ISSN:0975-9646



# Secure Mobile Adhoc Network using AES and RSA

**Anshul Jain** *SATI, Vidisha (M.P.)*

**Sumeet Dhillion** *SATI, Vidisha (M.P.)*

**Yogendra Kumar Jain** *SATI, Vidisha (M.P.)*

**Abstract-Mobile adhoc network has security issues over a large number of years. To maintain security several algorithms for authentication, authorization, integrity, non repudiation and confidentiality are proposed by various authors. In this paper security for MANET has been proposed using RSA, AES and SHA512 algorithm. RSA has been used for key generation, AES for symmetric encryption. Using AES both variable length and fixed length encryption schemes are compared. It is found that variable length encryption using AES has been more efficient in terms of time as compared to fixed length encryption.**

**Keywords: Integrity; Sha512; Message digest; Digital signature.**

## 1. INTRODUCTION

Starting in the late 1950s, computer networks evolved from small isolated networks centered on a mainframe, to the now omnipresent Internet, connecting computers around the globe. Until recently, computers were typically connected to a wall socket using a wire, limiting the mobility of the users. With the introduction of the 802.11 Wireless Local Area Network (WLAN) standards in the 1990s, it is now possible to make a wireless connection to an Access Point (AP), which replaces the traditional Ethernet socket. These recent advances in wireless technologies and further miniaturization of computer systems enable the next major evolutionary step: Mobile Ad hoc Networks (MANETs).

A **Mobile Ad Hoc Network** (**MANET**) [1].Sometimes called a mobile mesh network, is a self configuring network of mobile devices connected by wireless links [2].Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. They are also a type of mesh network, but many mesh networks are not mobile or not wireless.

The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid to late 1990s. Many academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures.

As ad-hoc and sensor networks become a growing part of our everyday life, they could become a threat if security is not considered carefully before deployment. There are several security goals in ad-hoc networks. The provision of authentication is a core requirement for secure and trustworthy communication in ad-hoc networks, and it is the focus of this work. Only if there is efficient authentication available in ad-hoc networks, secure protocols and applications can be designed. IT security is the enabler for innovative applications, and provision of authentication is the enabler of security. The security issues for ad-hoc and sensor networks are different than the ones for fixed traditional networks such as local area networks (LANs) and wide area networks (WANs). Mobile ad hoc networks are different from mobile wireless IP networks in that there are no base stations, wireless switches, and infrastructure services like naming, routing, certificate authorities, etc. Because mobile nodes join and leave the network dynamically, sometimes even without a notice, and move dynamically, network topology and administrative domain membership can change rapidly. Thus it is important to provide security services such as availability, confidentiality, authentication [3, 4], access control, integrity, and non-repudiation.


**Figure 1.1 Mobile Ad Hoc Wireless Networks**

## RELATED WORK

Lavanya et. al proposed a protocol that is used to store secured backup routes from multiple routes available

between source and destination, in order to provide the next possible route immediately when the link fails during the data transmission. Furthermore, it incorporates security attributes as parameters into Adhoc route discovery.

The proposed SBRP protocol involves three phases:
(1). Secured route discovery across the nodes.
(2) Back up node setup.
(3). Route maintenance across the nodes.

Nadeem et al broaden their previously developed algorithm AIDP and proposed a generalized intrusion detection and prevention mechanism. They used a combination of anomaly based and knowledge-based intrusion detection. This approach not only secures the MANET from a wide variety of routing attacks but also has the capability to detect new unforeseen attacks. Simulation results of a case study show that our proposed mechanism can successfully detect a variety of attacks, including multiple simultaneous different attacks, and identify and isolate the intruders with an affordable network overhead.

Intrusion detection and prevention (IDP) provides a way to protect nodes against routing attacks. There are two ID techniques: knowledge-based intrusion detection (KBID) and anomaly-based intrusion detection (ABID). KBID has a potentially low false detection rate but it can only detect attacks whose signatures are in the database. On the other hand ABID not only provides early warnings of potential intrusions but also can detect attempts to exploit new and unforeseen vulnerabilities; however it is more prone to generate false positives than KBID.

Mamatha et al proposed a scheme to secure the data forwarding functionality in mobile ad hoc networks. The proposed approach takes advantage of the principle of flow conservation in a network and used semantic mechanism. This states that all bytes/packets sent to a node and not destined for that node, are expected to bypass the node.

The proposed algorithm aims at efficient data forwarding in MANETS and in that process monitors the misbehaving nodes or links, so that such nodes or links are avoided in data forwarding. For this purpose there can be three functional modules- Sender module, Receiver module and Intermediate node modules. To develop the proposed system, a simple acknowledgement approach is used which has two way communications. Once the sender sends the message it waits for the acknowledgement back from the receiver, to indicate that the message sent has reached the receiver. Also there are particular data frame formats which specify the various fields in the data and acknowledgement frames.

Jian Ren et al. first propose a novel unconditionally secure source anonymous message authentication scheme (SAMAS) scheme that enables messages to be released without relying on any trusted third parties. While providing source privacy, the proposed scheme can also provide message content authenticity. After that they proposed a novel communication protocol for MANET that can ensure communication privacy of the two communication parties and their end-to-end communications. In the proposed protocol, the participants are referred as the *nodes* and are organized into multiple MANETs. The nodes are further classified into *normal nodes* and *super nodes.* A normal node is a network node that can only communicate with the nodes in the local MANET. A super node can be a normal node that can also provide message forward services to the other MANETs. It can also be a special node dedicated to providing message forwarding services to the other MANETs. Each MANET should have many normal nodes and multiple super nodes. The proposed network protocol can be used for critical information distribution, infrastructure protection and secure file sharing. The security analysis demonstrates that the proposed protocol is secure against various attacks. The theoretical analysis and simulation show that the proposed scheme is efficient and can ensure high message delivery ratio.

Mahmoud et al. analyzed one of the secure mobile ad hoc networks protocols, which is Authenticated routing for ad hoc networks (ARAN). Such protocol is classified as a secure reactive routing protocol, which is based on some type of query-reply dialog. That means ARAN does not attempt to continuously maintain the up-to date topology of the network, but rather when there is a need, it invokes a function to find a route to the destination. Authors present detail study of the security attacks that the ARAN protocol defends against, criticize how an authenticated selfish node can disturb the network by dropping packets or by not cooperating in the routing functionality and proposed a reputation-based scheme called Reputed- ARAN to detect and defend against selfish nodes.

## PROPOSED ALGORITHM

**1. Main Algorithm**

**{**

1. Configure mobile ad-hoc network for 50 nodes using network simulator.
2. Form 2 clusters with each having 25 mobile nodes.
3. Form a certification authority (CA) which handles key generation and management for configured cluster of MANET.
4. Generate keys for CA using RSA which will be used for digital signature and encryption using AES.
5. Distribute key pairs to all mobile nodes in networks by CA.
6. For every message calculate message digest using SHA512 and append it to message and apply digital signature.
7. Encrypt message containing message digest and signature using private key of the sender.

**}**

**2. Algorithm for node leave**

**{**

1. Key revocation of the node that had left network by CA.
2. Inform all nodes in network so that they can remove that nodes public key from their list.

}

**3. Algorithm for node join**

**{**

1. Generate key pair for new node by CA.
2. Public key distribution for new node in cluster it joined.

**}**

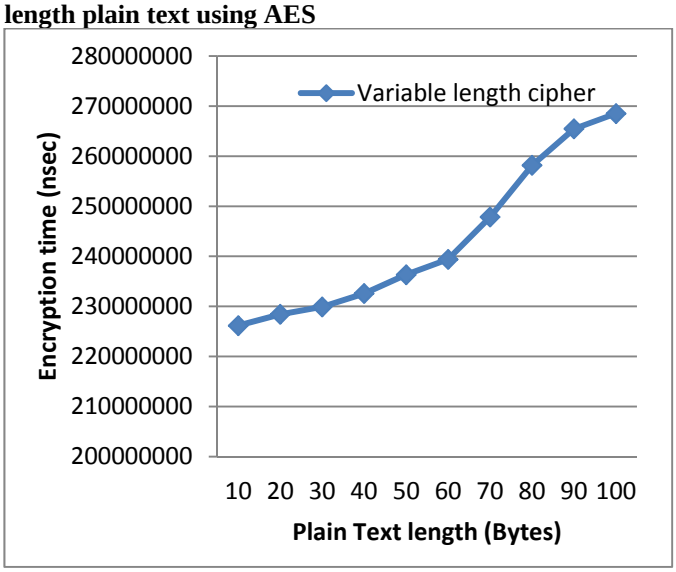
## EXPERIMENTAL SETUP AND RESULTS

In table shown below Table 1 shows results of variable length encryption. While table 2 represents fixed length encryption. Using AES algorithm. For key generation RSA is used. Time taken for key generation for variable prime numbers is shown below.

**Table 1: Encryption for different length plain text using AES (Variable length cipher)**

| PLAIN TEXT LENGTH(BYTES) | ENCYPTED TEXT LENGTH | ENCRYPTION TIME (NANOSEC) | DECRYPTION TIME |
|---|---|---|---|
| 10 | 24 | 226166489 | 1504546 |
| 20 | 44 | 228423120 | 1379516 |
| 30 | 44 | 229898746 | 1337995 |
| 40 | 64 | 232580589 | 1358522 |
| 50 | 88 | 236332618 | 1567060 |
| 60 | 88 | 239392560 | 1411240 |
| 70 | 108 | 247851999 | 1444830 |
| 80 | 128 | 258168397 | 1381849 |
| 90 | 128 | 265456951 | 1532070 |
| 100 | 152 | 268511294 | 1532070 |

**Graph 1: Comparison of encryption time for different length plain text using AES**




**Graph 2: Comparison of encryption time for variable length plain text using AES**

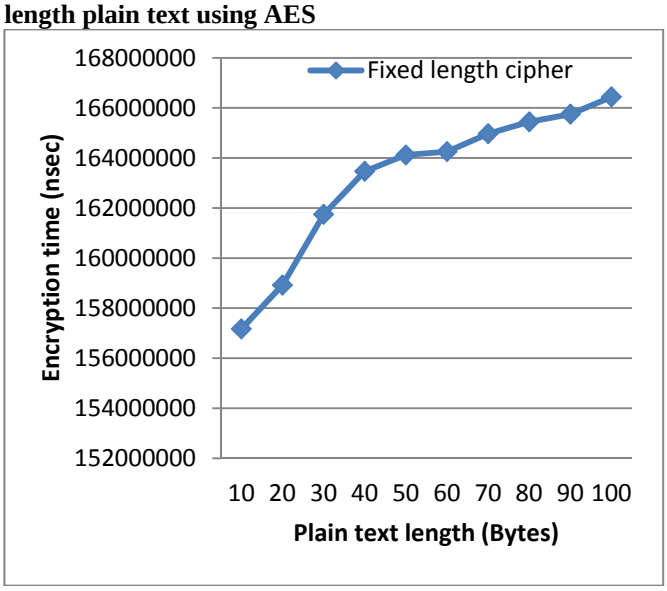



**Table 2: Encryption for variable length plain text using AES (Fixed length cipher)**

| PLAIN TEXT LENGTH(BYTES) | ENCYPTED TEXT LENGTH | ENCRYPTION TIME (NANOSEC) | DECRYPTION TIME |
|---|---|---|---|
| 10 | 172 | 157168283 | 7319321 |
| 20 | 172 | 158921929 | 6209456 |
| 30 | 172 | 161746322 | 6644724 |
| 40 | 172 | 163466392 | 7421957 |
| 50 | 172 | 164121621 | 6487038 |
| 60 | 172 | 164252729 | 7449948 |
| 70 | 172 | 164967672 | 6290632 |
| 80 | 172 | 165444466 | 6695575 |
| 90 | 172 | 165747237 | 6302761 |
| 100 | 172 | 166439556 | 6530426 |

**Table 3: Key Generation Time**

| KEY GENERATION TIME |
|---|
| 180153533 |
| 249778284 |
| 424945591 |
| 163546155 |
| 302510607 |
| 562974661 |
| 182961085 |
| 216574723 |
| 187088904 |
| 221254907 |

## CONCLUSION AND FUTURE WORK

Security has been a key issue in mobile adhoc network. There are 4 basic principles of security namely authentication, privacy, non repudiation and integrity. To maintain these principles RSA algorithm is used for pair wise key generation. AES is used for encryption to maintain privacy of data transmitted. Before any data transmission message digest is calculated using SHA512 and then digital signature is applied. Then the data packet containing message digest and signature is encrypted and transmitted. The proposed variable encryption and digital signature scheme reduces the overhead by 50%. In future key management and generation algorithms can be modified so that time taken can further be reduced.

## REFERENCES


1. Kazuo Takaragi, Kunihiko Miyazaki, Masashi Takahashi, *A Threshold Digital Signature Issuing Scheme without Secret Communication ICSAP '10. International Conference on , vol., no., pp.45-50, 9-10 Feb. 2013.*.
2. Nadeem, A.; Howarth, M.; , "A generalized intrusion detection & prevention mechanism for securing MANETs," *Ultra Modern Telecommunications & Workshops, 2013. ICUMT '09. International. Conference on* , vol., no., pp.1-6, 12-14 Oct. 2013.
3. Jian Ren; Yun Li; Tongtong Li, "Providing source privacy in mobile ad hoc networks," *Mobile Adhoc and Sensor Systems, 2013. MASS '13. IEEE 6th International Conference on*, vol., no., pp.332-341, 12-15 Oct. 2013.
4. Mamatha, G.S.; Sharma, S.C.; , "A New Secured Approach for MANETS against Network Layer Attacks," *Integrated Intelligent Computing (ICIIC), 2012 First International Conference on* , vol., no., pp.290-295, 5-7 Aug. 2012.
5. Bhalaji, N.; Shanmugam, A.; "Association between nodes to combat blackhole attack in DSR based MANET," Wireless and Optical Communications Networks, 2012. WOCN '12. IFIP International Conference on , vol., no., pp.1-5, 28-30 April 2012.
6. Vaidya, B.; Dong-You Choi; JongAn Park; SeungJo Han; "Investigation of Secure Framework for Multipath MANET," *Multimedia and Ubiquitous Engineering, 2012. MUE 2012. International Conference on* , vol., no., pp.182-185, 24-26 April 2012.
7. Stephan Eichler; Christian Roman; , "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC," Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE International Conference on , vol., no., pp.481-484, Oct. 2011.
8. Mohamed, Y.A.; Abdullah, A.B.; , "Implementation of IDS with response for securing MANETs," *Information Technology (ITSim), 2011 International Symposium in* , vol.2, no., pp.660-665, 15-17 June 2011.
9. Mahmoud, A.; Sameh, A.; El-Kassas, S, "Reputed authenticated routing for ad hoc networks protocol (reputed-ARAN)," *Mobile Adhoc and Sensor Systems Conference, 2010. IEEE International Conference on* , vol., no., pp.8 pp.-794, 7-7 Nov. 2010.
10. Lavanya, G.; Kumar, C.; Arokiaraj, A.R.M.; , "Secured Backup Routing Protocol for Ad Hoc Networks," *Signal Acquisition and Processing, 2010.*
11. C. Perkins, *Ad Hoc Networking*, Addison-Wesley 2008, ISBN 0201309769.
12. C K Toh, *Ad Hoc Mobile Wireless Networks*, Prentice Hall Publishers ,2005.
13. T.P. Pedersen, "*A Threshold Cryptosystem without a Trusted Party*", In Proc. Of Eurocrypt'91, Lecture Notes in Computer Science, LNCS 547, Springer Verlag, pp.522-526, 1991