# POR: Privacy-Preserving On-Demand Routing Scheme to Mitigate Malicious Nodes in Mobile Ad Hoc Networks

M. Gunasekaran
Bannari Amman Institute of Technology
Sathyamangalam, Tamil Nadu, India

K. Premalatha
Bannari Amman Institute of Technology
Sathyamangalam, Tamil Nadu, India

## ABSTRACT

A Mobile Ad Hoc Network (MANET) is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services. Providing privacy and security is a critical problem when implementing MANET in an adversarial environment. A malicious node may pose a serious security threats for communication in the network. Such nodes participate in the route discovery and data forwarding phase and degrade routing performance. A privacy-preserving on-demand routing (POR) scheme is proposed to mitigate the effects of malicious nodes through anonymity related features. The POR is designed based on the combination of an identity-based group signature scheme and cryptographic onion – a cryptographic scheme is used to achieve anonymity. The simulation results show the importance of anonymity through the analysis of traceable ratio and routing performance of the proposed scheme.

Index: Anonymity, Privacy, Security, Routing, MANET.

## 1. INTRODUCTION

MANETs is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes itself, i.e., routing functionality will be incorporated into mobile nodes. MANETs support dynamic communication environments and facilitate large-scale, real-time data processing in complex environments, which requires no fixed infrastructure, such as a base station or access points.

There are two types of MANETs exist: open and closed [1]. Closed MANETs don't have cooperation problems, since all nodes work towards a common goal and can easily be controlled. Open MANETs contain nodes that share their resources to ensure global connectivity but they many have different goals. However, the nodes in open MANETs are operated by multiple users, and they need not be forced to cooperate. There are two type problems introduced in ad hoc environments that are not commonly faced by traditional fixed network routing protocols. First one is the lack of fixed infrastructure support and the second one is frequent changes in network topology.

There are two categories of routing protocols: reactive and proactive [2]. Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and also assumes that all nodes are genuine and trustworthy. In this situation, a malicious node may take an active part in the network and can launch routing attacks to disrupt routing operations [3]. A malicious user may drops the packets selectively, leak confidential information and may consume resources of the network. Such malicious features degrade the routing performance of the protocols. In addition, a malicious may also listen to the network in order to know the identity or location of the nodes. A number of routing protocols [4],[ 5] have been proposed to secure ad hoc networks from security threats and to improve routing performance. But these protocols are compromised in many ways and most of the mechanisms discuss only about reliability not for anonymity. In this scenario, there is a need for anonymity during route discovery and data forwarding in order to achieve privacy and security for mobile nodes.

In this paper, POR scheme has been proposed to provide privacy and security for the nodes in an adversarial environment. The POR scheme is designed based on the combination of identity-based group signature [6],[7] and cryptographic onion [8] for secure anonymous communication. An identity-based group signature scheme makes use of a bilinear function over elliptic curves. The size of the group public key and the length of the signature are independent on the numbers of the group. The cryptographic onion used in this paper is Trapdoor Boomerang Onion (TBO) is used to create untraceable paths or packet flows in an on-demand environment with route pseudonymity approach. The design of route pseudonym is based "broadcast with trapdoor information" a cryptography concept used in this paper mainly for encryption and authentication.

The rest of the paper is organized as follows. The related works are discussed in Section 2. The proposed routing protocol is discussed in Section 3. Privacy and security analysis is analyzed in Section 4. Simulation setup and results are discussed in Section 5. The proposed work is concluded in Section 6.

# 2. RELATED WORKS

## 2.1 Anonymous Communication Schemes

Most of the works for anonymous communication is based on onion routing protocol [8] proposed by Reed et al. in which data is wrapped in a series of encrypted layers to form an onion by a series of proxies communicating over encrypted channels. Kong et al. [9] proposes an Anonymous On-Demand Routing Protocol (ANODR), is the first one to provide anonymous communication during route discovery and data forwarding in ad hoc networks. After this work, Seys et al. [10] proposed an Anonymous Routing Protocol (ARM) which uses one-time public/private key pairs and follows only anonymity in route discovery and data forwarding. Sy et al.[11] proposes On-Demand Anonymous Routing (ODAR) using public key cryptosystems for secure anonymous routing, but they assume that long-term public/private key pairs have been set up on each node for anonymous communication. Liu et al. [12] proposes a Hierarchical Anonymous Routing Protocol (HANOR) for MANET, which controls computational overhead using the hierarchical routing scheme and preserves routing anonymity. Zhang et al. [13] proposed Anonymous On-Demand Routing (MASK) which enables anonymous on-demand routing protocols with high routing efficiency by comparing with ANODR. Pan and Li [14] proposed an Efficient Strong Anonymous Routing Protocol (MASR) which overcomes the problems of MASK. Defrawy and Tsudik [15] proposes an Anonymous Location-Aided Routing in Suspicious MANETs uses group signature, but this protocols does not suitable for viable and practical approach to routing in mission-critical location-based environment because no analyses on protocol performance for privacy and security. Choi et al. [16] proposed Anonymous and Secure Reporting (ASR) of traffic forwarding activity in mobile ad hoc networks, which makes use of one-time public/private key pairs to achieve anonymity and unlinkability. Wan et al. [17] proposed an Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks (USOR) to provide privacy and security. This protocol uses combination of group signature and ID-based encryption for route discovery.

# 3. POR – THE PROPOSED SCHEME

## 3.1 Preliminaries

Let $G_1$ be a cyclic additive group generated by $P$, whose order is a prime $q$, and $G_2$ be a cyclic multiplicative group of the same order $q$. Let $a, b$ be elements of $Z_q^*$. Then assume that discrete logarithm problems in both $G_1$ and $G_2$ are hard. A bilinear pairings is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

(1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$;

(2) Non-degenerate: There exists $P$ and $Q \in G_1$ such that $e(P, Q) \neq 1$;

(3) Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

## 3.2 System Model

The proposed POR scheme assumes an ad hoc network with two entities i.e., the Offline Group Manager *(OGM)* and the users. In this paper the node or user has been used alternatively. A mobile node can communicate with other mobile node if it is in the same proximity otherwise, communication happen with multi-hop. Fig. 1 shows the system model for POR scheme that has three phases such as initial setup, user registration and anonymous routing.

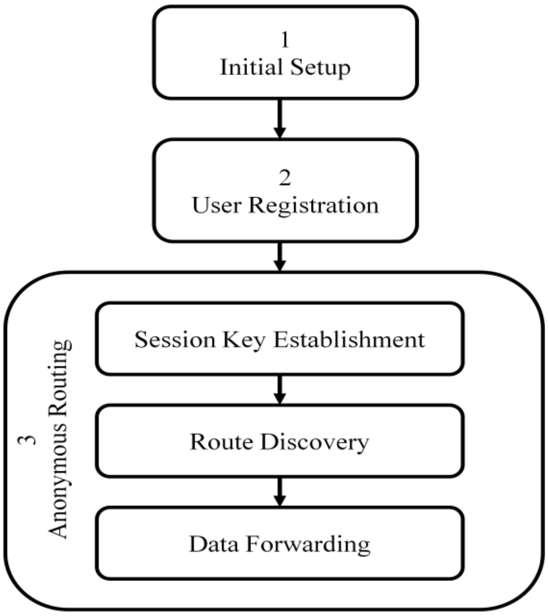


**Fig: 1 The System Model for POR**

### 3.2.1 Initial Setup (Offline)

The multi-hop network starts by the identity-based group signature scheme [6]. The *OGM* generates a group key (public/secret key pair) and sends announcement with group public key. The group public key $g_{pk}$ is publicly known by everyone and the private key $g_{sk}$ is only known by the respective mobile node.

The procedure as follows:

Step 1: *OGM* chooses $p, q, G_1, G_2$ as defined in the previous section 3.1.

Step 2: Then chooses two cryptographic hash functions:

$$H : \{0,1\}^* \to G_1,$$
$$H_1 : \{0,1\}^* \times G_1 \to G_1.$$

Step 3: Construct a bilinear function as defined in the previous section 3.1.

$$e : G_1 \times G_2 \to G_2.$$

Step 4: Selection a generator element $P \in G_1$, therefore $\Delta = e(P, P)$ is a generator element of $G_2$.

Step 5: Select an integer $a$ from $Z_q^*$ as the secret key of *OGM*; set $P_{pub} = aP$ as the public key of this group.

Step 6: Let a string $f \in \{0,1\}^*$ denoting an identifier of any group member of this group. *OGM* computes $Q_f = H(f)$ as the public key of this member.

Step7: Let $\{0,1\}^*$ be the message space. Therefore the group public key is: $g_{pk} = \{P, P_{pub}, \Delta, H, H_1\}$ and the private signing key $g_{sk_S} = a$ .

### 3.2.2 User Registration (Offline)

Registration is performed between *OGM* and a user. After this step, a user obtains a member public/secret key pair. A user who has completed the registration procedure is called a member of the network.
A user $U_i$ can join in to the network as follows:

Step 1: User $U_i$ interacts with the $OGM$ to determine his/her identity in the network. $U_i$ selects an identifier $f_i$ and forwards it to $OGM$ .

Step 2: $OGM$ computes $sk_i = aQ_{f_i}$ , and then sends them to $U_i$ .

Step 3: $U_i$ regards respectively the private value $b$ (secretly chosen by him/her) and her identifier $f_i$ as her personal secret key and personal public key. Suppose $bf_i \equiv 1 \bmod \varphi(n)$ , where $n$ is a product of two large prime numbers.

Step 4: $U_i$ and $OGM$ simultaneously execute a Schnorr identification protocol [18] and the user $U_i$ obtains a credential $t_i$ which is used to identify the membership of $U_i$ .

Step 5: $OGM$ has a transcriptor: $trans = \{< f_i, t_i >$ | for every authorized group member $U_{f_i}\}$ and adds a new entry $(f_i, trans)$ to the $mLIST$ .

Step 6: By the end of communication, the user $U_i$ becomes an authorized group member of the network. The user credential is $t_i$ ; personal secret key $SK_X$ is $\{b, sk_i\}$ personal public key $SU_X$ is $f_i$ . The user $U_i$ also verifies the items in $mLIST$ from the $OGM$ .

Step 7: Finally, the $OGM$ selects *S* item from the $gLIST$ (not including $(f_i, trans)$), and forwards them to $U_i$ . All $mLIST$ items are signed using the $OGM$ 's secret key, and thus can be verified by any user.

## 3.3 Anonymous Routing Scheme (Online)

The POR protocol divides the routing process in to three phases: (i) anonymous session key establishment, (ii) anonymous route discovery and (iii) anonymous data transmission. During first phase each user establishes a session key and with the protection of the session key the route discovery phase is initiated in second phase. In third phase, after the source node successfully finds out a route to the destination node, the source node can start anonymous data transmission with the protection of onion routing scheme. The proposed protocol works on top of AODV [19].

### 3.3.1 Anonymous Session Key Establishment

During anonymous key establishment, every node communicates with its direct neighbor within its proximity. Fig. 2, illustrates the anonymous key establishment process. Suppose a mobile node S with a private signing key $g_{sk_S}$ and the private key of the user $SK_S$ (obtained during registration process) in ad hoc network, surrounded by the number of neighboring nodes within its proximity, S interacts *X* to obtain a session key.

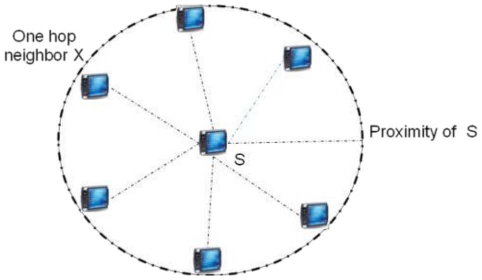


**Fig: 2 Anonymous Session Key Establishment**

Procedure for anonymous session key establishment:

```
Session_key_genertion ()
begin
$S$ generates a random number $rn_S \in Z_q^*$
  begin
    compute $rn_S P$            // $P$ is a generator of $G_1$
    compute signature $SIGN_{g_{sk_S}}(rn_S P)$
                                // anyone can verify using $g_{pk}$
    broadcast $< rn_S P, SIGN_{g_{sk_S}}(P) >$
                                // within its proximity
    end
if $X$ receives the $msg$
  if verification successful
    begin
        $X$ chooses $rn_X \in Z_q^*$
        compute $rn_X P$
        compute signature
        $SIGN_{g_{sk_X}}(rn_S P | rn_X P)$
        compute session key $sk_{SX} = H_2(rn_S rn_X P)$ and
        send to $S$ with its local broadcast key $sk_X$
      end
$S$ verifies the signature
  If signature is valid
    begin
        $S$ computes session key as
        $sk_{SX} = H_2(rn_S rn_X P)$
        $S$ generate local broadcast key and send to $X$
    end
    $X$ receives the $msg$ and computes the same session
     key $sk_{SX} = H_2(rn_S rn_X P)$,
     decrypts the $msg$ and gets local broadcast key $sk_S$
end
```

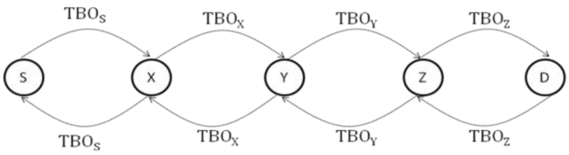
### 3.3.2 Anonymous Route Discovery

Anonymous route discovery establishes a privacy-preserving route based on the session key established in previous phase and cryptographic onion for an on-demand route. The route discovery process consists of route request *(RREQ)* and route reply *(RREP)*. The *RREQ* and *RREP* is based on cryptographic onion to achieve anonymous route discovery from source to destination. A user who wants to communicate initiates the route discovery procedure by assembling *RREQ* packet and locally broadcasting it locally. Suppose a source node *S* wants to find a route to destination node *D*, it floods the RREQ *packet* and is of the following format:

$$\langle RREQ, PK, seqnum, tr_{dest}, TBO \rangle$$

where $RREQ$ denotes Route Request Packet, $PK$ is one time public key from the private/public key pair of user, $seqnum$ is a globally unique random route pseudonym, $tr_{dest}$ is a cryptographic trapdoor that can only be opened by the destination and $TBO$ is Trapdoor Boomerang Onion, a cryptographic onion [9] as shown in Fig. 3.

$$TBO_S = SK_S(src)$$
$$TBO_X = SK_X(Nonce_X, SK_S(src))$$
$$TBO_Y = SK_Y(Nonce_Y, SK_X(Nonce_X, SK_S(src)))$$
$$TBO_Z = SK_Z(Nonce_Z, SK_Y(Nonce_Y, SK_X(Nonce_X, SK_S(src))))$$
$$TBO_D = SK_D(Nonce_D, SK_Z(Nonce_Z, SK_Y(Nonce_Y, SK_X(Nonce_X, SK_S(src)))))$$



$$TBO_D = SK_D(Nonce_D, SK_Z(Nonce_Z, SK_Y(Nonce_Y, SK_X(Nonce_X, SK_S(src)))))$$
$$TBO_Z = SK_Z(Nonce_Z, SK_Y(Nonce_Y, SK_X(Nonce_X, SK_S(src))))$$
$$TBO_Y = SK_Y(Nonce_Y, SK_X(Nonce_X, SK_S(src)))$$
$$TBO_X = SK_X(Nonce_X, SK_S(src))$$
$$TBO_S = SK_S(src)$$

**Fig: 3 TBO – Onion Construction and Opening**

The cryptographic onion is used to form random secret key $SK_x$ Trapdoor Boomerang Onion. The corresponding procedure is described below:

- When intermediate forwarding node *X* sees a *RREQ* packet, it embeds a random nonce $N_X$ to the Trapdoor Boomerang Onion, encrypts the result with a random secret key $SK_X$, then broadcasts the *RREQ* locally. The trapdoor information $N_X$ and $SK_X$ are only known to *X*.

- The Trapdoor Boomerang Onion will be bounced back by the destination. After each local *RREP* broadcast, only the source can correctly open the trapdoor correctly, which is made in the *RREQ* phase.

$$< RREP, \{N_{seed}\}_{PK}, N_{seed}(pr_{dest}, TBO) >$$

Where *RREP* denotes route reply packet, $N_{seed}$ is a random nonce same sa $N$, $pr_{dest}$ is same as $tr_{des}$ which can be opened only by source.

### 3.3.3 Anonymous Data Forwarding

Once the source receives *RREP* message from the destination, it encapsulates the data packets using outgoing random nonce in its forwarding table and then broadcasts the data packet locally. All the other local users must look up the random nonce in their forwarding tables and the user discards the data packet if no match is found. Otherwise, it changes the random nonce to the matched outgoing random nonce and then broadcasts the data packets locally. The procedure is repeated until the data packet arrives at the destination.

## 4. PRIVACY AND SECURITY ANALYSIS

## 4.1 Privacy Analysis

The major difference between POR and MASK is that: POR protocol adapts identity-based group signature scheme, this provides stronger anonymity means that except group the group manager nobody can trace the identity of the user. The POR protocol creates the session key anonymously with its one-hop neighbor and uses cryptographic onion for route discovery. This ensures that the POR protocol provides stronger privacy with two levels authentication. Whereas, MASK adapts one-time pairing based key which is very much prone to key depletion attack.

**Identity Anonymity:** User anonymity is implemented by identity-based group signature scheme, this scheme uses pseudonyms instead of real identities which ensures nobody can trace the identity except the *OGM*. In addition, the route discovery process uses cryptographic onion and data forwarding phase uses session key.

## 4.2 Security Analysis

**Eavesdropping**: In the proposed POR protocol, even though the cryptographic keys are compromised by eavesdroppers, it cannot get useful privacy information from the compromised node. The privacy information only contains the cryptographic secrets of compromised nodes one-hop neighbor. The POR protocol implements per-hop authentication and onion routing scheme during route discovery and data forwarding phase. So, the compromised node cannot extract location and real identities of the source/destination node.

## 5. PERFORMANCE EVALUATION

## 5.1 Simulation Setup

The routing protocols such as the proposed POR and MASK are implemented with ns2 simulator version 2.32 [20] for MANET. The Distributed Coordination function (DCF) of IEEE 802.11 is used as Medium Access Control (MAC) layer in this simulation. The radio propagation range of the each mobile node is 250 meters and the channel capacity is 2 Mbits/sec. In the simulation scenario an ad hoc network of size 700m × 700m consists of 100 mobile nodes uniformly deployed. The mobile nodes are moving in the field according to the random waypoint model. The bidirectional Constant Bit Rate (CBR) sessions are used to generate data traffic and all the data packets are 512 bytes long. The network scenario parameters and value used for simulation are listed in Table 1.

**Table 1: Scenario Parameters**

| Parameters | Value |
|---|---|
| Simulation Time | 700s |
| Scenario Dimension | 700m × 700m |
| Wireless Radio Range | 250m |
| Mobile Nodes | 100 |
| Node Speed | 0 – 10 m/s |
| Traffic Type | CBR 512-byte packet |
| Mobility Model | Random Way Point |

The identity-based group signature scheme is used for implementation for its supports for anonymity and efficiency. A 256-bit prime number is used as key and the computational cost is shown in Table 2.

**Table 2: Computational Cost**

| Scheme | Cost |
|---|---|
| Identity-Based Group Signature generation | 60ms |
| Identity-Based Group Signature verification | 50ms |
| SHA-1 | 10ms |

## 5.2 Simulation Results

In the simulation, a percentage of 10 and 50 members are marked as eavesdroppers. Fig. 4 depicts the traceable ratio over different path lengths of routes for POR and MASK with 10% of eavesdroppers. From the figure it has been observed that the traceable ratio is getting decreased for both the protocols. When the path length increases the traceable ratio for POR is reduced drastically this ensures the better performance POR than MASK.

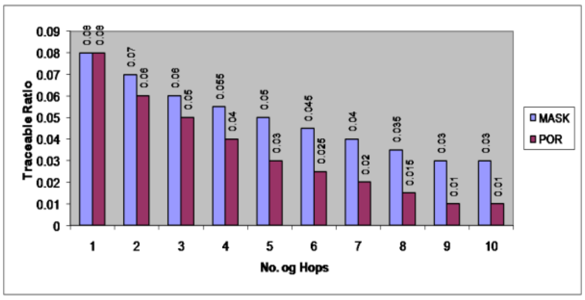


**Fig: 4 Comparison of Traceable Ratio with 10% of Malicious nodes**

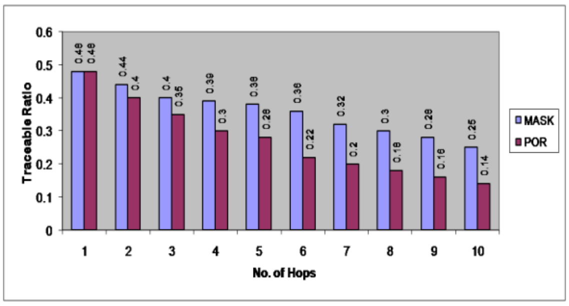


**Fig: 5 Comparison of Traceable Ratio with 50% of Malicious Nodes**

According to Fig. 5, with 50 percent eavesdroppers, MASK traceable ratio is very higher than POR when path length increases. When path grows longer, the traceable ratio will not exceed the percentage of intruded nodes. The result demonstrates POR's resistance to strong eavesdroppers with node intrusion capability.

The performance of POR is analyzed in terms of packet delivery ratio, end-to-end delay, routing packet overhead and throughput.

Fig. 6 demonstrates performance of POR and MASK at different moving speeds for the traffic load of 2 packets / second. According to Figure, POR has the better packet delivery ratio than MASK. The packet delivery ratio decreases as node speed increases. Under the light traffic load (2 packets/s), both the protocols has 90% and above packet delivery ratio at high node speeds, but POR shows better performance than MASK. The major difference between POR and MASK on packet delivery ratio is less than 10% initially and 20% under the mobility of 10 m/s.

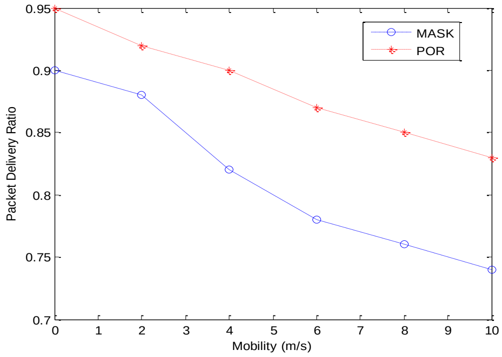


**Fig: 6 Packet Delivery Ratio Vs Mobility**

According to the Fig. 7, it has been observed that, the POR has the lower end-to-end delay than MASKUSOR, but the end-to-end delay difference between POR and MASK is less. Under the light traffic load of 2 packets/second POR's delay increases from 0.1 ms to 0.72 ms when node speed increases from 0m/s to 10m/s. For MASK it is 0.1 ms to 1 ms when the node speed increased from 0 m/s to 10 m/s. Due to the non-optimal paths and local key construction delay result in longer latency of MASK than POR.

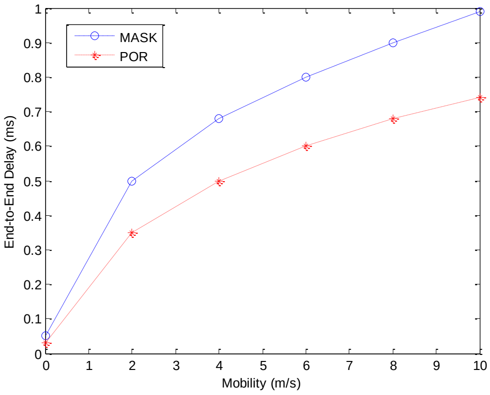


**Fig: 7 End-to-End Delay Vs Mobility**

Fig. 8 illustrates the routing cost for delivering a unit of data payload. There is a big strange that MASK have to send more control packets than POR. Since POR uses cryptographic onion whereas MASK uses one-time pairing based key for route discovery approach. According to the figure the proposed POR has less overhead than MASK.

According to Fig. 9, POR gives better throughput than USOR. The throughput decreases as node speed increases for the both protocols. Under the light traffic load (2 packets/s), both the protocols performs better, but POR dominates the MASK protocol in achieving better throughput for both the protocols. Under the light traffic load (2 packets/s), both the protocols performs better, but POR dominates MASK in achieving better throughput.

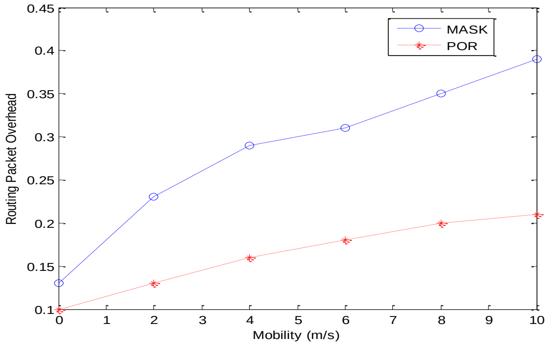


**Fig: 8 Routing Packet Overhead Vs Mobility**

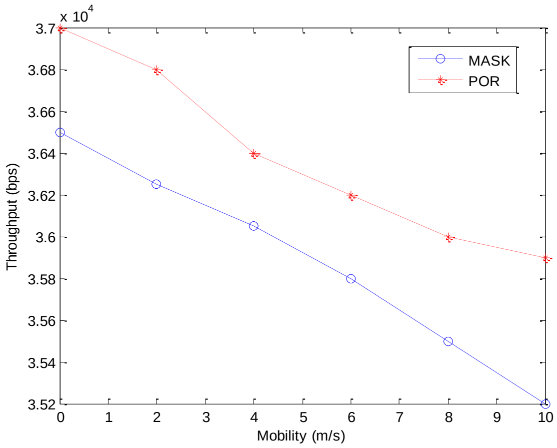


**Fig: 9 Throughput Vs Mobility**

## 6. CONCLUSION

In this paper, the POR protocol implemented the identity-based group signature scheme and achieved the privacy and security through anonymity related goals. The proposed protocol prevented the strong eavesdroppers, from exposing local wireless transmitter's identities and tracing ad hoc network packet flows. Moreover, POR also demonstrated the untraceable data forwarding through onion routing. The traceable ratio on hop length proved that the proposed POR outperforms and mitigates the malicious nodes in the network.

## 7. REFERENCES

[1] Miranda H. and Rodrigues H. 2002. Preventing Selfishness in Open Mobile Ad Hoc Networks, In Proceedings of CaberNet Radicals Workshop.

[2] Abusalah, L, Khokhar, A. and Guizani, M, "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE Communications Surveys & Tutorials, 2008, 10, (4), pp. 78-93.

[3] Kannhavong B., Nemoto Y. and Kato N., "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications, vol. 14, no. 5, pp. 85-91, 2007.

[4] Abusalah L., Khokhar A. and Guizani M., "A Survey of Secure Mobile Ad Hoc Routing Protocols, IEEE Communications Surveys and Tutorials, vol. 10, no. 4, pp. 78-93, 2008.

[5] Andel T. R. and Yasinsac A., "Surveying Security Analysis Techniques in MANET Routing Protocols", IEEE Communications Surveys and Tutorials, vol. 9, no. 4, pp. 70-84, 2007.

[6] Boneh D. and Frankliny M. 2003. Identity-Based Encryption from the Weil Pairing", In Proceedings of Advances in Cryptology.

[7] Han, S, Wang, J. and Liu, W. 2004. An Efficient Identity-Based Group Signature Scheme over Elliptic Curves", Springer LNCS.

[8] Reed, M, G, Syverson, P, F. and Goldschlag, D, M. "Anonymous Connections and Onion Routing", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 482-494, 1998.

[9] Kong, J. and Hong, H. 2003. ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks, In Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing.

[10] Seys, S. and Preneel, B. 2006. ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks, In Proceedings of the International Conference on Advanced Information Networking and Applications.

[11] Sy, D, Chen, R. and Bao, L. 2006. ODAR: On-Demand Anonymous Routing in Ad Hoc Networks, In Proceedings of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems.

[12] Liu, J, Hong, X, Kongt, J, Zheng, Q. and Bradford, P, G. 2006. A. Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks", In Proceedings of the International Conference on Military Communication.

[13] Zhang, Y, Liu, W, Lou, W. and Fang, Y, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE Transactions On Wireless Communications, vol. 5, no. 9, pp. 2376 – 2385, 2006.

[14] Pan, J. and Li, J. 2009. MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Networks, In Proceedings of the International Conference on Management and Service Science.

[15] Defrawy, K,E. and Tsudik, G, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE Transaction on Mobile Computing, vol. 10, no. 9, pp. 1345 –1358, 2011.

[16] Heesook C., William E., Jaesheungn S., Patrick D. M. and Thomas F. L. P., "ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks", Wireless Networks, pp. 525-539, 2009.

[17] Z. Wan, K. Kui, and M. Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", IEEE Transaction on Wireless Communications, vol. 11, no. 5, pp. 1922-1932, 2012.

[18] Schnorr, C, "Efficient Signature Generation from Smart Card", Journal of Cryptography, Springer – Verlag, vol. 4, no. 3, pp. 239-252, 1991.

[19] Perkins, C, Belding-Royer, E. and Das, S. 2003. Ad Hoc On-Demand Distance Vector (AODV) routing, RFC 3561.

[20] Fall K. and Varadhan K., ns manual.isi.edu /nsnam/ns/doc.