Implementation of hybrid cryptography for wireless networks

Madhushree N

MTech Student, Department of Computer Science and Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India

Abstract - *Nowadays wireless networks are becoming more popular and tremendously increasing due to various enhanced technologies. The major development in this technology is communicating via wirelessly where mobile nodes communicate with each other without use of any base station. These network are called as mobile ad hoc networks (MANET'S). As communication is done wirelessly, these type of networks are prone to several kind of attack. Thus, providing security to wireless network is challenging. Encryption, authentication usually acts as a first line of defense while next intrusion detection system (IDS) acts as a second line of defense. Therefore in this paper by using hybrid cryptography we are enhancing more secure transfer of data. This paper also extends to provide and enhance security for replay attack and message tampering attack.*

***Key Words*: plain text, cryptography, encryption, decryption, hybrid cryptography**

1. INTRODUCTION

A mobile ad hoc network is a group of mobile nodes which communicate via wirelessly without assistance or use of any base station. Nowadays communication plays a major role and an essential tool for any management, education, defense, airlines etc. Transfer of data with security is important. Cryptography provides secure communication in the presence of malicious third parties.

Nowadays many cryptographic algorithms have been implemented. These cryptographic algorithms are majorly classified into two different types symmetric and asymmetric. Now the idea is to combine the algorithm and enhance the security for data transmission. Cryptography usually converts the desired data or instruction into a format that the data is unreadable for unauthorized users. Many cryptographic algorithms are been proposed and implemented to enhance the security like integrity, confidentiality, authentication, confidentiality.

Authentication: Authentication is the process of confirming the identity. In other words, that the message arrived from the stated user that has not been modified by any other users that is sender identity has to be rectified.

Confidentiality: It is usually designed to guide policies for data or information security within an organization.

Integrity: Integrity means that the data or information which is sent during communication ensures that the information is not modified or altered at the receiving side.

1.1 TECHNIQUES IN CRYPTOGRAPHY

In order to enhance the security in a network cryptographic algorithm is to be implemented. This algorithm is divided into two types symmetric encryption and asymmetric encryption. Symmetric encryption algorithm is the oldest algorithm and can be the best encryption, symmetric key algorithm are algorithm for cryptography which uses the same key for both encryption of plain text and decryption of cipher text. It is also called as secret key cryptography. Both encryption and decryption of all messages that uses the same key.

The problem in symmetric algorithm is during exchange of secret key over a large network the message can be decrypted by other person who has the secret key it might fall to a wrong hand. Therefore key distribution has to be secure and it is one of the major issue t symmetric key encryption.

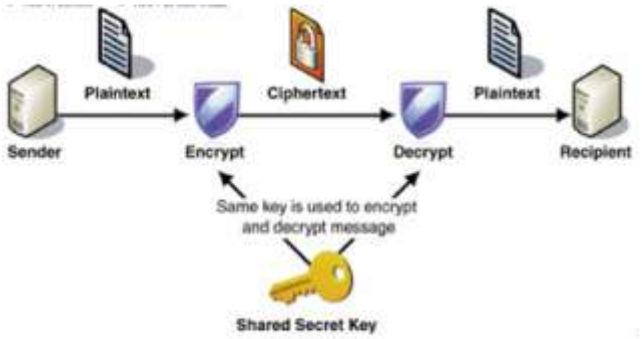


Fig -1: **symmetric encryption**

In general data cleaning involves several phases:

In order to deal with such type of issues we use an another method known as public key cryptography in which two keys are used that is public key and private key. Where public key is made freely available to everyone who wish to send a message. A private key is kept and resembled as a secret key so that only the person accessing it knows it. A message in form of text, files or documents that are encrypted using public key and can only be decrypted using private key by applying the same algorithm used.

The problem with asymmetric encryption is this algorithm is much slower than symmetric algorithm, and it also requires more processing power to carry out both encryption and decryption of the information during communication.

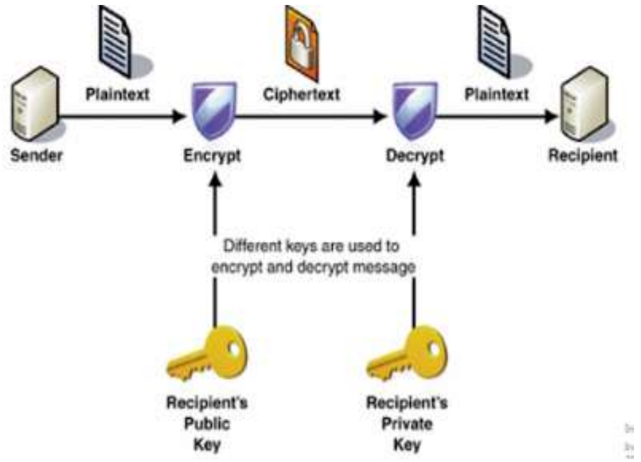


Fig -2: **asymmetric encryption**

1.2 HYBRID CRYPTOGRAPHY

Hybrid cryptography is using a multiple cipher of different types. One simpler approach is to generate a random secret key for a symmetric cipher and one has to encrypt this key via an asymmetric cipher using the recipient public key.

1.3 NEED FOR HYBRID CRYPTOGRAPHY

Communication plays a major role in today world, and it is very important to provide a high security during communication. The usage of traditional algorithm is not much enough for providing security. So we propose the use of hybrid cryptography algorithm in this paper.

2. LITERATURE SURVEY

Shashikanth kuswaha and Praful B proposed a hybrid security algorithm for transmission of data. The algorithm is designed in such a way that uses the combination of both AES and RSA. The implemented algorithm provides a better security as well as integrity. The algorithm which is designed is efficient and reliable technique for encryption of data.

Roshini Padate and Aamna proposed an encryption and a decryption technique of data using AES (advanced encryption standard) algorithm. It provides an efficient security for communication of information, where AES algorithm has been replaced by DES (data encryption standard)

Mohammad Trik, Sam Jabchdari proposed a security protocol. Algorithm like RSA, AES and ECC algorithm are combined together. Since, both type of algorithm are applied to an architecture thus the obtained one have more stability against errors. The proposed work is more secured which is applied by AES algorithm.

3. PROPOSED SYSTEM

In order to enhance with more security we proposed hybrid cryptography, where it is combination of both symmetric and asymmetric cryptography. In this paper we have also enhancing the security for replay attack as well as the message tampering attack. Replay attack is a form of network attack in which a data transmission is maliciously repeated or delayed. Whereas message tampering is the art of altering or modifying a message. It is carried out by hybrid encryption and hybrid decryption process.

Initially, the content or a text file or with any other format the file has to be encrypted and send it to a decryptor in secure and efficient way. The text file initially generate a randomly an AES key, once generated the key using this key the file content is encrypted and obtain an encrypted content, by AES key it is able to generate RSA key using this we can generate both public and private key. Thus by using RSA public key we can encrypt the AES key. Hash is introduced where sequence of strings of characters are transformed into fixed length of values. The hash obtained also has to be encrypted using public key. Thus encrypted key, encrypted content, encrypted hash are send to a decryptor through a socket.

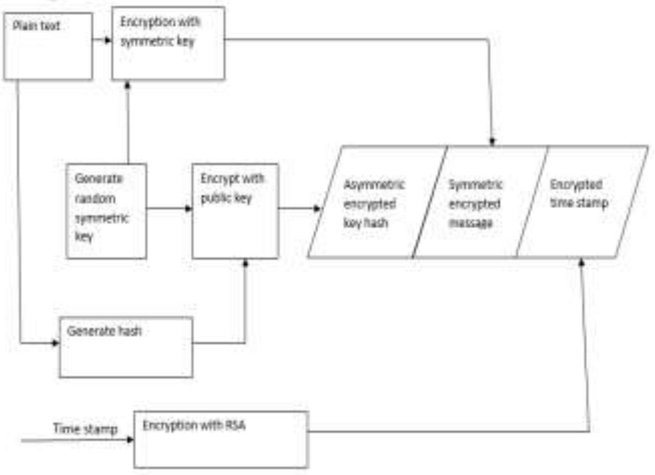

Plain text
Encryption with symmetric key
Generate random symmetric key
Encrypt with public key
Asymmetric encrypted key hash
Symmetric encrypted massage
Encrypted time stamp
Generate hash
Time stamp
Encryption with RSA

Fig -3: **hybrid encryption**

At the receiving end that is, at decryptor initially feed with a private key. Encryptor shares the private key only to an authorized users, who can only access the information. Using the obtained private key we can decrypt and get an AES key using the AES key we can decrypt the content and get an original message.

For wireless mode of transmission. Mobile nodes are prone to several kinds of attacks, during the transmission the message might get modified or altered that is tampering of message may occur in order to overcome we have to find the hash of the content and decrypt the hash using private key and find the hash. If both the hash are equal then no one has attacked or modified. In this paper we also introduced the time stamp suppose the message is delayed or arriving late one can suspect that someone might be performing a replay attacks represented in the figure if the arrival of the packet is greater than 300 sec then the packet is dropped and indicating it as a replay attack.

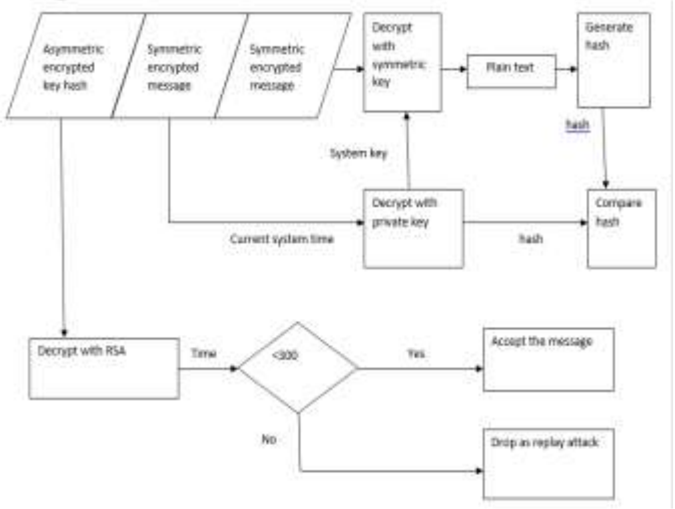
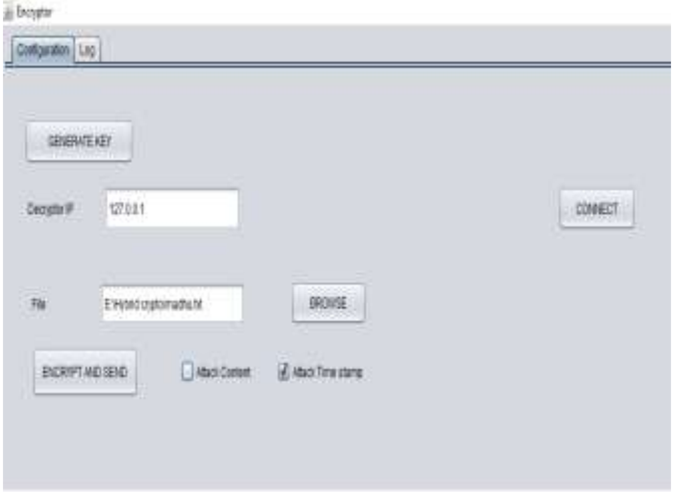


Fig -4: **hybrid decryption**

4. RESULTS



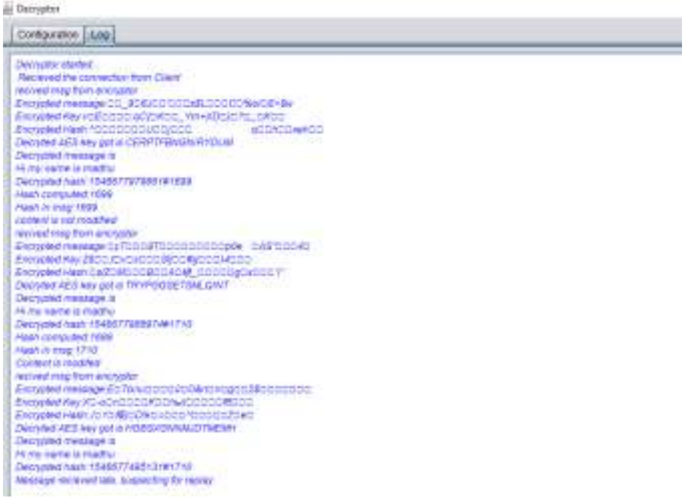
Decryptor IP 127.0.0.1

File E:\Hybrid cryptomadhu.txt

□ Attach Content ☑ Attach Time stamp

Fig -5: **screenshot of encryptor**

The above screen shot indicates the encryptor which is at client mode it indicates how can a person generate key and send message to one whom he has to communicate.



```
Decryptor started
 Recieved the connection from Client
recived msg from encryptor
Encrypted message:[illegible]
Encrypted Key:[illegible]
Encrypted Hash:[illegible]
Decryted AES key got is [illegible]
Decrypted message is
Hi my name is madhu
Decrypted hash 15486779788[illegible]
Hash computed 1699
Hash in msg 1699
content is not modified
recived msg from encryptor
Encrypted message:[illegible]
Encrypted Key:[illegible]
Encrypted Hash:[illegible]
Decryted AES key got is [illegible]
Decrypted message is
Hi my name is madhu
Decrypted hash 154867788[illegible]
Hash computed 1699
Hash in msg 1710
Content is modified
recived msg from encryptor
Encrypted message:[illegible]
Encrypted Key:[illegible]
Encrypted Hash:[illegible]
Decryted AES key got is [illegible]
Decrypted message is
Hi my name is madhu
Decrypted hash 154867748[illegible]
Message recieved late. suspecting for replay
```

Fig -6: **screenshot of decryptor**

The above screen shot indicates decryptor which is at server mode all the messages are decrypted and sent and also notifies if someone has perform the message tampering or replay attack

5. CONCLUSION

Nowadays many cryptographic algorithms have been implemented. These cryptographic algorithms are majorly classified into two different types symmetric and asymmetric. Now the idea is to combine the algorithm and enhance the security for data transmission. Cryptography usually converts the desired data or instruction into a format that the data is unreadable for unauthorized users. Many cryptographic algorithms are been proposed and implemented to enhance the security like integrity, confidentiality, authentication, confidentiality. Therefore in this paper by using hybrid cryptography we are enhancing more secure transfer of data. This paper also extends to provide and enhance security for replay attack and message tampering attack.

REFERENCES

[1] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc network", IEEE Network, vol. 13, pp 24-30, Dec 1999.

[2] JP. Brutch and C. Ko, "Challenges in intrusion detection for wireless adhoc networks", IEEE Applications and the Internet Workshops, pp. 368373, 2003.

[3] Deb, M. Chakraborty, and N. Chaki, "A state of the art survey on IDS for mobile ad-hoc networks and wireless mesh networks", Communications in Computer and Information Science, vol. 203, pp 169-179, 2011.

[4] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto and N. Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Vehicular Technology , vol.58, , pp. 2471-2481, June 2009.

[5] William Stallings, "Cryptography and Network Security", Fourth Edition, June 3, 2010.