Hybrid Security Mechanism for MANET

DhrutiGoswami[1], Krunal Panchal[2]

Student, Information Technology engineering, L.J.I.E.T, Gujarat, India
Assistant Professor, Computer engineering, L.J.I.E.T, Gujarat, India

ABSTRACT

MANET is a type of network where the group of mobile devices generates the network without any kind of Infrastructure. In MANET mobile nodes cooperatively forward the packet to the nodes which is not in its direct range. Any node is free to join and leave the network when they want. Due to its self-configuration and infrastructure less characteristics it is very vulnerable to different types of attacks. There are two types of problems in this kind of network is network performance and security. Proposed technique provides secure data transmission in MANET. Technique involves hybrid cryptography; it uses symmetric key cryptographic technique (MAES) for data encryption and asymmetric key cryptographic technique (ECC) for session key encryption. For integrity it also uses MD5 algorithm. The proposed Hybrid Security Mechanism is implemented in NS2 environment. The outcome shows that as the number of node increases performance of network decreases.

Keywords: MANET, Hybrid cryptography, MAES, ECC, MD5

1. Introduction

1.1 MANET

Wireless ad hoc network is new generation Communication Technology. That is basically invented for those conditions where the management of huge infrastructure and maintenance is costly. That suffers from various performance and security issues. MANET is defined by its own characteristics: it is self-organizing, Distributed operation, Multi hop routing. In mobile communication topologies are dynamically created due to the ad hoc nature of the network infrastructure and mobility. [4]

MANET does not require any additional infrastructure and the nodes act as end device as well as routers. The lack of infrastructure and the open architecture, in which no restriction is placed on nodes to join or leave the network, make MANET vulnerable to a variety of attacks.

The attacks can be on the data packets payload or on routing protocol control packets. The attacks on the control packet payload are with the aim of misdirecting the data packets or denial of service. The routing protocols in the MANET assume a trusted behavior of the nodes and therefore have not incorporated any security measures. Securing of routing protocols is not only difficult but very complex. It is an active area of research and is being done by either use of cryptographic techniques or by monitoring the behavior of the nodes. [5]

MANET does not require a fixed network infrastructure; every node works as both a sender and receiver. The security solutions for wireless networks are to provide security services, such as authentication, confidentiality, integrity.[9]

1.2 AODV Routing Protocol

Ad hoc on-demand distance vector (AODV) routing protocol uses an on demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. [5]

In an on demand routing protocol, the source node floods the RouteRequest packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single RouteRequest.

It uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination.When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination.The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RouteRequest packet.

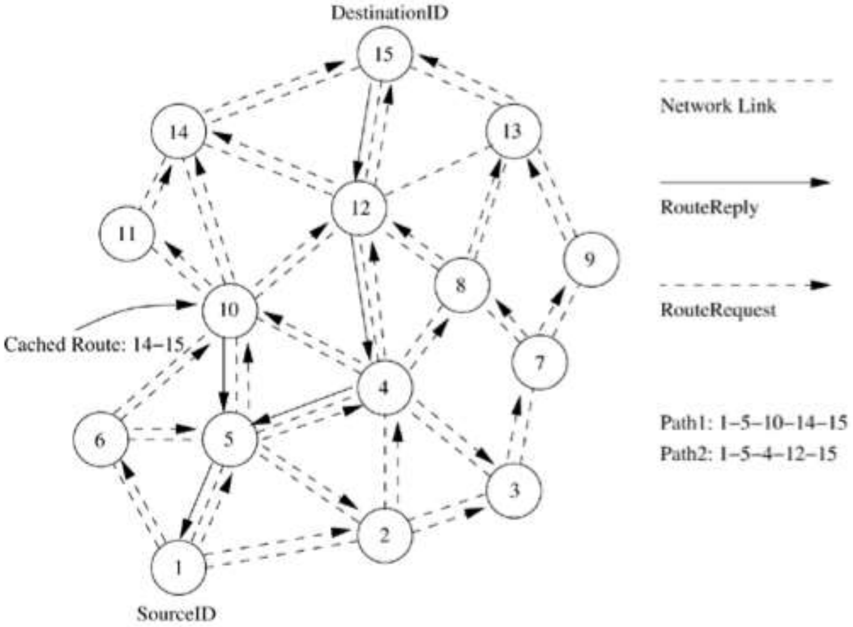


Figure 1: Route Establishment in AODV[6]

1.3 MAES Algorithm

Modify AES is to provide less computation and better security for data. The modify AES algorithm adjusts to provide better encryption speed. In Modified-AES the block length and the key length are specified according to AES specification: three key length alternatives 128, 192, or 256 bits and block length of 128bits.[7]
To overcome the problem of high calculation skip the Mixcolumn step and add the permutation.
A single 128-bit block is the input to the encryption and decryption algorithms. This block is a 4×4 square matrix consisting of bytes. This block is copied into the state array. The state array is modified at each stage of encryption or decryption. Similarly the128-bit key is also depicted into a square matrix. The 128bit key is expressed into an array of key schedule words: each word is of four bytes. The totals key schedule words for ten rounds are 44 words; each round key is similar to one state.[7]
The functions Substitution Bytes and ShiftRows are also interpreted as 128 bits whereas the Permutation function takes 64 bits. Then divide the consequential bits of ShiftRows function into two parts of 64 bits and then take each part of 64 bits as input of permutation tables and shift bits one by one according to the table.

1.4ECC (Elliptical Curve Cryptography)

ECC is one of the fastest computational methodologies with smaller key sizes, lower power consumption topology, lower bandwidth.
The equation of elliptical curve is given as,

$$y^2=x^3+ ax+ b$$ [8]

In the encryption process a selected number d with a range of n is selected.

$Q=d*p$ [8]
Where, Q is the public key,
d is the selected random number private key with
p as the curve point
Let m be the message sent with the implementation details.
The selected k is represented within k from 1 to (n-1).
Two cipher texts are generated based on the analysis they are,
$C_1 = k * p$ [8]
$C_2 = M + k * Q$ [8]
After encrypting the message the information should be sent to the original form which is represented as,
$M = C_2 - d * C_1$[8]

2. Related work

2.1 Hybrid Cryptography for Malicious Behavior Detection and Prevention System for MANETs[1]

Shreyas S. Jathe , VidyaDhamdhere[1] proposed to reduce network overhead, packet delivery ratio caused byDigital Signature Algorithmwe are using the concept of (RSA) Rivest, Shamir Adleman and (DES) Data Encryption standard algorithm. Compared to present approaches Hybrid Cryptography determining higher malicious action detection rates, in certain states while does not greatly affected the network performances. [1]

Packet dropping and hacking is the most critical concern in MANET's when security issues are considered. For that we have given IDS named Hybrid Cryptography with some new techniques and methods for prevention of attacks, which are added. [1]

2.2 Improved acknowledgement intrusion detection system in MANETs using hybrid cryptographic technique[2]

TruptiPatil ,Dr.Bharti Joshi[2] proposed this paper introduces a hybrid technique to reduce Network Overhead, which is caused by the digital signature and provides security to a network. Here hybrid technique of RSA and AES is used, to make the system more secure as RSA algorithm is used to communicate with the receiver through session key and AES algorithm is used to encrypt this session key which makes the key more secure as a result enhancing the security level.[2]

A hybrid cryptographic technique which is proposed in the system uses RSA and AES algorithms. The combination of both algorithms in a protocol uses multiple ciphers with their advantages. In this proposed system, we present a new circle symmetric algorithm to encrypt the plaintext and asymmetric algorithm RSA with AES are used to encrypt the symmetric key.[2]

2.3 A secure and efficient certificate based authentication protocol for MANET[3]

Utpal Kumar Verm, Sushil Kumar, DitipriyaSinha[3]proposed this paper presents a robust and secure mechanism for authentication of nodes in the MANET. The proposed authentication protocol is based on certificate exchange between the nodes. This protocol also uses digital signature with a hash function to maintain the authenticity of certificates. In addition, it also has less computation and communication overhead, which makes it suitable for MANETs.
This paper presents an authentication protocol for MANET, which is based on certificate exchange. In this proposed protocol, certificate exchange is mutual and all the nodes in the MANET have a considerable role in the authentication of new node. [3]

2.4 Secure data transmission on MANET by hybrid cryptography technique[4]

Ashish sharma, Dinesh Bhuriya, Upendrasingh[4] proposed system to provide security and increase performance in MANET, we have applied SAODV protocol andour solution uses Hybrid Cryptography Technique (DES, RSA Algorithms) on SAODV. This paper presents comparison based on simulation of

AODV, SAODV routing protocol of MANET with Different parameters like energy, packet delivery ratio and throughput.

2.5 Secure data transfer in MANET using symmetric and asymmetric cryptography[5]

Raj Kamal Kapur, Sunil Kumar Khatri[5]In this paper we have proposed a technique which provides secure transmission of data. The secure transmission of data over MANET is a critical requirement. The technique involves encryption of data using symmetric cryptographic technique, and also generating the digital signature of the data using the asymmetric cryptographic technique from the Hash of the data. The encrypted data is transmitted through the network to the destination where the received data and digital signature of the data are validated using symmetric and asymmetric cryptography. The data on validation is accepted thus ensuring secure data transmission. The proposed technique provides confidentiality, integrity, authenticity and non-repudiation to the data.

3. Proposed Work:

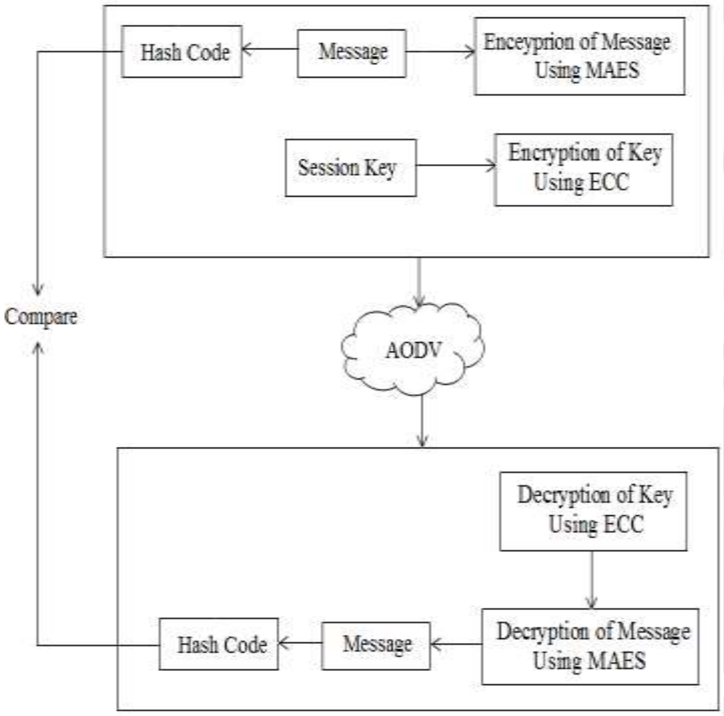
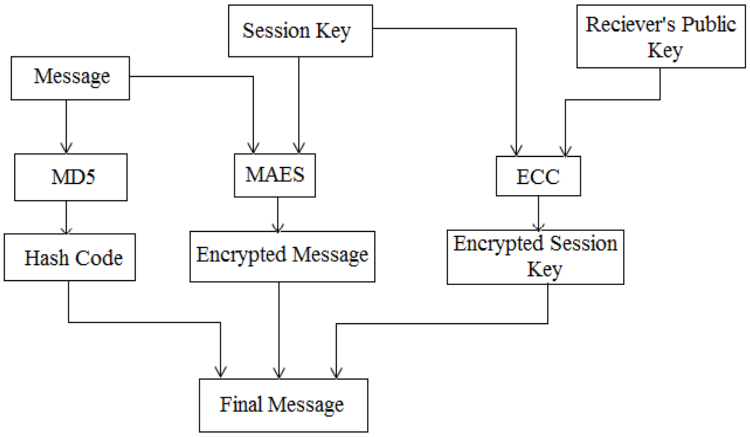

Hash Code
Message
Enceyprion of Message Using MAES
Session Key
Encryption of Key Using ECC
Compare
AODV
Decryption of Key Using ECC
Hash Code
Message
Decryption of Message Using MAES

Figure: 2 Proposed Model

In proposed technique, once the route is discovered by AODV routing protocol, original data which sender desired to send is applied to message digest algorithm and hash code of original message will be generated. After hash code is generated original message is encrypted with session key and symmetric key algorithm which is MAES. Once message is encrypted session key will be encrypted using receiver's public key and ECC algorithm, so that only receiver could decrypt message with his/her private key. After this entire process sender send packet which contains hash code, encrypted key and message to receiver. By using this technique we can improve the network performance like overhead, packet delivery ratio and energy of existing system and we can achieve same level.



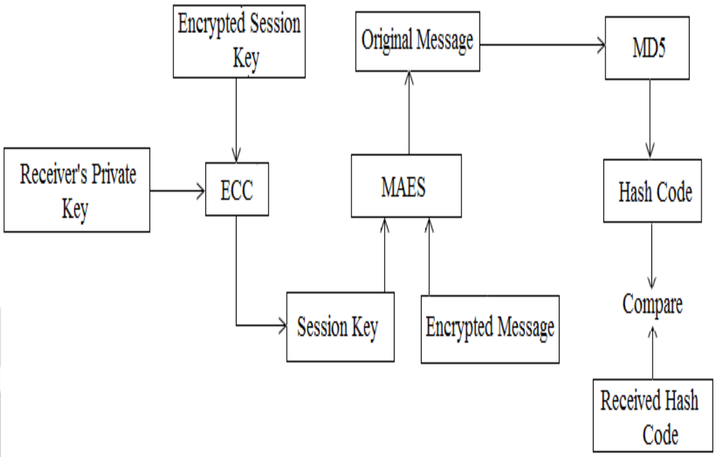


Figure: 3 Work Flow at Sender side

Figure: 4 Work Flow at Receiver side

Node which wants to send data packet will first generate hash of the data with MD5 algorithm. Once this process is completed encoding process will start in which sender will encrypt the message using symmetric key cryptosystem, i.e. MAES. Now for better security key used in symmetric cryptosystem i.e. session key will be encrypted using asymmetric key cryptosystem i.e. ECC key to be used is receiver's public key. And after sender will club hash code, encrypted message and encrypted session to a packet and transmits it to intended destination.

At the receiver side receiver first decrypts the session key by applying its own private key which is known to that node only and the algorithm is ECC for session key decryption. When receiver node gets session key, decryption process will be carried out. In which session key and MAES algorithm is used. When original message is achieved by node, node will calculate hash code of decrypted message and compare both hash codes i.e. received by the source node and hash code which is calculated by that node only. If both the hash codes are same then and then node will accept the message otherwise message will be rejected assuming that message is modified. In this way we can achieve integrity.

5. Result Analysis

Simulation parameters:

Simulation parameter	**Value**
Number of nodes	50
Network size	1100*1100
Simulation duration	50(sec)
Channel Type	Wireless channel
Radio propagation Model	Tow-Ray Ground
Network Interface type	Wireless Phy

MAC type	802.11
Interface Queue type	Droptail Queue
Interface Queue length	50
Node size	70
Antenna Type	Omni Antenna

As mentioned in above scenario we have implemented AODV. We took different scenario with different numbers of nodes in the network and compared the results to achieve tradeoff between performance of network and security. We have results of packet delivery ratio, overhead and throughput for network with 40 nodes and 50 nodes.

Packet Delivery ratio:

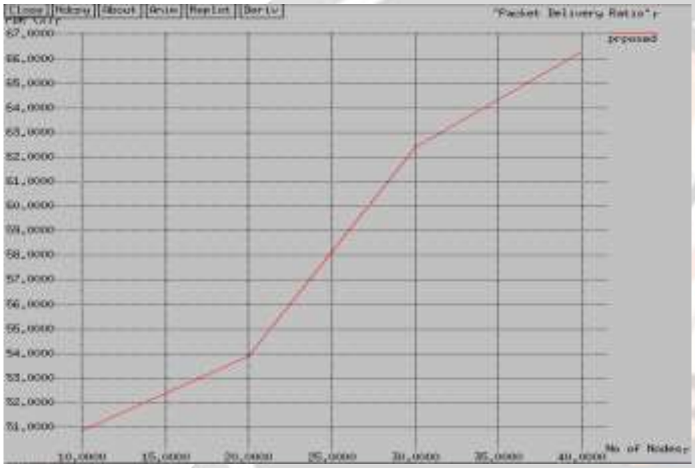


Figure: 5 Packet delivery ratio for 40 nodes

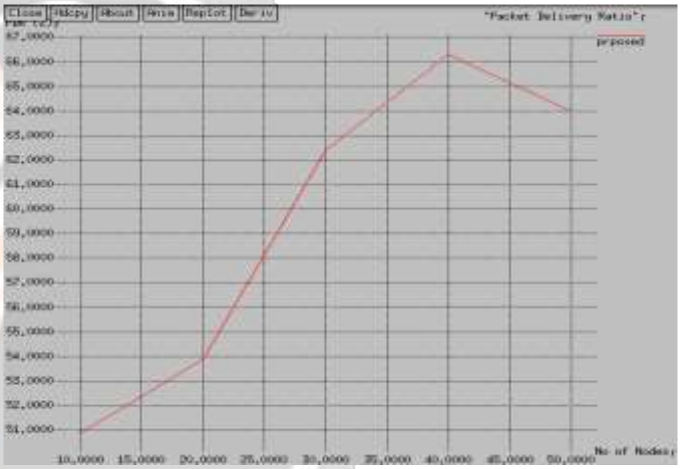


Figure: 6 Packet delivery ratio for 50 nodes

Throughput:

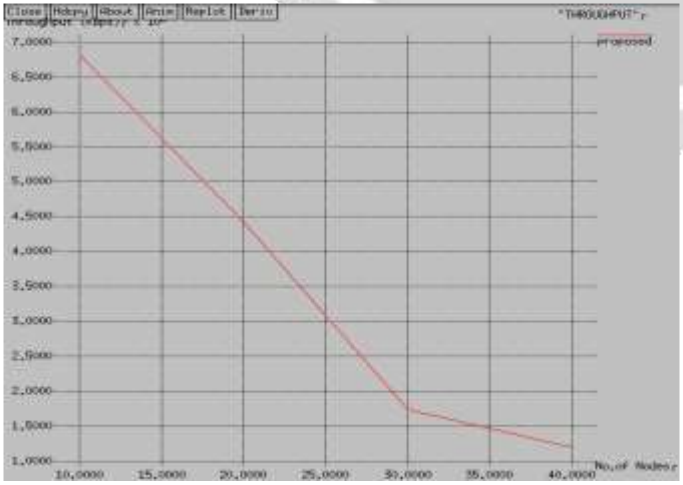


Figure: 7 Throughput for 40 nodes

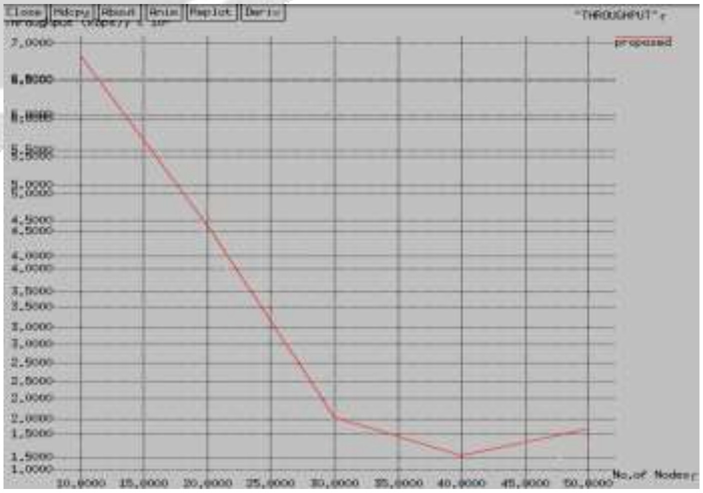


Figure: 8 Throughput for 50 nodes

Overhead:

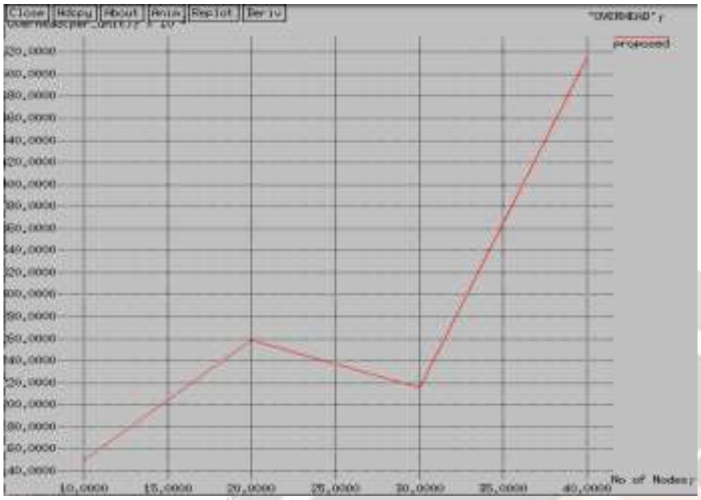


Figure: 9 Overhead for 40 nodes

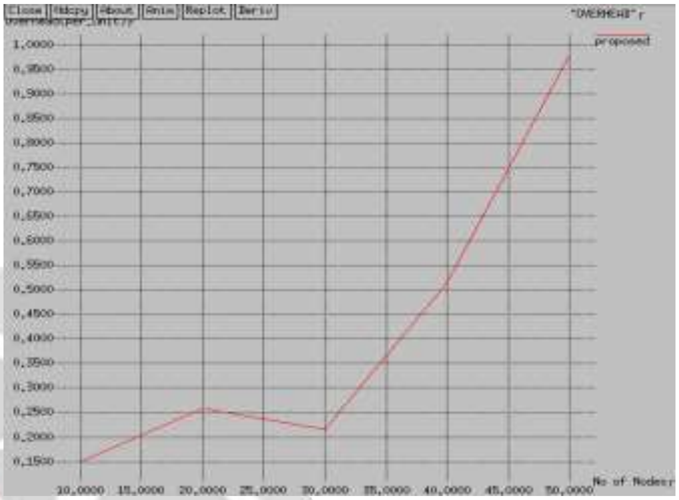


Figure: 10 Overhead for 50 nodes

4. Conclusion

According to, literature survey cryptography is very much in trend to provide security to networks. MANET is very vulnerable to different attacks. Hybrid cryptography can be used to make communication more secure in MANET. Any digital data can be transmitted securely using this scheme. Proposed work considers parameters such as, energy, packet delivery ratio, throughput and overhead to achieve energy efficient and secure communication. We have improved PDR, Throughput, Overhead and energy than existing system. To set trade-off between performance and security we took different number of nodes to check performance of the network. As shown in result we can say that as the number of node increases in network PDR decreases, Throughput increases and overhead is not much variant.

5. References

[1] Jathe, S. S., &Dhamdhere, V. (2015). “Hybrid Cryptography for Malicious Behavior Detection and Prevention System for MANETs”. *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*. doi:10.1109/cicn.2015.218, pp.1108-1113

[2] Patil, T., & Joshi, B. (2015). “Improved acknowledgement intrusion detection system in MANETs using hybrid cryptographic technique”. *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. doi:10.1109/icatcct.2015.7456962, pp.636640

[3] Verma, U. K., Kumar, S., & Sinha, D. (2016). “A secure and efficient certificate based authentication protocol for MANET”. *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*. doi:10.1109/iccpct.2016.7530346

[4] Sharma, A., Bhuriya, D., & Singh, U. (2015). “Secure data transmission on MANET by hybrid cryptography technique”. *2015 International Conference on Computer, Communication and Control (IC4)*. doi:10.1109/ic4.2015.7375688

[5] Kapur, R. K., & Khatri, S. K. (2015). “Secure data transfer in MANET using symmetric and asymmetric cryptography”. *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)*. doi:10.1109/icrito.2015.7359293

[6] Murthy, C. Siva Ram., and B. S. Manoj. *Ad Hoc Wireless Networks: Architectures and Protocols*. Upper Saddle River, NJ: Prentice Hall/PTR, 2004

[7] Vandana C. Koradia. (2013). "MODIFICATION IN ADVANCED ENCRYPTION STANDARD". 2013 *Journal of Information, Knowledge and Research in Computer Engineering (jikrce)*. doi:10.1109/jikrce.2013. 6760

[8] M.CharlesArockiaraj,&Dr.P.Mayilvahanan. (2016). "OVERHEAD MINIMIZATION IN MANET USING IMPROVED ELLIPTICAL SECURITY ALGORITHM". *2016 International Journal of Scientific Engineering and Applied Science (IJSEAS)*. doi:10.1109/ijseas.2016.7359293

[9] Sivaranjani, S., and S. Rajashree. "Secure Data Transfer in MANET Using Hybrid Cryptosystem." *International Conference on Information Communication and Embedded Systems (ICICES2014)* (2014)