AN EFFECTIVE KEY AGREEMENT USING CHAOS THEORY COMPARED TO RSA AND ECC IN MANETS

[1]Ayesha, [2]Amena Begum,[3]Syeda Hazequa, [4]C Atheeq
[1,2,3]Student, [4]Assistant Professor
[1,2,3,4] Department of Computer Science Engineering
[1,2,3,4] Deccan College of Engineering and Technology, Hyderabad, India.

Abstract: MANET is wireless ad hoc network that is self-configuring, infrastructure less network of mobile devices which are connected wirelessly to secure environment. Especially data transfer from one system to another system needs to be done in a secure way. In order to provide data integrity, authentication plays an important role in data communication. RSA, ECC are widely used algorithms in real world but authentication using thesealgorithms is time consuming. Towards this, various algorithms came into existence with different security primitives. However, it is important to study the key agreement process among these security mechanisms. Therefore our aim is to design chaos based mutual authentication algorithm that takes less time than these existing algorithms and evaluate them in terms of attack resiliency, Packet delivery ratio, delay, throughput and overhead. Simulation results show the result of the concept. Comparison of proposed system presents better results when compared to RSA, ECC in terms of key generation mechanism. Chaos can be evaluated in terms of attack resiliency, Packet delivery ratio, delay, throughput and overhead.

Index Terms **-MANET, security, authentication, chaos, hash.**

1. INTRODUCTIONTOMANETS

A mobile ad hoc network, also known as wireless ad hoc network is a self-configuring, infrastructure less network of mobile devices which are connected wirelessly which usually have routable networking environment. They consist of a peer to peer, self-forming network. It can be a standard Wi-Fi connection, or another medium as a cellular or satellite transmission. Some MANETs are restricted to a local area of wireless device such as a group of laptop computers, while others may be connected to the Internet. The nature of high bit error rates of wireless connections are more profound in a MANET. Ad hoc networks are multi-hop mobile wireless networks where information packets are transmitted. Control and management of the network is distributed and the communication links between them are symmetric.Mobile ad hoc networks are different due do following factors: No infrastructure-flat network, Radio communication: shared medium,Every device (node) is a router as well as end host ,Nodes are in general autonomous, Mobility: dynamic topology, Limited energy and computing resources.

The challenges in MANET are flat addressing since there is no hierarchy, mobility as topology keeps changing frequently which affects the adaptability and reactiveness, heterogeneity arises because all nodes are not equal, Network-to-network connectivity such as internet access. The characteristics of MANETS includes Dynamic Topologies: Multihops tend to change randomly and rapidly with time and form unidirectional or bi-directional links. Bandwidth constrained, variable capacity links: wireless links may have lower reliability, efficiency, stability and capacity as compared to wired network. The throughput of wireless communication is less than a radio's maximum transmission rate after dealing with the constraints like multiple access, noise, interference conditions. Autonomous Behavior: Each node can act as a host and router, which shows its autonomous behavior. Energy Constrained Operation**:** As some or all the nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized with less memory,

power and light weight features.Less Human Intervention: They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature. Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate. Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead. Hidden terminal problem: The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver. Packet losses due to transmissionerrors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, unidirectional links, frequent path breaks due to mobility of nodes. Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes. Battery constraints: Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.Beside these characteristics it possess the followingadvantages: Separation from central network administration, every node can possess two roles of router and host which shows autonomous nature, Self-configuring and self-healing nodes, less expensive if compared to wired networks, as it accommodates the addition of more nodes in the network, Improved Flexibility, Robust due to decentralize administration, The network can be set up at any place and time. MANETs are majorly found in Military battlefield, Collaborative work, Local level application in home networks where devices can communicate directly to exchange information. Personal area network and Bluetooth, Commercial Sector also uses MANETs for various purposes.

Security issues in MANETS: Security in mobile ad hoc networks is difficult to achieve because of the vulnerability of wireless links, limited physical protection of nodes and the dynamically changing topology, also the absence of a certification authority, and the lack of a centralized monitoring or management point. Earlier studies on mobile ad hoc networks (MANETs) aimed at proposing protocols for some fundamental problems, such as routing, and tried to cope with the challenges imposed by the new environment. These protocols, however, fully trust all nodes and do not consider the security aspect. They are consequently vulnerable to attacks and misbehavior.

The remaining part of the paper is organized as follows: Section II deals with survey, Section III describes the proposed work followed by section IV which presents the Performance and section V concludes the paper.

2.LITERATURE SURVEY:

RSA:

RSA is one of thepublic key cryptosystem which is based on the factorization of product of two large prime numbers. The name RSA is an abbreviation of the initials of names of professors Rivest, Shamir and Adleman. With the discovery of RSA, for the first time we had one system to encrypt and another system to decrypt.

Many approaches have been proposed[13-17] in which security is based on sharing of secret keys. Two keys used in this are: public key and a private key. The private key is known to everyone but the private key

is kept secret. Steps involved are the key encryption, key generation and key decryption. The messages are encrypted using the public key but are decrypted using the private key as shown in the fig1.

In[1] key generation of RSA is significantly slower than ECC. For better and stronger security of databigger key sizes are required .This means that there is an overhead on computing systems. In [2] after comparing RSA and ECC, it was proved that ECC involves much fewer overheads than RSA. RSA provides same level of security but ECC outperforms over RSA in operational efficiency and security.ECC has shown many advantages due to its ability to provide security using the shorter keys.

RSA Algorithm for Authentication:

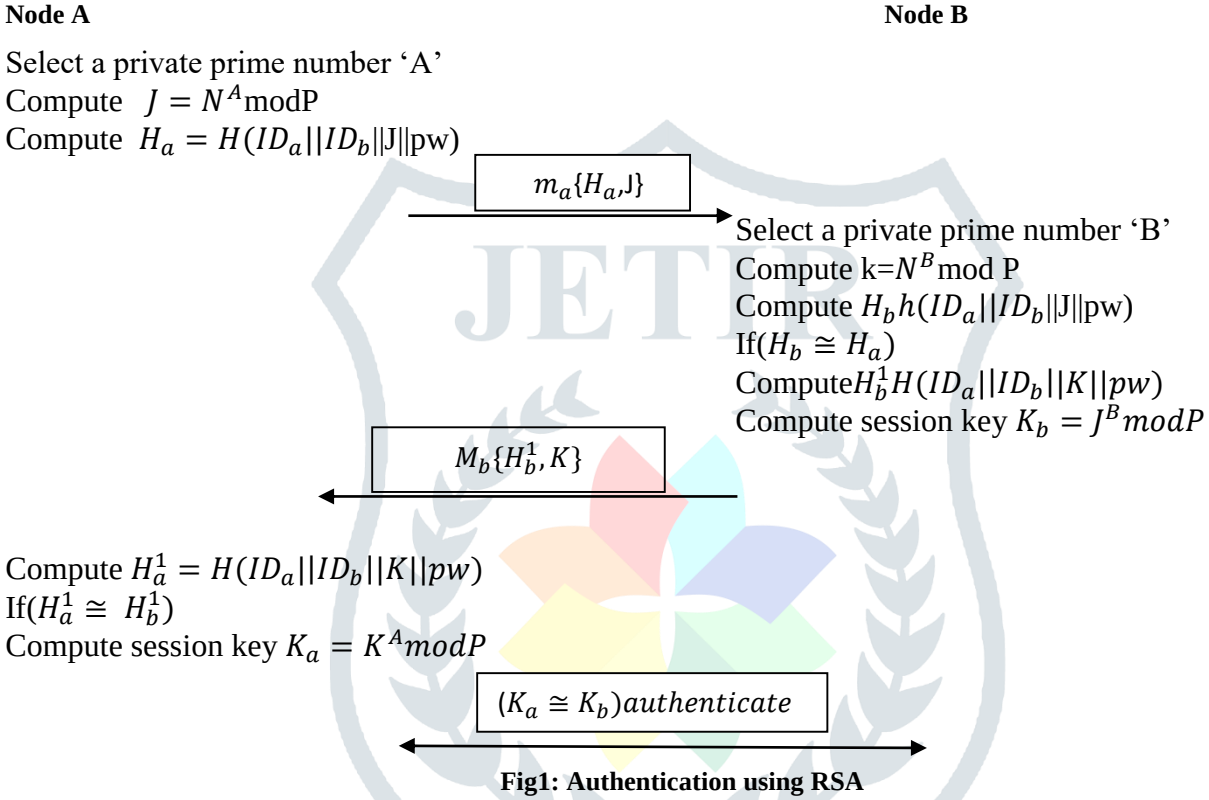

Fig1: Authentication using RSA

ECC:

Elliptic curve cryptography is an approach to the public key cryptography based on the algorithm structure of the elliptic curves over finite fields.The locus of a point, whose coordinates conform to a particular cubic equation along with the point at infinity O (the point at which the locus in the projective plane intersects the line at infinity,) is known as an **elliptic curve**.This encryption technique uses the properties of elliptic curve in order to generate keys instead of using the traditional methodology of generation of keys using the product of two very large prime numbers. ECC is a public key cryptosystem where each user has two keys: public key and private key. Public key is used for encryption and signature verification where as private key is used for decryption and signature generation as shown the below figure 2. In [2,3] The primary benefit provided by ECC is smaller key size which reduces the storage and also reduces the transmission requirements. An elliptic curve group can provide the same level of security given by RSA with a large modulus.

ECC Algorithm:

Node A **Node B**

Select a prime number n

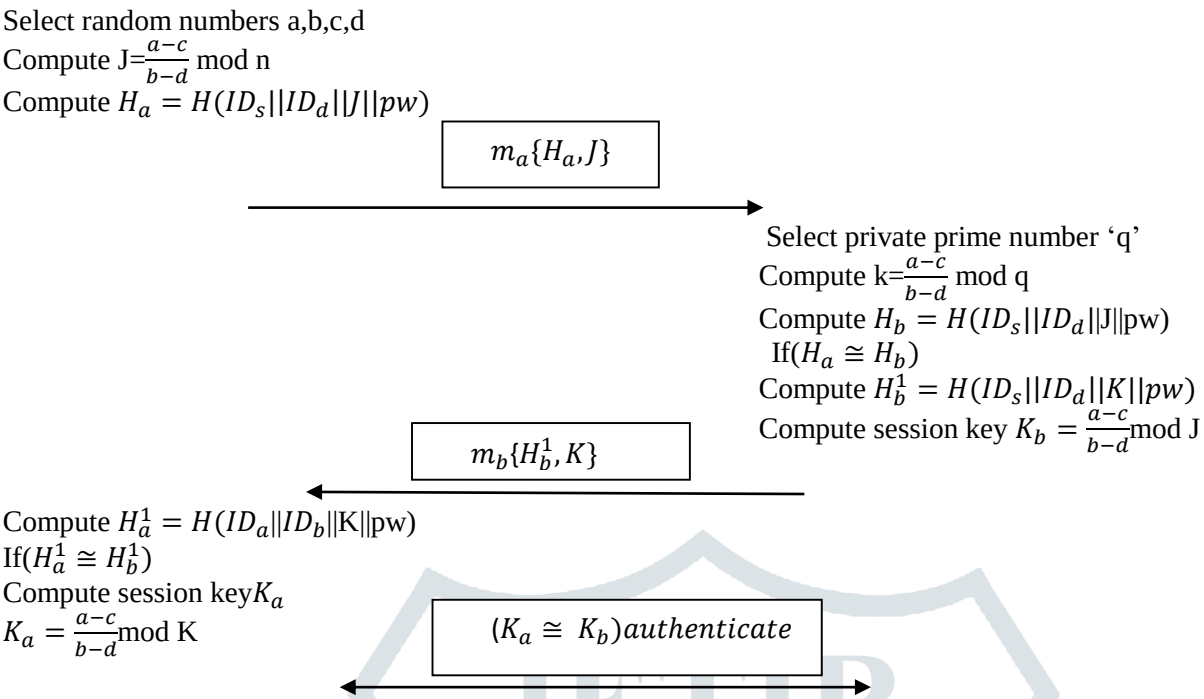

Fig2: Authentication in ECC

The RSA algorithm provides slow signing and decryption and thus it can be replaced by ECC which is computationally faster in encryption and decryption processes. In[4,5,6] The ECC signatures can be computed in two stages as shown in fig2 and are more secured than RSA in which signatures are difficult to implement securely. ECC provides excellent protocols for the key exchange whereas the RSA is very vulnerable to attacks. Also the binary curves are really fast to implement in hardware.Both RSA and ECC provide security but the computational overhead is more. However our proposed system overcomes all this problems and provides better security.

3. PROPOSED WORK

CHAOS better than traditional cryptosystem

. In[7] Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings. In[8,9] It is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity.

Thus the key generation time in ECC is smaller when compared to RSA, but the key generation time is larger in ECC when compared to CHAOS. Hence CHAOS is better than the traditional cryptosystems.

Proposed system can be explained by the Chebyshev polynomial:

Chebyshev polynomial composition property is presented by Mason and Handscomb.

This shows the theory of two element key agreement idea which permits the imparting elements to trade open keys via unprotected channel and creates a common secret key among them.

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

Chebyshev polynomialTn(x):[–1,1] → [–1,1] is defined as

Tn(x) = cos(narccos(x)).

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

T_n*x=2xT_{n-1}(x)-T_{n-2}(x), where n≥2,T_0(x)=1, and T_1(x)=x.

Hash Function

- **properties** of hash function h:a→b in cryptosystem are as follows:
- The method h accepts the data content of subjective size as input and generates the data content digest of non-variable size as output.
- The method h is unidirectional as provided a, which is simple to calculate h(a)=b, nevertheless, provided b, which is difficult to calculate h–1(b)=a.
- Consider a and its computing is not feasible to discover a' with the end goal that a'≠a, but h(a')=h(a).

With the fast improvement of chaotic concept identified with cryptography, large amounts of key management protocols that uses chaos theory are analyzed strongly. Depending upon the number of users, the protocols that use chaos concept can be seen in three types: key agreement protocols for authentication with two-tier, three-tier and multi-tier architectures. As of late, the key management technique for authentication based on password for three-tier architecture utilizing modular exponentiation on an elliptic curve is broadly presented. In any case, these plans require substantial calculation weights and even latest, the exploration is still stay on key management scheme for authentication on three-tier architecture.

CHAOTIC MAPS

Chaos theory is a branch of mathematics focusing on the behavior of dynamical systems that are highly sensitive to initial conditions. 'Chaos' is an interdisciplinary theory stating that within the apparent randomness of chaotic complex systems, there are underlying patterns, constant feedback loops, repetition, self-similarity, fractals, self-organization, and reliance on programming at the initial point known as *sensitive dependence on initial conditions*.

Chaos Theory deals with nonlinear things that are effectively impossible to predict or control, like turbulence, weather, the stock market, our brain states, and so on

CHAOS Algorithm:

Let us suppose that the source is node A, and the destination be node B.
Node A is the source
Step 1: Select a private prime number i.e. 'm'
Step 2: ComputeT_m(x)=cos($m\ \cos^{-1}(x)$)
H_a=H ($D_a$ll$D_b$llT_m(x)llpw)
now considering the 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(1$D_a$ll1$D_b$ll1$D_b$llT_f(x)llpw)
Step 5: the values of m_b{H_{b^1},T_f(x)} are sent to the source.
Now, the values at the source
Compute H_{a^1}=H(1$D_a$ll1$D_b$llT_f(x)llpw)
If(H_{a^1}==H_{b^1})
Now computing T_m(T_f(x)) on the source and computing T_f(T_m(x))
Both the source and destination agrees on a session key.
Therefore,
T_m(T_f(x)=T_f(T_m(x)) Hence, this the algorithm for chaos.

Fig3: Encryption in CHAOS

This work presents the secure mutual authenticated key agreement protocol based on chaos in the integration of internet and MANET as shown in the fig4.In[9] The algorithm shows better performances compared to existing RSA based mutual authenticated key agreement protocol. In[10,11] The proposed

method's computational overhead is much less compared to existing approaches. Therefore chaos takes less time for key generation than RSA and ECC. Our work aims is to accomplish protective communication with security objective authentication as it is the best approach to accomplish trustworthiness and non-denial in information correspondence between MN in MANET and FN in internet.

4.RESULT ANALYSIS:

We analyze the results of the above algorithms using the Network Simulator tool(NS2) version NS2.34 and NS2.35 The performance is analyzed using the parameters such as delay, throughput, overhead and packet delivery ratio. The results are represented in the graphs.

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

Table1: Simulation parameters

1.Delay: The difference between the time at which the sender generated the packet and the time at which receiver receives the packet.
2.Overhead: Overhead defines how many packets are being used in data communication.
3.Packet Delivery Ratio: Packet delivery ratio defines ratio of packets being sent by the source and received at the destination.
4.Throughput: Throughput can be defined as number of bytes of data being sent.

Table2: values in 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	0.0564600680372853	0.11219283632110533	0.11245267722426608
2	0.0382344335777105	0.076099617934844252	0.076229538548960765
2.5	0.0321552220913555	0.064065345139461868	0.064151958990994393
3	0.0291218163480867	0.05805580874168631	0.058120769212332467
3.5	0.0272923329023728	0.054443046903101547	0.054495015345433342
4	0.0260786772718179	0.052036672344021907	0.052079979434391369
4.5	0.0252085803928539	0.05031623337326957	0.050353353783849919
5	0.0245606077335474	0.049027304145190256	0.049059784546113296
5.5	0.0240531623320071	0.048024803634462515	0.048053675139139426
6	0.0236456060108161	0.047219443225918839	0.047245427613709381

6.5	0.0233167326569850	0.046566184709774167	0.046589806911195498
7	0.0230400048621939	.046017002613041598	0.046038656325897445
7.5	0.0228052351897421	0.045918494366083959	0.045575744292281846
8	0.0226047468990562	0.045918494366083959	0.045174733977866054
8.5	0.0224309903804441	0.045918494366083959	0.044829858372125435
9	0.0222803534266345	0.045918494366083959	0.044528292217189874
9.5	0.0221447090557047	0.045918494366083959	0.044262298551153011

As show in above table, it is evident that the performance in terms of End to End delay is presented for RSA, ECC and Chaos algorithms.

The results are observed at different simulation time intervals. The simulation time is considered from 0 to 9.5 seconds. We can clearly observe that chaos having less delay compare to other algorithms.

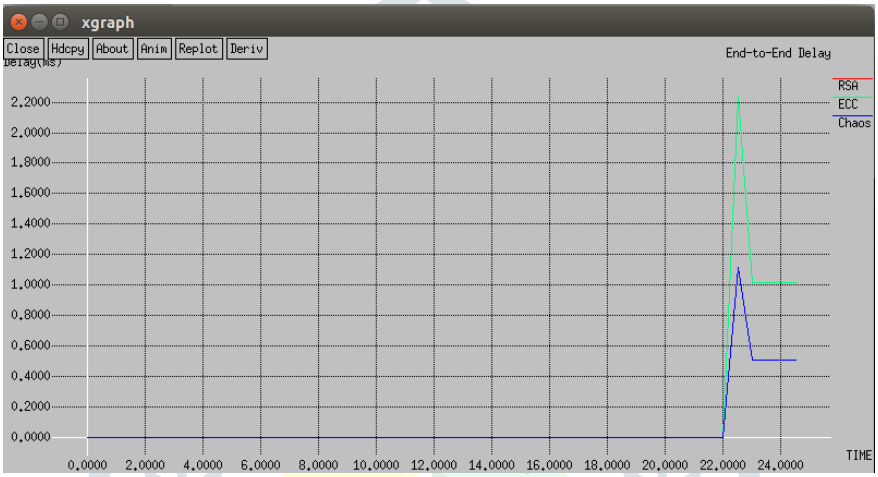

Fig 4: Graph on delay

End to end delay is the average time required by a data packet in order to reach the destination. In this graph we show the result of end to end delay of different algorithms. The simulation time in seconds is plotted in horizontal axis while the vertical axis shows end to end delay. We differentiate end to end delay using RSA,ECC and Chaos algorithms. Our proposed Chaos algorithm having less delay compare to RSA, ECC algorithm.

Table3: 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

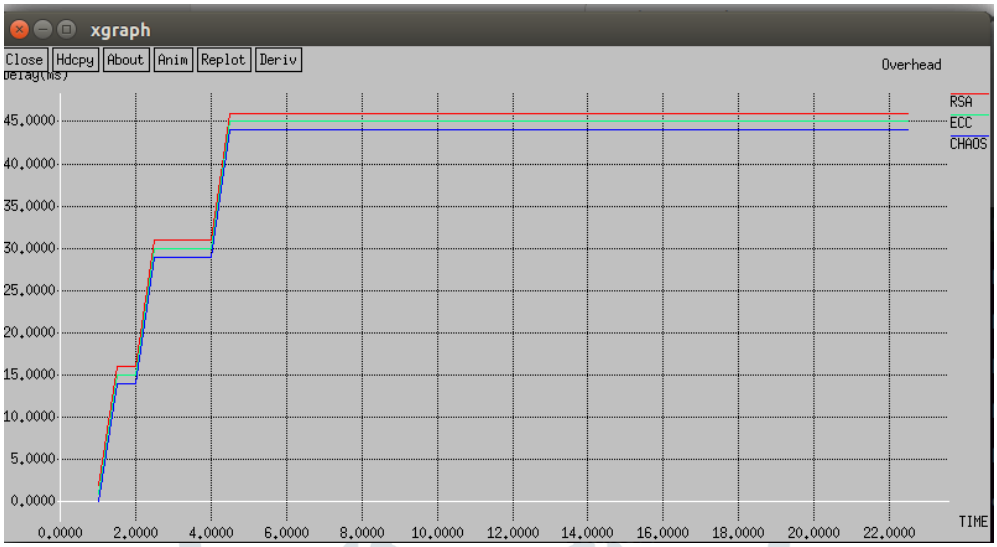

Fig 5: Graph on Overhead

The simulation time is considered from 1 to 9.5.The simulation time in seconds is plotted on horizontal axis whereas the overhead is shown along the vertical axis. From above graph we can observe that chaos has less overhead than RSA and ECC

Table4: 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

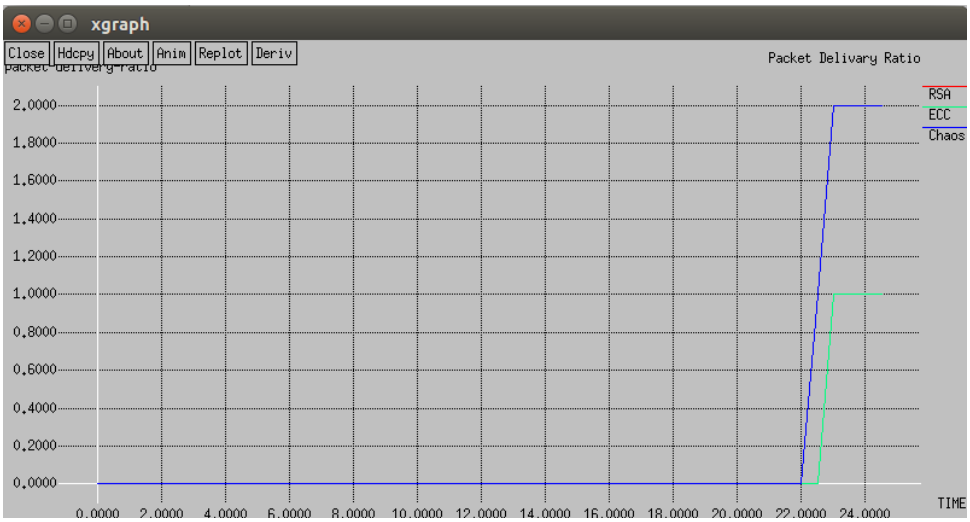

Fig 6:Graph on Packet Delivery Ratio

The simulation time is considered from 0 to 9.5.The results are observed at different time intervals.From graph we can observe that Packet delivery ratio of chaos is higher than RSA and ECC. Formula for calculating the packet delivery ratio is given by:

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

Table5: 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

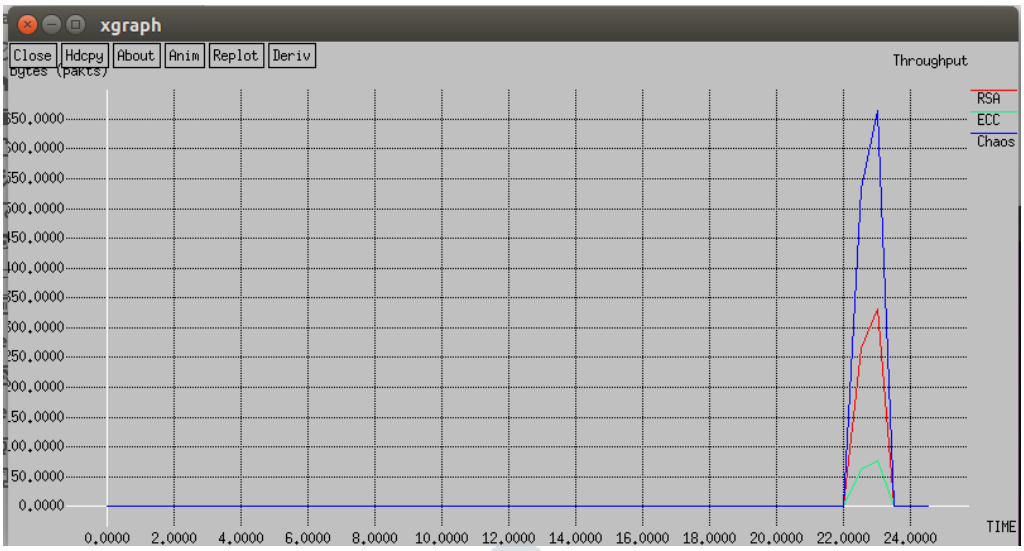

Fig 7: Graph on Throughput

The graph is plotted against the time along horizontal axis and throughput along the vertical axis. In above graph we can observe that chaos throughput is higher than RSA and ECC.

Table 5 presents the comparative analysis of Chaos with the RSA and ECC algorithms used for authentication[3]

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

Table 6: Performance comparison of RSA,ECC and CHAOS

5.CONCLUSION:

We have implemented the cryptographic algorithms RSA, ECC and Chaos maps based key agreement process for authentication of end nodes using the Network Simulator Tool (NS2) and evaluated the above algorithms with respect to delay, throughput, packet delivery ratio and overhead on the basis of 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 by enhancing the chaos maps for authentication based on biometric, digital signature and passwords.

REFERENCES:

[1] Jansma,N.and Arrendondo.B..2004 Performance Comparison of elliptic curve and RSA Digital Signatures.
[2] A Survey on Elliptic Curve Cryptography for Pervasive 2010
[3]V.B.Kute et al, ”A Software Comparison of RSA and ECC IJCSAVol2No1 April/May 2009
[4]V. Miller, "Use of elliptic curves in cryptography", Crypto 85, 1985.
[5] Vanstone, S.A., “Next generation security for wireless: elliptic curve cryptography”, Elsevier „Computers and Security“, Vol. 22, No. 5, July 2003, 412-415.
[6] Sun Microsystems Inc., “Speeding up Secure Web Transactions Using Elliptic Curve Cryptography”, see http://research.sun.com/projects/crypto
[7] W. Diffie and M. Hellman, ”New directions in cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, Nov. 1976, pp. 644- 654
[8] S. Blake-Wilson, D. Johnson, A. Menezes, Key agreement protocols and their security analysis," Proc. of the 6th IMA International Conference on Cryptography and Coding, 1997, pp.30(45)

[9] S.K. Ha_zul Islam, G.P. Biswas, \An improved pairing-free identity-based authenticated key agreement protocol based on ECC," International Conference on Communication Technol-ogy and System Design 2011, Procedia Engineering, vol. 30, 2012, pp. 499{507)
[10] L. Kocarev and Z. Tasev, ”Public-key encryption based on Chebyshev maps,” In Proceedings of the International Symposium on Circuits and Systems (ISCAS ’03), vol. 3, May 2003, pp. III-28-III-31.
[11] P. Bergamo, P. D’Arco, A. Santis, and L. Kocarev, ”Security of publickey cryptosystems based on Chebyshev polynomials,” IEEE Transactions on Circuits and Systems-I, vol. 52, no. 7, Jul. 2005, pp. 1382-1393
[12] S. Han, ”Security of a key agreement protocol based on chaotic maps,” Chaos, Solutions & Fractals, vol. 38, no. 3, Nov. 2008, pp. 764-768
[13] Atheeq, C. and Rabbani, M.M.A., 2017. Mutually authenticated key agreement protocol based on chaos theory in integration of internet and MANET. *International Journal of Computer Applications in Technology*, *56*(4), pp.309-318.
[14] Atheeq, C. and Rabbani, M., 2017. Secure Intelligence Algorithm for Data Transmission In Integrated Internet MANET. *International Journal of Computer Science & Applications*, *14*(2).
[15] Mohammad, A.A.K., Mirza, A. and Razzak, M.A., 2015. Reactive energy aware routing selection based on knapsack algorithm (RER-SK). In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2* (pp. 289-298). Springer, Cham.
[16] Mohammad, A.A.K., Mahmood, A.M. and Vemuru, S., 2019. Providing Security Towards the MANETs Based on Chaotic Maps and Its Performance. In *Microelectronics, Electromagnetics and Telecommunications* (pp. 145-152). Springer, Singapore.
[17] Atheeq, C. and Rabbani, M.M.A., 2016. Secure Data transmission in integrated internet MANETs based on effective trusted knowledge algorithm. *Indian Journal of Science and Technology*, *9*, p.47.