International Journal of Computer and Communication Technology

Volume 8 | Issue 2 Article 14

April 2017

Probabilistic Anonymous Routing in Mobile Ad-Hoc Networks

Dhaval Moliya
Computer Science & Information System Department BITS Pilani Hyderabad Campus, Hyderabad, AP, INDIA, moliyadhaval@gmail.com

Rusheel Jain
Computer Science & Information System Department BITS Pilani Hyderabad Campus, Hyderabad, AP, INDIA, rusheeljain@yahoo.co.in

Vakul Mohanty
Computer Science & Information System Department BITS Pilani Hyderabad Campus, Hyderabad, AP, INDIA, vakul.mohanty@gmail.com

Chittaranjan Hota
Computer Science & Information Systems Department BITS – Pilani, Hyderabad Campus Hyderabad, A.P. (INDIA), hota@bits-hyderabad.ac.in

Probabilistic Anonymous Routing in Mobile Ad-Hoc Networks

Dhaval Moliya[1], Rusheel Jain[2], Vakul Mohanty[3], Chittaranjan Hota[4]
Computer Science & Information System Department
BITS Pilani Hyderabad Campus, Hyderabad, AP, INDIA
moliyadhaval@gmail.com, rusheeljain@yahoo.co.in, vakul.mohanty@gmail.com, hota@bits-hyderabad.ac.in

***Abstract*— In this paper, we propose a routing protocol which ensures route anonymity, for the user. Amongst all suboptimal paths between source and destination, path for data transfer is chosen randomly at each intermediate node. Route anonymity becomes essential for preventing attacks like traffic monitoring. Bayesian approach has been employed for route discovery phase of the protocol. The protocol is simulated using NCTUNS network simulator. The robustness of our protocol is evaluated against known security attacks.**

***Index Terms*— Anonymity, ad hoc networks, mobile, routing, mobile, route anonymity**

I. INTRODUCTION

MOBILE ad-hoc networks (MANETs) are autonomous collection of mobile nodes. MANET usually lacks any type of fixed infrastructures. As nodes in MANET are mobile, so the link failure and re - establishment of routes takes place frequently. It is difficult to keep track of all these nodes and their locality centrally. So it is essential to find out the geographic location of nodes only when communication channel has to be established, in this wireless environment wherein bandwidth available for the communication is constrained. Moreover, these nodes keep moving with different speed and power is an important constraint for them all the times. On top of this, communication link is subject to various attacks for the adversaries. Malicious nodes in the networks act as an adversary and they participate in the activities like: Dropping the packet which comes to it, which is otherwise its responsibility to forward; deploying the denial of service attack; in association with other adversaries present in the network, deploying distributed denial of service attack etc. Lot of research has been done so far in the field of routing in MANET in the trusted environment. But little has been done under above mentioned relatively untrusted environment.

In this paper we present a routing protocol for a Mobile Ad-Hoc Network. The protocol seeks to achieve anonymity without the use of cryptography and also nullifies the requirement of padding of data packet to prevent traffic analysis and traffic monitoring. In the protocol, the next hop is dynamically and randomly chosen by each intermediate node. So path taken by data packet cannot be predicted and hence complete path between the sender and destination cannot be found. In route discovery, Bayesian probabilistic approach has been used for discovering routes.

The rest of this paper is organized as follows: we present related work in Section 2; in Section 3, we present our algorithm (protocol), in Section 4, we present Simulation Model; in Section 5 & 6, we present the simulation results and analysis of our protocol respectively; finally, in Section 7, we summarize our work and point out several future research directions.

II. RELATED WORK

Because of some limitations of wireless communications compared to wired communication which has fixed infrastructure, achieving anonymity in MANET is not that straight forward task. Onion routing [1,3] uses multiple layers of encryptions wrapped around the message. Each router in the path of the onion receives a message, performs a set of cryptographic operations on the message and then forwards it. At receiving end, each router uncovers a layer of encryption using its private key, to gain access to the routing instructions for the next router. This process continues until the message reaches the last router. Onion routing has huge cryptographic overhead. Papadimitriou and Haas [2] proposed a secure routing protocol for MANETs using a security association between source and destination to validate the integrity of a discovered route. In [4], Chao-Chin Chou *et al.* proposed an efficient anonymous communication protocol for P2P (Peer to Peer) applications over MANET, which employs probabilistic flooding with broadcast for discovery of paths between the communicating pair. In [5], Min-Hua Shao *et el.* described trust aware routing for anonymity protection based on pseudonym based and allowed two communicating parties to choose the path that is free of untrustworthy nodes. In [6], Lianyu Zhao *et al.* discussed an algorithm that provides source, destination and route anonymity. It is achieved by splitting the routing path in multiple steps with no specific pattern. In [7], Dijiang Huang proposed a two-step unlinkability approach for MANET applying the evidence theory-based unlinkability measuring methods to derive the unlinkability evaluations of the 802.11b MANET. In [8], Weichao *et al.* proposed polynomial

based personal keys for group based location information access to achieve the privacy and authentication of communicating parties in MANETs. In the proposed protocol, location information is pre-distributed to the group of nodes with different level of trust. In [9], Sisheng Chen *et al.* proposed a secure anonymous routing scheme for clustered wireless ad hoc networks to prevent the traffic monitoring. It provides sender, receiver, link anonymity and privacy through bloom filters to establish the trust. Xiaodong Lin *et al.*[10] proposed new attacks for anonymous networks called Snare attack which compromises very important node in the route of source and the destination to trace the route. They also discussed several countermeasures for this attack. Yang Yin *et al.* [11] showed a comparative study of various solutions to the problem of point-to-point communications. Point-to-point communication relations expose the traffic pattern on physical and MAC layer.

I. PROPOSED ROUTING PROTOCOL

A. Introduction

The proposed Routing Protocol is a novel approach of achieving the anonymity in MANETs using the Bayesian probabilistic method [13][14] for route discovery. This protocol ensures the use of suboptimal paths between the source and destination. In existing routing protocols, even if there exist multiple paths between source and destination, the actual path is used for the data communication is decided initially, which is not changed randomly at any intermediate nodes. In the proposed routing protocol, the next hop at each intermediate node is chosen dynamically and randomly.

In the proposed routing protocol, each node maintains a history table, which contains the destination node's id and the value of the attributes used for calculating the Chance Index (CI). This history is used in calculating own chance index while sending or rejecting a route request (RREQ).

Each intermediate node upon receiving RREQ checks their routing table (RT) to find if the path to the destination is known or not. If known, a route reply (RREP) is generated back to the source via the same path. Otherwise, the node compares the stored CI value for that particular destination in their RT with the CI contained in RREQ. If CI in route request is less than the minimum stored CI in RT, the node discards RREQ. Otherwise node will add its own CI value in the RREQ and will broadcast the RREQ. Since the CI of destination for itself will be 1(highest), hence, upon receiving a RREQ, destination replies back by adding 1 to the CI contained in the RREQ. Upon receiving RREP, intermediate nodes forward the RREP to the source. When a route reply is received by the source, it can start regular data transfer.

In regular data transfer phase, each node selects the next hop randomly for routing data packet until that data packet reaches to the destination.

Upon route failure, intermediate node tries to repair route locally only if it has lost all the routes towards destination. If route couldn't be repaired locally, route failure (RFAIL) is generated and sent back to the previous node. Now upon receiving RFAIL, each node forwards this failure message only if it has no node as its next hop otherwise the only action taken is that the node from which RFAIL was received is removed from RT. The source will start a fresh route discovery if it receives RFAIL and source also has lost all the paths to destination (ensuring reduction in control packet overhead).

B. Calculating Chance Index

Chance index (CI) is a probability which is calculated using Bayes Theorem [13][14], based upon historical data. Through this we can find out how much probable it is for a particular node to transfer the data packet to the desired destination. As per to Bayes Theorem $P(S_i/A) = \{ P(A/S_i) P(S_i) \} / P(A)$

Here, S_i is the status showing whether reply was received for the RREQ sent. And $A = \{ A_1, \ldots\ldots, A_N \}$ i.e. the various attributes upon which the probability will depend. P(X) does not depend upon C_i is used only for normalization. So $P(S_i/A)$ will be maximum when $P(A/S_i) P(S_i)$ is maximum[14]. Hence,

$$AI = P(S_{yes}) \prod_{\forall i} P(A_i/S_{yes}).$$

Assuming that every attribute A_i is independent of other attribute A_j (j‘“i), and then we can say that

$$P(A/S_i) = \prod_{k=1}^{n} P(A_k/S_i) \text{ and}$$
$$CI = P(S_i) \prod_{\forall k} P(A_k/S_i)$$

The probability (and hence CI) can become null because the probabilities of each and every attribute is being multiplied. As a result; even if one of the attributes has a zero probability; the whole index will become zero. So, null probability will be replaced with a very low probability (0.0001).

C. Example

In the example below, source S broadcasts a request for destination D. It calculates its own Chance Index (CI) and puts it in the Route Request (RREQ). Upon receiving RREQ, nodes A, B and C compare the CI in RREQ with CI in their Routing Table (RT). Every intermediate node upon receiving RREQ, compares CI in their RT with CI in RREQ. If CI in RT is less, they broadcast RREQ by adding their own CI in it, as shown in Fig.1. Now the destination upon receiving the

route requests chooses RREQ which has CI greater than the minimum CI in RT of destination; and generates RREP by adding 1 to the CI in RREQ received. Now each intermediate node (i.e. A, B, C) will forward route reply (RREP) to previous node as shown in Fig.2. Now, in regular data transfer phase, as shown in Fig.3 and Fig.4, every node randomly & dynamically chooses its next hop for sending the packets.

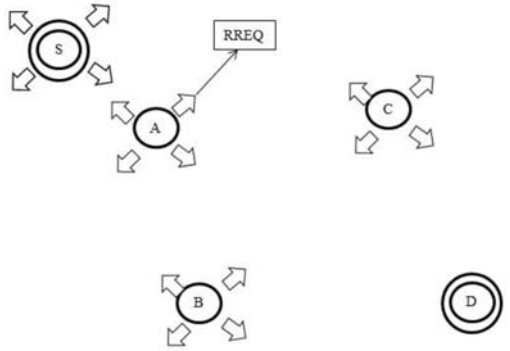
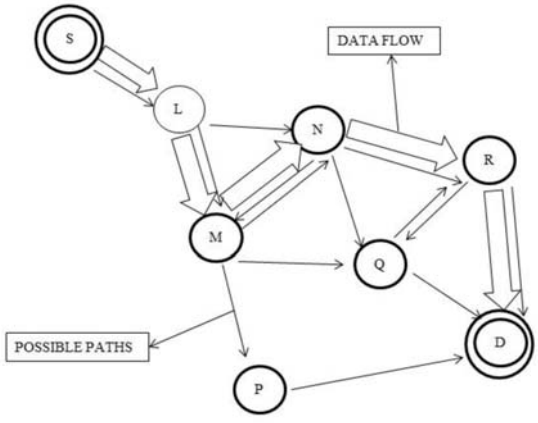


Fig. 1: Broadcast of Route Request Packet

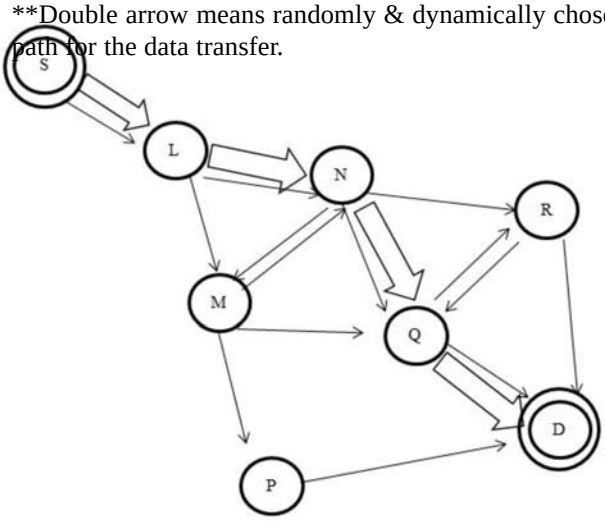
Fig. 2: Unicast of Route Reply
**Solid line means the route used for sending the data packets.
**Dotted lines mean path to previous node (to which reply must be sent)



Data Flow through one of the possible paths

Fig.3: PATH used for regular data transfer
**Simple arrow means path from source to the destination
**Double arrow means randomly & dynamically chosen path for the data transfer.

Fig.4: Different PATH used for regular data transfer
**Simple arrow means path from source to the destination
**Double arrow means randomly & dynamically chosen path for the data transfer.



Data Flow through another Path

IV. ALGORITHM

A. Route Discovery

1) Sending RREQ (route request)

```
for (each node in Neighborhood)
begin
   1.Calculate Chance Index (CI)
   2.broadcast(RREQ(req_ID, source,
destination,CI(rreq)));        3.insert (history(req_ID, source,
destination, region, time,
      status));
end
```

2) Receiving RREQ (route request)

```
for (each intermediate node)
begin
if (route to the destination already exists)
      i.    Update routing table
      ii.   Generate RREP (route reply)
      iii.  Unicast RREP to the source node
end
else  //assuming CI in RREQ is greater
      i.    Insert received RREQ in the control
            packet's table
      ii.   Insert the identity of the node in RREQ
      iii.  Calculate CI , and add it in CI of RREQ
      iv.   Broadcast RREQ to all neighboring nodes
end
//At destination node Accept/Reject the path on the basis of CI
begin
 if(path is Rejected) then Discard RREQ packet,
end
else
  1.Update routing table
  2.Generate RREP (req_ID, source, destination, ordered list
of
    intermediate nodes, receiver ID)
  3.Insert RREP into control packet's table
  4.Unicast RREP to the source node traversing the same path
    it used while arrival
end
```

3) Receiving RREP (route reply)

```
//Intermediate node receives RREP
if(req_ID exists in routing table)
begin
```

1) Regular data transfer

Repeat until data packet reaches to its destination

i. Fetch the routing table entry(req_ID, source, destination, next hops)
ii. Choose the node randomly and dynamically from all available next hops
iii. Forward the data packet to the chose node

2) Route Failure (RFAIL)

```
if ( (any neighboring node N goes out of vicinity) OR
(receives RFAIL from neighboring node N) )

begin

if(N exists in the routing table of the
detecting node)
begin
```

I. SIMULATION MODEL

The NCTUNS [12] is used for evaluating the proposed technique in this paper. A total of 60 nodes are simulated over a network space of 3000m x 3000m. The traffic pattern is modeled as 8 CBR sources with data sent in 1400-byte packets at rate of 5 packets per sec. We chose the above configuration as it allows a reasonably timed simulation, while stressing protocols with a sufficiently high load without causing congestion in the network.

The following describes our performance metrics of interest:

- *Route discovery overhead*. The sum of routing packets generated by each node due to route discovery. This includes both RREQ and RREP packets. Each hop-wise transmission is counted as one transmission. This is reflected in control packet overhead.
- *Throughput*. Total amount of data transferred per second through the network.
- *Collision Packets*. Total number of collision packets.

Parameter	Setting
Mobility model	Random waypoint
Traffic model	8 CBR sources
Network space	3000m x 3000m
Number of nodes	60 nodes
Maximum node speed	10 m/s
Packet sending rate	5 packets/s
Data payload	1400 bytes

Table 1: Summary of parameters

Below is a snapshot of the simulation model used.

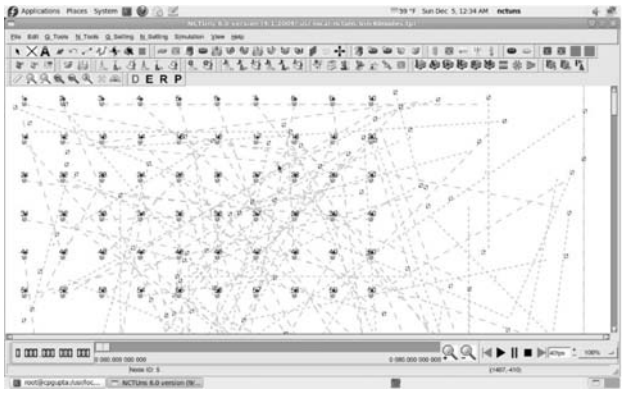


Fig. 5: Network Topology

VI. SIMULATION RESULTS

A. *Effect of PATHS on Throughput*

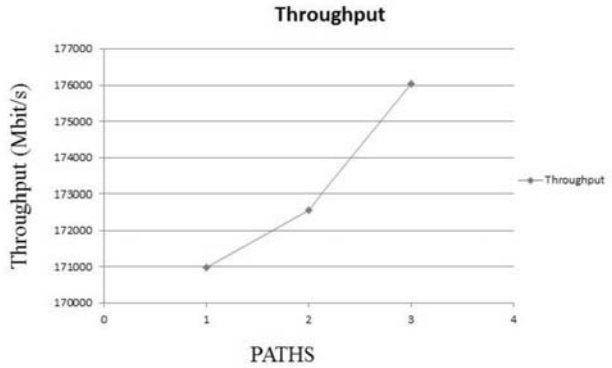


Fig. 6: Throughput of the proposed protocol for three different PATHS

B. Effect of PATHS on Collision Packets

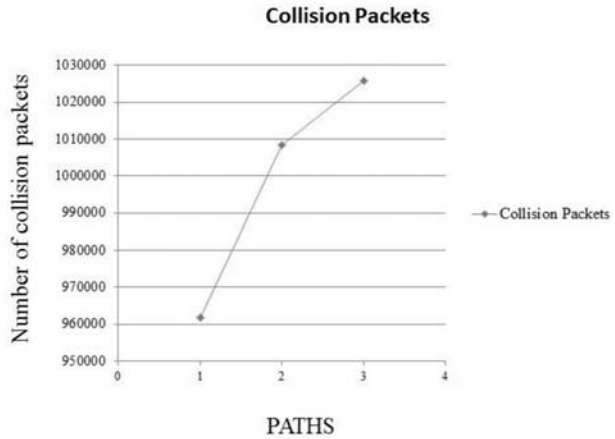


Fig. 7: Number of collision packets for different PATHS

C. Effect of PATHS on Control Packet Overhead

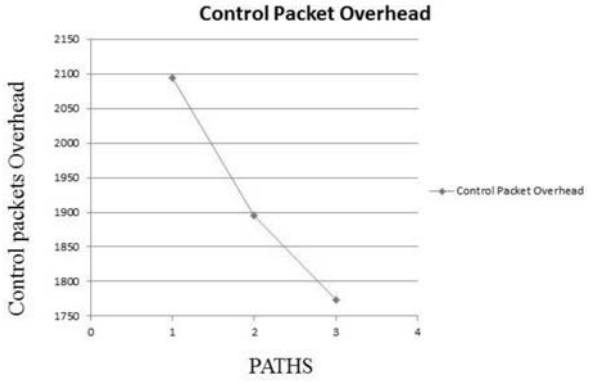


Fig. 8: Number of control packets for different PATHS

As the number of PATHS increases, the choices available at each node for selecting next hop increases. So, with the rise in the number of PATHS, total network throughput improves, as shown in Fig 6. But, this results in higher number of collision packets as the number of overlapping paths for 8 source – destination pairs may increase (Fig. 7). Fig. 8 shows that there is a significant drop in the control packet overhead with the increase in PATHS. This is due to the fact that any node does local repair (or generates route error messages) only if it has not has even a single route to destination. Hence, with the increase in PATHS, number of routes increases and so, number of control packets reduce.

A. *Effect of Network & Traffic Load on Control Packets*

In the Fig 9, 10 & 11, legend "4 Pairs" represent the results when the network size was 32 nodes and the number of source – destination pairs were reduced to 4 whereas legend "8 pairs" means that the network size was kept at 60 nodes with 8 pairs of source and destination. The mobility was kept at 10 m/s and value of PATHS is 2 for these three figures.

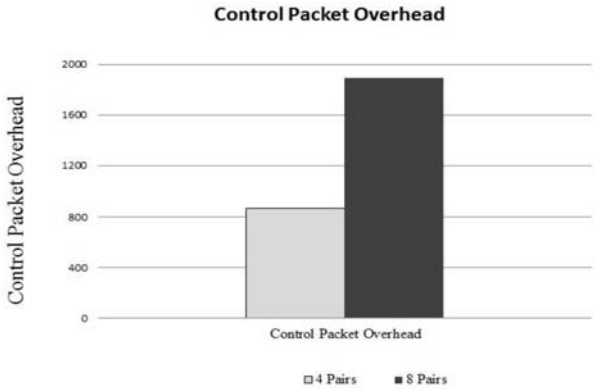


Fig. 9: Effect of network size and traffic load on control packet overhead

E. Effect of Network & Traffic Load on Throughput

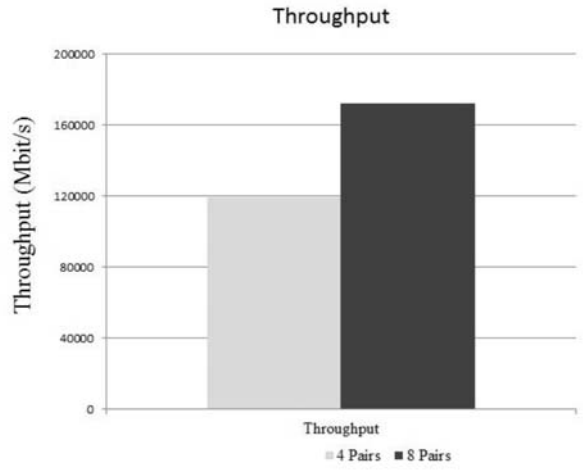


Fig. 10: Effect of network size and traffic load on throughput

A. Effect of Network & Traffic Load on collision packets

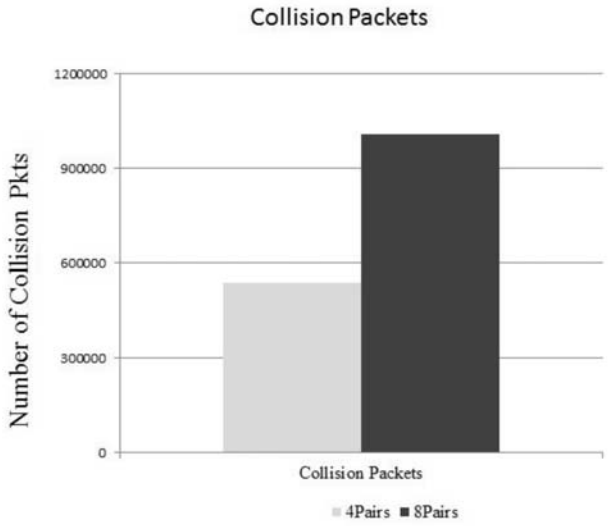


Fig. 11: Effect of network size and traffic load on number of collision packets

In Fig 9, it can be clearly seen that as the traffic load and size of the network is reduced (other parameters being same), the total count of control packets are reduced to almost half. The reason is that, now there is lesser number of nodes that will be generating and forwarding control packets. Same type of result is evident in Fig 10, and Fig 11, where the throughput and collision packets, respectively, decreases because the number of control packets as well as data packets are reduced.

I. ANALYSIS

A. Anonymity analysis

Route Anonymity: In our protocol, no adversary can trace a flow of packet because of random selection of next hop and thereby leading to dynamic path selection. Any adversary on the route has no information about the path other than the next hop. So route anonymity is achieved.

B. Possible Attacks

End-To-End Attack: In anonymous routing protocols like the onion routing end-to-end attack are a major threat. This is a passive attack in which if the first or the last router is malicious then either the sender or the destination's address is exposed. This is a consequence of analyzing the length of the padding added to the data. From the size of **the** padding the router can infer its location in the route. As the proposed protocol eliminates the need for padding, end-to-end attacks cannot succeed against this protocol.

Route Rediscovery Attack: One possible attack is that adversaries send fake route failure packets to begin route rediscovery. But in this protocol, only source node can issue route rediscovery. Hence protocol has no vulnerability against route rediscovery attack.

Traffic Monitoring: One of the most simplest types of attack on the protocol can be that of an adversaries or selfish node silently refuse to perform functions requested in the protocol or sniff the communication being done in the network and do traffic analysis on it. Passive attacks are very difficult to detect but they act as supplementary to active attacks. In our protocol, any node chooses the next hop from the next hop field of routing table entry randomly. And hence these passive attacks can be avoided.

C. Cryptographic Overhead

In our protocol, we don't use multiple layers of cryptography to achieve anonymity. Hence at each stage of the routing protocol delay incurred by highly expensive cryptographic operations is avoided. This reduces the cryptographic overhead. More importantly it makes the protocol fast and less computationally intensive.

Another important feature in our routing protocol is that even if an adversary makes his or her CI = 1 (i.e. highest probability), still he cannot seriously affect the data transmission. The reason being that by making CI = 1 it can only improve his chances of being included in one of the routes of data transmission. But still, it does not guarantee whether the actual data flow will take place through the

path containing the adversary, as at all nodes the next hop is decided randomly from one of the possible next hops.

II. CONCLUSION

Because of dynamic random selection of path, route anonymity is achieved, which is very important in MANET under byzantine environment. Very little or no cryptographic overhead makes it more attractive. In future, we aim at doing even rigorous simulation with different mobility, traffic load, and network size. We also aim at providing more security.

REFERENCES

[1] *Reed*, M., *Syverson*, P., and *Goldschlag*, D. Anonymous connections and *Onion Routing.* IEEE J. Selected Areas in Commun. 16, 4 (May 1998), pp. 482-494.

[2] Papadimitratos and Haas: Secure Routing for Mobile Ad hoc Networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[3] Jian Ren, Jie Wu. Survey On Anonymous Communications In Computer Networks. Comput. Commun. (2010), Vol. 33, No. 4 pp. 420-431.

[4] Chao-Chin Chou Wei, D.S.L. Kuo, C.-C.J. Naik, "Anonymous Peer-to-peer Communication Protocol over Mobile Ad-hoc Networks", Proc. IEEE Global Telecommunications Conference, 2006. GLOBECOM '06, pp. 1-5, DEC-2006.

[5] Min-Hua Shao And Shin-Jia Huang, "Trust Enhanced Anonymous Routing In Mobile Ad-Hoc Networks", Proc. 9th International Conference On Parallel And Distributed Computing, Applications And Technologies, PDCAT 2008, Pp. 335-341, DEC-2008.

[6] Lianyu Zhao and Haiying Shen, "A Low-Cost Anonymous Routing Protocol in MANETs", Proc. 18th International Conference on Computer Communications and Networks, ICCCN 2009, AUG-2009, pp. 1-6.

[7] Dijiang Huang, "Unlinkability Measure for IEEE 802.11 Based MANETs", IEEE Transaction on Wireless Communications, Vol. 7, Issue 3, pp. 1025-1034, MAR-2008.

[8] Weichao Wang and Cheng Cui, "Achieving Configural Location Privacy in Location Based Routing in MANET", Proc. Military Communication Conference, MILCOM-2008, pp. 1-7, NOV-2008.

[9] Sisheng Chen, Li Xu, and Zhide Chen, "Secure Anonymous Routing in Trust and Clustered Wireless Ad Hoc Networks", 2nd International Conference on Communications and Networking in China, CHINACOM '07, pp. 994-998, MAR-2008.

[10] Xiaodong Lin, Rongxing Lu, Haojin Zhu, Pin-Han Ho, Xuemin Shen and Zhenfu Cao, "ASRPAKE: An anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks", IEEE International Conference on Communications, ICC '07, pp. 1247-1253, JUN-2007.

[11] Yang Yin, Yin Dijiang Huang, and Shah N, "A comparative study on anonymous 802.11n protocols", IEEE Military Communications Conference, MILCOM 2008, pp. 1-7, NOV-2008.

[12] http://nsl.csie.nctu.edu.tw/nctuns.html

[13] Shabbir Ahmed, "Message Forwarding In People Centric Delay Tolerant Networks," Wireless Communications and Networking Conference (WCNC), 2010 IEEE.

[14] George F Luger, "Artificial Intelligence", ed. 4, pp. 333-338.

[15] Vakul Mohanty, Dhaval Moliya, Chittaranjan Hota, and Muttukrishnan Rajarajan, Secure Anonymous Routing for MANETs Using Distributed Dynamic Random Path Selection, in Proc. Fourteenth Pacific-Asia Workshop on Intelligence and Security Informatics (PAISI'2010), PAKDD 2010, Hyderabad, INDIA, H. Chen et al. (Ed.s), Lecture Notes in Computer Science, LNCS 6122, June 2010, pp.65-72.