Secure Transmission in Wireless Sensor Network using AODV Routing Protocol

Nidhi Chhajed
Research Scholar, CSE Department
Sanghvi Institute of Management and Science,
Indore (M.P), India
nidhichhajed31@gmail.com

Mayank Kumar Sharma
Assistant Professor, CSE Department
Sanghvi Institute of Management and Science,
Indore (M.P), India
mayank.sharma@sims-indore.com

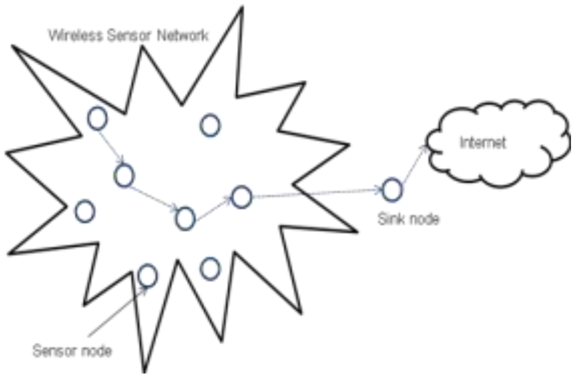
Abstract**—** Wireless sensor networks (WSN) rely on wireless connections between sensor nodes, which mean lesser amount of security & higher rate of disconnections between nodes. In this contrast WSN is under the research and many researchers provide the various techniques to implement security in WSN. In this work, we proposed hybrid algorithm for enhancement of security during transmission with modified RSA algorithm applied in AODV routing protocol. This scheme is useful for increasing security of routing protocol while delivering the data and by reducing packet delivery ratio.

Keywords- Wireless sensor network (WSN), Public Key Infrastructure (PKI), RSA, Diffie Hellman, Security mechanism , AODV, Network Simulator 2 (NS-2).

*****

I. Introduction

Wireless Sensor Networks [1,2] consist of specialized nodes, called sensor nodes. These nodes have transducer with a communication infrastructure that uses a monitoring device for recording physical or environmental conditions. These special nodes are equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from a battery.



.

Figure 1: Wireless Sensor Network

Apart from the above mentioned applications, WSNs also have applications in disaster areas, military operations, surveillance, and automobile applications [3]. The WSNs can be used to analyze the current battle situation in military based applications and providing information to the soldiers regarding the weapons, vehicles etc. [4]. WSNs are used to build network in order to gather the data about the states of a vehicle and driver and supply it to the user in automobile industry. Despite of all the advantages and important applications of Wireless Sensor Networks, there are some issues and challenges which have to be dealt with. The most important challenge is security of wireless sensor networks [5].

There are many characteristics of wireless network which makes it different from wired networks. These characteristics are self organization that means they are capable of making decisions by themselves; low cost makes it inexpensive for deployment; flexible in adding wireless nodes in the network; small size so that they can be deployed in less area; disposable means they can’t be charged once get discharged and many more.

Because of its usage in various crucial and sensitive applications security [6] becomes very important, increases need of security mechanism during transmission and reception of data packets so that only intended user can receive the information and no outsides can read the information sent. There are many security mechanisms provided by various persons to achieve security in wireless nodes. The proposed work also describes a new way of data transmission securely in wireless nodes during transmission using a hybrid algorithm which combines two very popular algorithms RSA and Diffie Hellman. The hybrid algorithm is applied to data packet and transmitted using AODV as routing protocol. In this paper, we proposed a novel security mechanism in order to achieve more security. Section 2 describes various other security mechanisms for wired network, wireless sensor network and MANET. Section 3 contains proposed scheme for providing security in the network with flowchart of proposed work. Section 4 compares the result of normal AODV routing protocol without applying any security mechanism and AODV protocol after applying the proposed secure mechanism. Section 5 concludes the paper.

II. Literature Review

Firstly we discuss the approach given by Chungen Xu and Yanhong Ge. They introduced a Public Key Infrastructure(PKI) scheme [7] which solves the problem of security in wireless sensor networks by the use of public key cryptography thereby ensuring authenticity. This scheme uses RSA algorithm with the process of simplified SSL handshake. The simplified handshake is used to setup a secure key between any two sensors in the network as the one in SSL. A handshake between each pair of sensors is done in order to transfer the data from one sensor node to the other. RSA is composed of two phases, the first phase comprises the sensor to base station handshake in which the base station and a given sensor node unite a session key to safeguard end to end link between them, this handshake is protected and authenticated by means of the public key of the base station. The second phase is the make use of this session key for data encryption to ensure confidentiality and ensuring the veracity of the exchanged data using the MAC joined to each packet. One of the major drawbacks of this scheme is that it is very defenceless against capture attacks to which the sensors are very often out and exposed. The second problem in this method is that the handshaking is not energy saving and it may consume lot of network resources if the trusted third party is far from the pair of nodes.

Another technique to increase the security was given by Shilpi Gupta and Jaya Sharma [8]. They introduced hybrid encryption algorithm based on RSA and Diffie-Hellman. This method follows the same steps of RSA till the generation of private key (E). After the generation of the private key (E) this method generates 3 random prime constants namely R, S, G. After taking (generating) the three prime constants two public numbers namely X and Y are calculated with the help of public, private key and R. After this step session key is generated with the respective formulas by taking the help of R, S, G, X, Y which is further used to encrypt the plain text. One of the major drawbacks of this algorithm is that till the RSA algorithm is being used the message length should be less than the bit length otherwise it would be of no use also it is quite complex because of extra operations involved in it like generation of session key, XOR operation to generate cipher text. Due to the extra operations involved memory consumed would be more thereby exploiting CPU's bandwidth.

Ishwarya M and Dr.Ramesh Kumar introduced a method called Privacy Preserving Updates for Anonymous and Confidential Databases Using RSA Algorithm [9]. The privacy is a chief concern in several applications such as data mining, medical research, intelligence research, cloud computing techniques etc. This paper introduces a new concept to implement a real world unspecified database which improvises the secure competent system for guard of data by restricting the access to data yet by the administrator thus maintaining the privacy of individual patient. This technique applies in medical field in order to amplify the security and efficiency. The limitation of this algorithm is it takes much time to compute the result.

Thanuja R. Dilip Kumar S. Proposed a new approach to Diffie-Hellman key exchange algorithm [10]. In the proposed approach the private key is generated using pseudo-random number mechanism thereby restricting the factors that are known to the program. One of the major drawbacks of this technique is that once the prime numbers are known it is easy to apply hit and trial method to find the key which will lead to the breaking up of the technique and thus the algorithm is compromised.

B. Persis Urbana Ivy, Purshotam Mandiwa, Mukesh Kumar[11] proposed a modified RSA cryptosystem based on 'n' prime numbers. In this approach instead of taking 2 prime numbers which is done in conventional RSA algorithm , here 'n' prime numbers are taken, value of n>2. The main purpose of this approach is to make it difficult to factorise the large prime numbers. This makes it very hard to break the algorithm. In this method four prime numbers were used. On security constraint this method is quite secure but again the major drawback is that if the prime numbers are known the algorithm can be broken, also the calculation of public and private key involves much CPU bandwidth as compared to conventional RSA algorithm.

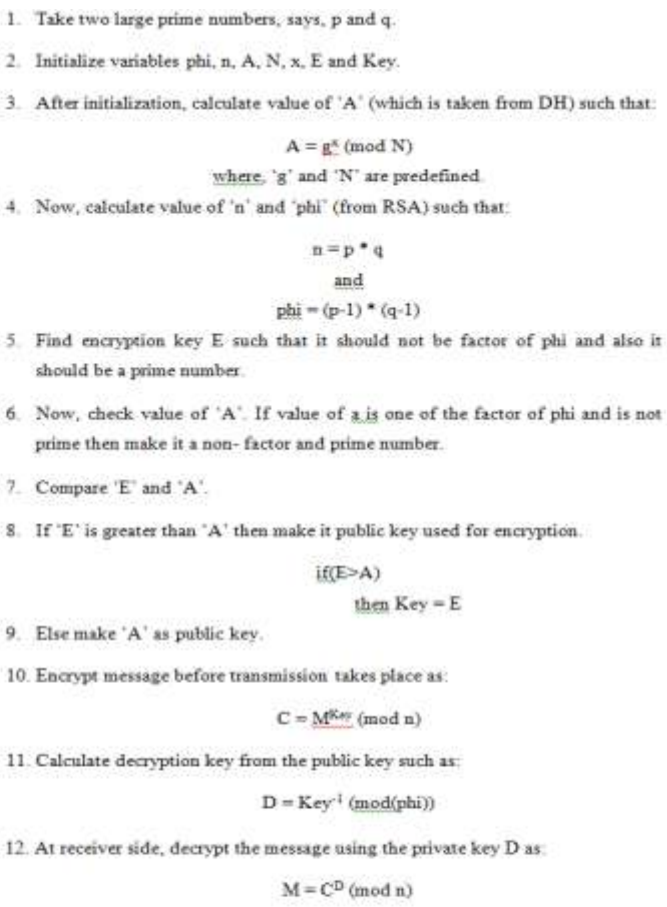
Sakthi Nathiarasan A, Yuvaraj K. [12] introduced a novel technique to securely exchange key by applying mathematical approach to Diffie-Hellman key exchange algorithm. In this technique man in the middle attack is rectified along with reply attacks by introducing simple mathematical techniques and timestamps. In the initial steps of the proposed technique the first recipient chooses a prime number and calculates (obtains) the key which is sent to the second recipient along with timestamp. On the other side this key and time stamp is verified and then accepted. This algorithm ensures that man in the middle attack and reply attacks are prevented. The major drawback of this algorithm is that the additional overload has to be handled on both the sides in the form of timestamp in order to avoid the reply attacks which makes this algorithm slow.

III. PROPOSED ALGORITHM

In a wireless network, threat of steeling data is very high. As data moves openly in the network and flow to and from in the network, thus becomes very easy to be hacked by malicious node. Transmitting data from source to destination in a secure way becomes very important for some applications. While sending information through AODV protocol there is no mechanism of providing security is given, which makes it easy to capture data packets by intermediate nodes. Therefore, in the proposed work, a new secure and improved algorithm is developed. In this work, a combination of two popular cryptographic algorithms, RSA and Diffie Hellman (DH) algorithm is used for encrypting data packets. Data packets are sent and received in an encrypted form so that only the source node and the destination node can read the encrypted data packet. All other nodes which do not have the key can't read the information. Only the intended receiver is allowed to access the information.

In the proposed work for providing security mechanism to wireless sensor networks of a new technique of transmitting packets using AODV protocol is shown. In this mechanism, firstly, the packet is encrypted in the sender side and then transmits the packet over the network. The packet contains information such as routing protocol, destination address etc. which is useful for correct recipient of packet at correct location. When the receiver receives the packet, it is in encrypted form which can be decrypted by only the other key which is present at receiver node previously. After decrypting the packet, the original message can be read from that packet. Thus, this will increase security of network during data transmission.

IV. Steps Of Proposed Algorithm



1. Take two large prime numbers, says, p and q.
2. Initialize variables phi, n, A, N, x, E and Key.
3. After initialization, calculate value of 'A' (which is taken from DH) such that:

$$A = g^{x} \pmod N$$

where, 'g' and 'N' are predefined

4. Now, calculate value of 'n' and 'phi' (from RSA) such that:

$$n = p * q$$

and

$$phi = (p-1) * (q-1)$$

5. Find encryption key E such that it should not be factor of phi and also it should be a prime number.
6. Now, check value of 'A'. If value of a is one of the factor of phi and is not prime then make it a non- factor and prime number.
7. Compare 'E' and 'A'.
8. If 'E' is greater than 'A' then make it public key used for encryption.

if(E>A)
then Key = E

9. Else make 'A' as public key.
10. Encrypt message before transmission takes place as:

$$C = M^{Key} \pmod n$$

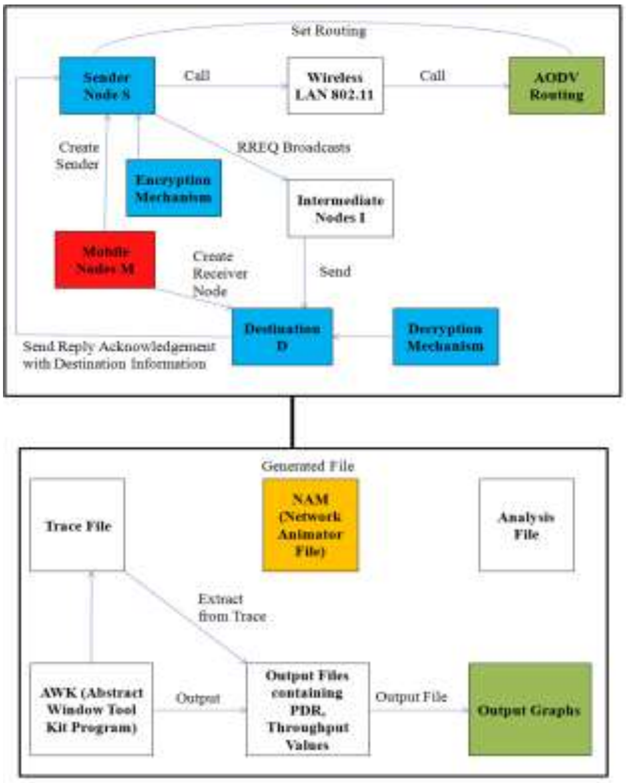
11. Calculate decryption key from the public key such as:

$$D = Key^{-1} \pmod{phi}$$

12. At receiver side, decrypt the message using the private key D as:

$$M = C^{D} \pmod n$$

V. Flowchart Of Proposed Algorithm



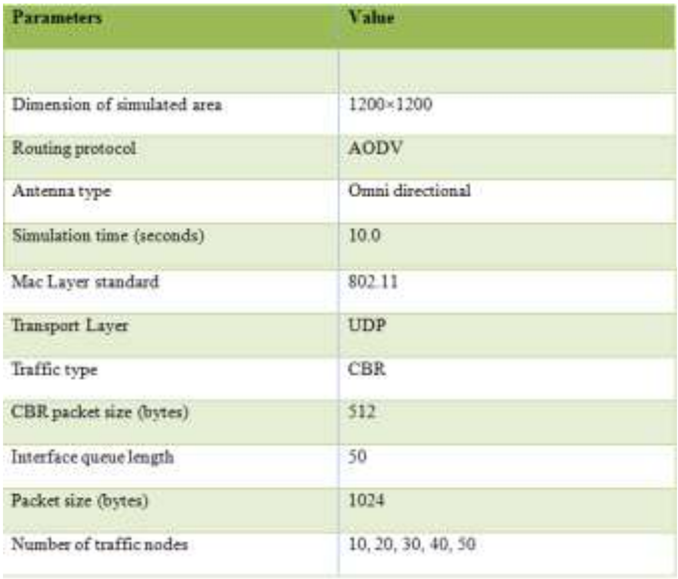
VI. Simulation and Simulation Strategy

Actual implementation takes place in this phase. Implementation strategy explains actual code of the designed algorithm. It is method of converting psudocode into executable form. This phase contains implementation of the desired security algorithm. As described before, for packet encryption and decryption a new hybrid security algorithm is designed by combining two most popular security algorithms named RSA and diffie hellman. The new algorithm provides better security for wireless nodes as the data is sent in the network in an encrypted form rather than being sent it directly. Thus, in this work, a secure way of transmitting the data using AODV as routing protocol is proposed.

SIMULATION TOOL

Simulation tool used for developing project is Network Simulator version 2.35. This tool helps in creating and developing different-2 network scenarios in a very easy and convenient way. NS-2 supports various routing protocols both for wired and wireless networks.

SIMULATION PARAMETERS



Parameters	Value
Dimension of simulated area	1200×1200
Routing protocol	AODV
Antenna type	Omni directional
Simulation time (seconds)	10.0
Mac Layer standard	802.11
Transport Layer	UDP
Traffic type	CBR
CBR packet size (bytes)	512
Interface queue length	50
Packet size (bytes)	1024
Number of traffic nodes	10, 20, 30, 40, 50

Table 6.1: Network Simulator Parameters for Simulation

VII. Result Analysis

NETWORK ANIMATOR

Here we shows figure 7.1 network animator graph genrated by TCL (tool command language). We have taken scenario with 50 mobile node considering AODV as routing protocol by applying security during transmitting and receiving of data packets.

The node who wants to initiate the communication will broadcast route request packet for the first time to find destination. After getting route to destination, sender transmit the data in encrypted form by making transmission secure which also increases the performance of the network. After receiving the data, the destination node apply decryption key and converts encrypted message into original one. Thus, the information is securely transmitted over the wireless channel without being read by any other node.

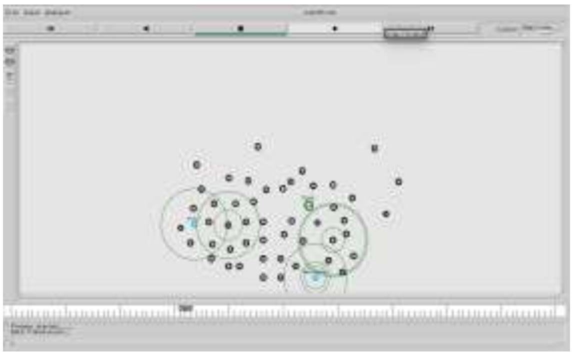


Figure 7.1: Network Animator Scenario-I

RESULT EVALUATION

PACKET DELIVERY RATIO

In the simulation, different scenarios of mobile nodes with AODV routing and AODV routing with security mechanism is calculated taking packet delivery ratio (PDR) as network parameter. PDR is higher that means our performance is better as shown in figure 7.2 and table 7.1. AODV technique that shows through the blue line and data transferring by applying security algorithm is shown through red line.

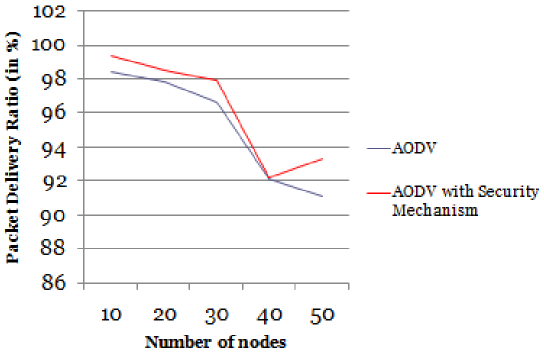


Figure 7.2: Packet Delivery Ratio Analysis Graph

Table 7.1 PDR Comparison Table of AODV and AODV with security mechanism

No. of Nodes	AODV(in %)	Modified AODV(in %)
10	98.4	99.6
20	97.8	98.5
30	96.6	97.9
40	92.1	92.2
50	91.1	93.3

As shown by the table average packet delivery ratio is 95.2 whereas average throughput of AODV after applying security mechanism derived is 96.38.

THROUGHPUT

In the simulation, different scenarios of mobile nodes with AODV routing and AODV routing with security mechanism is calculated taking throughput as network parameter. Throughput is higher that means our performance is better as shown in figure 7.3 and table 7.2. AODV technique that shows through the blue line and data transferring by applying security algorithm is shown through red line.

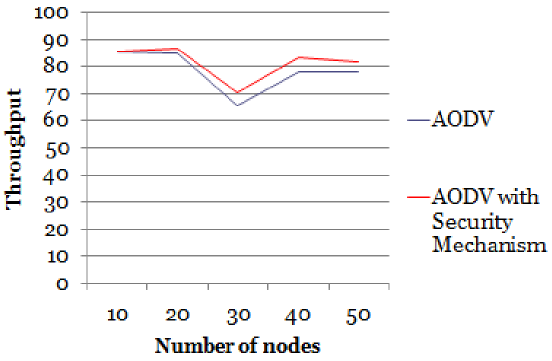


Figure 7.3: Throughput Analysis Graph

Table 7.2 Average Throughput Comparison Table of AODV and AODV with security mechanism

No. of Nodes	AODV	Modified AODV
10	85.63	85.63
20	84.90	86.69
30	65.51	70.65
40	78.13	83.33
50	77.80	81.79

Here average throughput of AODV derived is 78.394 whereas average throughput of AODV after applying security mechanism derived is 81.618.

END TO END DELAY

In the simulation, different scenarios of mobile nodes with AODV routing and AODV routing with security mechanism is calculated taking end-to-end delay as network parameter. End-to-end delay is more that means our performance degrades here as shown in figure 7.4 and table 7.3. AODV technique that shows through the blue line and data transferring by applying security algorithm is shown through red line.

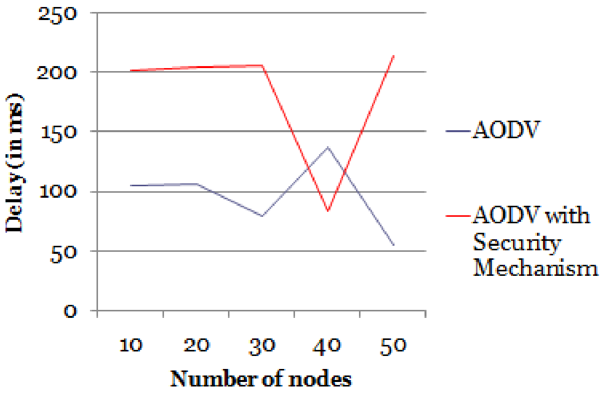


Figure 7.4: End to End delay Analysis Graph

Table 7.3 End to End Delay Comparison Table of AODV and AODV with security mechanism

No. of Nodes	AODV(in ms)	Modified AODV(in ms)
10	104.938	202.356
20	106.820	204.993
30	79.4738	205.548
40	137.474	83.1049
50	54.6495	214.066

Here average delay of AODV derived is 92.67 ms whereas average throughput of AODV after applying security mechanism derived is 182.01 ms. Thus performance of network decreases after applying security algorithm.

VIII. Conclusion

Finally after developing our proposed scheme Hybrid Approach i.e. RSA with Diffie Hellman and 802.11 for WSN after the result analysis, we conclude following points:

1. On applying proposed algorithm with AODV routing protocol provides better performance than existing AODV routing protocol.

2. Using proposed algorithm we found that packet delivery ratio is greater as compare to normal AODV routing.

3. In AODV with security mechanism and AODV without security mechanism, we also analyze the results of packet type, packet received, total packet send, and end to end delay and get our proposed hybrid security scheme gives better result as compare to normal AODV.

IX. References

[1] Nidhi Chhajed and Mayank Kumar Sharma, “Different Security Mechanisms for Wireless Sensor Networks,” International Journal on Recent and Innovation Trends in Computing and Communication, September 2015, Issue 9 Volume 3, pp. 5608-5613.

[2] Pooja, Manisha and Dr. Yudhvir Singh, “Security Issues and Sybil Atack in Wireless Sensor Networks”, International Journal of P2P Network Trends Technology, Volume3 Issue1 (2013), p.p. 7-13.

[3] Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications: Asar Ali, Zeeshan Akbar, Master’s Degree Thesis-(October 2009).

[4] Sushma, Deepak Nandal and Vikas Nandal, “Security Threats in Wireless Sensor Networks”, International Journal of Computer Science & Management Studies (May 2011), Vol. 11 Issue 01, pp. 59-63.

[5] Nidhi Chhajed and Mayank Kumar Sharma, “Different Security Mechanisms for Wireless Sensor Networks,” International Journal on Recent and Innovation Trends in Computing and Communication, September 2015, volume 3 Issue 9, pp. 5608-5613.

[6] Kalpana Sharma and M K Ghose, “Wireless Sensor Networks: An Overview on its Security Threats” IJCA “Mobile Ad-hoc networks” MANETs (2010), pp-42-45.

[7] Nidhi Chhajed and Mayank Sharma, “Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks (WSN’s): A Review,” International Journal of Advanced Research in Computer Science and Software Engineering, November 2014, vol 4 Issue 11, pp. 326-329.

[8] Shilpi Gupta and Jaya Sharma, “A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman,” IEEE International Conference on Computational Intelligence and Computing Research, 2012.

[9] Ishwarya M, Dr.Ramesh Kumar, “Privacy Preserving Updates for Anonymous and Confidential Databases Using RSA Algorithm,” International Journal of Modern Engineering Research (IJMER), Sep.-Oct. 2012 , Vol.2, Issue.5 , pp-3717-3722.

[10] Thanuja R. Dilip Kumar S., “A New Approach to Diffie-Hellman Key Exchange Algorithm,” International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 3, pp.534-536.

[11] B. Persis Urbana Ivy, Purshotam Mandiwa, Mukesh Kumar, “A Modified RSA Cryptosystem based on ‘n’ Prime Numbers,” International Journal Of Engineering And Computer Science, November 2012, Volume1 Issue 2, pp 63-66.

[12] Sakthi Nathiarasan A, Yuvaraj K., “Secure Key Exchange Algorithm – Mathematical Approach,” International Journal of Advanced Research in Computer Science and Software Engineering, June 2013, Volume 3, Issue 6, pp. 549-552.