Performance Based Comparison Study of RSA and Chaotic Maps in MANET

[1]ZebaNaaz, [2]Kauser Fatima, [3]C.Atheeq
[12]Student, [3]Assistant Professor, CSE, DCET, India

Abstract

Mobile ad hoc networks consist of mobile nodes that communicate with one another through radio communication channel. As MANETs are dynamic nature, mobile nodes enters and leaves the MANETs region at any time so there is possibility that the malicious nodes may also involve in the communication process. So MANETs need a security mechanism to have secure communication from attackers as they are vulnerable to security attacks. Different security mechanisms have been designed to solve the security issues via cryptographic techniques. However, these security mechanisms should not have much overhead on network, particularly in constrained resource environment such as Mobile Ad hoc Networks. This work compares the performance overhead of cryptographic techniques such as Chaotic Maps based & RSA based key agreement in MANETs environment. Performance results shows that RSA is considered to be most used in cryptographic techniques but its overhead of time complexity is greater than the Chaotic Maps based cryptography technique. This overhead greatly impact on end to end delay in intended communication. However, Chaotic Maps based cryptography technique is well alternative to RSA with better performance in terms of minimum computational load and lesser key generation time.

Keywords: *MANETs, Security, Authentication, RSA, Chaotic Maps.*

I. INTRODUCTION

A mobile ad hoc network (MANET) is an infrastructure less network that consists of collection of autonomous nodes [1],which comprises of heterogeneous mobile devices as shown in Fig 1. As these mobile devices are interconnected openly, thereby exposing its networking infrastructure, which may lead to a problem arising in network security? The goals of security includes confidentiality, authentication, authorization, information integrity and non-repudiation. Focussing on authentication plays key role in providing security and also it provides a way to achieve other goals of security. It is essential to ensure the identity of the users for communication [2, 3].

When compared to the existing works [4, 5, 6], it is necessary to provide more secure data transmission from source node to destination node. So authentication is the technique which verifies that the user in its communication is trusted and not an imposter. The aim of mutual authentication in a network is to confirm two communicating users to authenticate each other and simultaneously agree on a common session key. In order to verify the identity of the remote user, whether it is active or a malicious intruder, complex cryptography based algorithms are required. Security goals can be achieved by using these Cryptographic techniques i.e., by the method of converting the plain text to cipher text with the help of suitable key. Thus in these techniques key management, distribution & maintenance play a vital role.

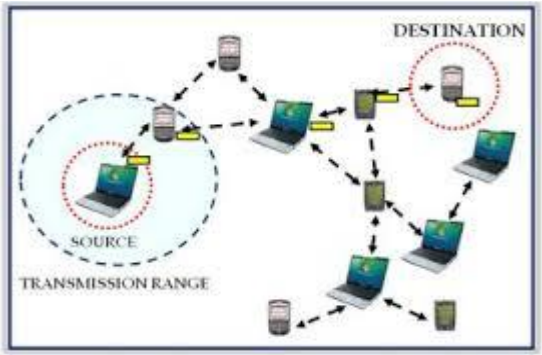

Fig 1: Mobile Ad hoc Network

In our work we are comparing complex cryptographic key agreement algorithms RSA, chaotic maps in static and dynamic network environments. We presented a systematic performance study on RSA and chaotic maps in static environment and MANETs environment with respect to computational overhead. Although there is lot of revenue work carried out by researchers to calculate the performance analysis of RSA with different key agreement algorithms. Our work includes a different key agreement algorithms i.e..Chaotic maps .this performance comparisons i.e., RSA and chaotic maps in static and dynamic environment is a novel aspect of our work

Importance of Security in our proposed algorithm,

- Our algorithm offers smaller key size, faster computation, memory and energy saving when compare to the key generation algorithm such as RSA ,therefore it is well suited for MANETs characteristics.
- We have used the security component based on Chaotic Maps Based Diffie Hellman problem for calculation.

II. CRYPTO GRAPHIC TECHNIQUES (RSA AND CHAOTIC MAP)

A. RSA

RSA is a asymmetric cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. It was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. It, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both keys can be used for encryption purpose; the opposite key from the one used to encrypt a message is used to decrypt it. This is the reason why RSA has become the most widely used asymmetric algorithm. It provides a method of assuring the confidentiality, authenticity, integrity of electronic communications and data storage.RSA strength lies in by deriving its security from the difficulty of factoring large integers that are the product of two large numbers Multiplying these two numbers is easy, but determining the original prime numbers from the total factoring is considered infeasible due to the time it would take even using today's super computers. Its major disadvantage is that it requires keys of at least 1024 bits for good security (versus 128 bits for symmetric-key algorithms), which makes it quite slow. The RSA method is based on some principles from number theory. The RSA algorithm works as follows.

1. Choose two large primes *p* and q (typically 1024 bits).

2. Compute $n=p*q$ and $z=(p-1)*(q-1)$.

3. Choose a number relatively prime to *z* and call it *d.*

4. Find e such that $e*d=1 \bmod z$.

With these parameters computed in advance, we are ready to begin encryption. Divide the plaintext (regarded as a bit string) into blocks, so that each plaintext message P, falls in the interval $0 \leq P<n$. Do that by grouping the plaintext into blocks of k bits, where k is the largest integer for which $2k<n$ is true.The fundamental concept beyond RSA is the examination that it is concept to determine three very big positive integers' e, d & n such that with modular exponentiation for all m:

$$(m^e)^d \equiv m \bmod(n)$$

Even knowing e & n or even m it can be exceedingly incredible to calculate d. Moreover, for some calculations it is convenient that the order of the two exponentiations can be changed & that this relation also implies

$$(m^d)^e \equiv m \bmod(n)$$

The key can be distributed between communicating entities in MANETs through specific authenticated key agreement protocols.

Some Disadvantages of RSA:

- The main disadvantage is its slow speed as it requires at least 1024 bits key for encryption process.
- It can't achieve authentication and confidentiality along with integrity in single step.
- If private keys of users are not available, it is vulnerable to impersonation(attack or attacker).

B. Chaotic Maps

Chaotic Maps, another and an efficient way to key agreement between communicating nodes. It is based on Chebyshev polynomials(Chaos theory). Our proposed work is based on Chebyshev polynomials (Chaos theory) which is the field of study in mathematics that deals with the behaviour of Dynamical systems that are highly sensitive to initial conditions, where Dynamical system is a system in which a function describes the time dependence of a point in a geometrical space.

Chebyshev polynomial is defined as follows [7]:

$\cos(n\theta)$could be written in the polynomial of $\cos(\theta)$

$$\cos(n\theta) = T_n * \cos(\theta) \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\cos\big((n+1)*\theta\big) = 2*\cos(n\theta)*\cos(\theta) - \cos\big((n-1)*\theta\big)$$

$$T_{n+1}\cos(\theta) = 2*T_n\cos(\theta)*\cos(\theta) - T_{n-1}\cos(\theta)$$

$$T_{n+1}(x) = 2*x*T_n(x) - T_{n-1}(x) \quad \ldots\ldots\ldots\ldots (2)$$

Equation 2 shows the chebyshev polynomial in $T_n(x)$ is a polynomial in 'X' degree 'n'. To achieve

authentication, one can uses semi group property of Chebyshev polynomials as below

$$T_n(x) = 2 * x * T_{n-1}(x) - T_{n-2}(x) \ldots\ldots\ldots\ldots(3), \quad n \geq 2$$

In our previous work [8,9], we uses the Chebyshev polynomial's semi group property to provide authentication between communicating entities, which shown in below equation.

$$T_n(x) = 2x * T_{n-1}(x) - T_{n-2}(x) * (\text{mod } N) \ldots(4), \quad n \geq 2$$

Where N is a big prime number and $X \in (-\infty, +\infty)$, in equation (4) it is incredible to compute the value of 'n' with given values of $T_n(x)$, X, N and this property known as Chaotic Maps-Based Discrete Logarithm problem.

The property "Chaotic Maps Based Diffie Hellman problem" state that in given equation (5) it is incredible to compute the value of $'T_{nm}(X)'$ with given values of $T_n(x)$, X, N&$T_m(X)$and this property known as Chaotic Maps-Based Discrete Logarithm problem.

$$T_m(T_n(X)) = T_n(T_m(X)) = T_{mn}(X) * (\text{mod } N) \ldots\ldots\ldots\ldots\ldots(5), n \geq 2$$

III. KEY MANAGEMENT IN PROPOSED SYSTEM USING CHAOS THEORY

The strength of the algorithm depends on how the sender and receiver agree on the secret key effectively. Our proposed mechanism is based on chaotic maps which use chebyshev polynomials in order to generate the secret key at both the ends and how they manage the key. By using chaos theory, the key is generated at sender as well as at receiver side and it is compared. This process of mutual authentication in our proposed protocol take minimum computational load when compared to the RSA based algorithm in the same environment.

Let us consider an example of Key exchange process between the sender and receiver in MANETs is as follows

The public data is:$(x,T_n(x))$and $(x,T_m(x))$

The private data is: n and m

Sender side:

Let $\theta = 73°$

$x=\cos\theta = \cos(73) = 0.2923717047$

Let n=17(senders private key)

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

=cos(17*73)

=-0.9455185756

$(x,T_n(x)) = (0.2923717047,-0.9455185756)$.

Therefore, sender sends $(x,T_n(x))$ as public key to receiver.

After receiving the public key of receiver i.e, $(x,T_m(x))$ sender performs following computation;

$T_{nm}(x) = T_n(T_m(x))$

=$T_n(0.9961946981)$=cos(n.cos^{-1}(0.9961946981)

=cos(17*4.999999995) =0.08715574274

Receiver side:

Let m=5(receivers private key)

$T_m(x)$ =cos(m.cos^{-1} x)

=cos(5*73)

=0.9961946981

$(x,T_m(x)) = (0.2923717047,0.9961946981)$

Therefore receiver sends $(x,T_m(x))$ as public key to sender.

Now, $T_{mn}(x) = T_m(T_n(x))$

=T_m(-0.9455185756)

=cos(m.cos^{-1}(-0.9455185756))

=cos(5*161)

=0.08715574274.

Therefore we conclude that $T_{nm}(x) = T_{mn}(x)$

From the above calculations it is clear that the sender and receiver in MANET acquires the same secret key by using the chaos theory and does the mutual authentication in an effective manner. This method increases the complexity for the intruder to crack the secret key. Thereby it is clear that the sender and receiver in MANET have secure data communication and protecting the data to be disclosed to the intruders.

IV. PERFORMANCE ANALYSIS:

A. Computational comparison between RSA and Chaos in static environment.

We have evaluated and compared the performance of RSA & Chaotic Maps in the identical environment i.e. in static environment with processor x64 based core 2.40 GHz processor,6 GB RAM, 911 GB Hard Disk Capacity. We varied the prime number size up to 1024 bits long, and evaluated the computational time of each algorithm. From our analysis it is very much clear that chaotic maps computational capacity is very much less when compared with RSA as shown in Fig 2.

Computational time affects the network performance by increasing the end to end delay, consumes energy, and occupies buffer space.

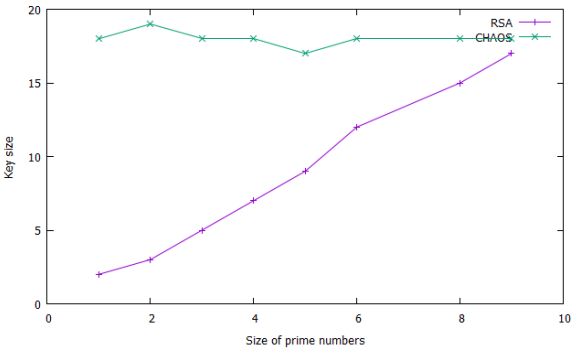

Fig 2: Bit Size Comparison between RSA and Chaotic Maps w.r.t Key size

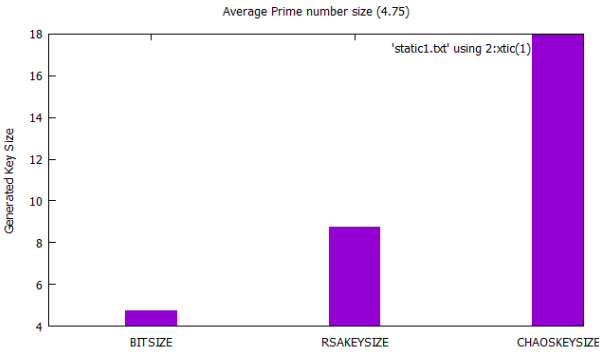

Fig 3: Key Size comparison between RSA and Chaotic Maps

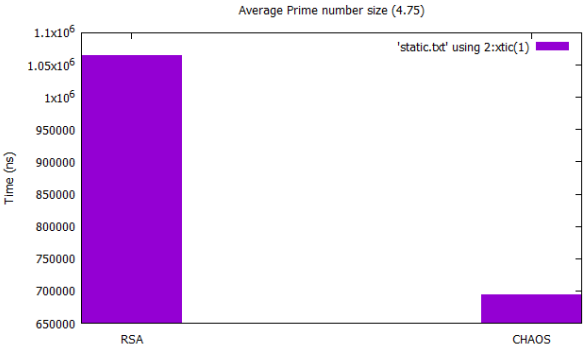

Fig 4:Comparison between RSA and Chaotic Maps in computational time.

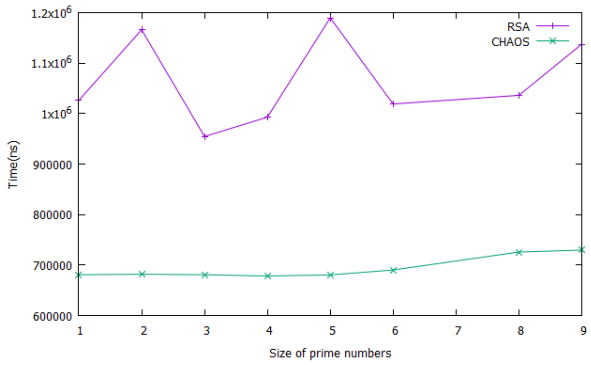

Fig 5: Comparison between RSA and Chaotic Maps in computational time w.r.t Bit Size

B. Computational comparison between RSA and Chaos in Dynamic environment(MANETS)

MANET is a type of wireless network with absence of central coordinator & thus network layer functionality must be carried out by nodes. It can acquire any type of topology(i.e., bus, star, ring etc.) as it supports mobility to its nodes. In case of stand-alone MANET, due to limited connectivity it has limited applications. MANET user can have better utilization of network resources only when it is connected to the Internet. MANETs are used in various research areas such as Green Communication, Machine-To-Machine Networks (M2M), Internet of Things (IOT), Device-to-Device (D2D) communication, disaster relief areas. However sending the packets/messages in this environment requires selection of better route/path which should be secure. Routing is the process responsible for deciding which output line an incoming packet should be transmitted on . Routing is the making of higher-level decision for packet switching from source to destination in the network.

While routing [8], packets on the communication channel over the network may be vulnerable to different attacks. False misbehaviour is one such attack in routing, in which malicious node sends false message to source as shown in Fig 6.

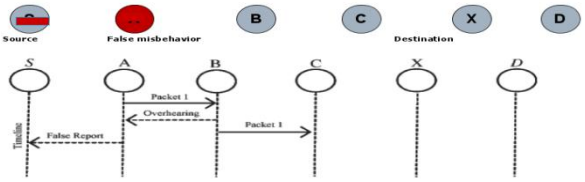

Fig 6: False Misbehaviour.

Node A sends back a misbehaviour report even node B forwarded the packet to C.

To overcome this attack encrypted acknowledgement is required which is achieved through our proposed chaos theory.

In this section we implement the RSA & Chaotic maps based key agreement between communicating entities above the underlying routing algorithms protocols such as AODV, AOMDV and DSR [7, 9, 10] and evaluated the performance of network with respect to end to end delay. As computational time of algorithm directly affect the end to end delay of communicating entities. In order to provide QoS in network or to achieve better performance delay is one of the most vital issue. Particularly in real time traffic like multimedia or voice transmission delay should be less other vise

communication traffic is unacceptable. It is clear from our evaluation in previous section, chaotic maps computational time is less than the RSA in particular static identical environment. Ad hoc On-Demand Distance Vector (**AODV**) basically works when one node wants to communicate with remote node i.e., the one which is not in range by establishing a route through intermediate nodes.

Ad hoc On-Demand Multipath Distance Vector (**AOMDV)** shares several characteristics with AODV. It is based on the distance vector concept and uses hop-by-hop routing approach. In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency.

Dynamic Source Routing (**DSR**) is a routing protocol for wireless mesh networks. It is similar to AODV in that it establishes a route on-demand when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

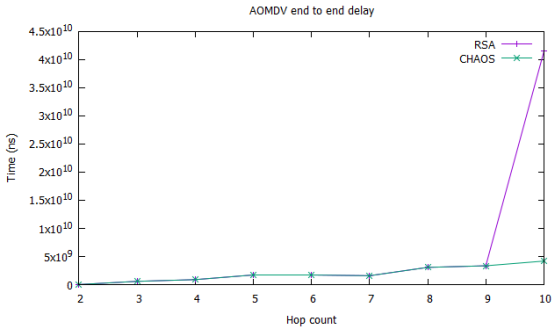

Fig7: AODMV end to end delay performance under RSA & Chaotic Map

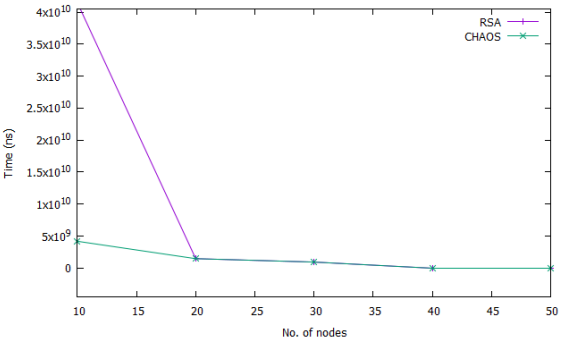

Fig 8 :AOMDV delay performance under RSA &Chaotic Map

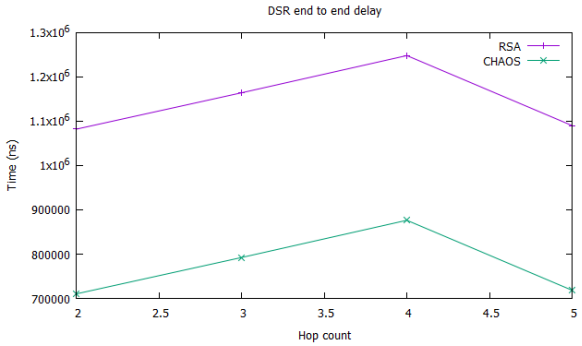

Fig 9 : DSR end to end delay performance under RSA & Chaotic Map

Table I-AODV End to End Delay Performance Under RSA & Chaotic Map

Hop Count	RSA Average Delay	CHAOS Average Delay
2	0.5664742864	0.5661024413
3	0.5664742864	0.5661024413
4	0.8781232864	0.8777514413
5	2.015432286	2.015060441
6	0.6188612864	0.6184894413
7	0.7505782864	0.7502064413
8	1.088627286	1.088255741
9	0.8964752864	0.8961034413
10	0.8407962864	0.8404244413

Table II -AODV Performance Under RSA & Chaotic Map

No. of nodes	RSA Average Delay	CHAOS Average Delay
10	840796286	840424441
20	1463628286	1463256441
30	935345286	934973441
40	7146286	6774441
50	7295286	6923441

MANETs is peer to peer networks, where nodes perform the task of routing. Thus the load of every node is high as it is doing the task of router, means it is receiving the packets, making the decision of packet based on protocol and forwarding the packet, which requires the time, energy and memory of the node to accomplish. However, providing security is most challenging task and much desirable due to its characteristic, but it must have minimum overhead in terms of network performance. Authentication is the easy convenient way to achieve security in MANETs. Thus one can provide authentication by the use of RSA and Chaotic Maps by authenticated key agreement between communicating entities. Thus we have evaluated the RSA & Chaotic Maps based key agreement in MANETs environment. It is clear from figures that the overhead of RSA is more than Chaotic maps key agreement protocol. Computational time of Chaotic Maps is less in comparison with RSA algorithm key

agreement. From our results we demonstrate that in order to provide security in MANETs Chaotic map is best suitable replacement of RSA. Security point of view, work [4] concluded that adversary cannot compute the chaotic maps authentication key in polynomial time

V. CONCLUSION

Security solutions are vulnerable in adhoc networks due to its open wireless medium and constrained resources. In order to solve the issue of security, authentication is needed between communicating entities by authenticated key agreement. Cryptographic techniques such as RSA and Chaotic Maps ensures authentication. In identical environment computational cost of RSA is greater than Chaotic Maps which directly reflects on end to end delay in MANETs, there by reflecting the network parameters such as energy, buffer & processor. We conclude that Chaotic Maps authenticated key agreement is best to replace RSA with enhancement of network performance with appropriate security. In Future we can strengthen the proposed security solutions for MANETs i.e., providing authentication in key agreement can be enhanced in several ways by making use of Passwords and Message digest(Hash functions) as a part of authentication process.

REFERENCES

[1] Kumar, R., Misra, M. and Sarje, A.K., 2007, December. An efficient gateway discovery in ad hoc networks for internet connectivity. In Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on (Vol. 4, pp. 275-282). IEEE.

[2] Wakikawa, R., 2002. Global connectivity for IPv6 mobile ad hoc networks. Internet-Draft, draft-wakikawa-manet-globalv6-02. txt.

[3] Manoharan, R. and Mohanalakshmie, S., 2011, June. A trust based gateway selection scheme for integration of MANET with Internet. In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on (pp. 543-548). IEEE.

[4] Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Analytical Model for Evaluating the Bottleneck Node in MANETs. Indian Journal of Science and Technology, 9(31).

[5] Atheeq, C. and Rabbani, M.M.A., 2016. Secure Data Transmission in Integrated Internet MANETs Based onEffective Trusted Knowledge Algorithm. Indian Journal of Science and Technology, 8(1).

[6] C.Atheeq, M.MunirahamedRabbani "Effective cluster key mechanism for integrated internet MANETs " International journal of applied engineering research vol.10 No.44, 2015

[7] Siddiqua, A., Sridevi, K. and Mohammed, A.A.K., 2015, January. Preventing black hole attacks in MANETs using secure knowledge algorithm. In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on (pp. 421-425). IEEE.

[8] Sana, A.B., Iqbal, F. and Mohammad, A.A.K., 2015, January. Quality of service routing for multipath manets. In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on (pp. 426-431). IEEE.

[9] 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 International Publishing..

[10] Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. Indian Journal of Science and Technology, 9(26).

[11] Mohammad, A.A.K. and Atheeq, C., MUTUAL AUTHENTICATED KEY AGREEMENT SCHEME FOR INTEGRATED INTERNET MANETS

[12] Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Energy Aware Routing For Manets Based On Current Processing State Of Nodes. Journal of Theoretical and Applied Information Technology, 91(2), p.340.