International Journal for Rapid Research in Engineering Technology and Applied Science
ISSN (Online): 2455-4723
Vol 1 Issue 1 December 2015

A Secure Communication using RSA Cryptography in Mobile Ad-hoc Networks

Ankush Jain*, Er. Sandeep Gupta**
Dept. of Electronics & communication, SD Bansal College of Technology, Indore
*ankushjain0712@gmail.com**, *sandeep.guptap@gmail.com***

Abstract: A mobile ad hoc network is a special type of wireless network in which a collection of mobile hosts with wireless network interfaces may form a temporary network. Without the aid of proper fixed infrastructure, providing secure communications is a big challenge. The strength of the security solutions very much depends on the cryptographic keys used for communication. Efficient key management is an important requirement of such networks. For networks like MANET which are basically constrained networks with minimum resources, identification of suitable asymmetric cryptosystem is a vital one. Hence an attempt has been made to improve the security during communication by maintaining minimum overhead. A RSA algorithm with Diffie-Hellman Key exchange will be used to achieve confidentiality during communication in MANET.

I. Introduction

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predetermined organization of available links. A MANET is referred to as an infrastructure less network, because the mobile nodes in the network dynamically set up paths among themselves to transmit packets. Application of MANET includes battlefield applications, search and rescue operations as well as civilian applications such as e-commerce, business, vehicular services and shopping and other networking applications. Since MANET can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses in sensor network applications or virtual classrooms. The main challenges of MANET are Absence of infrastructure, Wireless links between nodes, Limited physical protection, Lack of centralized monitoring, Security, Routing, Quality of Services (QoS) and Reliability. Of which, Security is an important issue for Mobile ad hoc Network. Basic security requirements of MANET are Authentication, Confidentiality, Integrity, Non repudiation and availability. Security is considered as an important requirement due to the reason that many upcoming applications demand high security infrastructure. Key management is the core component of the security infrastructure.

Several important desktop computing applications have emerged in recent years that use an Internet-scale decentralized architecture to simultaneously connect millions of users to share content, form social groups and communicate with their contacts. These applications are classified as peer-to-peer because of the elimination of servers to mediate between end systems on which the applications run, and their network behavior is described as an overlay network because the peer protocols form a virtualized network over the physical network. While peer-to-peer (P2P) applications have had a rapid ascent and wide impact, in the future P2P overlays are likely to enable important new applications following from these technology trends:

1. Continued improvements in the fidelity of the consumer entertainment experience and network and computing capacity of the associated entertainment devices.
2. The development of dense and ubiquitous sensing grids with real-time data collection of all types of phenomena
3. The wide deployment of broadband wireless networks (Wi-Max, 802.11n, UWB, LTE)
4. The proliferation of mobile smart phones and other broadband-enabled mobile devices
5. The use of personal networks, body-area networks, and vehicle networks, to connect both real-time sensors and embedded computing devices.

The wide adoption of these technologies will enable high-fidelity and pervasive information collection, content

publishing and distribution, and sharing of environmental and personal real-time sensed data and information on a global scale. The benefits of this include increased awareness of one's personal environment, more precise context-awareness in interactions with others, and enhanced situation awareness for applications ranging from immersive entertainment and recreation, environment management, homeland security, and disaster recovery.

Overlays are an important component of this future vision, due to their high scalability, flexibility for different types of applications, and low barrier of entry. The evolution of contemporary P2P overlays to enable this future vision is an important research direction.

The proposed work will use RSA algorithm using asymmetric key cryptography and Diffie-Hellman Key Exchange Algorithm to achieve high level security with minimum key distribution overhead. It will also encrypt message and key using symmetric key to achieve confidentiality. The complete idea concludes that, proposed work will not only give a hybrid model for secure communication but achieve secure authentication too.

II. Related Work

This paper [1] explere the basic survey of cryptoyropic algorithm and their need in secure communication. They try to explain public key cryptoyrophy and security overhead.

Shrini Vararao,p. Adchess that cryptoyrophy in data communication provide help to maintain security on sensitive data. They explere that hrutefore attack is one of severe security threat attack to compromise cipher text using forye secret key. It uses hit and try technique and uses all possible keys to break encryption algorithm . They propose a encryption technique based an subsittution and random encryption known and PSR.

In this Paper [2] Anthors considere RSA as base algorithm and compare results on basis of time, execution time ,key length and message size. They explain the comparision b/w DES and RSA .Here DES is private key or symmetric key algorithm where RSA is a asymmetric key based algorithm .They also implement LDES algorithm for performance observation five different data size file in between 15 to 75 KB has been used an input and evalute and observe the encryption and decryption execution time for DES ,2DES and RSA.

Present data encryption and decryption process in network environment using RSA algorithm .They address that RSA alogrithm with specific block size may use to achieve confidentility and authentication ever senitive and private data. A java prototype has been developed and evalvet over dropping .

In this paper [3] a combination of MDS and RSA algorithm has been propered. This hybrid approach has been implemented in MANET and terted in NS2 simulator. Propered algorithm give faster result than traditional RSA algorithm.

In this paper [4] author proposed file encryption and decryption approach using RSA aglorithm .They implement the propered solution.In java platform propered model may take input from variable file type but perform same process for secure communication .time and size overhead has been evaluted.

A comparitive analysis of RSA algorithm with M-RSA has been prospered in [5]. They consider variable input are calculation. Execution time of key process,encryption and decryption a mathematical factorization has been consider.

III. Security Issues

To establish and maintain a reliable secure network, security solutions should provide security services including confidentiality, availability, authentication, integrity and non-repudiation.

- **Confidentiality:** Confidentiality or privacy implies that the information being exchanged must make sense to the desired nodes only. It should be protected from unauthorized access or the information should not be comprehensible to other users for whom it is not meant.
- **Availability**: Normal services required by authorized entities has to granted even if connection ports are inaccessible or data routing or/and forwarding algorithms are not working because of various attacks.
- **Integrity:** The data received at the destination should be exactly same as transmitted by source. During the

process of data exchange between two nodes data should not be modified in any manner (neither accidentally nor maliciously) by any node within the network.

- **Non-repudiation:** A non-repudiation service grants that a sender must not be able to deny sending its own message, and a receiver cannot deny that a message had been received.
- **Authentication:** It grants a confidence about a single node or entity's identity and surety that message has been sent by authentic user and not by any imposter.

There are two basic techniques for encrypting information:

1. Symmetric encryption
2. Asymmetric encryption

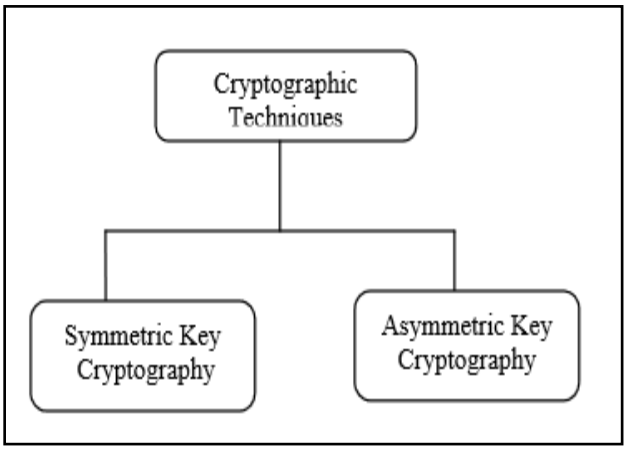

Figure 1: Encryption technique

A. Symmetric Encryption

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

In simple words it is a cryptographic algorithm that uses the same key to encrypt and decrypt data. Diffie Hellman Key Exchange algorithm or DES is the best examples for symmetric key cryptography.

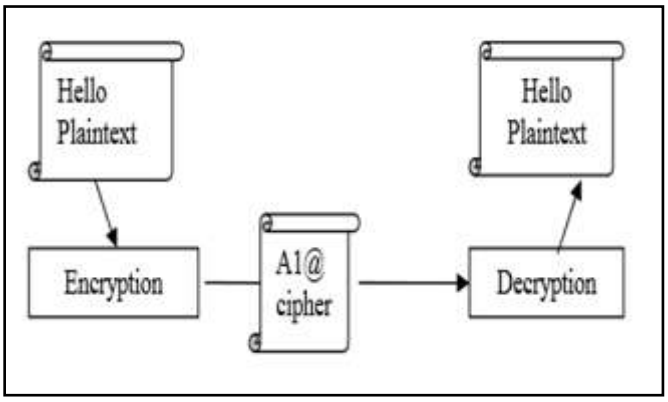

Figure 2: Symmetric Encryption

The problem with secret or symmetric keys is how to securely get the secret keys to each end of the exchange and keep them secure after that. For this reason, an asymmetric key system is now often used that is known as the public key infrastructure (PKI).

B. Asymmetric Encryption

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to. It is shown in below figure.

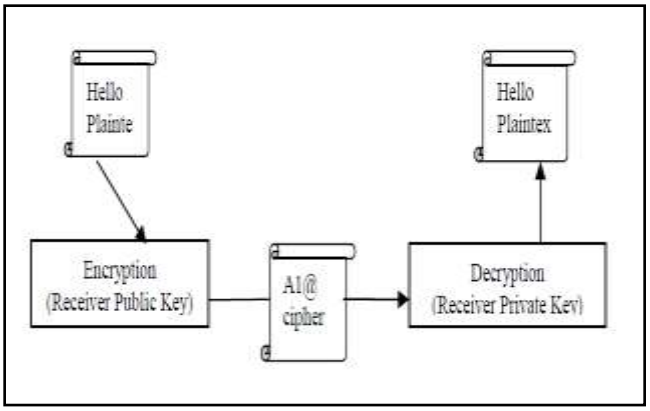

Figure 3: Asymmetric Encryption

In cases where the same algorithm is used to encrypt and decrypt, such as in RSA, a message can be securely signed by a specific sender: if the sender encrypts the message using their private key, then the message can be decrypted only using that sender's public key, authenticating the sender.

This also allows for the exchanging of securely signed and one-to-one messages, as follows. The sender encrypts the message using the common algorithm and his own secret key. They then sign the result, encrypt it again (with their signature in clear text) using the recipient's public key, and send it. The recipient decrypts the received message using their own secret key, identifies the sender from their now-cleartext signature, and then decrypts the result using the sender's public key. This ensures the recipient that whoever composed the message had access to the sender's private key, and that nobody tampered with the message or read it along the way.

In symmetric cryptography, the same key is used for both encryption and decryption. This approach is simpler in dealing with each message, but less secure since the key must be communicated to and known at both sender and receiver locations.

IV. Problem Definition

RSA is a 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.

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, 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 the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm. It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

RSA derives its security from the difficulty of factoring large integers that are the product of two large prime 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.

The public and the private key-generation algorithm is the most complex part of RSA cryptography. Two large prime numbers, *p* and *q*, are generated using the Rabin-Miller primality test algorithm. A modulus *n* is calculated by multiplying *p* and *q*. This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length. The public key consists of the modulus *n*, and a public exponent, *e*, which is normally set at 65537, as it's a prime number that is not too large. The *e* figure doesn't have to be a secretly selected prime number as the public key is shared with everyone. The private key consists of the modulus *n* and the private exponent *d*, which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of *n*.

Considering arithmetic modulo n, let's say that e is an integer that is coprime to the totient φ(n) of n. Further, say that d is the multiplicative inverse of e modulo φ (n). These definitions of the various symbols are listed below for convenience:

n = a modulus for modular arithmetic

φ (n) = the totient of n

e = an integer that is relatively prime to φ(n)

[T his guarantees that e will possess a multiplicative inverse modulo φ(n)]

d = an integer that is the multiplicative inverse of e modulo φ(n)

The computational steps for key generation are

1. Generate two different primes' p and q
2. Calculate the modulus $n = p \times q$
3. Calculate the totient $\varphi(n) = (p - 1) \times (q - 1)$
4. Select for public exponent an integer e such that $1 < e < \varphi(n)$ and $\gcd(\varphi(n), e) = 1$

5. Calculate for the private exponent a value for d such that

$$d = e-1 \bmod \varphi(n)$$

6. Public Key = [e, n]
7. Private Key = [d, n]

The complete work observes that Mobile ad-hoc networks require routing protocols to discover route from source to destination. AODV routing protocols are usually used to discover route from source to destination. AODV is reactive routing protocol having minimum routing overhead and hop count parameter for route selection. The major problem with AODV routing protocol is it does not have any security policy or security mechanism to maintain privacy during communication. The main problem with MANET is fear of safety violation during communication. The complete work concludes that, in secure and hostile communication is major problem with MANET. There is need to develop security mechanism to achieve secure communication.

Furthermore, Work also observed that Asymmetric Key cryptography based RSA is a good solution to achieve confidentiality but suffer with extra overhead of key distribution. Whereas Diffie Hellman key exchange is good approach to generate symmetric key with minimum overhead. Work also examine that transmission require more energy than computation.

The complete study generate a requirement to develop security policy to establish secure communication among mobile nodes by maintain minimum security overhead.

In short, major concern with AODV is:-

- Insecure Routing
- Packet Dropping
- Security
- Uphold Confidentiality.

V. Solution Domain

One of the objectives of this research paper is to mitigate the effects of eavesdropping and reduce worry about compromising the communication. Proposed solution will implement cryptography technique to provide protection layer against messages and information.

RSA is a asymmetric key based cryptographic algorithm used to convert plain text into cipher text. Proposed solution will implement RSA algorithm with routing protocol to convert each and every data packet into cipher text format.

Proposed solution will create a virtual secure communication link between source and destination and provide confidentiality against information.

VI. Conclusion

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in MANET theoretically and through simulation. The complete work concludes that proposed solution will implement RSA algorithm to achieve confidentiality and privacy during communication.

References

[1] Manita, Vinay Nassa, Kapil Chawla, "Improving AODV Protocol by Nature Inspired Technique against Blackhole and Grayhole Attacks in MANETs", in Journal of International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 8, Aug.-14.

[2] Rashmi, Ameeta Seehra, "Detection and Prevention of Black-hole Attack in MANETs", in Journal of International Journal of Computer Science Trends and Technology(IJCST), Vol. 2, Issue 4, Aug.-14.

[3] Ravinder Kaur, Jyoti Kalra, "Detection and Prevention of Blackhole Attack with Digital Signature", in Journal of International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 8, Aug.-14.

[4] Raghvendra Prasad, Kuntal Barua, "Implementation, Detection and Prevention of Blackhole Attack for MANET using NS-2 ", in Journal of International Journal of Science and Research, Vol. 3, Issue 3, March.-14.

[5] Ravinder Kaur, Jyoti Kalra, "A review of Blackhole Attack in MANETs", in Journal of International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 8, Aug.-14.