International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

Secure Data Transmission in MANET using Hybrid-RSA Algorithm

Arun Kumar S[1]
Computer Science & Engineering
Sapthagiri College of Engineering
Bangalore, India

Deepak N[2]
Computer Science & Engineering
Sapthagiri College of Engineering
Bangalore, India

R Rashika[3]
Computer Science & Engineering
Sapthagiri College of Engineering
Bangalore, India

***Abstract*— Network is a group of computers or servers connected which communicates over a wired and wireless network to exchange the information in a secure manner. In wired networks, there are firewalls and a secured gateway which prevents the malicious hackers from corrupting the data, but in the case of a wireless network like MANET (Mobile Ad-hoc Network) providing security is one of the biggest challenges. Security is an important factor in networks required to lessen the risk of unauthorized information disclosure, modification, and destruction. It is at the forefront of every conversation in all the sectors. Many network security threats like viruses, worms, hacker attacks, identity theft, and denial of service attacks etc. spread over the Internet. It is important to prevent the data from being infected by an intruder. One of the widely used techniques is encrypting the data by exchanging a common key which is used to decrypt it. By increasing the complexity of the key, security can be increased which in turn increases the time to encrypt and decrypt the data. To transmit the data efficiently, both speed and security play a vital role. In this paper, HRSA (Hybrid-RSA) algorithm has been proposed which increases the security of data during the transmission without having to compromise the speed of encryption and decryption and achieves strong privacy by increasing the complexity of the key.**

Keywords*— MANET, Cryptography, Security, Encryption, Decryption, Key Complexity, HRSA (Hybrid-RSA)

I. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is a collection of multiple mobile nodes connected wirelessly which are free to move randomly in any direction without having centralized and fixed infrastructure. MANET consists of open peer-to-peer, self-configuring, self-healing multi-hop networks where each node act as both host and a router. Since the nodes are mobile in nature, network topology changes rapidly. MANETs are more prone to attacks when compared to wired network but they are more advantageous which makes it as the finest medium in networks. The main advantages of MANETs are flexibility, low cost, and robustness. MANETs are widely used in military application. [8]

The ad hoc routing and data packet forwarding are the two main operations performed by the network-layer in MANETs. The routing messages are exchanged between the nodes and the routing table are maintained by MANET protocol. Based on the states in the routing table, the source forwards the data packets to the destination through intermediate nodes along an established path. The intermediate nodes are used to communicate with the destination, when it is not in the range of source node. These intermediate nodes can act as both host and a router. This dual role of nodes may cause packet drop and the intermediate node might transfer the data to the wrong destination. The routing and packet forwarding operations are more prone to malicious attacks. [9]

The architecture of MANET which evolves with time has the potential to resolve issues such as disconnection from the network. Since the data can take multiple paths, single point failure in MANETs are reduced. The MANETs have no fixed infrastructure which makes it more suitable for the applications such as environmental monitoring. On the contrary, MANETs have some drawbacks. One of biggest drawback is reduced data rates. The wave characteristics of wireless communication causes inefficient transmission of data when compared to wired networks. Routing packets between any pair of nodes is a challenging task due to its constant change in network topology. [10]

MANETs are used to provide security services such as confidentiality, authentication, integrity, availability, and anonymity. Both authorized network users and malicious hackers can access the wireless channel. As a result, providing protection is a challenge from security design perspective. Proactive and Reactive are the two approaches used to secure MANETs. In proactive approach, various cryptographic techniques are used to prevent security threats. On the other hand, the reactive approach detects threats and react accordingly. These two approaches have its own advantages and are suitable for addressing different issues. [11]

Security has become a primary concern when setting up a network due to the high rate threat of malicious hackers who try to harm as many networks as possible. It has been one of the active research topics in wireless networks. In MANET, many types of security attacks can occur which disturb the operation of data transmission. To intercept the unauthorized users from corrupting and stealing the data, several encryptions and decryption techniques have evolved over time. In cryptography, it is an important process that is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

been carried out before communication happens between two parties. In this work, the security issues and existing solutions in MANET which has not been widely addressed has been examined. We are focusing on secure transmission of data using HRSA algorithm in MANET. [11]

II. LITERATURE SURVEY

A Secure Intrusion Detection system is implemented using public RSA algorithm [1]. This system is used to identify the presence of an intruder in the network. The public and private keys are generated using RSA algorithm which is made available to all the nodes in the network. The keys being sent only to the nodes in the network, the intruder cannot obtain the data being transmitted since it doesn't have a public and private key. The drawback of this approach is that the intruder can obtain the keys as no complexity is involved in the key generation.

The RSA algorithm [2] uses more than two prime numbers to improve the security. The time required to encrypt and decrypt the input messages are reduced. Two public keys are generated which are sent separately. This makes the attacker difficult to obtain the keys and unable to decrypt the message. This algorithm is complex which increases the security level. However, generating and transmitting two public keys occupies more bandwidth. The loss of one key makes it impossible to decrypt the input message which is in turn not suitable for MANET since the nodes are mobile.

An enhanced RSA cryptographic algorithm [3] has been introduced to transmit the messages in a secure manner. Four prime numbers are used in the place of two. The complexity of the key is increased which increases the security level. The drawback is that the time taken to encrypt and decrypt the message is very large when compared to the traditional algorithm. As a result, the proposed algorithm lacks in the speed of encryption and decryption of data.

In this RSA algorithm [4], a new concept is introduced where the speed of the algorithm is increased, and offline storage is used. Three prime numbers are used which increases the value of modulus n. The key parameters of the algorithm are stored in the database before the algorithm starts. The index of the private and public key is used at the time of encryption and decryption which speeds up the algorithm. The drawback back of this approach is that an intruder can easily hack the database.

The new approach [5] uses two public keys which are sent separately. The attacker won't be aware of these keys and cannot hack the data. This approach consumes more bandwidth as two keys are transmitted for each message which decreases the speed of transmission. To transmit the data efficiently, both speed and security play an important role. Therefore, this approach can be used only in a scenario where high security is required and not in the system which requires high speed.

The ESRKGS (Enhanced and Security RSA Key Generation Scheme) algorithm [6] reduces the brute force attacks that occur in RSA. The encryption and decryption time is reduced when compared to other modified RSA algorithm which uses four prime numbers. Based on the value of N, the calculation of public and private key is performed. The key complexity is increased which makes the attacker hard to find the prime number from the product of prime numbers.

The AODV protocol is used to implement the RSA algorithm where the complexity of the algorithm is reduced. The performance of modified AODV [7] protocol is compared with RSA digital signature. This algorithm utilizes minimum CPU resources, minimum memory and consumes less energy as compared to RSA digital signature. This RSA digital signature is designed to implement in MANET.

III. METHODOLOGY

The proposed HRSA algorithm emphasis on reducing the encryption and decryption time. The traditional RSA uses two prime numbers which can be easily found using factoring methods thereby making it less efficient. Here the proposed algorithm uses the product of four prime numbers which increases the key size. This algorithm is more efficient as the user can choose the rate of complexity. The private and public keys are multiplied by the user chosen complexity number. With the knowledge of the product of prime numbers, the hacker cannot find all the prime numbers and the private key. The encryption process is performed using public key, but the decryption process cannot be performed using private key alone. The complexity number is required to decrypt the message which makes it more efficient when compared to other modified RSA algorithms.

Algorithm for Key Generation

These are the following steps to generate public and private keys-

1. Construct a set which contains prime numbers within the range of ST.
2. Choose any four prime numbers A, B, C, D from the set ST.
3. Choose a key complexity number 'q'
4. Compute N (product of prime numbers)
   $N=A * B * C * D$
5. Compute $\Phi(N)$,
   $\Phi(N)=(A-1) * (B-1) * (C-1) * (D-1)$
6. Calculate X (public key), such that
   $GCD (X, \Phi(N)) =1$
   where $2 < X < \Phi(N)$ and X is multiplied by q after GCD operation
7. Calculate Y (private key), such that
   $Y * X \bmod \Phi(N) =1$
   where $1 < Y < N$ and Y is multiplied by q after modulus operation
8. Calculate KGT (Key Generation Time)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

Algorithm for Encryption process

These are the following steps to encrypt the PT (Plain Text)-

1. Encryption of a message is performed character by character.
2. Convert the message into their respective ASCII values that has to be encrypted.
3. Compute K to reduce the encryption time,
   $K = X/q$
4. Calculate CT1 (Cipher text),
   $CT1 = (PT1 * K) \bmod N$
5. Calculate ET (Encryption Time)

Algorithm for Decryption process

These are the following steps to decrypt the CT2-

1. If CT1 is equal to CT2 then,
   i. Compute J to reduce the decryption time,
      $J = J/q$
   ii. Perform Decryption operation to compute PT2,
      $PT2 = (CT2 * J) \bmod N$
   iii. Convert the ASCII values back to their original form
   iv. Calculate DT (Decryption Time)
   v. Calculate total time, T=KGT + ET + DT
2. If CT1 is not equal to CT2 then,
   Print error message "Cipher text do not match"

IV. COMPARISON RESULTS AND DISCUSSION

PERFORMANCE ANALYSIS

The performance of existing modified RSA algorithms is tested. By varying the length of input in bits, the performance analysis is performed. The performance of proposed HRSA algorithm is measured by comparing the key generation time, encryption time and decryption time with traditional RSA and other modified RSA algorithms which are depicted in the below table.

Table 1: Key Generation time (in ms)

Length of p, q, r and s (bits)	RSA1	RSA2	ESRKGS	Modified RSA	HRSA
100	72	110	113	137	143
128	92	144	165	178	197
256	133	216	237	242	253
512	352	313	389	421	417
1024	889	922	1168	1328	1290
2048	4315	7471	11,164	11256	14089
4096	91,542	93,899	181,811	720,600	234,156

Table 2: Encryption time (in ms)

Length of p, q, r and s (bits)	RSA1	RSA2	ESRKGS	Modified RSA	HRSA
100	1	2	1.5	1.7	0.4
128	1.1	2.5	2	2.9	2.3
256	1	4	3	5	3.7
512	3	21	16	24	13
1024	21	170	105	121.07	83
2048	183	1393	784	968.6	194
4096	1380	10,907	6620	7749	2107

Table 3: Decryption time (in ms)

Length of p, q, r and s (bits)	RSA1	RSA2	ESRKGS	Modified RSA	HRSA
100	1	1.7	1.3	1.8	0.3
128	1.1	2.2	2	2.1	5.7
256	1.1	3	2	4	3.4
512	3	23	16	67	19
1024	22	169	106	271.25	111
2048	169	1379	745	1085	475
4096	1381	10,957	6647	2170	4876

In table 1, we can observe that the key generation time of HRSA algorithm is greater than RSA1, RSA2, ESRKGS and Modified RSA. This justifies the fact that the complexity is introduced by increasing the key size which increases the strength of the algorithm. In table 2, the encryption time is greater than the traditional RSA but less than the algorithm which uses four primes such as RSA2, ESRKGS and modified RSA algorithm. In table 3, the decryption time varies according to the complexity chosen by the sender.

SECURITY ANALYSIS

In RSA algorithm there are various possible attacks that may occur in the system. The key generation, encryption, decryption time are analysed and compared with existing modified RSA algorithms which is depicted in the below graph.

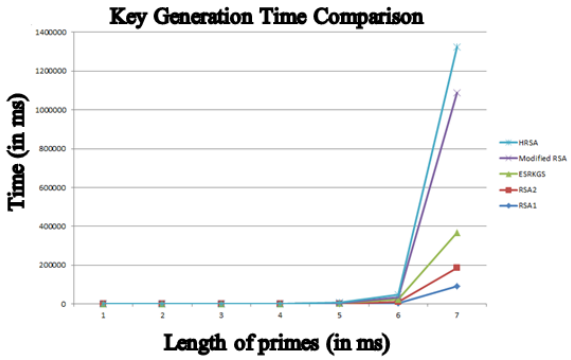

Figure 1: Key Generation Time Comparison

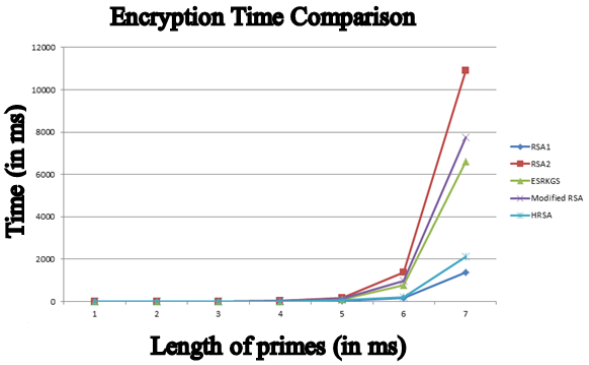

Figure 2: Encryption Time Comparison

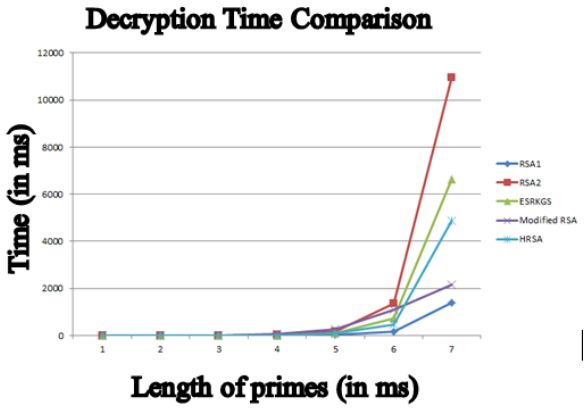

Figure 3: Decryption Time Comparison

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

The key generation time of existing RSA and proposed RSA are compared in Figure-1. We can observe that, the time taken to generate a public key and private key is more compared to others, because the user will choose the rate of complexity for public and private keys. In encryption and decryption, the time taken to complete cryptanalysis is compared which is shown in Figure-2 and Figure-3. By analysing the graph, we can notice that in HRSA encryption time is higher than traditional RSA and lower than the modified RSA. However, in Figure-3, the decryption time is higher than the RSA1 and Modified RSA but is lesser than the RSA2 and ESRKGS. Hence the decryption time is not constantly reducing, it depends on key complexity.

SCREEN SHOTS

The proposed HRSA algorithm is implemented using GUI application. The implementation of HRSA algorithm is shown in snapshots.

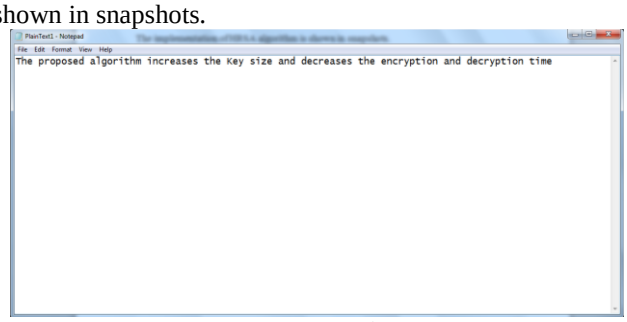

Figure 4: Plain Text File before Encryption

In Figure 4, the input message that has to be send to the receiver is stored in a file. This file is uploaded and encryption is performed on the text by the sender.

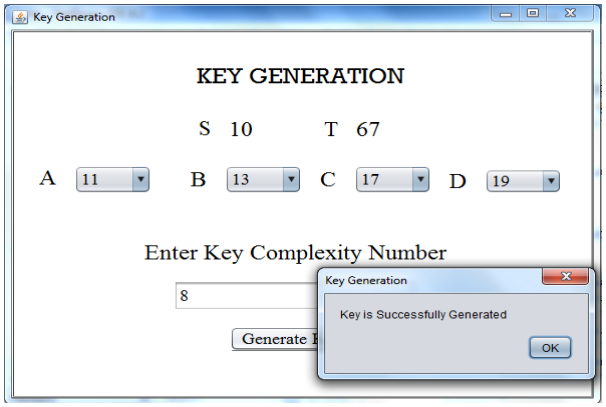

Figure 5: Key Generation

In Figure-5, the key generation technique is demonstrated, and has attempted to allow the user to choose a complexity number based on which the public and private keys are computed.

In Figure-6 and Figure-8, the encryption and decryption techniques are demonstrated.

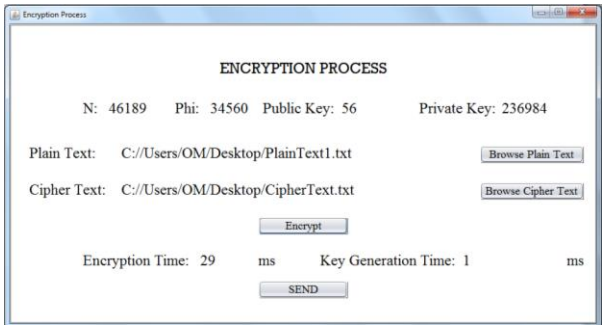

Figure 6: Encryption of Plain Text

In Figure-6, the sender uploads the plain text file and selects a file in which the plaintext must be encrypted and stored. Once the path is set, the sender will encrypt the input message and send the file along with the private key to the receiver as shown in Figure-6.

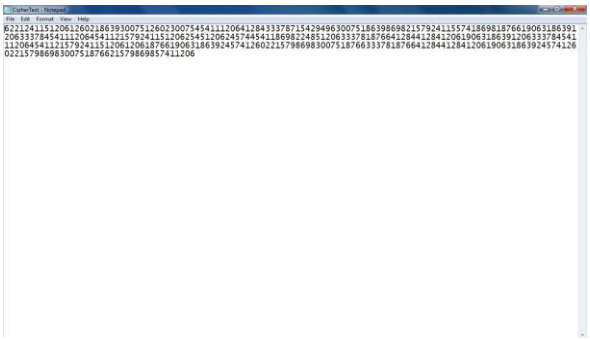

Figure 7: Cipher Text File after Encryption

Once the encryption is performed the encrypted message is stored in a separate text file which is indicated in the Figure-7. This cipher text file is sent to the receiver. Using the private key shared, the receiver will decrypt the content in this file to obtain the original message.

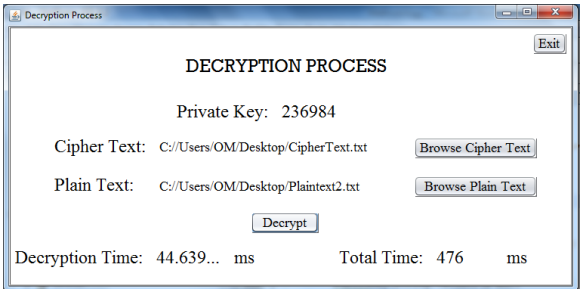

Figure 8: Decryption of Cipher Text

On the other hand, the receiver receives the cipher text file. The receiver uploads the cipher text file and selects the path to store the plain text. Then, the receiver will decrypt the cipher text file using his private key as shown in Figure-8.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 06, June-2018

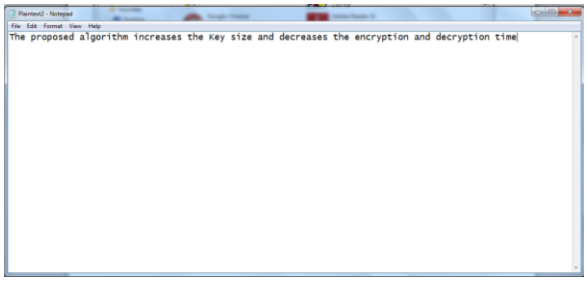

Figure 9: Plain Text File after Decryption

The message received from the sender is decrypted. The Figure-9 indicates that the plain text before encryption and the plain text after encryption match. As a result, successful communication has occurred between the sender and the receiver.

CONCLUSION

In this paper, a Hybrid-RSA algorithm called HRSA is proposed. Here, four prime numbers are used instead of two, thereby making it difficult for an intruder to extract the prime numbers from the value of N which are subsequently required to find the private key. Using key complexity number and N, the public and private keys are computed. With the knowledge of the private key, an intruder cannot decrypt the original message unless he is aware of the key complexity number which increases the strength of the algorithm. The encryption and decryption time is significantly reduced when compared to existing modified RSA algorithms, but greater than traditional RSA algorithm. The performance of the algorithm is quantified by comparing the key generation time, encryption time, and decryption time with other RSA algorithms. From the analysis made, we can conclude that the proposed HRSA algorithm guarantees high security and speed of the algorithm is also increased.

REFERENCES:

[1] Sankaranarayanan.S, Murugaboopathi.G, “Secure Intrusion Detection System in Mobile Ad Hoc Networks using RSA Algorithm”, Second International Conference on Recent Trends and Challenges in Computational Models, 2017

[2] Shikha Mathur, Deepika Gupta, Vishal Goa, Manoj Kuri, “Analysis and design of Enhanced RSA Algorithm to improve the security”, 3rd IEEE International Conference on Computational Intelligence and Communication Technology, 2017

[3] Bello Musa Yakubu, Mr. Pankaj Chajera, Dr. Ahmed Baita Garko, “Advanced Secure method for data transmission in MANET using RSA algorithm”, International Journal of Advanced Technology of Engineering and Science, Vol.no.3, September 2015

[4] Ms. Ritu Patidar, Mrs. Rupali Bhartiya, “Implementation of Modified RSA Cryptosystem Based on Offline Storage and Prime Number”, IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014

[5] Amare Anagaw Ayele, Dr. Vuda Sreenivasarao, “A Modified RSA Encryption Technique Based on Multiple public keys”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2013

[6] M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya, “An Enhanced and Secured RSA Key Generation Scheme”, Department of Information Technology, Anna University, Chennai, 2014, Elsevier

[7] Spinder Kaur, Harpreet Kaur, “Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature”, International Journal for Advance Research in Engineering and Technology, Volume 3, Issue V, May 2015

[8] Karamjeet Singh, Chakshu Goel, “Using MD5 AND RSA Algorithm Improve Security in MANETs Systems”, International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue 2 , June 2014

[9] Sandeep Kumar, Monika Goyal, Deepak Goyal, Ramesh C. Poonia, “Routing Protocols and Security Issues in MANET”, International Conference on Infocom Technologies and Unmanned Systems (ICTUS'2017), Dubai, Dec 2017

[10] Sampada Ganesh Datey, Taha Ansari, “Mobile Ad-Hoc Networks Its Advantages and Challenges”, International Journal of Electrical and Electronics Research, Vol. 3, Issue 2, pp: (491-496), June 2015

[11] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communications, Feb 2004