	0.022144	0.045918	0.044262

Table 3. Values of computational overhead in RSA, ECC, and Chaos

TIME	RSA	ECC	CHAOS
1	2	1	0
1.5	16	15	14
2	16	15	14
2.5	16	15	14
3	16	15	14
3.5	16	15	14
4	16	15	14
4.5	16	15	14
5	16	15	14
5.5	16	15	14
6	16	15	14
6.5	16	15	14
7	16	15	14
7.5	16	15	14
8	16	15	14
8.5	16	15	14
9	16	15	14
9.5	16	15	14

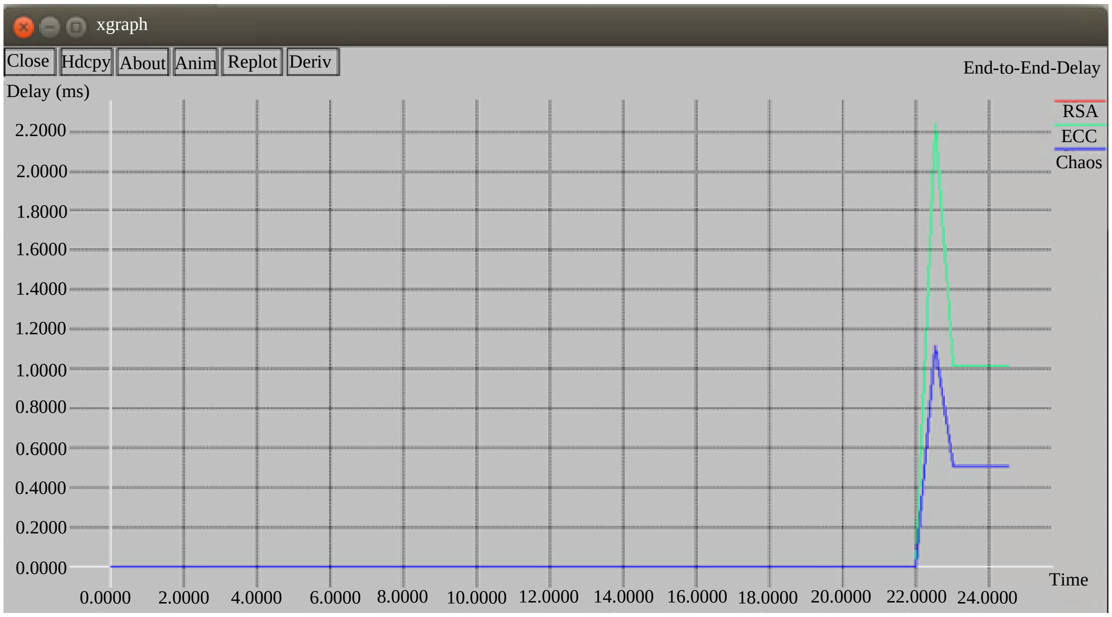

Fig. 4 Graph with delay

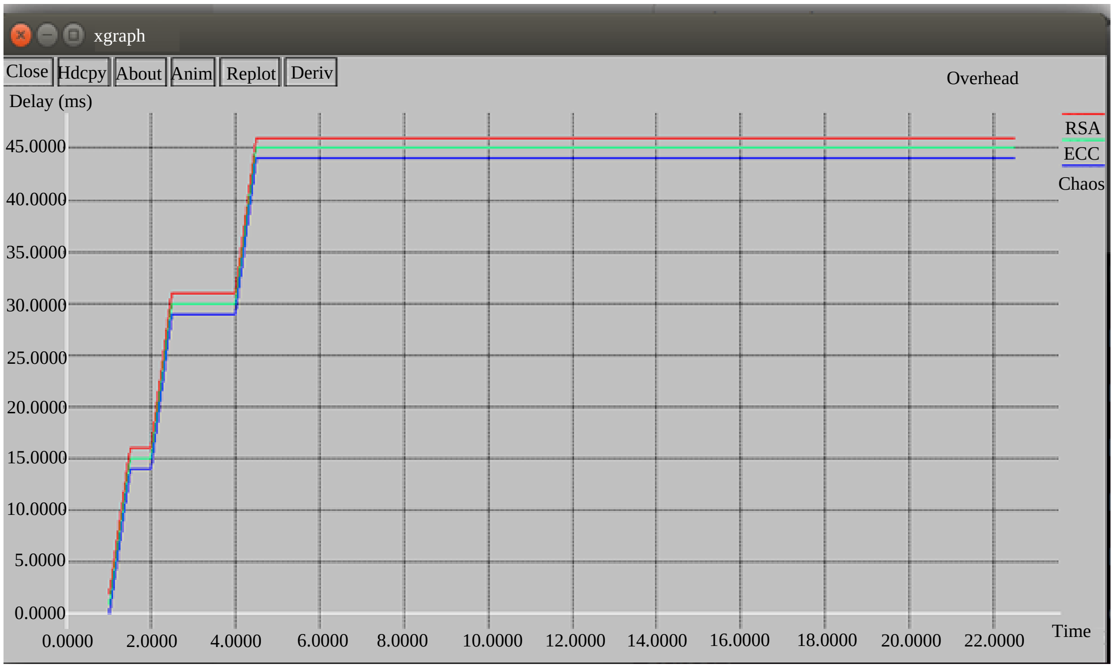

Fig. 5 Graph of overhead

The range of the simulation time is 1 to 9.5. The overhead is displayed along the vertical axis, and the simulation time in seconds is plotted on the horizontal axis.. From Figure 5, we can observe that Chaos has less overhead than RSA and ECC.

Packet Delivery Ratio: The packet delivery ratio defines the ratio of packets being sent by the source and received at the destination. It is presented in Table 4. The simulation time is considered from 0 to 9.5. The results are observed at different time intervals. From Figure 6, we can observe that the packet delivery ratio of Chaos is higher than RSA and ECC. Formula for calculating the packet delivery ratio is given by:

$$PDR= \frac{number\ of\ packets\ successfully\ recieved\ at\ the\ destination}{total\ number\ of\ packets\ sent\ by\ the\ source}$$

Throughput: Throughput can be defined as the number of bytes of data being sent, which is presented in Table 5.

Table 4. Rate of packet delivery in RSA, ECC and CHAOS

TIME	RSA	ECC	CHAOS
0	0	0	0
0.5	0	0	0
1	0	0	0
1.5	0	0	1
2	1	1	2
2.5	1	1	3
3	2	2	5
3.5	3	3	6
4	3	3	7
4.5	4	4	8
5	5	5	10
5.5	5	5	11
6	6	6	12
6.5	6	6	13
7	7	7	15
7.5	8	7	16
8	8	7	17
8.5	9	7	18
9	10	7	20
9.5	10	7	21

Table 5. Values of throughput in RSA, ECC, and CHAOS

TIME	RSA	ECC	CHAOS
0	0.0	0.0	0.0
0.5	0.0	0.0	0.0
1	0.0	0.0	0.0
1.5	332.0	78.0	665.0
2	332.0	78.0	665.0
2.5	332.0	78.0	665.0
3	332.0	78.0	665.0
3.5	332.0	78.0	665.0
4	332.0	78.0	665.0
4.5	332.0	78.0	665.0
5	332.0	78.0	665.0
5.5	332.0	78.0	665.0
6	332.0	78.0	665.0
6.5	332.0	78.0	665.0
7	332.0	78.0	665.0
7.5	332.0	15.0	665.0
8	332.0	0.0	665.0
8.5	332.0	0.0	665.0
9	332.0	0.0	665.0
9.5	332.0	0.0	665.0

The graph is plotted with the time along the horizontal axis and throughput along the vertical axis. In Figure 7, we can observe that the chaos throughput is higher than RSA and ECC. Table 6 presents the comparative analysis of Chaos with the RSA and ECC algorithms used for authentication.

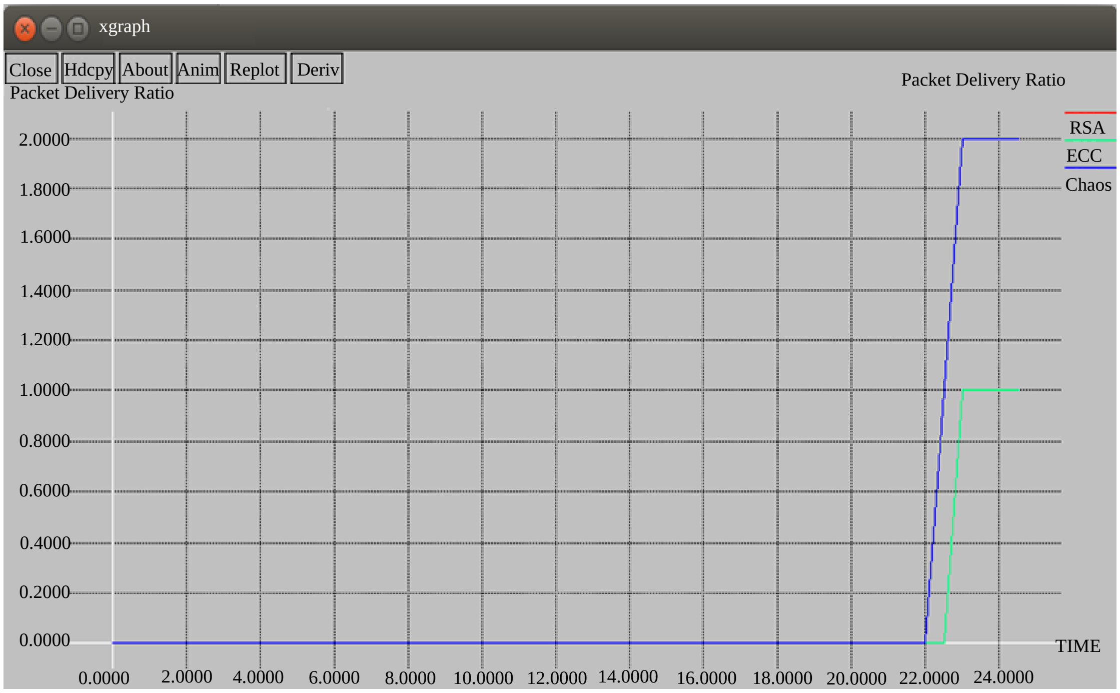

Fig. 6 Graph of packet delivery ratio

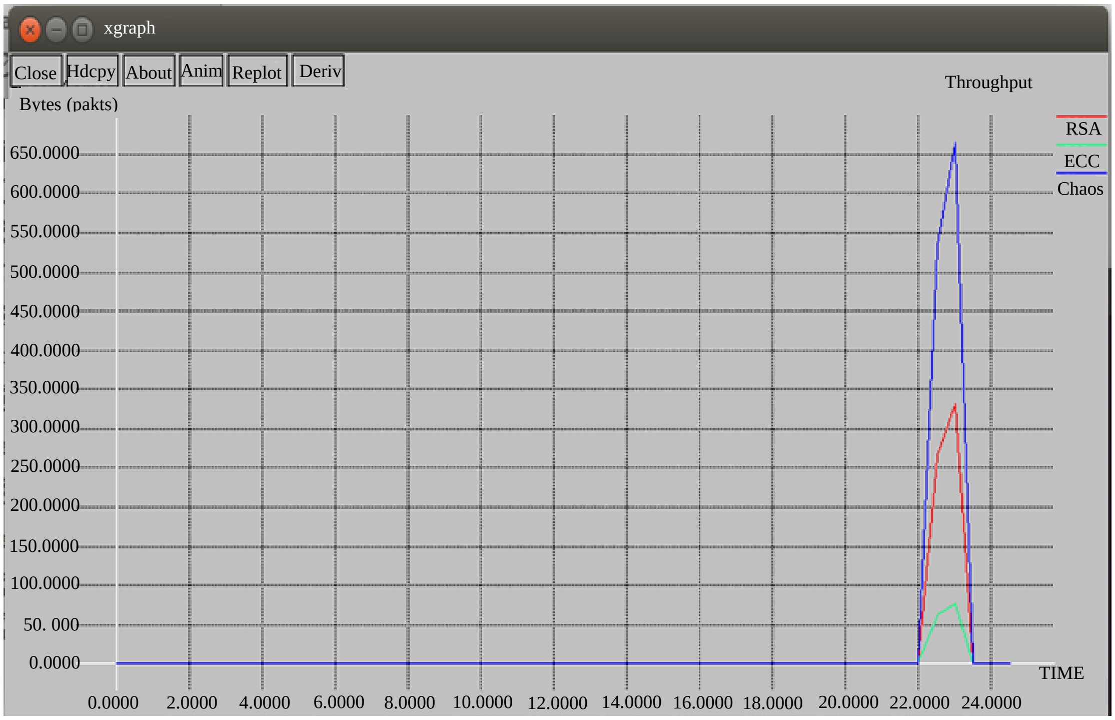

Fig. 7 Graph of throughput

Table 6. Performance comparison of RSA, ECC and CHAOS

Parameters	ECC	RSA	CHAOS
Computational overhead	10 times less than RSA	More	Less than both
Bandwidth	Saves bandwidth	Lesser saving of bandwidth	Saves bandwidth
Key generation	Fast key generation	Slow key generation	Better key generation than both
Efficiency	More efficient	Less efficient	More efficient
Key generation function	Modular function	Modular exponentiation	Chebyshev polynomials

6. Conclusion

We have implemented the cryptographic algorithms RSA, ECC, and Chaos map-based critical agreement process for authentication of end nodes using the Network Simulator Tool (NS2) and evaluated the above algorithms concerning delay, throughput, packet delivery ratio and overhead based on security and efficiency.

From the results, we can conclude that our proposed system gives better performance when compared to RSA and ECC. The work can be further carried out by enhancing the chaos maps for authentication based on biometric digital signatures and passwords.

Current and Future Developments

In this paper, the work is focused on the authentication process that is presented with different techniques and their merits and demerits. The work can be enhanced in the future by using authentication-based lightweight methods like smart cards, biometrics, and digital signatures.

Acknowledgment

This work is implemented with the collaboration of the research members P. Venkat Reddy, C. Atheeq, Arshed Ahmad Khan Mohammad, Mohammad Arif Abdul, Khaja Mohammad Nizamuddin, (GITAM University), Altaf C(Osmania University).

References

[1] Xiang Shihu, and Yang Jun, “Performance Reliability Evaluation for Mobile Ad Hoc Networks,” *Reliability Engineering & System Safety*, vol. 169, pp. 32-39, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Wu Di et al., “Equilibrium Analysis of Bitcoin Block Withholding Attack: A Generalized Model,” *Reliability Engineering & System Safety*, vol. 185, pp. 318-328, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Annie Ezhilarasi M, and Parthasarathy P, “Detection Algorithms of the Wormhole Attacks in MANET,” *International Journal of P2P Network Trends and Technology (IJPTT)*, vol. 7, pp. 26-29, 2017. [Publisher Link]

[4] Shraddha Kamble, B. K. Mishra, and Rajesh Bansode, “Detection of Routing Misbehaving Links in MANET by Advance EAACK Scheme,” *International Journal of P2P Network Trends and Technology (IJPTT)*, vol. 6, no. 3, pp. 1-5, 2016. [CrossRef] [Publisher Link]

[5] Neeraj Kumar Jarouliya, and Nirupama Tiwari, “Utilization of Particle Swarm Optimization (PSO) Use as Clustering Algorithm in MANET,” *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 11, pp. 10-14, 2019. [CrossRef] [Publisher Link]

[6] R. Rajesh, “An Identity-Based Key Management in MANET with Threshold Sharing,” *SSRG International Journal of Mobile Computing and Application*, vol. 4, no. 2, pp. 8-12, 2017. [CrossRef] [Publisher Link]

[7] R. Rajesh, “A Novel Security Approach in MANET with Certificateless Cryptography,” *SSRG International Journal of Computer Science and Engineering*, vol. 4, no. 4, pp. 5-12, 2017. [CrossRef] [Publisher Link]

[8] Anugraha, and Krishnaveni, “An Efficient and Secure Routing in MANET using Trust Model,” *International Journal of Engineering Trends and Technology*, vol. 70, no. 9, pp. 330-336, 2022. [CrossRef] [Publisher Link]

[9] Zeba Naaz, Kauser Fatima, and C. Atheeq, “Performance-Based Comparison Study of RSA and Chaotic Maps in MANET,” *SSRG International Journal of Electrical and Electronics Engineering*, vol. 4, no. 2, pp. 17-22, 2017. [CrossRef] [Publisher Link]

[10] Nicholas Jansma, and Brandon Arrendondo, “Performance Comparison of an Elliptic Curve and RSA Digital Signatures,” *Efficiency Comparison of an Elliptic Curve and RSA Digital Signatures*, pp. 1-20, 2004. [Google Scholar] [Publisher Link]

[11] S. A Vanstone, “Next Generation Security for Wireless: Elliptic Curve Cryptography,” *Computers and Security*, vol. 22, no. 5, pp. 412-415, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[12] Ruchika Markan, and Gurvinder Kaur, “Literature Survey on Elliptic Curve Encryption Techniques,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 9, 2013. [Google Scholar]

[13] Akash Singh et al., “Security and Trust Management in MANET,” *Information Technology and Mobile Communication*, New York: Springer-Verlag, vol. 147. pp. 384-387, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[14] Antonio Tedeschi et al., “Statistically-Enhancing Diagnosis of Packet Loss in *WSNs*,” *International Journal of Mobile Network Design and Innovation*, vol. 7, no. 1, pp. 3-14, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] C. Atheeq, and M. Munir Ahmed Rabbani, “Secure Intelligence Algorithm for Data Transmission in Integrated Internet MANET,” *International Journal of Computer Science and Applications*, vol. 14, no. 2, pp. 142-163, 2017. [Google Scholar] [Publisher Link]

[16] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, “A Password Authentication Scheme over Insecure Networks,” *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727-740, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[17] Zygmunt Haas, and Panagiotis Papadimitratos, *Secure End-To-End Communication in Mobile Ad Hoc Networks*, United States Patent Application, 2003. [Google Scholar] [Publisher Link]

[18] S. Syed Abdul Syed, and T. Senthil Kumaran, “FCM Based Segmentation for Medical Images,” *Research Journal of Pharmacy and Technology*, vol. 10, no. 12, pp. 4350-4352, 2017. [CrossRef] [Publisher Link]

[19] Nikhat Naaz Aslam Shaikh, and Vaishali Bagade, “Performance Evaluation and Detection of Grey, Warm, Flooding, Misrouting & Modification of Attacks in Vanet,” *SSRG International Journal of Electronics and Communication Engineering*, vol. 8, no. 4, pp. 10-17, 2021. [CrossRef] [Publisher Link]

[20] C. Atheeq, and M. Munir Ahmed Rabbani, “Mutually Authenticated Key Agreement Protocol Based on Chaos Theory Integrating Internet and MANET,” *International Journal of Computer Applications in Technology*, vol. 56, no. 4, pp. 309-318, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[21] S. K. Hazul Islam, and G. P. Biswas, “An Improved Pairing-Free Identity-Based Authenticated Key Agreement Protocol Based on ECC,” *Procedia Engineering*, vol. 30, pp. 499-507, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[22] Simon Blake-Wilson, Don Johnson, and Alfred Menezes, “Key Agreement Protocols and their Security Analysis,” *Cryptography and Coding*, pp. 30-45, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[23] Y. V. S. Sai Pragathi, and S. P. Setty, “Design and Implementation of Secure LAR Routing Protocol in MANETs,” *International Journal of Computer & Organization Trends (IJCOT)*, vol. 6, no. 4, pp. 1-3, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[24] P. G. V. Suresh Kumar, “Implementation of MAODV and Tree Maintenance in Overlay Multicasting Protocol for MANETs,” *International Journal of Computer & Organization Trends (IJCOT)*, vol. 24, no. 1, pp. 24-28, 2015. [Publisher Link]

[25] R. Navinkumar, and N. Prabaharan, “Improve Routing Process with Feature Based Packet Transmission Technique in MANET using GRBR Algorithm,” *International Journal of P2P Network Trends and Technology (IJPTT)*, vol. 6, no. 2, pp. 1-11, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[26] Sebastian Terence, Jude Immaculate, and P. Geethanjali, “Survey on Packet Dropping Detection Techniques in Wireless Sensor Network,” *International Journal of Engineering Trends and Technology*, vol. 71, no. 6, pp. 259-273, 2023. [CrossRef] [Publisher Link]

[27] C. Atheeq, and M. Munir A Rabbani, “CACK-A Counter Based Authenticated ACK to Mitigate Misbehaving Nodes from MANETs,” *Recent Advances in Computer Science and Communication*, vol. 14, no. 3, pp. 837-847, 2021. [CrossRef] [Google Scholar] [Publisher Link]