Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 6, June-2016

# Secure Authentication Approach for Routing in MANET using Group Signature

**Nidhi J. Patel[1], G.B.Jethava[2]**

[1]*Student of M.E(CE) Parul Institute of Engineering and technology India*
[2]*Asst. Professor Parul Institute of Engineering and technology India*

**Abstract** — *A Mobile ad hoc network (MANET) sharing a wireless channel among collection of mobile nodes without any centralized control. Set a secure path for data transfer from one node to another node is difficult Due to dynamic topology of network. The nodes which exist inside the network cannot be always trusted. During transmission Security of routing information is major concern. There are several routing protocols are available for secure data transfer from one node to another but still they venerable from verity of attacks. Many techniques are available for secure routing information but still security is not fully satisfied. An attempt has been made to improve the security during transmission in MANETs with minimum overhead. RSA public key encryption provide secure routing of data and can defend against attacks like black hole*

***Keywords- MANET, Security, Authentication, RSA Asymmetric Encryption Scheme***

## I. NTRODUCTION

A mobile ad hoc networks (MANETs) are continuously, infrastructure-less, self-configuring network of mobile nodes connected without wires. MANET have dynamic topology, any node can free to join the network and remove from network Each device in a MANET is free to move freely in some direction and thus modification its links to other devices commonly [12]. MANET is group of mobile devices which share wireless channel without any centralized control over a mobile nodes of network and they can move independently in network.

In MANET each node serve as independent router to forward the message which is sent by another mobile node. The nodes which exist inside the network cannot be always trusted. Due to dynamic characteristic of ad hoc network, Secure routing in ad hoc network become a challenging task. Most of threats target the routing protocol and causes verity of attacks. Providing secure path from source to destination and defend against verity of attacks is necessary. Secure path can be provide by proper authentication. There are several authentication technique available which shown in literature survey, but still security is not fully satisfied.

Further this paper is organized as follows: In section II, Present the literature done for authentication technique. In section III, proposed method is explained. Section IV discuss the experimental results and finally section V concludes the paper

## II. RELATED WORK

There are many authentication algorithm are proposed for secure routing. These algorithm presented in this literature survey.

In [1], Author proposed method used the authentication technique like “nested message authentication code to secure the routing packet” in AODV and avoid occurred attacks such as black hole attacks, modifying routing attacks. Key pre distribution is used and “Nested Message Authentication Code (NMAC)” is used where different keys are designated based on the hop count value from key table, so it is not identify by the opponent because this technique used hop by hop technique(HBKS).

In [2], In this paper Author proposed “secure token” by cryptographic algorithm AES and hashing algorithm SHA2 to secure the data and provide privacy between the sender and receiver. To secure data packet, adding a digital signature by symmetric cryptography using the AES algorithm and the SHA2 hash function. It is more suitable to a mobile environment. Data integrity and confidentiality can be achieved by data encryption using strong symmetric key algorithm such as AES. Without having digital certificate node can’t participate in network communication.

In [3],In this paper Author gave maximum priority to Security of the routing information. Author proposed “Zone Routing Protocol (ZRP) and hashing algorithm, keyed-Hash Message Authentication Code – Secure Hashing Algorithm 256 (HMAC-SHA256)” is used for the Authentication purpose, Which ensure data Integrity of information which have been sent. Author also proposed in addition a “Trust-Based system” is formed for avoiding the Denial-of- Services (DoS) Attacks.

In [4], In this paper, authors proposed new routing protocol, authenticated anonymous secure routing (AASR). They used “group signature” for providing authentication which protect against potential active attacks. The “key encrypted Onion routing” is used with secret root verification message is designed to avoid intermediate nodes from assuming a real destination for packet. In

AASR for unidentifiability and unlinkability, proof of identity of nodes and routes are replaced by "random numbers or pseudonyms" for protection purposes.

## III. PROPOSED WORK

**Group Signature Scheme:** Mobile ad hoc networks(MANETs) is a group of mobile nodes allocation a wireless channel without any centralized control. Group Signature scheme is used for Authentication purpose. Group signature involve entire network T as a group and every nodes in a group have public key and private key pair. The group public key represented by $G_{A+,}$ which is same for all nodes in a group and the group private key represented by $G_A$- which is different for each nodes in a group.

**Asymmetric Encryption Algorithm:** In mobile ad hoc network secure path from source to destination is important task. MANET which are mostly constrained networks with slightest resources, identification of suitable asymmetric cryptosystem is a vital one. RSA is public cryptosystem which is used for secure transmission over network. Public cryptosystem also known as asymmetric cryptography.
In this kind of cryptosystem, publicly available key is the encryption key and same to the genuine nodes and differs from the decryption key which is unique for all nodes its need to be kept secret. RSA create and then publish public key using two long prime numbers, p and q, which need to be kept secret.

Numerous 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)
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 number p and q
The p,q are the integer must be chosen at random manner, and must be similar in magnitude but different in length by a few digits to make factoring harder.
2. Calculate the modulus $n = p \times q$
Here, n is used for the modulus for both the public and private keys. Its length is usually expressed in bits which known as a the key length.
3. Calculate the totient $\varphi(n) = (p - 1) \times (q - 1)$
Where φ is Euler's totient function. This value is kept private.
4. Select for public exponent an integer e such that $1 < e < \varphi(n)$ and $\gcd(\varphi(n), e) = 1$
Here, *e* and φ(*n*) are coprime.
5. Calculate for the private exponent a value for d such that $d = e^{-1} \bmod \varphi(n)$
Where, d is the modular multiplicative inverse of e (modulo φ (*n*)).
6. Public Key = [e, n]
7. Private Key = [d, n]

**Encryption**
For encryption purpose, Suppose node A want to send data packet "m" to node B, then node A encrypt the data packet through public key which is shared between all nodes of group.

$$C = m^e \pmod n$$

**Decryption**
Node B receive data packet in encrypted form and B decrypt received packet using its private key which is unique one. Node B can recover original data by applying decryption.

$$C^d = (m^e)d = (\text{mod } n)$$

## IV. EXPERIMENTAL RESULTS

In proposed work we can successfully implemented asymmetric encryption algorithm in mobile ad hoc network. We are using RSA for asymmetric encryption purpose. Proposed system performance examine by proving security by RSA asymmetric encryption, its provide hop by hop authentication. Results shows the comparison of with detection black hole and used RSA asymmetric encryption for security purpose and without detection of black hole (ex. DSR protocol ). Simulation parameter and results are shown below.

**Simulation Parameters**
Simulation parameters are shown in the table below:

| | |
|---|---|
| Simulation Used | NS-2.32 |
| Number of Nodes | 50,60,70,80,90,100 |
| Dimension of Simulation Area | 1000 * 1000 |
| Routing protocol | TBEED (DSR,RSA) |
| Simulation Time | 794.3 ms |
| Antenna Type | Omni Antenna |
| MAC Protocol | IEEE 802.11 |
| Queue | DropTailPriQueue |
| Channel Type | Wireless Channel |
| Packet Size | 152 byte |

***Table 1 Simulation Parameters***

**Packet Delivery Ratio:** It is the ratio of number of packets received and number of packet send from source to the destination.

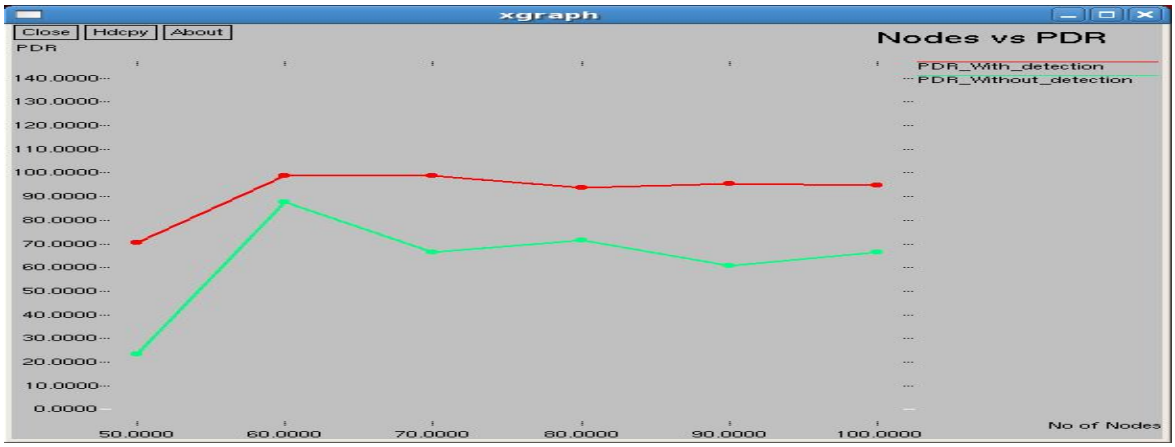
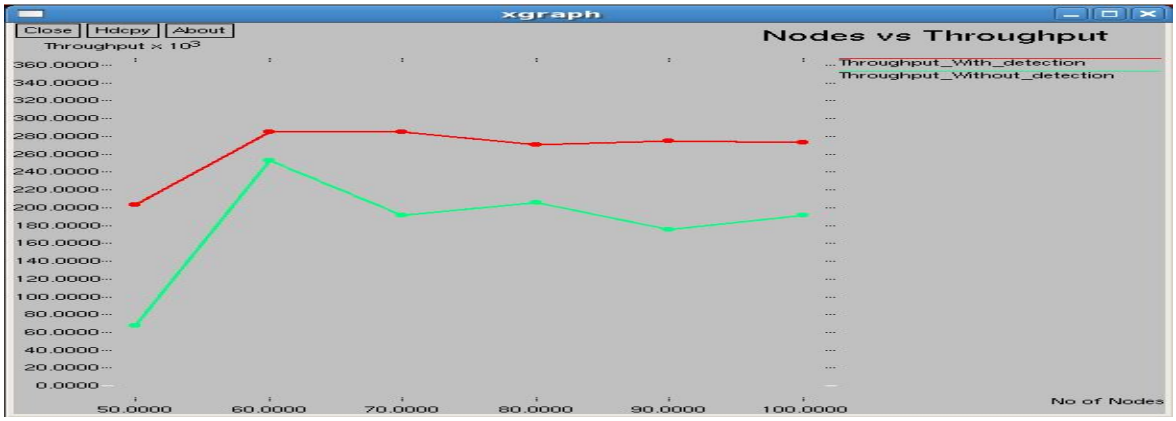



***Figure. 1 Comparison with detection and without detection of (PDR v/s Nodes)***

**Throughput:** Throughput is the rate of production or the rate at which something can be processed. Throughput or network throughput is the rate of successful message delivery over a communication channel per unit time.




***Fiagure. 2 Comparison with detection and without detection of (Throughput v/s Nodes)***

**Overhead:** The time it takes to transmit data packet on a wireless network. Each packet requires extra bytes of format information that is stored in the packet header, which is reduces the overall transmission speed of the raw of data.

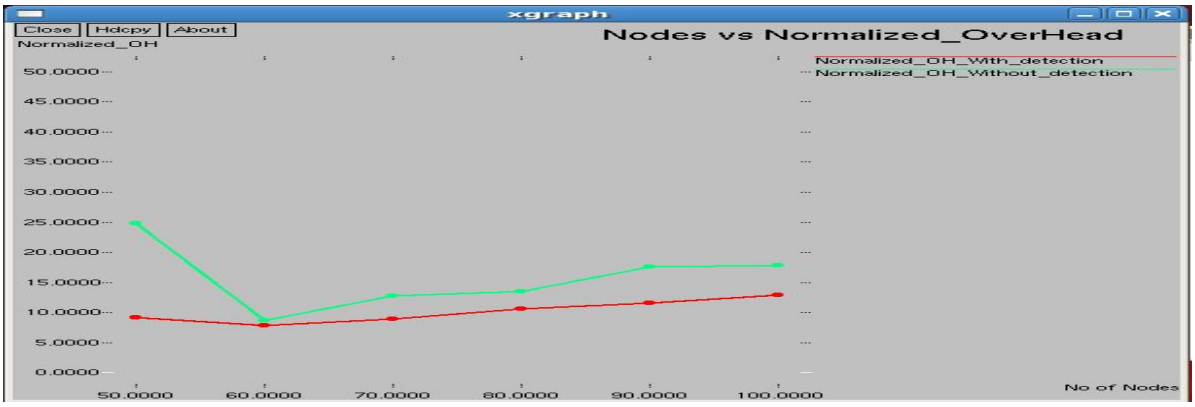



***Figure. 3 Comparison with detection and without detection of (Normalized_OverHead v/s Nodes)***

## CONCLUSION & FUTURE WORK

Mobile Ad Hoc Networks (MANETs) has the advantage that it can be deployed quickly by mobile nodes without any pre-existing network infrastructure. However, dynamic topology by movement of nodes makes it difficult to set secure path for the data transfer and make the network susceptible to a variety of attacks. The nodes inside the network cannot always be trusted. Security of routing information is a major concern. Main aim to provide securely data transfer using authentication approach. Group Signature technique used for authentication to provide secure path. RSA asymmetric encryption algorithm is used for provide secure path during routing packets, and defend against attacks like black hole.

In Future work try to use another technique of low weight asymmetric encryption technique and compare the corresponding result.

## REFERENCES

[1] K. V. Arya, Shyam Singh Rajput," Securing AODV Routing Protocol in MANET using NMAC with HBKS Technique", IEEE, pp. 281-285, 2014

[2] S.S.Zalte, Prof.(Dr.)Vijay R.Ghorpade, "Secure Token for Secure Routing of Packet in MANET",IJCSIT vol. 5(6), pp. 6916 – 6919, 2014

[3] Dilli Ravilla,Dr Chandra Shekar Reddy Putta," Routing Using Trust Based System with SHA-2 Authentication ", ELSEVIER vol-46, pp.1108 – 1115, ICICT 2014

[4] Wei Liu, Member, Ming Yu," AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments",IEEE vol. 63, pp. 4585 – 4593, November 2014

[6] Miss Morli Pandya, Associate Prof. Ashish Kr. Shrivastava, "Review on security issues of AODV routing protocol for MANETs", IOSR Journal of Computer Engineering vol-14, pp. 127- 134, Sep. - oct.2013

[7] Sarvesh Tanwar, Prema K.V, "Threats & Security Issues in Ad hoc network: A Survey report",IJSCE vol-2, pp 138-143, January 2013

[8] Devesh Kumar pal, Dr. pallavi Murghai Goel," Survey Security Issues in Mobile Ad Hoc",IJCSIT vol-5, pp. 3732-3735, 2014

[9] Vivek Richhariya,Praveen Kaushik," A Survey on Network Attacks in Mobile Ad Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering vol – 4, pp. 131- 133, May 201

[10] Ali Dorri, Seyed Reza Kamel, Esmail kheyrkhah "SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY",IJCSES vol-6, February 2015

[11] Spinder Kaur1, Harpreet Kaur2," Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature", ijaret vol-3 pp. 24-28, May 2015

[12] https://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[13] https://en.wikipedia.org/wiki/RSA_(cryptosystem)