ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 4, April 2013

# Improving authentication mechanism for using extended public key cryptography in mobile adhoc network

**Mr.Sandip A.Kahate, Mr.Onkar V.Chandure**

*Abstract*—**Mobile ad hoc network is a special kind of wireless networks formed without any centralized administration. It is a collection of mobile nodes without having aid of establish infrastructure. In mobile ad hoc network, it is much more vulnerable to attacks than a wired network due to its limited physical security, volatile network topologies, power-constrained operations, intrinsic requirement of mutual trust among all nodes in underlying protocol design and lack of centralized monitoring and management point. The main aim of this work is to provide secure data transmission between the source and destination. The proposed mechanism will authenticate the node and ensure the security of important routing information in AODV protocol.**

*Index Terms*— **Security, AODV, Routing protocol, Extended Public Key, Hybrid Cryptography, Adhoc network, nodes.**

## I. INTRODUCTION

Mobile ad hoc network consist large number of node, it form temporary network with dynamic topology Wireless cellular system has been in use since 1980s. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to other. In wireless system the device communicate via radio channel to share resource and information between devices. Due to presence of a fixed supporting structure, limits the adaptability of wireless system, so this generation of wireless system is required easy and quick deployment of wireless network. Recent advancement of wireless technologies like Bluetooth. Introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) [1], which operate in the absence of central access point. It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time.. In this network each node communicates with each other through radio channel without any central authority. In MANETs each node operates in a distributed peer-to- peer modes, serves as an independent router to forward message sent by other nodes.

MANETs has shows distinct characteristics, such as:

- Weaker in Security
- Device size limitation
- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

Apart from these limitation MANETs has many extensive application like: Military application, Natural disaster, Medical service. In ad hoc network there can be node that will try to disrupt the proper functioning network. These nodes can be malicious or selfish. They try to disrupt network function by modifying packets, injecting packets or creating routing loops. So, security is an important task, because MANETs has characteristics such as; dynamic topology, infrastructure less. There are large numbers of secure routing protocols proposed by many researchers they fulfill different security requirements and prevent specific attacks. They are divided into three categories: Reactive routing protocol [5, 6], Proactive routing protocol [5] and hybrid routing protocol [6]. In reactive routing protocol the route is discovered when it required, in proactive each node maintain network information regarding to network connectivity and route information to all others node within the network and proactive is one which is neither reactive nor proactive.

Now, the Most of the solution uses cryptography mechanism to detect selfish, malicious behavior of nodes and securing information from other types of attacks. The mechanisms which are used by different secure routing protocol to detect malicious and selfish node have address separately in different protocol. No secure mechanism has been proposed till date that can address to detecting malicious and selfish node collectively. We proposed a mechanism, Extended Public key Cryptography (EPKCH) [12] that able to detect the malicious nodes and selfish nodes collectively in order to achieving security goals such as; Authentication, Integrity, Confidentiality. Also, we proposed a routing protocol named Authenticate and Secure Routing protocol for mobile Ad hoc Network (AMSRP). We implemented EPKCH mechanism in monitor mode of AMSRP to securing MANETs. To design of this protocol follows the table-driven approach, in which each node maintain the information, regarding to network structure and route from a particular source to its all possible destination in its node info table. AMSRP is a reactive secure routing protocol.

***Mr.Sandip A.Kahate****, Asst. Prof.Department of I.T., J.D. Institute of Engg. & Technology, Yavatmal (MS) INDIA .*
***Mr.Onkar V.Chandure****, Asst. Prof.Department of I.T., J.D. Institute of Engg.&Technology,Yavatmal(MS)INDIA.*

## II. SECURITY PROBLEM WITH EXISTING ADHOC ROUTING PROTOCOL

The main assumption of the previously presented ad hoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of the protocol [7]. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks. In ad hoc network the routing function can be disrupted by internal or external attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes [9]. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. Internal attackers having capability to complete access the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers.

### A. *Design & Implementation of proposed mechanism*

The proposed mechanism is a model of secure and reliable multi-path reactive routing protocol for mobile ad hoc networks. It is divided into four modules in order to facilitate its analysis. Module I analysis of discovery and maintenance of nodes using AODV reactive routing protocol for preparation of different type of security nodes. Module II implementation of AES (Advanced Encryption Standard ) Symmetric Cryptography for encryption and decryption of 128 bit using 128,192 and 256 session key . Module III implementation of RSA Asymmetric Cryptography with MD5 pure algorithm using 1028 Extended public key cryptography for Authentication and integrity of MANET nodes. Module IV implementation of Hybrid Cryptography with combination of 128 bit using 128,192 and 256 session key and RSA Asymmetric Cryptography ,MD5 pure algorithm using 1028 Extended **Text** public key
Cryptography.

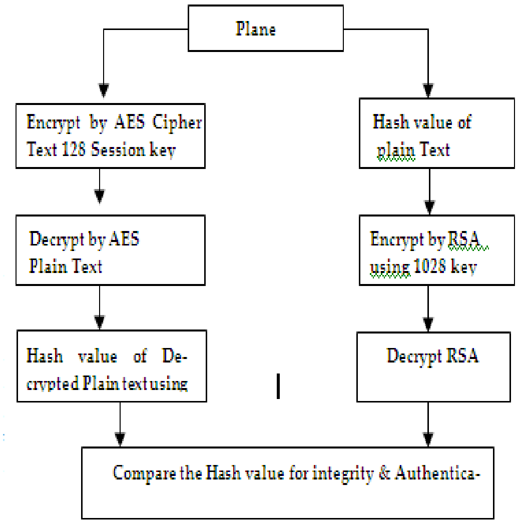

Plane
Encrypt by AES Cipher Text 128 Session key
Hash value of plain Text
Decrypt by AES Plain Text
Encrypt by RSA using 1028 key
Hash value of De-crypted Plain text using
Decrypt RSA
Compare the Hash value for integrity & Authentica-

Fig.1.Proposed architecture

### B. *Hybrid security protocol architecture*

As shown in the figure, the Symmetric Key Cryptographic Techniques such as AES Cryptography and MD5 are used to achieve both the Confidentiality and Integrity. The Asymmetric Key Cryptography technique, Dual RSA used for Authentication.

The above discussed three primitives can be achieved with the help of this Security Protocol Architecture. The Architecture is as shown in the **Figure 1**. As shown in the figure, the Symmetric Key Cryptographic Techniques such as AES Cryptography and MD5 are used to achieve both the Confidentiality and Integrity. The Asymmetric Key Cryptography technique, RSA with *Extended Public Key Cryptography* 1028 used for Authentication.

The new Security Protocol has been designed for better security. It is a combination of both the Symmetric and Asymmetric Cryptographic Techniques(Hybrid Cryptography). It provides the Cryptographic Primitives such as Integrity, Confidentiality and Authentication.

The given plain text can be encrypted with the help of AES Cryptography 128 session key, AES and the derived cipher text can be communicated to the destination through any secured channel. Simultaneously, the Hash value is calculated through MD5 for the same plain text, which already has been converted into the cipher text by AES. This Hash value has been encrypted with RSA and the encrypted message of this Hash value also sent to destination.

The intruders may try to hack the original information from the encrypted messages. He may be trapped both the encrypted messages of plain text and the hash value and he will try to decrypt these messages to get original one. He might be get the hash value and it is impossible to extract the plain text from the cipher text, because, the hash value is encrypted with RSA and the plain text is encrypted with AES. Hence, the message can be communicated to the destination with highly secured manner.

The new hash value is calculated with MD5 for the received originals messages and then it is compared with decrypted hash message for its integrity. By which, we can ensure that either the original text being altered or not in the communication medium. This is the primitive feature of this hybrid protocol.

## III. IMPLEMENTATION

Module Implementation Status

a) Phase1:Performance Analysis of AODV

b) Phase2:AES Implementation Module

c) Phase3:RSA & MD5 Implementation Module

**Phase 1: Performance Analysis of AODV (Route Discovery & Maintenance):**

• *Route Request Message RREQ:*
Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

• *Route Reply Message RREP:*
A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

• *Route Error Message RERR:*
Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, Route error (RERR) message is generated by the node in order to notify other nodes that the link is do

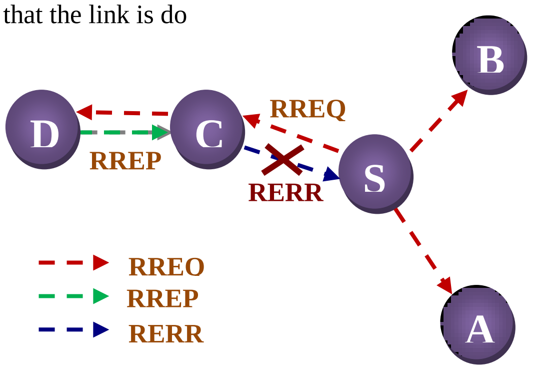


Fig.2 Route Discovery

*Route Discovery in AODV:*

- A source node S wishes to communicate with destination node D broadcast a Route Request (RREQ) to its neighbors
- Intermediate nodes forward the RREQ to their neighbors
- The destination node sends a Route Reply Message (RREP) back to the source node
- An intermediate node may send a RREP provided that it knows a 'fresh enough' route to the destination
- Nodes maintain routing table entries only for active routes, unused routes are removed from the routing table after *active_route_timeout* interval
-

**Phase 2:AES Implementation Module**

This standard specifies the Rijndael algorithm a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.Mathematical properties that are useful in understanding the algorithm. Algorithm specification, covering the key expansion, encryption, and decryption routines; Implementation issues, such as key length support, keying restrictions, and additional block/key/round sizes.The algorithm was designed to have the following characteristics:

• Resistance against all known attacks
• Speed and code compactness on a wide range of platforms
• Design simplicity
• Input to the encryption algorithm, decryption algorithm in a single 128 bit block
In AES, four different stages are used
1. Substitution bytes
Use S-box to perform byte-to-byte substitution of the block
2. Shift rows
A simple permutation
3 Mix columns

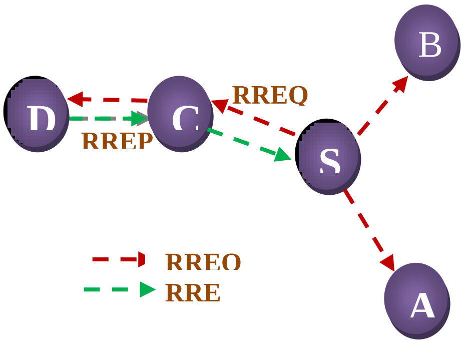
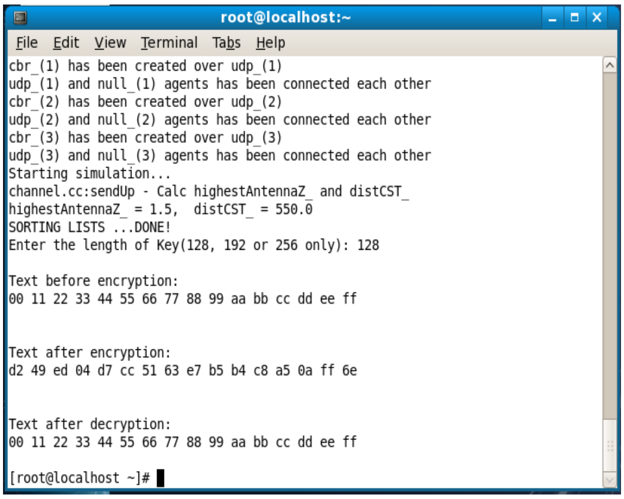


Fig.3 Route maintenance



```
cbr_(1) has been created over udp_(1)
udp_(1) and null_(1) agents has been connected each other
cbr_(2) has been created over udp_(2)
udp_(2) and null_(2) agents has been connected each other
cbr_(3) has been created over udp_(3)
udp_(3) and null_(3) agents has been connected each other
Starting simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Enter the length of Key(128, 192 or 256 only): 128

Text before encryption:
00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff


Text after encryption:
d2 49 ed 04 d7 cc 51 63 e7 b5 b4 c8 a5 0a ff 6e


Text after decryption:
00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

[root@localhost ~]# 
```

Fig.4Screenshot of AES Encryption & Decryption Process

using length of key 128 in NS2

**Phase 3: RSA & MD5 Implementation Module**

**i) RSA Algorithm**

The RSA algorithm uses two keys, *d* and *e*, which work in pairs, for decryption and encryption, respectively.

- A plaintext message P is encrypted to cipher text by: C = P*e* mod *n*
- The plaintext is recovered by: P = C*d* mod *n*
- Because of symmetry in modular arithmetic, encryption and decryption are mutual inverses and commutative. Therefore,

P = C*d* mod *n* = (P*e*)*d* mod *n* = (P*d*)*e* mod *n*

- Thus, one can apply the encrypting transformation first and then the decrypting one, or the decrypting transformation first followed by the encrypting

**ii) RSA & MD5 Implementation Module:**

- MD5 algorithm can be used as a digital signature mechanism.
- This presentation will explore the technical aspects of the MD5 algorithm.
- Takes as input a message of arbitrary length and produces as output a 128 bit "message digest" of the input.
- It is computationally infeasible to produce two messages having the same message digest.

- Intended where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as RSA

## IV. IMPLEMENTATION WORK

### ❖ Hybrid Cryptography

**Overview of Hybrid Encryption Approach**

This proposed mechanism presents a secure communication between the mobile nodes using Hybrid cryptography. A scenario of data transmission between the two mobile nodes has been considered. Whenever a source wants to transmit the data packets to the destination, it ensures that the source is communicating with real node. The authentication service uses a key management to retrieve the extended public key, which is trusted by the third party for identification of the destination. The destination also used similar method to authenticate the source. After execution of the key management module, a shared key is invoked; this is used by both source and destination for further communication confidentially. In this way, all the important messages are transmitted to the destination.

### ❖ Hybrid Encryption Technique

In this hybrid encryption approach, sender side using 128-bit session key value with AES-Rijndael to encrypt the message. The hash value of message was encrypted using RSA algorithm with 1028 bit Extended Public key of the receiver. In the receiver side the decryption done for the encrypted message using AES-Rijndael with 128-bit session key value. To calculate the hash value using hash function MD5 for the original message. Using RSA with 1028 bit extended private key of the receiver to decrypt the encrypted hash value. To ensure the integrity the comparison performed between calculated and decrypted hash values. Figure 5 and figure 6 explain this process.

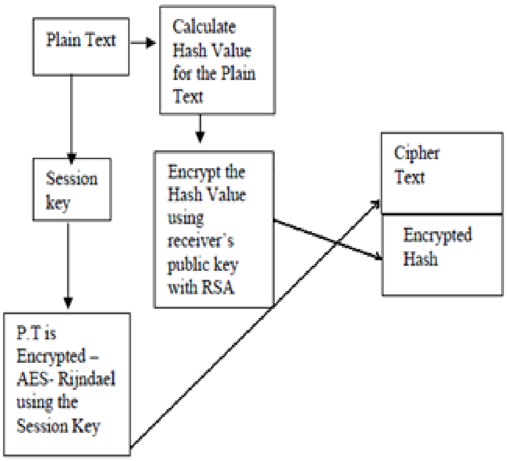

Plain Text
Calculate Hash Value for the Plain Text
Session key
Encrypt the Hash Value using receiver's public key with RSA
Cipher Text
Encrypted Hash
P.T is Encrypted – AES- Rijndael using the Session Key

Fig.5. Hybrid Encryption Approach

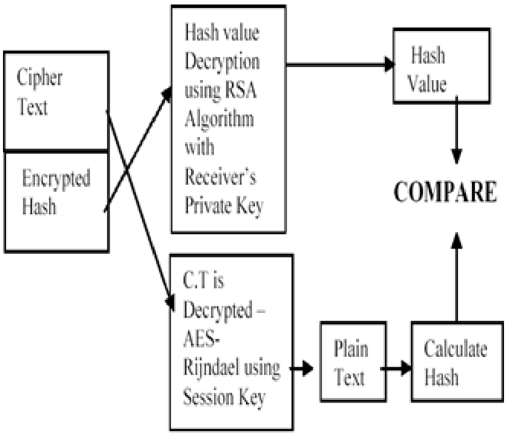

Cipher Text
Encrypted Hash
Hash value Decryption using RSA Algorithm with Receiver's Private Key
Hash Value
COMPARE
C.T is Decrypted – AES- Rijndael using Session Key
Plain Text
Calculate Hash

Fig.6. Hybrid Encryption Technique

## V.IMPLEMENTATION AUTHENTICATION SECURITY IN MANET

### A) Algorithm

**Step 1:** The public key and private key for each node is generated using RSA algorithm

**Step 2:** After generating private key and public keys, the source (S) and destination (D) performs public key exchange using its own private key

**Step 3:** encryption of message at S and decryption by D occurs.

**Step 4:** Once the sender starts its transmission, each node will generate its own certificate using MD5 pure algorithm

**Step 5:** The neighbor node will check the certificate and after making verification, it will deliver the packet meant for destination

**Step 6:** If any node which is not a member of this transmission process tries to get the packet by issuing a certificate,

**Step 7:** the node may be considered as an intruder and the certificate will be considered as a bad certificate.

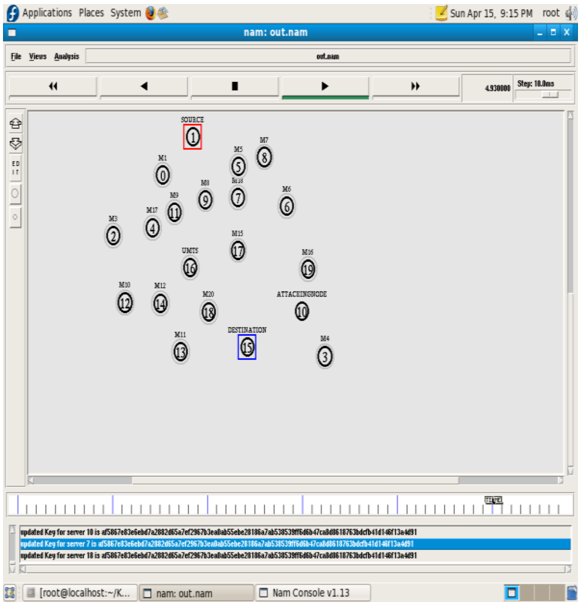
## VI. RESULT & DISCUSSION

*A Scenario Description*

Routing is done with *Authentication Mechanism Secure Routing Protocol (AMSRP)* using AODV protocol. Encryption and Decryption by AES Algorithm. Certificate generation is by MD5 pure Algorithm for integrity and Authentication provided by RSA. Initially all the nodes are fully energized. It prepares to start its transmission. The red shade square indicates that a node has source node (Node 1) i.e. active mode. The blue shade square indicates that it has gone for destination node (Node 15). The source starts its transmission in active mode and then to destination node.

The recipient after getting the message goes to destination node in order to transmission packets. The next state is , some nodes may go into weak state which is shown by an yellow shade as each node may spent its energy by encrypting and decrypting and in certificate checking by CA node (Node 3).

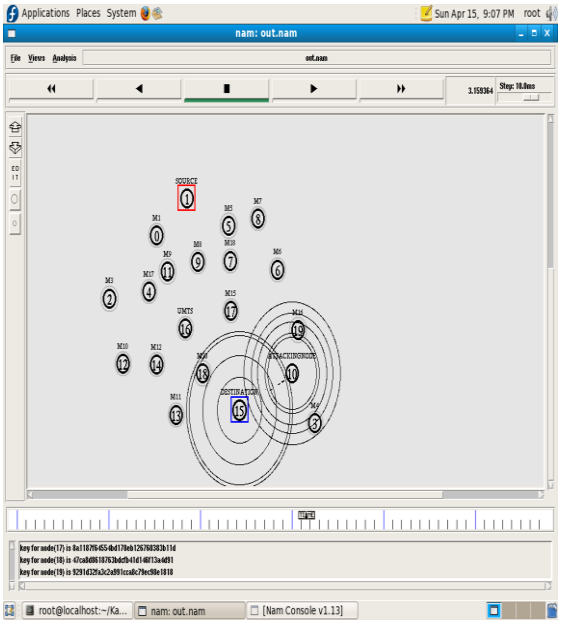
But the malicious node (node 10) which is with full energy level may try to interpret the message from the destination. Now, the malicious node (node 10) enters into the zone and tries to intercept the message from its nearest destination and sends a fake certificate to active neighboring nodes. As the node finds it, the malicious node's request gets rejected. So some of the energy is spent and so, to retain its remaining energy, the node again moves to before the time scale comes to an end, many nodes go to sleep state as they get exhausted in certificate checking and verifying. The figure 7 shows the simulation scenario of the nodes. This process affirms an end-to-end authentication security for the entire period of transmission. As the security feature is much concentrated, it minimizes some delay and increases throughput.



```
updated Key for server 10 is af5867e83e6ebd7a2882d65a7ef2967b3ea0ab55ebe28186a7ab538539ff6d6b47ca8d8618763bdcfb41d146f13a4d91
updated Key for server 7 is af5867e83e6ebd7a2882d65a7ef2967b3ea0ab55ebe28186a7ab538539ff6d6b47ca8d8618763bdcfb41d146f13a4d91
updated Key for server 18 is af5867e83e6ebd7a2882d65a7ef2967b3ea0ab55ebe28186a7ab538539ff6d6b47ca8d8618763bdcfb41d146f13a4d91
```

Fig.7

Node Scenario



```
key for node(17) is 8a1187f64554bd178eb126760383b11d
key for node(18) is 47ca8d8618763bdcfb41d146f13a4d91
key for node(19) is 9291d32fa3c2a991cca8c79ec98e1818
```

Fig 8. Communication between nodes

To evaluate the improving authentication performance efficiency, the Event driven simulator NS-2.34 is used for simulations of proposed protocol.

Following table shows the simulation parameters used for this project

| Parameters | Values |
|---|---|
| Simulator | Ns-2(version 2.32) |
| Simulation Time | 20 (s) |
| Number of Mobile Nodes | 20,50,80,100 |
| Topology Area | 1200 * 1200 (m) |
| Routing Protocol | AODV |
| Packet size | 512 Bytes |
| Malicious Node | 01 (Node 10) |
| Communication Traffic | TCP |

Table 1. Simulation Parameter

### *B. Simulation Results*

The results that are presented here consist of the comparison between reactive Ad-hoc On-demand Vector Routing Protocol (AODV) & Authenticate Mechanism Secure Routing Protocol (AMSRP). Two scenarios have been constructed, one using AODV and another using AMSRP Protocol. Following figures 6.4 and 6.5 shows the graph for throughput of packets. Throughput of packet using AMSRP is more as compared to AODV, because packet loss in AMSRP is minimum as shown in figure 6.5. Hence the numbers of packets transmitted are more with AMSRP protocol.

*1.Throughput:* It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations

Throughput = Σ number of packets delivered / Time interval length

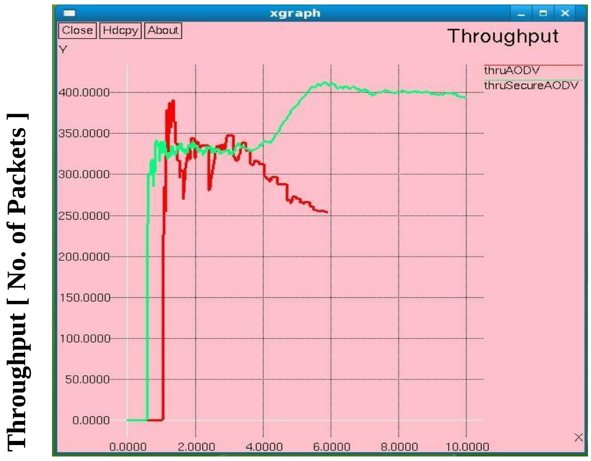


Fig.9.Throghput of packets

The above graph shows the comparison of standard AODV protocol with the proposed AMSRP in terms of network throughput. On X axis, simulation time is shown and Y axis shows network throughput. The red line indicates network throughput obtained by AODV protocol and green line indicates network throughput obtained by proposed protocol.

- **Evaluation of Throughput For AODV and AMSRP (Kbps)**

| **Nodes** | **20** | **50** | **80** | **100** |
|---|---|---|---|---|
| **AODV** | 253.94 | 312.60 | 321.62 | 136.39 |
| **AMSRP** | 312.6 | 287.51 | 321.62 | 322.12 |

Table 2. Throughput For normal AODV and AMSRP

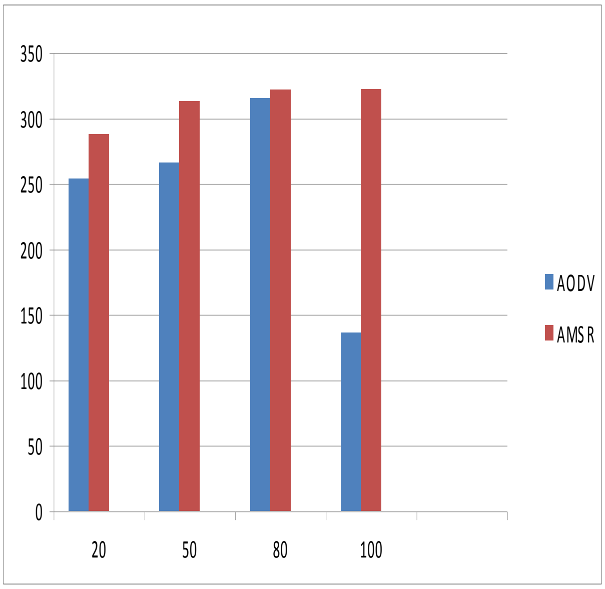


Fig.10 Throughput For normal AODV and AMSRP

*2. End to delay (e2e):* it refers to the time taken for a packet to be transmitted across a network from source to destination

End to end delay D =Td-Ts
Where Td is the packet receive at the destination
Ts –Packet send by the source node

The above graph depicts the comparison of standard AODV protocol with the proposed AMSRP protocol in terms of end to end delay. On X axis, number of packets are shown and Y axis shows delay in seconds. The red line indicates delay in AODV protocol and green line indicates delay in proposed protocol.

- **Evaluation of End to End Delay for AODV & AMSRP**

In this, e2e delay is calculated for normal aodv protocol with different mobile nodes.(simulation time 20 s)

| Nodes | 20 | 50 | 80 | 100 |
|---|---|---|---|---|
| AODV | 2.78985 | 2.78985 | 2.78985 | 2.78985 |
| AMSRP | 0.598157 | 0.598157 | 0.598157 | 0.598157 |

Table.3 E2e Delay For Normal AODV and AMSRP

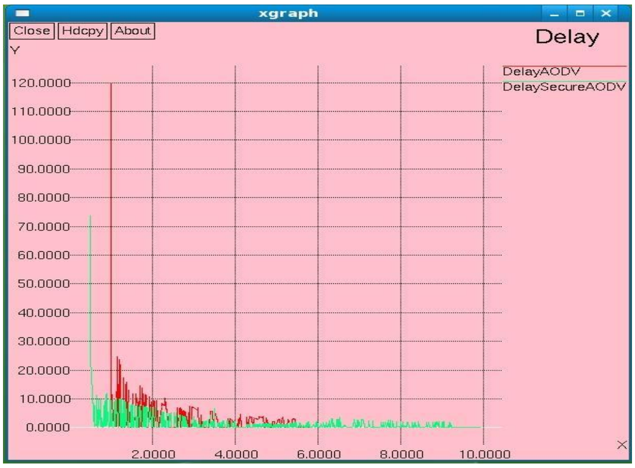


Fig.11.end to end delay comparison

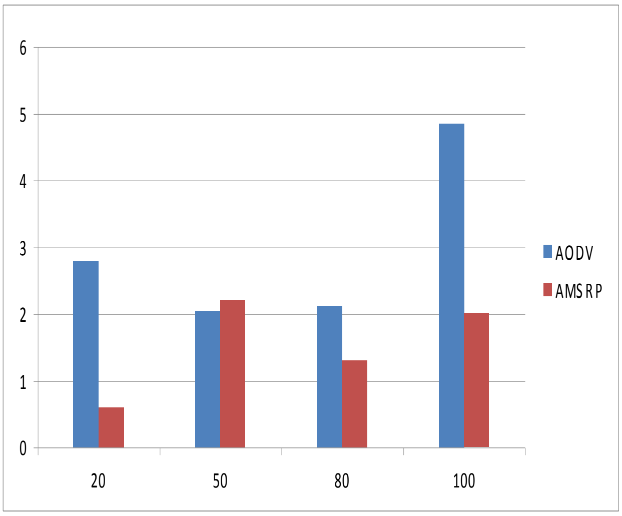


Fig.12 Number of Nodes & E2e For AODV and AMSRP

## VII. CONCLUSION & FUTURE WORK

There are various MANET protocols proposed by the subject to a variety of attacks through the modifications or fabrications of routing message or impersonations of other nodes. Wireless mobile ad hoc networks present difficult challenges to routing protocol designers. Mobility, constrained bandwidth, and limited power cause frequent topology changes. The very basic nature of the mode of communication is the main concern because anything that moves over the open air medium is susceptible to be picked up by unauthorized access. For any mission critical or organizationally sensitive information, ad hoc networks add an element of insecurity

It allows the attackers to influence the victim's selection of routes or enable the denial of service attacks. In this mechanism, we have implements the security issues for MANETs.

In the existing secure routing protocols most of the security attacks are possible with a compromised node. In this work we have focus on how to detect malicious and selfish node and to design and implement a secure routing protocol.

In AMSRP protocol we discuss various activity of node which they are shown during the MANET operation and these activities are grouped into modes along their working. We also discussed the packets that are going to be exchanged in different mode of nodes. The conclusion that comes are given below.

**I.** The problems of malicious and selfish node are handling simultaneously. We discussed Extended Public key cryptography mechanism to handle the malicious and selfish node during network operation. As the selfish node cannot malicious at same time, but if nodes are not malicious then they may be malicious.

II. The protocol is handling the some special situation like nodes joining the network, node leaving the network and nodes are changing its position within the network. The monitor mode of AMSRP handles all three situations.

III. The protocol has to develop in the way so that the future modifications are possible without changing overall protocol.

The proposed secure routing protocol, AMSRP, is based on reactive routing protocol on demand distance vector approach. For the future work we can use the hybrid approach in AMSRP to implement a new secure routing protocol. We can also add another mode or existing one can be extended to handle some exceptional conditions. The public key cryptography algorithm can also be extended to securing MANET.

## REFERENCES

[1] Rachika Gupta (2011) *"Mobile adhoc network(MANETS):Proposed solution to security related issues*", Indian J. Computer Science and Engineering (IJCSE) 2(5):748-46

[2] Sameer Hasan Al-Bakri1, M. L. Mat Kiah1, A. A. Zaidan2,4, B. B. Zaidan *"Securing peer-to-peer mobile communications using public key cryptography: New security strategy"*, International Journal of the Physical Sciences Vol. 6(4), pp. 930-938, 18 February, 2011,IJPS ISSN 1992 - 1950 ©2011 Academic Journals

[3] Shashi Mehrotra Seth, Rajan Mishra,*"Comparative Analysis Of Encryption Algorithms For Data Communication"* International Journal Of Computer Sci Ence And Technology, Ijcst Vol. 2, Iss Ue 2, June 2011 ISSN : 2229-4333 (PRINT) | ISSN : 0976-8491 (On LINE ),

[4] Haghparast and I. FauziI, Snin R. Eslaminejad *"Detection Wormhole in Wireless Ad-hoc Network"*, International Journal of Computer Science & Telecommunications ,Volume 2, Issue 7, October 2011 ISSN 2047-3338

[5] Mr. Bhushan M. Manjre 1, Mrs.Veena A. Gulhane *"Secure and Reliable Ad-Hoc on Demand Multipath Distance Vector Routing Protocol for Mobile Ad Hoc Networks"* 2, 2011 International Conference on Information and Network Technology, IPCSIT vol.4 (2011) © (2011) IACSIT Press, Singapore.

[6] B. Sreedevi S. Ramanujan, Centre, Sastra University, Kumbakonam, Y. Venkatramani, *Saranathan "Implementing End-To-End Reliability and Energy Conservation Routing to Provide Quality of Service in Mobile Ad hoc Networks"* European Journal of Scientific Research ISSN 1450-216X Vol.55 No.1 (2011), pp.28-36

[7] S. Subasree and N. K. Sakthivel, *"Design of a New Security Protocol Using Hybrid Cryptography Algorithms"* IJRRAS 2 (2) , February 2010

[8] Shervin Ehrampoosh and Ali Khayatzadeh Mahani, *"Secure Routing Protocols: Affections on MANETs Performance"*,First International Conference on Communication Engineering,22-24 Dec2010,University of siston & Balucheston.

[9] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan, *"Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption"* Standard International Journal of Computer Theory and Engineering, Vol. 2, No. 2 April, 2010 1793-8201

[10] Subashri T1, Arunachalam R, *"Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory"* International journal of VLSI design & Communication Systems (VLSICS) Vol.1, No.4, December 2010

[11] Syed S Rizvi (2010) *"Combining private and public key encryption techniques for providing extreme secure environment for an academic institution application"*. Int. J. Network Security & Its Application (IJNSA), 2(1)2010.

[12] Dr. E. Ramaraj1, S. Karthikeyan2 and M. Hemalatha3, *"A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA)"* International Journal of Computer ScienceVolume3,Issue 5, 2010.

[13] Liana Khamis Qabajeh1 Miss Laiha Mat Kiah1, *"A Scalable and Secure Position-Based Routing Protocol for Ad-Hoc Networks"* Malaysian Journal of Computer Science, Vol. 22(2), 2009

[14] Dr. Harsh Sadawarti and Anuj K. Gupta, *"Secure Routing Techniques for MANETs "*, IAENG, International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009 1793-8201

[15] M. Gunasekaran1, P. Sampath, B. Gopalakrishnan, *"AAS: An Authenticated Acknowledgement- Based Scheme for Preventing Selfish Nodes in Mobile Ad Hoc Networks"* International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009

[16] A. Arul Lawrence Selvakumar, and C. Suresh Ganandhas, *"A Study of Crypt analysis Hash function"*, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009

[17] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, *"A Survey of Secure Mobile Ad Hoc Routing Protocols"*, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 10, NO. 4, FOURTH QUARTER 2008

[18] YihChun Hu Carnegie, David B. Johnson *"Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols"*,*WiSe 2003*, September 19, 2003, San Diego, California, USA.Copyright 2003 ACM 1581137699/03/0009

[19] Geetha Jayakumar† and Gopinath Ganapathy *"Performance Comparison of Mobile Ad-hoc Network Routing Protocol"*, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007

**AUTHORS PROFILE**

**1. Sandip A. Kahate –** B.E. in computer science and engg. from Amravati university**,** M.E.in Wireless Communication and Computing,from Nagpur University and preparation for Ph. D. registration. He is currently working as a Assistant Professor in Information Technology Department, Jawaharlal Darda Institute of Engineering and Technology, MIDC, Lohara, Yavatmal-445001.(M.S.), India., He has 8 years of teaching experience. He is author of 1 research paper, with 2 paper in international journal and 1 in international conference in India. His areas of interest are Wireless Communication and computing, network security and Ad-Hoc Network.

**2. Onkar V. Chandure** received his Bachelor Degree in Information Technology With distinction from Amravati University Amravati, INDIA in 2008.He has also received Master Degree in Information Technology in 2012 From Sant Gadge Baba Amravati University,Amravati,INDIA. He recently towards his PhD. He is currently working as an Assistant Professor in Information Technology Department J.D. Institute of Engineering & Technology, Yavatmal, India. His fields of interest include mobile adhoc network.