A Secure Routing Cryptography Algorithm In Mobile Ad Hoc Network

Kim, Do-Moon

Department of Information Security Engineering, Kyungdong University, Korea

Summary
Mobile Ad Hoc Networks (MANET) infrastructure less network and no existence between connection nodes. Nodes forward data on behalf of each other in mobile ad hoc networks. In mobile ad hoc networks eavesdropper can easy to capture and analyze and data communication. To attention at very protocol design about secure routing in mobile ad hoc network, but some its attention to anonymous also these have not definition perfect of anonymity. Thus in this paper we present a novel anonymous secure routing scheme for mobile ad hoc networks. It's satisfaction definition anonymity. Malicious intermediate nodes in MANETs are a threat concerning security as well as anonymity of exchanged information .In this protocol we try prevention attacks target to Anonymity and also we try prevention attacks sybil and attacks wormhole and attacks DOS. The proposed protocol is simulated in NS-2. Simulation results show that various design choices in anonymous routing indeed trade performance with anonymity protection. We conclude that extensive performance study is needed to evaluate the practicality of any enhancement of these proposed schemes and any new anonymous routing schemes.

Keywords
Secure Routing Mobile Ad Hoc Networks, Anonymity, Cryptography, On-demand Routing, Pseudonmity

1. Introduction

In a Mobile Ad hoc Network (MANET), nodes communicate with each other from time to time and maintain dynamic and temporary connectivity through peer-to-peer wireless communication. If nodes move unpredictably at a high speed, disconnections between nodes can be frequent and a path between any node-pair may not be always possible. Compared to wired networks, MANETs are more vulnerable to both active and passive attacks. Wireless transmissions are easy to capture remotely and undetected, while the lack of central management and monitoring make network nodes susceptible to active attacks .Recently researchers have also Check out the problem of anonymity in wireless networks. If the secure routing protocols that are currently available for network routing is used, Then the enemy can be listening to routing packet and data packet with the same route Profile, Route discovery and the location and identity of nodes beginning and the end to take the path followed in the case of physical attacks will be able to organize these nodes. However, if a routing protocol used with solutions anonymity without the enemy will not be able to easily find other information from such access. It is clear that providing anonymity in ad hoc networks is ID remain hidden source and destination nodes from view intermediate and outside nodes, ID Intermediate nodes to remain hidden from view ID Source and destination, ID Remain hidden intermediate nodes from view intermediate nodes , Location
To stay hidden source and destination nodes, Location to stay hidden intermediate nodes, Hiding hop count information from intermediate nodes, Inability to detect trace route packets by adversaries.
This paper is organized as follows: Section II is the review of related works about Anonymous secure routing protocols and secures routing protocols, and section III is the introduction Contributions of our Work. In section IV, the adversary model is introduced, and then in section V, Our Proposal: ASRPMANET or anonymous secure routing protocol mobile ad hoc network. In section VI, there Analysis of our protocol and section VII will be the Conclusions and Future Works of the whole paper.

2. Related Work

There exists related work on anonymous routing algorithms in ad hoc wireless networks. These protocols each have strengths and weaknesses that we will study them. Research results have yielded anonymous routing protocols, such as ASR [2], MASK [3], ANODR [1], SDAR [4] and ODAR [6].The Anonymous Secure Routing (ASR) protocol proposed by Zhu and Wan [2] satisfies all the six requirements of anonymity. A secret key (symmetric key) is distributed between the nodes. As a result of which the Source and destination before starting are aware to communicate. ASR also supports limited hop count and destination verification by intermediate node so as to provide more security properties. But due to not changing of the data field and its fixed contents, in each step there will be the possibility of tracking the data packets and so the discovering of the route. DOS attack is problem for these protocols , attacker can launch a Denial-of-Service (DoS) attack based on that ID, but ASR solves this problem by a scheme in which node one sends a temporary

Manuscript received July 5, 2012
Manuscript revised July 20, 2012

public key to node two in Routing Request, and in Routing Response node two transmits its pseudonym encrypted by the key to node one. Besides location privacy and route anonymity, ASR also supports limited hop count and destination verification by intermediate node so as to provide more security properties.

Another protocol [3] proposed an anonymous on-demand routing protocol, termed MASK, and on based a new cryptographic concept called pairing. An anonymous neighborhood authentication protocol is used and MASK fulfills the routing and packet forwarding tasks without disclosing the identities of participating nodes under a rather strong adversarial model. With all these important advantages MASK is multi-path Support that influences the anonymous route. In MASK, nodes use pseudonyms instead of their real identifiers in the routing process. If one node uses one pseudonym all the time, it won't help to defend against traffic analysis because the pseudonym will be analyzed the same way as the real identifier. Therefore, each node should use dynamically changing pseudonyms. For this purpose, the trusted authority (TA) furnishes each node *IDi* with a sufficiently large set PSi of collision-resistant pseudonyms and a corresponding secret point set as Si = *gH1(* PSi *)* = { *Si,j* } ={ *gH1(PSi,j)* ∈ Ǫ1} ($1 \leq j \leq |$ PSi $|$). Since the discrete logarithm problem (DLP) is believed to be hard in Ǫ1, given one pseudonym and secret point pair < *PSi,j* , *Si,j*>, adversaries cannot deduce the system master key with non-negligible probability. In addition, there is no one but the TA can link a given pseudonym to a particular node or identity, or deduce the corresponding secret point with non-negligible probability.

Kong and Hong presented a protocol called ANDOR in [1].The contribution of this work is to present a untraceable and intrusion tolerant routing protocol for mobile ad hoc networks. . This design protocol used method Onion Routing protocol and broadcast with trapdoor information but is different from above approaches in that each forwarding node adds an encrypted layer to the route request message like an onion. Although it is a pseudonym, the attacker can launch a Denial-of-Service (DoS) attack based on that ID. There are three types of ANODR route discovery, which are described as follows:

1. ***ANODR-PO*** *(Anonymous route discovery – public key protected)*

RREQ phase: Each *RREQ* forwarding node X propend the incoming hop to the PO structure, encrypts the result with its own public key PKX, then broadcasts the *RREQ* locally.

RREP phase: When the destination receives an *RREQ* packet, the embedded PO structure is a valid onion to establish an anonymous route towards the source.

2. **ANODR-BO** (Anonymous route discovery – Boomerang Onion)

RREQ phase: When intermediate forwarding node X sees an *RREQ* packet, it propend the incoming hop to the boomerang onion, encrypts the result with a random symmetric key KX, then broadcasts the *RREQ* locally.

RREP phase: The boomerang onion will be bounced back by the destination. Like the public key version, when node X sees an *RREP* packet, it strips a layer of the boomerang onion and locally broadcasts the modified *RREP* packet. Finally the source will receive the boomerang onion it originally sent out.

3. **ANODR-TBO** (Anonymous route discovery – Trapdoor Boomerang Onion)

RREQ phase: When intermediate forwarding node X sees an *RREQ* packet, it embeds a random nonce NX to the boomerang onion (this nonce is not a route pseudonym nonce), encrypts the result with a random symmetric key KX, then broadcasts the RREQ locally. The trapdoor information consists of NX and KX, and is only known to X.

RREP phase: The boomerang onion will be bounced back by the destination. After each local *RREP* broadcast, only the next hop (i.e., the previous hop in *RREQ* phase) can correctly open the trapdoor it made in the *RREQ* phase.

Another protocol SDAR [4] the main idea of the routing nodes is based on assurance levels. In SDAR [4] all intermediate nodes add an encrypted version of their identity to the RREQ before forwarding it. Only the destination is able to decrypt the identities collected in the RREQ. The destination uses these collected identities to create a Route Reply (RREP) message that will be returned to the source of the RREQ. Trust Management SDAR node uses a *proactive* and *explicit* neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. It periodically sends out a HELLO message holding the certified public key of the node and at the same time collects other nodes' public keys. By observing behavior of one-hop neighboring nodes or using other approaches, a node classifies its one-hop neighbors into different trust levels. Keys corresponding to these levels are negotiated among same-level nodes. They are later used to enforce trust-based secure communication.

Finally, in ODAR [5] an On-Demand Anonymous Routing protocol, which provides node, link and path anonymities in ad hoc networks based on Bloom, filters. The use of Bloom filters additionally gives ODAR the storage, processing and communication-efficiencies, making it suitable in the ad hoc network environments. Castelluccia et al. were the first to use Bloom filters to compress source route information after the source route is discovered using DSR [17], [18].

ODAR provide the following anonymities:

- ✓ Identity anonymity: A node receiving or sending data packets cannot be identified by its neighbors. It is computationally difficult for adversaries to search and determine the node's true identity.
- ✓ Route/path anonymity: A node forwarding packets must not be able to infer the identities of other nodes that also participate in the data forwarding.
- ✓ Topology/location anonymity: Routing information maintenance does not reveal the distance, neighbor link information of a node, nor the true routing path or tree information. Neither can they be deduced from routing information in the packets.

In contrast to previous work, our proposed ASRPMANET protocol is based on a symmetric cryptosystem and trapdoor and forwarding mechanism and pseudonym, any other anonymous routing protocol available to date requires an asymmetric cryptosystem for path encryption, link encryption, or both, to satisfy anonymity the requirements. Compared to an asymmetric cryptosystem, a symmetric cryptosystem typically brings a 4-order-of-magnitude speed-up [5] and a significant decrease in key length. Such a high speed and low overhead makes the ASRPMANET protocol fast enough to route real-time traffic in a timely fashion. In such a situation has been trying to design protocol, satisfy anonymity factors in routing mobile ad hoc network. Anonymity factors in routing are as follows:

- ✓ Remain hidden source and destination IDs: This means that the identities of the source and destination nodes aren't revealed for other nodes.
- ✓ Remain hidden intermediate nodes IDs from the source and destination nodes: this means that the identities of the intermediate nodes aren't revealed source and destination nodes.
- ✓ Intermediate nodes ID remain hidden from enemy and other intermediate: that means that the identities of the intermediate nodes remain hidden from outside network nodes and inside network nodes.
- ✓ Remain hidden Location of source and destination nodes: that means no node in the network is aware of the exact location of the source and destination nodes.
- ✓ Location to stay hidden intermediate nodes: that means no node in the network is aware of the exact location of the intermediate nodes.
- ✓ Number of hop to hop path hidden from intermediate nodes: the intermediate nodes have any information about the location of source and destination including the distance and hop count.
- ✓ Lack of detection of route discovery packets for external observers: The framework and contents of the routing packets and the procedure of their forwarding in the network must be in a way so that the enemy is never able to track the packets.
- ✓ Supporting the multi path routing: that means As a result the determination of the route and recognition of the source and destination nodes shall not be easily possible.

3. Adversary and attack Model

In this paper we assume two distinct adversaries .The first adversary is an external global passive adversary Passive eavesdroppers may be omnipresent in a hostile environment. A passive adversary obtains information only by eavesdropping. The second adversary we assume is a cooperating node inside the network. This means that we assume that every node that is part of the network is a potential adversary. A active adversary one may post route requests, inject messages, tamper with, or even drop received messages to gain information .Thus we design our schemes to be secure against a powerful adversary with unbounded eavesdropping capability but bounded computing and node intrusion capability. In this model we prevention Sybil attack we for prevention this attack using public key. It is assumed that the source and destination nodes share their public key. This public key may be accessed by the nodes at the time of network configuration or by a key server through the Diffe- Hellman method [7]. In Section VI further explains.

4. Our Proposal: ASRPMANET

In this section, we introduce our secure routing protocol for establishing anonymous in ad hoc wireless networks.

4.1 Assumptions

In this paper we have two assume that (1) here the wireless links have been considered to be symmetric Namely, if node A is in transmission range of some node B,

then B is in transmission range of A as well, (2) It is assumed that the source and destination nodes get A pair of public-key of certification authority (CA). (3) Adversaries have unbounded eavesdropping capability but bounded computing and node intrusion capabilities.

4.2 Route Discovery

Each node intending to communicate with another node creates Route request packet RREQ and sends its neighbors. In this packet the source node transmits the temporary public key (the public key which is only used in this Session) along with the Session ID and one trapdoor which has been encrypted with the source Public key. This packet shall be in the following format:

<RREQ, SID, TPKi, TR>

SID: Session ID that is mad bye hashing source ID and time stamp: h (IDS, TS).

TPKi: Node i temporary (one-time) public key

TR: Trapdoor generated by the source has got the following Format:

PK_D *(well-known nonce, Ks)*

PK_D: Destination node public key

Ks: Source nod symmetric key

source node Producer packet RREQ stores the information of SID, IDD, KS in a table called Session Requests (SREQ) so that at the time of receiving route reply packet . Each node i+1 which receives the RREQ, first tries to open the TR field If it is able to decrypt the TR, it finds out that it is the destination node itself, otherwise it will replace the received TPKi with its own related TPKi+1 in the RREQ packet and Stores the session ID information, its own temporary public key and the previous node and the private key in Reverse Routing Table (RRT). Then it broadcasts the RREQ packet. When a route request packet is received Its SID is compared with SIDs stored in the RRT and if they are repeated, the packet is dropped. Than received RREQ to destination, if next received packet stopped Operation, then enemy who is eavesdropping the communications inside the network will face the stoppage of transmission of RREQ in one node and it will find that this is the destination node of a new session. To prevent this problem we using forwarding mechanism (FM), destination node receiving the RREQ packet manipulate its TR field and replace it with invalid quantities. In the next step it rebroadcasts the new packet in the network. In this situation, since the SID field is repeated in the Transmitted RREQ packet, this packet is distributed throughout the network only once and then exterminated and in this way the enemy shall not have any possibility to discover the destination node.

4.3 Route Reply

When node destination received RREQ, try to decrypt Trapdoor it produces the route reply packet (RREP) and transmits it to its neighbors. The RREP packet format is:

<RREP, TPKi, TPKi (Ki+1, PSi+1, SID), TR'>

Ki+1: symmetric key of node i+1

PSi+1: pseudonym of node i+1

TR': TR response which has got the following format:

KS (KD, well-known)

KD: symmetric key of destination node

When node i receives the RREP packet, it first searches for TPKi field in its Reverse Routing Table. In case TPKi is found in RRT, the node i finds out that it is one the route reply In the next step, the 3rd field of RREQ packet will be decrypted with TPKi corresponding private key. if the node receives the RREP, will be the source node, it will find out the receiving of RREP packet from the relevant destination upon comparison of SID received with SIDS generated by itself (in SREQ session request table). Destination nodes receiving the RREQ packet manipulate its TR field and replace it with invalid quantities. In the next step it rebroadcasts the new packet in the network. Nodes know repeated in the Transmitted RREQ packet than delete it. When the RREP packet is verified, node i will produce its pseudonym, PSi, and its symmetric key, Ki, and encrypt them together with SID by the public key of the inferior node and the RREP packet is changed in the following format. Then the produced packet is transmitted to the neighbors.

<RREP, TPKi-1, TPKi-1 (Ki, PSi, SID), TR'>

Also the node i stores the information of the pseudonyms and symmetric keys in the routing table.

4.4 Data Forwarding

After the RREP packet reaches the source, this node encrypt the related data with symmetric key of the Destination and then re encrypt the result bye symmetric key of next hop node and finally generate the data packet. The data packets transmitted from node i to i+1 has the following format:

<DATA, Ki+1(KD (Data, Well-Known Nonce), PSi+1), PSi+1>

Since the contents of the data packets are changed hop-by-hop and the length of the packets is fixed, these Packets are not traceable. To avoid attacks such as Packet Counting, we can also use FM for transmission of the data packets.

Also for Multi-Path Routing support, after receiving the first *RREQ* packet, the destination node waits for a period of time, and in this period it collects all *RREQ*s belonging to the same session. In the next step, it makes the route reply Packet for all *RREQ*s received and transmits the same.

It is possible that a node is common in two or more routes. In this case the time it receives two or more different *RREP*s, it stores them in routing table, due to their session number. At the time of transmitting of the data, when the node *i* receives a data packet it looks at its routing table and in case it has stored several separate routes for that session, it selects one of these routes by random, through which it transmits the data packet.

4.5 Route Maintenance

In the mobile ad hoc network (MANET) nodes have able move in the network than each link in time possible disconnect, also occur possible add new link in network. We have to consider a method so that these disconnections will have the least influence in the performance of the protocol. In ASRPMANET, each node i periodically transmits ne present messages (PM) to the neighbors. These messages have got the following format:

<PM, IDi, (PSn ……PSm)>

Each node receive the PM packet they will produce the present messages reply packet (PMR) with the following format and send it to node i:

<PMR, IDi, PSi+1)>

The node i receive the PMR packet than update routing table also if PMR packet no receive of each neighbors so node i delete node in the routing table.

5. Anonymous Analysis and Attack Analysis

Firstly, we need to make clear that the Security term discussed in this section does not include issues about security of the content of data packets being transmitted. It is easy to see that security of the content of data packets is orthogonal to anonymity and security and efficiency of the route protocol.

5.1 Analysis anonymous secure routing

According to the definition provided for anonymous in part we have to investigate each of these cases.

- Remain hidden source and destination IDs: because our in the packets (RREQ and RREP) using of hash (IDs and Time stamps) than remain hidden source and destination IDs.
- Remain hidden intermediate nodes IDs from the source and destination nodes: Unlike the method of Onion Routing Information intermediate nodes in are not Packet routing than Path remains hidden.
- intermediate nodes ID remain hidden from enemy and other intermediate:
  - ✓The route discovery packet, Intermediate nodes using the public key A time consumption, Therefore, this keys cannot be consistent with the IDs of nodes than Intermediate nodes in the path Are not aware of the identity of the next nodes.
  - ✓When sending data using by Pseudonym than Intermediate nodes not be able to recognize real identity next node.
- Remain hidden Location of source and destination nodes: information Location in the route discovery packet is not Existence.
- Location to stay hidden intermediate nodes: pay attention to the route discovery packet format, Penultimate nodes do not know where the path have been, to a source and destination nodes somehow place to discover.
- Number of hop to hop path hidden from intermediate nodes: pay attention to Fix the length of routing packets and no increase or decrease their length along the path cannot discover number of hop path Number.
- Lack of detection of route discovery packets for external observers: Using the FM (forwarding mechanism) in the Sending packets routing and data Slake Possible Track package.
- Supporting the multi path routing: After receiving the first RREQ packet, the destination node waits for a period of time, and in this period it collects all RREQs belonging to the same session. In the next step,

it makes the route reply packet for all RREQs received and transmits the same .In each time of sending the RREP by the destination. At the time of transmitting of the data, when the node i receives a data packet it looks at its routing table and in case it has stored several separate routes for that session, it selects one of these routes by random, through which it transmits the data packet.

Table 1 shows the comparison of the anonymity-related properties achieved in known anonymous routing protocols in mobile ad-hoc networks. In the table, ANODR and ASR and ODAR and MASK and SDAR stand for the anonymous routing protocols proposed in [1] and [2], and [6], and [3] and [4], respectively.

Table 1: COMPARISON OF THE ANONYMITY PROPERTY OF ROUTING PROTOCOLS

Protocol / Anonymity Property	SDAR	MASK	ODAR	ASR	ANODR	ASRP MANET
S&D ID privacy	✓	×	×	✓	✓	✓
Intermediate nodes ID privacy from S&D	×	✓	✓	✓	✓	✓
Intermediate nodes privacy from each other and adversary	✓	✓	×	✓	✓	✓
S&D location privacy	✓	×	✓	✓	✓	✓
Intermediate location privacy	✓	×	✓	✓	✓	✓
Hop count privacy	×	✓	✓	✓	×	✓
Packet intractability	×	✓	×	×	×	✓
multi path routing	×	✓	×	×	×	✓

5.2 ATTACK ANALYSIS

Sybil Attacks: In Sybil Attacks [19],an attackers IDs several claim Or changing IP address, Their legitimate node replace in the network. In this protocol As previously mentioned in section 4, Nodes before entering the network get A pair of public-key of certification authority (CA). then nodes Already by CA authenticated, Thus, each node cannot receive some public key, than attackers cannot have same IDs.

Wormhole Attacks: In Wormhole Attacks [12], an attacker records packets received at one location in the network, tunnels them to another location, and retransmits them into the network. Hu, Perrig, and Johnson propose an approach to detect wormhole attacks based on packet leashes [12]. The key intuition is that by authenticating either an extremely precise timestamp or location information combined with a loose timestamp, a receiver can determine if the packet has traversed a distance that is unrealistic for the specific network technology used. Both of the solutions can be easily integrated into ASRPMANET without any conflict. In fact, ASRPMANET can provide a simple method to detect wormhole attacks. As mentioned in Section 5, in ASRPMANET, the destination knows the length of each route, as long as the length does not exceed Hmax. Therefore, a verification mechanism can be employed to detect anomalies when comparing the metric.

DoS Attacks: According to the target of the attack, DoS attacks in the context of anonymous routing can be classified into two types: Multiple-to-One attacks and One-to-Multiple attacks. In the former attacks, multiple adversaries (or one adversary with strong power) may cooperate to exhaust the resource of a given target In ASRPMANET, such attacks are prevented by little computation, i.e., a symmetric key decryption to check whether the node is the expected destination, is involved in handling the RREQ packet; employ hop-by-hop authentication on the RREP packet.

Table 2 shows the comparison of the security properties achieved in known anonymous routing protocols in mobile ad-hoc networks. In the table, ANODR and ASR and ODAR and MASK and SDAR stand for the anonymous routing protocols proposed in [1] and [2], and [6], and [3] and [4], respectively.

TABLE 2 COMPARISON OF THE SECURITY PROPERTY OF ROUTING PROTOCOLS

Protocol / Attack	SDAR	MASK	ODAR	ASR	ANODR	ASRP MANET
Sybil	×	×	×	×	×	✓
Wormhole	✓	✓	✓	✓	✓	✓
DOS	×	×	×	✓	×	✓

5.3 Efficiency protocol

In this section, we compare the packet sizes of several anonymous routing protocols. The processing overhead of each node has been considered based on the actual measurement on a pocket PC [11]. Table 3 shows the results of this measurement for different encoding systems. For encoding systems with public key, the process delay and for encoding systems with symmetric key, the process rate based on bit rate have been shown. In order to calculate the encoding in ASRPMANET, RSA has been considered as the encryption algorithm of the public key and AES/Rijndeal has been considered for symmetric key encryption.

Table 3: Encoding Overhead of Different in Asymmetric key and Symmetric key

Method	Encryption	Decryption
Asymmetric key(RSA)	188.7ms	10.8ms
Symmetric key(AES)	29.2Mbps	29.1Mbps

6. Experiments

In this section, we estimate the performance of the proposed ASRPMANET protocol with extensive experiments. We estimate the performance of the proposed ASRPMANET protocol with extensive experiments.

Firstly, we compare the computational overhead of AES encryption/decription with that of numerical multiplication by benchmark testing. The hardware configuration of the machine used for the benchmark testing is: AMD 64 bit 2 Ghz processor with 960 MB RAM. The code for AES encryption/decryption using 256 bit keys in CBC and CFB modes is written in C++ and compiled in Microsoft Visual Studio 2005. The code to perform multiplications over a finite field is written in Maple 9. The time taken for performing a single AES decryption and a single multiplication over a field is calculated for various message sizes. A simulation has been done to calculate the efficiency and such parameters as end-to-end delay packet delivery ratio and etc. The simulation has been carried out with different scenarios and by NS-2[14] software. The simulation conditions are like [16], so that we can compare the results obtained with other protocols.

7. Performance Results

In this section, we give simulation results for different network scenarios, namely, increasing mobility and increasing traffic load.

7.1 Impact from mobility

Figure 1 illustrates the data packet latency. Because of the public key cryptographical overhead, SDAR and ODAR show significant longer end-to-end latency. ANODR and ASR have similar average data packet latency. ASRPMANET and MASK have the lowest and nearly the same data packet delay with original AODV, thanks to the efficient symmetric encryption algorithms and hash functions used. When there is little mobility, all protocols display small data packet latency, because once a route is established, a stable network allows a longer average route lifetime. When mobility increases, data packet latency increases accordingly.

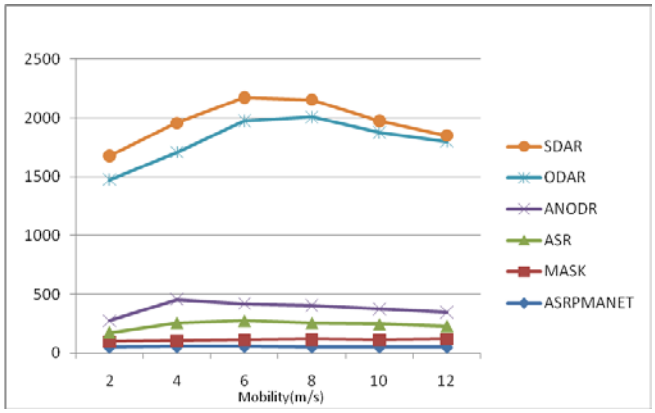

Fig. 1. Data Packet Latency (ms)

7.2 Impact from traffic load

The network traffic load is increased by increasing the number of communication pairs. Figure 2 shows the impact of traffic load on end-to-end data packet latency. No surprise, the data latency is extendedas the traffic load increases. This is caused by longer queueing delay in contenting the wireless medium, and more needs for route re-discovery. Protocols with longer computation delay always suffer more under heavy traffic load.

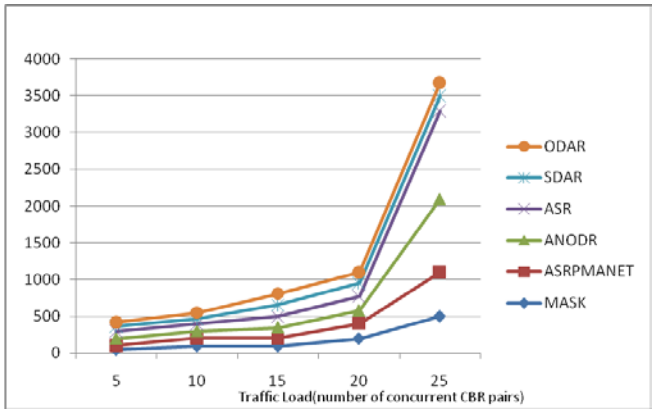

FIG. 2. DATA PACKET LATENCY (MS)

8. Conclusions and Future Works

Problem anonymous secure routing in the mobile network is an important, thus in this paper we start looking at this issue by introducing an anonymous secure routing protocol, ASRPMANET, Design has attempted to overcome possible drawbacks of existing methods was,

Mechanism using symmetric key encryption of data in a step by step and inability to control and data packets and also supports multi-path ASRPMANET, And also to prevent attacks such as a sybil and wormhole and DOS it is the most important benefits. As we know between network performance and security always a Trade-off exists, in the ASRPMANET when due because of created to deal with attacks and no more than a name we use FM some bandwidth will be wasted. This is an attempt to save bandwidth protocol extent appropriate to prevent. One of the other discussions which could be taken into consideration in future works is the improvement of these protocols in order to make them resistant against active attacks and focus on transmission power control from a security and network perspective.

REFERENCES

[1] J. Kong and X. Hong. ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In Proceedings of the 4th ACM International Symposium on Mobile Ad hoc Networking and Computing (MobiHoc 2003), pages 291–302. ACM Press, 2003.

[2] B. Zhu, Z. Wan, M. Kankanhalli, F. Boa, and R. Deng. Anonymous secure routing in mobile ad-hoc networks. In Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN 2004), pages 102–108. IEEE, 2004.

[3] Y Zhang, W Liu, W Lou, Y Fang. ”MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks“ IEEE Transactions on Wireless Communications, Vol. 5, pp. 2376-2385, 2006.

[4] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks. In 29th IEEE International Conference on Local Computer Networks (LCN’04), pages 618–624, 2004.

[5] A. Menezes, P. van Outshot, and S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[6] D Sy, R Chen, L Bao. “ODAR: On-Demand Anonymous Routing in Ad Hoc Networks“. IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 267-276,, 2006.

[7] W Diffie, M Hellman. “New Directions in Cryptography”. IEEE Transaction on Information Theory, Vol. 2, pp. 644–654, 1976.

[8] M G Zapata. “Secure ad hoc on-demand distance vector routing”. ACM SIGMOBILE Mobile Computing and Communications Review, pp. 106-107, 2002.

[9] S Jiang, N H Vaidya. “A mix route algorithm for mixnet in wireless mobile ad hoc networks”. IEEE International Conference on Mobile Ad-hoc and Sensor Systems, pp. 406-415, 2004.

[10] J Liu, J Kong, X Hong, M Gerla. ”Performance Evaluation of Anonymous Routing Protocols in MANETs”, IEEE Wireless Communications and Networking Conference, Vol. 2, pp. 646-651, 2007.

[11] V Gupta. “Performance Analysis of Elliptic Curve Cryptography for SSL”, ACM Workshop on Wireless Security, pp. 87-94, 2002.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), 2003.

[13] NS-2, http://www.isi.edu/nsnam/ns/ns-build.html

[14] VINT Project , A Collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC. The ns Manual. July 2007

[15] V *Gupta.* “Performance Analysis of Elliptic Curve Cryptography for SSL*”, ACM Workshop on Wireless Security*, pp. 87-94, 2002.

[16] J Liu, J Kong, X Hong, M Gerla. ”Performance Evaluation of Anonymous Routing Protocols in MANETs”, IEEE Wireless Communications and Networking Conference, Vol. 2, pp. 646-651, 2007.

[17] C. Castelluccia and P. Mutaf. Hash-Based Dynamic Source Routing. In IFIP Networking, LNCS 3042, pages 1012–23, 2004.

[18] D.B. Johnson and D.A. Maltz. Mobile Computing, chapter Dynamic Source Routing in Ad Hoc Wireless Networks, pages 153–181. Kluwer Academic,Publishers,1996.

[19] J. Douceur, "The Sybil Attack," in Proc. Intl Wkshp on Peer-to-Peer Systems(IPTPS),2002.

Kim, Do-Moon received Ph.D Degree in Computer Engineering form Soongsil University, 1994 and 2004., respectively. He is an associate Professor in Kyungdong University(2012). Research Laboratory in about Network Security, Routing for Mobile Ad Hoc Network, Mobile Security, PKI, and DRM in the Networks,